Installation, Administration & User Guide

iPlanet Portal Server Plug-in for the Identrus System

Version 2.0

March 2001

Contents

Table of Figures

Chapter 1

Introduction

This Chapter discusses the main components that are required to participate in the Identrus Scheme. It explains how the iPlanet Portal Server Plug-in for the Identrus System facilitates secure email messaging. The objectives of this chapter are to provide an overview of:

- Layout of the guide
- The Identrus Scheme itself
- SmartCard Users wishing to logon and check their email via the Portal Server
- Certificate Status Checks done either via the Identrus scheme or by an appropriate Certificate Authority

Related Documents

Solaris 8 and Java Development Kit 1.2.1

http://docs.sun.com

http://java.sun.com/products/jdk/1.2/download-docs.html

iPlanet Portal Server 3.0

http://docs.iplanet.com/docs/manuals/ips.html

iPlanet Certificate Management System

http://docs.iplanet.com/docs/manuals/cms.html

Oracle 8i Installation and Configuration Guides

http://www.oracle.com

Hardware Security nCipher KeySafe 1.0 and CAFast

http://www.ncipher.com

http://active.ncipher.com/documentation/PKCS11/solaris-4.01/nforce.pdf

Identrus Message Specifications

http://www.identrus.com

Overall Layout

The document is intended to assist Three kinds of users:

- An email User who will need to check his/her mail and perform certificate status checks.
- System Administrators who may be a bank employee or your Local Product Support Representative, both of whom must be able to install, configure and maintain the system.
- Developers wishing to deploy their own applications within the Portal Server that are also Identrus enabled.

The document comes in four parts:

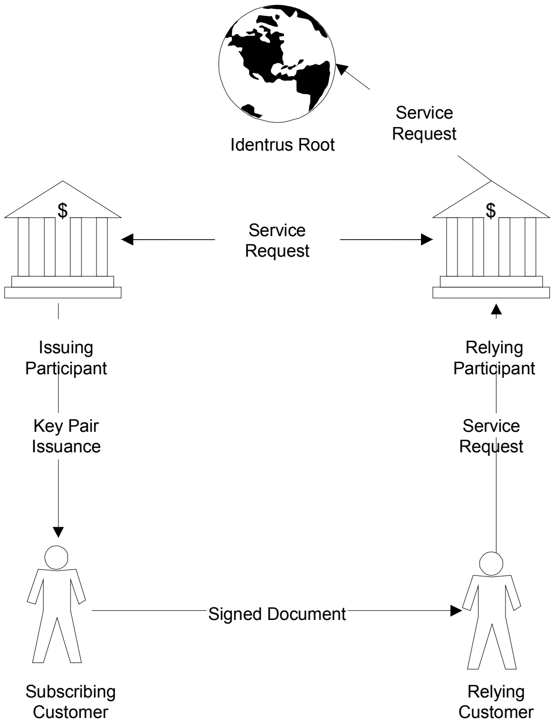
- The Installation section runs through special considerations over and above those mentioned in the iPlanet Portal Server 3.0 Installation Guide
- The Administration section is intended for Administrators setting up Netmail users, assigning certificates and defining Certificate Status Check Responders.
- The User section describes: Logging on using a Smart Card, Digitally signing email messages and the general management of secure messaging.
- The Deployment section illustrates how to develop the source code necessary to perform an Identrus enabled Certificate Status Check.

About the Identrus Scheme

Identrus was formed to establish and operate a highly secure system for identifying parties over electronic networks, including the Internet. Identrus is comprised of regulated financial institutions coming together to combine the basic technology provided by public key cryptography and PKI with adherence to a common set of operating rules that facilitate electronic commerce.

The “Four Corner” model, as depicted below, forms the basis of the Identrus PKI network.

Figure 1 Identrus Four-Corner Model



The four corners consist of:

- Issuing Participant – Bank (or other financial institution) issuing smart cards containing private keys and certificates to Subscribing Customers.

- Subscribing Customer – Member of the Issuing Participant bank authorised to participate in Identrus activities.

- Relying Customer – Party with whom the Subscribing Customer initiates a signed transaction.

- Relying Participant -- Bank with which the Relying Customer communicates to obtain some level of trust in the signed data received from the Subscribing Customer.

A typical transaction using the Four-Corner Model includes the following steps:

- The Subscribing Customer uses his/her SmartCard to sign a transaction request that the system sends to the Relying Customer.

- The Relying Customer verifies that the signed data came from the Subscribing Customer and was not modified in transit.

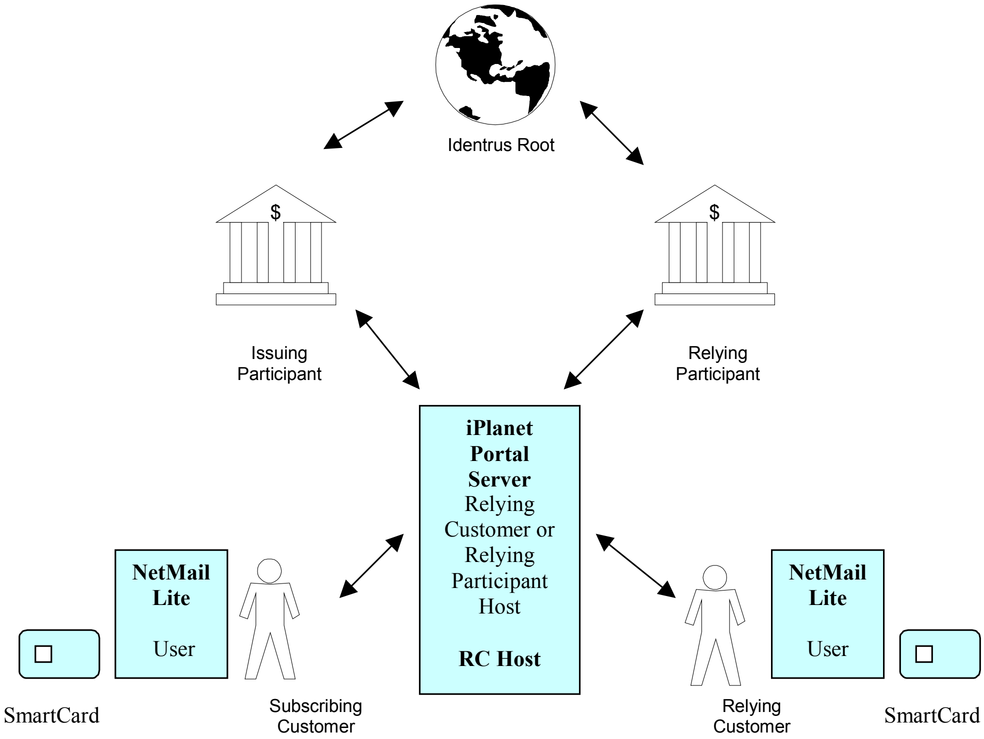
- The Relying Customer requests services from his/her bank; for example, he/she can ask its bank to perform a status check on the Subscribing Customer's certificate to make sure it is still valid (has not been revoked).

- The Relying Participant requests services of the Issuing Participant and the Identrus Root to fulfill the Relying Customer's service request.

- Based on the response from his/her bank the Relying Customer fulfills or rejects the request from the Subscribing Customer.

In order to accommodate the Identrus Scheme, the iPlanet Portal Server Plug-in for the Identrus System utilises a host system connected to the Portal Server as illustrated below:

Figure 2 iPlanet Portal Server and the Identrus Scheme



iPlanet's Portal Plug-in solution

The iPlanet Portal Server Plug-in for the Identrus System is designed for those Developers, Users and Administrators wishing to achieve reliable messaging when sending and receiving email messages. Messages gain meaning if in some way they have:

- Authentication i.e. You know who your email message came from
- Integrity i.e. You know your email message has not changed
- Non-repudiation i.e. The sender cannot disavow the message

The iPlanet Portal Server Plug-in for the Identrus System utilises:

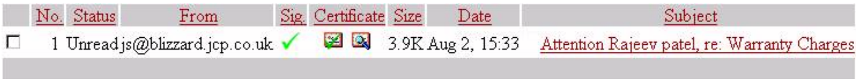
- A digital signature ✓ to achieve integrity
- A certificate ▤ in order to validate the sender of a message

If and only if there exists both a valid digital signature and a verified certificate can we say that a message be non-repudiable. Without these mechanisms in place this cannot happen, and as such, the purpose of this document is to explain the main components associated with:

- Firstly configuring a system so that appropriate trusted certificate hierarchies are in place to authenticate messages via a certificate status check.
- Secondly how users should view appropriately messages, containing digital signatures and certificates, that they receive and send.
- Thirdly how developers can deploy their own applications that are Identrus enabled

The iPlanet Portal Server Plug-in for the Identrus System achieves these aims by attaching the above icons to all email messages sent and received within the email message header summary of NetMail Lite. Thus, allowing the user the ability to determine the status of each message received and also to send messages with integrity if they so wish.

Figure 3 Example Message Header

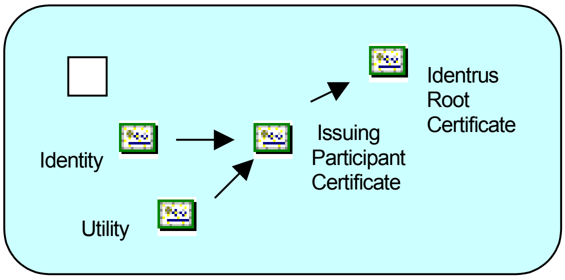


	No.	Status	From	Sig.	Certificate	Size	Date	Subject
□	1	Unread	js@blizzard.jcp.co.uk	✓	▤ 🔍	3.9K	Aug 2, 15:33	Attention Rajeev patel, re: Warranty Charges

Inside an Identrus SmartCard

Part of setting up the iPlanet Portal Server Plug-in for the Identrus System involves issuing users with a SmartCard. Every Smart Card contains certificates that has an Identrus Hierarchy that defines which users can logon to the Portal Server as illustrated below.

Figure 4 A SmartCard illustrating its Certificate Hierarchy



If a chain of trust can be built between a specific SmartCard certificate and a trusted CA, the certificate can be trusted (by inference). In such circumstances, any user that is an Identrus member can log onto the Portal Server, provided the administrator, for the Identrus member, sets an appropriate Certificate to contain an Identrus Certificate hierarchy.

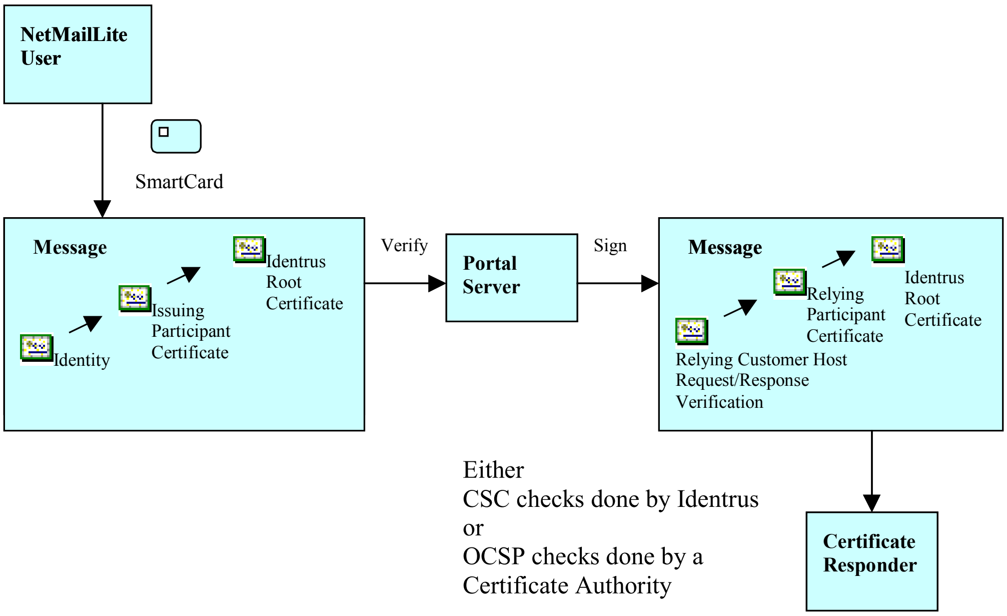
In order to become Identrus-enabled, the following certificates are needed:

- An Identrus enabled Identity Certificate that provides information about who the user is.
- An Identrus enabled Utility Certificate that provides information about what access the user is authorised to have.
- An Identrus enabled Identity Certificate Authority Certificate that issues the users identity.
- An Identrus enabled Utility Certificate Authority Certificate that issues the users utility.
- Identrus Root Certificate

The Identrus Certificate Scheme

Administrators wishing to install the iPlanet Portal Server Plug-in for the Identrus System need to be aware of the main components that go into enabling users to achieve these aims. The diagram below illustrates an example of how messages typically might be validated and checked for integrity using certificates that have been issued by appropriate certificate Authorities within the Identrus Scheme.

Figure 5 Overview of Certificate Verification for the Identrus Scheme


NetMailLite User
SmartCard
Message
Identity
Issuing Participant Certificate
Identrus Root Certificate
Verify
Portal Server
Sign
Message
Relying Customer Host Request/Response Verification
Relying Participant Certificate
Identrus Root Certificate
Either
CSC checks done by Identrus
or
OCSP checks done by a
Certificate Authority
Certificate Responder

In order to achieve these aims of authenticating email and sender/recipient integrity, three kinds of certificates are needed for the Identrus Scheme:

1) Application Authorisation Certificates

- Trusted Login CA Certificate. This is normally the Relying Participant Bank under such circumstances only customers of the RP Bank can login. This certificate is used for Verification purposes.

- Trusted Email Certificate. This is normally the Identrus root itself and under such circumstances all email received by any Identrus member can be validated.

2) Certificates for Certificate Status Checks

- Request Signing Certificate. Outgoing, from RC Host to Identrus CSC or OCSP, status checks are signed by this certificate.

- Response Signing Certificate. Signing certificate is used to sign the status messages returned to the RC host's user.

- Trusted Response Verification Certificate. The Certificates used by the RC host to verify responses, whether they are OCSP or Identrus CSC.

3) Certificates for Transport Authentication and Integrity

- SSL Client Certificate. Signs the SSL transport handshake between client and server.

Chapter 2

Installation

Installing the iPlanet Portal Server Plug-in for the Identrus System requires a complete Portal Server Installation as a pre-requisite. This chapter runs through the installation procedure that then follows to enable users of the identrus system to use NetMail Lite. The chapter covers:

- Software and hardware Prerequisites
- Installation procedure and verification
- Post Installation steps
- Backup and Removal Considerations

Pre-requisites

The following Software and hardware peripherals must be installed prior to installing the iPlanet Portal Server Plug-in for the Identrus System:

- iPlanet™ Portal Server 3.0 SP2 and its email application NetMail Lite. e.g. http://www.iplanet.com/downloads/patches/2012.html

- iPlanet™ Certificate Management Server (Optional) (See for instance http://www.iplanet.com/downloads/download/2042.html)

- A SmartCard, such as a credit card, which will be issued to you by a thirty party vendor. An Identrus compatible SmartCard is a mandatory requirement. iPlanet Portal Server Plugin for the Identrus Network V2.0 is currently compatible with the GemPlus SmartCards GemSAFE IS 16000. See http://www.gemplus.com/app/banking/gemsafe_is_mkt.htm

- A SmartCard Reader with browser plug-in, which will be issued to you by a third party vendor. An Identrus compatible SmartCard Reader is a mandatory requirement. iPlanet Portal Server Plugin for the Identrus Network V2.0 is currently compatible with the GemPlus Card Readers GemPC430 and GemPC410 see http://www.gemplus.com/products/hardware/index.htm

- GEMSafe Enterprise Workstation 1.0 software is compatible with iPlanet Portal Server Plugin for the Identrus Network V2.0 see http://www.gemplus.com/products/software/gemsafe/index.html

- The Netscape Navigator v4.7x or above. Internet Explorer 4.0 and Internet Explorer 5.0. These should be configured automatically with the software that comes with your SmartCard and SmartCard Reader.

- The Client browser is compatible with GemPlus SmartCard and the Portal Server Plug-in as such the following operating systems are supported: Windows NT 4.0 Service Pack 5 see http://www.microsoft.com/ntserver/nts/downloads/recommended/sp5/allsp5.asp or alternatively Windows 98 see http://www.microsoft.com/Windows98/

- The Hardware Security Module, CAFast (see http://www.ncipher.com), to accelerate cryptographic operations and securely store keys. This is an administrator requirement for Identrus member banks and does not require user intervention. Note CAFast is also referred to as nFast.

- In order to run iPlanet Portal Server Plug-in for the Identrus System you must have a relationship with a bank or an authority that is capable of acting as either an OCSP Responder or connected to the Identrus Network.

- Java 2 Standard Edition (1.2.2_06 Localized) Production Release for the Solaris Operating Environment. iPlanet Portal Server V3.0 consists of a Web Server and a Gateway (see http://docs.iplanet.com/docs/manuals/portal/30/install/overview.htm). The Gateway and the web server typically reside on separate machines. The gateway restricts access to the web server. The mere act of placing the gateway and web server on separate machines ensures that they will be running in separate VM's. Typical setup: (1) only the gateway can "see" the web server. (2) The gateway only has access to the web server and cannot see the same "world" as the web server. (3) Clients can only access facilities provided by the web server via the Gateway. (4) Clients cannot access the web server. If the gateway and server are put on separate machines then no pre-requisite is required since this is done during Portal installation and configuration. If the gateway and server are put on the same machine, e.g. for testing and development purposes, then the instructions below must be applied. (1) Download Java from http://www.sun.com/software/solaris/java/download.html (2) This should be installed separately on two different areas within the same machine. Under such circumstances, JAVA_HOME needs to be adjusted within the scripts ipsgateway and ipsserver to reflect this (for an example illustrating this see the penultimate chapter on Deploying Applications on page 69).

- Oracle 8.0.5 and JDBC™ for Oracle 8.1.5 http://www.oracle.com/java/jdbc/html/jdbc.html

Installation procedure

You need to follow the guidelines defined in the iPlanet™ Portal Server 3.0 Installation Guide. Before installing the iPlanet Portal Server Plug-in for the Identrus System, a fresh install of the Portal Server is required. Note the location of its installation, as this will be required when running the subsequent scripts:

- Login as root and from the shell prompt type the following:

```
domainname
```

- If the above command returns nothing then type domainname <domain_name>. For example

```
domainname uk.sun.com
```

- Go to the root directory of the installation CD- rom for example:

```
cd /dev/cdrom
```

- The portal server must be running (See the iPlanet portal Server Documentation for details).

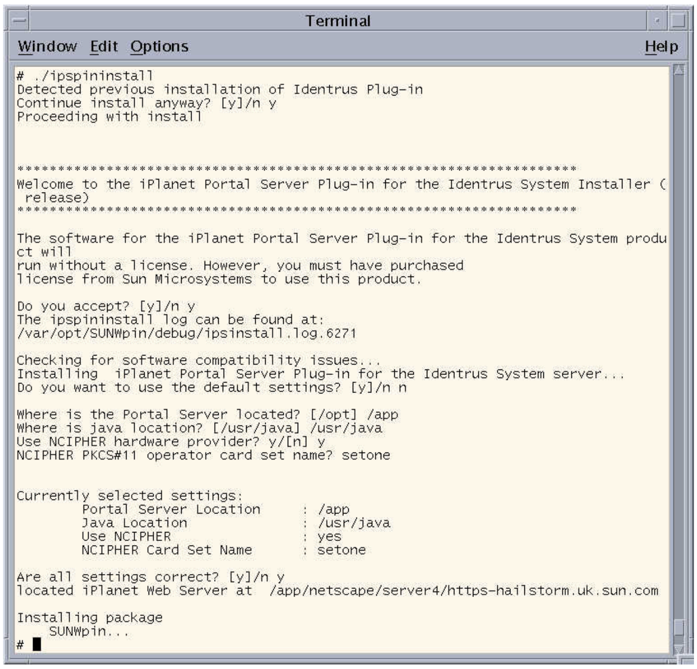
- Execute the installation script by typing the following command:

```
./ipspininstall
```

- If you have installed the Portal Server in the default location /opt then you can accept the defaults for the iPlanet Portal Server Plug-in for the Identrus System installation. Otherwise you must supply the location of the portal server installation and iPlanet Web Server Installation.

- The figure below illustrates a typical installation.

Figure 6 Example Installation Script



```
# ./ipspininstall
Detected previous installation of Identrus Plug-in
Continue install anyway? [y]/n y
Proceeding with install



*********************************************************************
Welcome to the iPlanet Portal Server Plug-in for the Identrus System Installer (
 release)
*********************************************************************

The software for the iPlanet Portal Server Plug-in for the Identrus System produ
ct will
run without a license. However, you must have purchased
license from Sun Microsystems to use this product.

Do you accept? [y]/n y
The ipspininstall log can be found at:
/var/opt/SUNWpin/debug/ipsinstall.log.6271

Checking for software compatibility issues...
Installing  iPlanet Portal Server Plug-in for the Identrus System server...
Do you want to use the default settings? [y]/n n

Where is the Portal Server located? [/opt] /app
Where is java location? [/usr/java] /usr/java
Use NCIPHER hardware provider? y/[n] y
NCIPHER PKCS#11 operator card set name? setone


Currently selected settings:
        Portal Server Location      : /app
        Java Location               : /usr/java
        Use NCIPHER                 : yes
        NCIPHER Card Set Name       : setone

Are all settings correct? [y]/n y
located iPlanet Web Server at  /app/netscape/server4/https-hailstorm.uk.sun.com

Installing package
    SUNWpin...
# █
```

- As detailed in the prerequisite section of this document you must obtain the Oracle JDBC Drivers (typically oracle-jdbc-815.zip). Place this file into the following location.

```
<portal_install_directory>/SUNWips/lib
```

- Set the classpath in the Portal Web Server directory by editing the file (to reflect Oracle filename oracle-jdbc-815.zip):

```
/opt/netscape/server4/https-hailstorm/config/jvm12.conf
```

- Ensure you have database access, taking note of the login id's and configuration. Then to set up the tables required by the portal server plug-in you will also need to run the SQL script

```
<portal_install_directory>/SUNWpin/sql/OracleCertStore.sql
```

- You can also remove tables and data using the script:

```
<portal_install_directory>/SUNWpin/sql/Drop_OracleCertStore.sql
```

- Your iPlanet Portal Server Plug-in for the Identrus System has now been successfully installed. Please consult the Post Installation section on how to start and stop the Portal Server (see section headed Post Installation procedureon page 24).

- You can verify the installation by running the Sample CSC program from your browser. See the section headed Running the sample program on page 76

- Please consult the next section for details on HSM configuration.

HSM Configuration

HSMs are accessed through the PKCS#11 libraries shipped by HSM vendors. In order to use an HSM, the HSM must first be correctly configured for PKCS#11 operation, and then the iPlanet Portal Server Plug-in must be configured to recognise the HSM.

Configuring the HSM

An HSM should be configured according to its vendor's instructions. A brief description of the process for nCipher HSMs is provided here, along with a reference to the vendor documentation

Configuring an nCipher HSM

- Refer to the nCipher documentation for definition of terms and further instructions on Security Worlds and Operator Card Sets: Chapters 6 and 7 of the document found at http://active.ncipher.com/documentation/PKCS11/solaris-4.01/nforce.pdf are particularly enlightening

- Install the nCipher PKCS #11 library usually into:

```
/opt/nfast
```

- The iPlanet Portal Server Plug-in requires a 1 of N Operator Card Set to use an nCipher HSM in PKCS#11 mode. One Operator Card is required for each module in the HSM. Create such an Operator Card Set as specified in the nCipher documentation. The password used must be the same as the password configured in iPlanet portal Server Plugin for the Identrus System (see Administrator Login Procedure on page 27)

- Create a new text file cknfastrc in the directory in which you installed the nCipher software, usually /opt/nfast, and add the lines:

```
CKNFAST_NO_UNWRAP=1
CKNFAST_LOADSHARING=1
CKNFAST_NO_ACCELERATOR_SLOTS=1

export CKNFAST_NO_UNWRAP CKNFAST_LOADSHARING CKNFAST_NO_ACCELERATOR_SLOTS
```

- Check the installation using

```
/opt/nfast/bin/ckcheckinst
```

- In the following sections, where the vendor PKCS#11 library is referred to, take that reference to mean

```
/opt/nfast/gcc/lib/libcknfast.so
```

- Additionally, the name of the PKCS#11 token upon which private keys will be generated and stored is the name of the Operator Card Set created for use with the nCipher PKCS#11 interface

Configuring the iPlanet Portal Server Plug-in

There are two steps to be taken in configuring the iPlanet Portal Server Plug-in :

- Identifying the HSM vendor's PKCS#11 library to the Plug-in PKCS#11 cryptographic services

- Configuring the iPlanet Portal Server Plug-in to use the HSM based PKCS#11 tokens for key storage. This may be done as part of the installation procedure, but the manual operation is detailed here to permit an HSM to be installed after installation

Identifying the vendor PKCS#11 libraries

- Change to the directory. If the .netscape directory does not exist, create it

```
<portal_install_directory>/https-<servername>/config/.netscape
```

- If the file secmod.db does not exist in the .netscape directory create it as follows:

```
<portal_install_directory>/bin/https/admin/bin/modutil
  -dbdir . -nocertdb -create
```

- If modutil created a secmodule.db rather than a secmod.db, move the file

```
mv secmodule.db secmod.db
```

- Add the vendor PKCS#11 library to the database of PKCS#11 modules, using an appropriate module name, e.g. nFast for an nCipher nFast module

```
<portal_install_directory>/bin/https/admin/bin/modutil
  -dbdir . -nocertdb
  -add <moduleName>
  -libfile <vendorPKCS#11Library>
  -mechanisms RSA:DSA
```

- Check that the module was installed using

```
<portal_install_directory>/bin/https/admin/bin/modutil
  -dbdir . -nocertdb -list
```

- The output should look something like this

```
Using database directory ....
Listing of PKCS #11 Modules
Listing of PKCS #11 Modules
----------------------------------------------------------
1.<moduleName>
library name: <vendorPKCS#11Library>
slots: # slots attached
status: loaded
slot: ####-####-####-#
token: <tokenName>
slot: ####-####-####-#
token: <anotherTokenName>
...
2. Netscape Internal PKCS #11 Module
slots: 2 slots attached
status: loaded
slot: Communicator Internal Cryptographic Services Version 4.0
token: Communicator Generic Crypto Svcs
slot: Communicator User Private Key and Certificate Services
token: Communicator Certificate DB
---------------------------------------------------------
```

Configuring the iPlanet Portal Server Plug-in to use a PKCS#11 token

- If the iPlanet Portal Server Plug-in was configured at install time to use a PKCS#11 token, and the correct token name was chosen, then no further steps need be taken, and the Portal Server Plug-in will use the HSM for key generation and storage

- If the iPlanet Portal Server Plug-in was not installed to use a specific PKCS#11 token, or the token name was specified incorrectly, then these actions should be followed

- Change directory to

```
cd <portal_install_directory>/lib
```

- remove any existing directory named jssconfig

```
rm -rf jssconfig
```

- Unpack the jssconfig.tar archive

```
tar xvf jssconfig.tar
```

- Edit the file

```
<portal_install_directory>/lib/jssconfig/trustbase/security/jsstokenk
eystore
```

- Change the key.token property line contained therein thus:

```
key.token=<tokenName>
```

- Save the file, leaving other lines untouched

- Restart the iPlanet Portal Server, which is now configured to use the PKCS#11 token with the given name for key generation and storage operations

Post Installation procedure

After ensuring you have followed the installation and HSM configuration steps, the Portal Server must be shut down and restarted. Please ensure you start and stop the Portal Server using the specially installed plug-in scripts:

```
<portal_install_directory>/SUNWips/bin/SUNWpinStart
<portal_install_directory>/SUNWips/bin/SUNWpinStop
```

Note this does not start the gateway. This is normally achieved by typing the following commands:

```
<portal_install_directory>/SUNWips/bin/ipsgateway start
<portal_install_directory>/SUNWips/bin/ipsgateway stop
```

However Please refer to the Portal Server Documentation for details on how to start and stop the Portal gateway.

```
http://docs.iplanet.com/docs/manuals/portal/30/install/server_i.htm
```

Software Uninstallation

To remove the iPlanet Portal Server Plug-in for the Identrus System but maintain the Portal Server installation perform the following steps:

- Ensure the Portal Server is running
- Login as root
- Execute the following command

```
pkgrm SUNWpin
```

- Shut down and restart the Portal Server. Consult the Portal Server documentation to do this.

To remove iPlanet Portal Server consult

http://docs.iplanet.com/docs/manuals/portal/30/install

Chapter 3

Administration

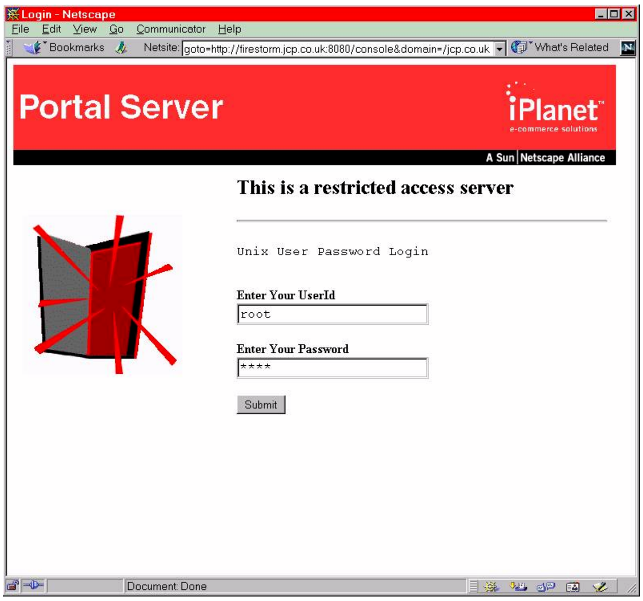
Administering the iPlanet Portal Server Plug-in for the Identrus System involves setting up appropriate certificates that allow authentication and authorisation of Identrus member users. The objectives of this chapter are to cover:

- Administrator Login Procedure
- Certificate Status Check Configuration
- Relying Customer Host Configuration
- Setting up Login Authorisation for Identrus member users
- Certificate Status Check
- Configuration of Transport authentication through the SSL Communication

Administrator Login Procedure

- From your browser select the url to the Portal Server. Normally this will be http://<machine name>:<port>/console. For example: http://firestorm.jcp.co.uk:8080/console

Figure 7 Administrator Login Screen



Login - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: goto=http://firestorm.jcp.co.uk:8080/console&domain=/jcp.co.uk
What's Related
Portal Server
iPlanet™
e-commerce solutions
A Sun | Netscape Alliance

This is a restricted access server

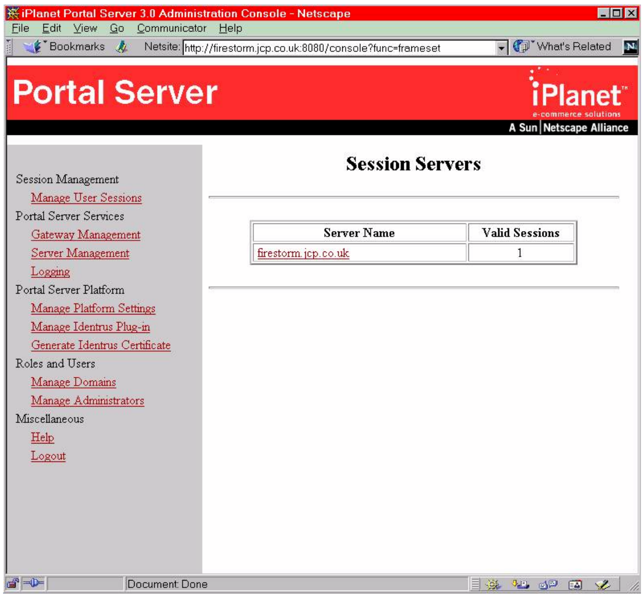
Unix User Password Login

Enter Your UserId: root

Enter Your Password: ****

- Login to the Portal Administrator account and the following screen appears:

Figure 8 Administration Main menu

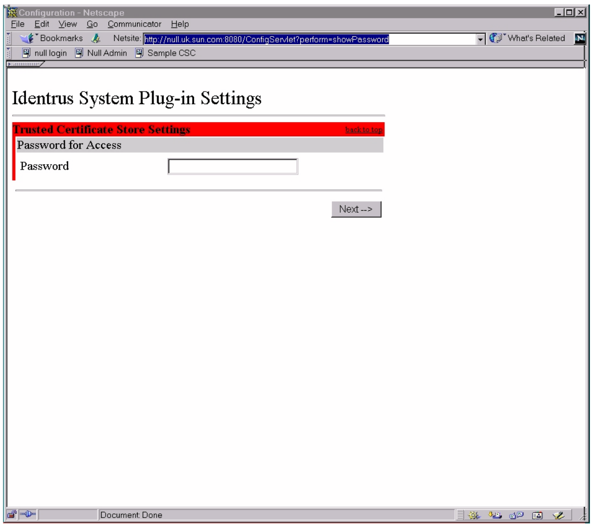


Session Servers

Server Name	Valid Sessions
firestorm.jcp.co.uk	1

- Select <Manage Identrus Plug-in> On first occurrence, this jumps to the Trusted Certificate Store Password Screen. Enter the password you wish to use to gain access to the certificate store. This should be the same password as for your PKCS11 token password (see section on HSM Configuration on page 22). This only applies if you are using an external HSM.

Figure 9 Certificate Store Password



http://null.uk.sun.com:8080/ConfigServlet?perform=showPassword

Identrus System Plug-in Settings

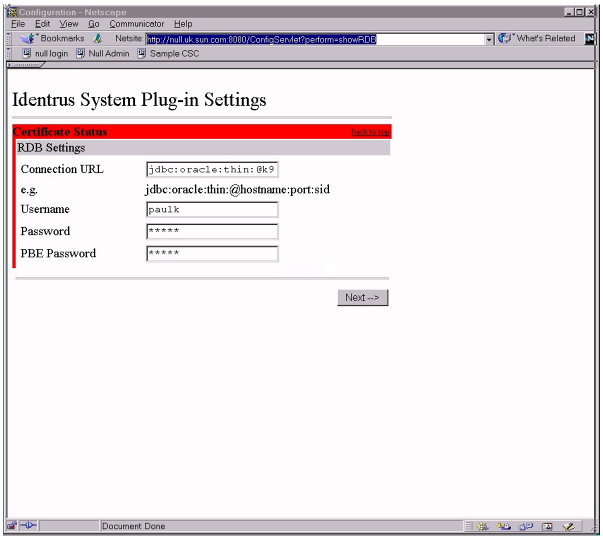
Trusted Certificate Store Settings

Password for Access

Password	

- Select <Next> Here you should make your RDB settings as illustrated below:

Figure 10 RDB Settings



http://null.uk.sun.com:8080/ConfigServlet?perform=showRDB

Identrus System Plug-in Settings

Certificate Status

RDB Settings

Connection URL	jdbc:oracle:thin:@k9
e.g.	jdbc:oracle:thin:@hostname:port:sid
Username	paulk
Password	*****
PBE Password	*****

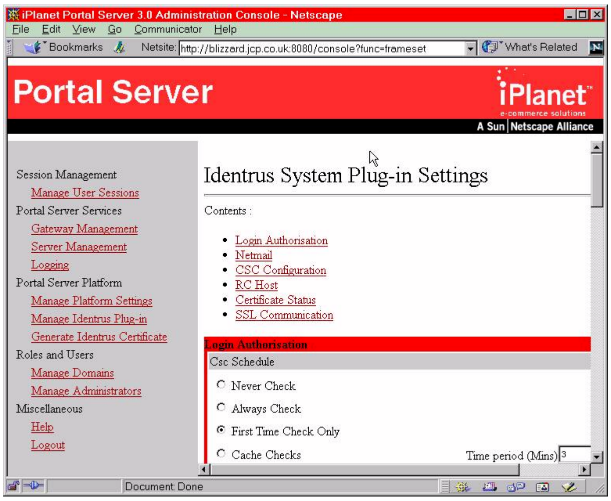
- The following settings are required:
  - <Connection URL> i.e. the location of your oracle database.
  - <Username> i.e. the username to allow you access onto the oracle framework database
  - <Password> i.e. the password to allow you access onto the Oracle framework database.

  - <PBE Password> i.e. the password that allows you access to the encrypted data held within the certificate Storage locations running within the Oracle database.

- Select <Next> when you have finished making your selections

- In all subsequent occurrences, when selecting <Manage Identrus Plug-in>, the following menu appears:

Figure 11 iPlanet Portal Server Plug-in for the Identrus System Main Menu Options


iPlanet Portal Server 3.0 Administration Console - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: http://blizzard.jcp.co.uk:8080/console?func=frameset
What's Related
Portal Server
iPlanet™
e-commerce solutions
A Sun | Netscape Alliance
Document: Done

Session Management
Manage User Sessions
Portal Server Services
Gateway Management
Server Management
Logging
Portal Server Platform
Manage Platform Settings
Manage Identrus Plug-in
Generate Identrus Certificate
Roles and Users
Manage Domains
Manage Administrators
Miscellaneous
Help
Logout

Identrus System Plug-in Settings

Contents :

- Login Authorisation
- Netmail
- CSC Configuration
- RC Host
- Certificate Status
- SSL Communication

Login Authorisation

Csc Schedule

○ Never Check

○ Always Check

● First Time Check Only

○ Cache Checks Time period (Mins) 3

After explaining the different procedures for obtaining certificates, we then discuss these choices in turn:

- <Generate Identrus Certificate> for certificates requiring verification

- <Login Authorisation>, <Netmail> decide who can use the system and also how they can use the system.

- <CSC Configuration>, <RC Host>, <Certificate Status>

- <SSL Communication> allowing transport authentication

Note All configuration options should be considered in turn and when you have finished making your configuration selections scroll down to the bottom right hand corner and press Save to make your selections take effect.

Generating Identrus Certificates

The following Certificates are used for signing purposes, allowing integrity and avoiding email messages that have been tampered with, and as such require a PKCS10 request from the Identrus system and a PKCS7 Response from your CA:

- Request Signing Certificate
- Response Signing Certificate
- SSL Client Certificate signs the handshake request.

All other Certificates are needed for validation/verification purposes, allowing authentication and authorisation, and should be obtained directly from your CA:

- Trusted Login CA Certificate
- Trusted Email Certificate
- Trusted Response Verification Certificate

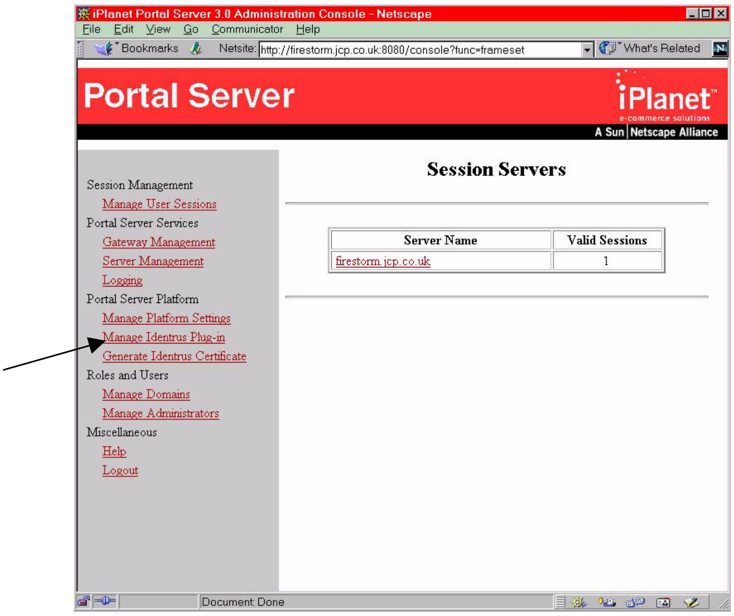
Note How the Certificate Authority sets this procedure up will depend on its security policy. If in doubt you should give this to your CA operator who will process it and return a Certificate back to you.

Adding a Certificate for Authentication and Authorisation purposes

In this case a PKCS10 request is not needed and as such the following procedure applies:

- From the iPlanet Portal Server main screen, select <Manage Identrus Plug-in>

Figure 12 Portal Administrator Main Screen

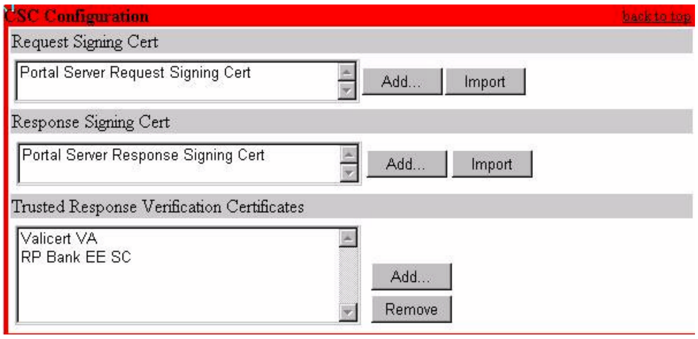


Session Servers

Server Name	Valid Sessions
firestorm.jcp.co.uk	1

- Select <CSC Configuration>, Select <Add>, for example <Trusted Response Verification certificate> as illustrated below:

Figure 13 CSC Configuration



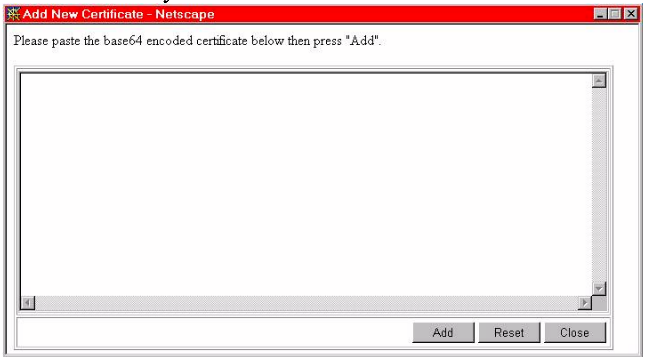
Request Signing Cert: Portal Server Request Signing Cert

Response Signing Cert: Portal Server Response Signing Cert

Trusted Response Verification Certificates:
Valicert VA
RP Bank EE SC

- Certificates can be added by pasting in a certificate you obtained directly from your CA.

Figure 14 Pasting a base64 encoded certificate into your iPlanet Portal Server Plug-in for the Identrus System



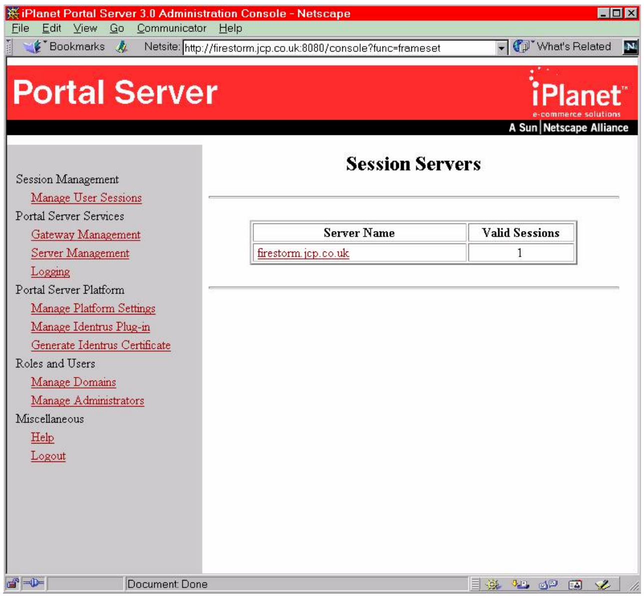
Please paste the base64 encoded certificate below then press "Add".

Adding a Certificate for Signature purposes

There are two main steps to this (Generating a signature request using a PKCS 10 Request from the Identrus System and getting a PKCS 7 Response from your Certificate authority):

- From the main Menu Select <Generate Identrus Certificate>:

Figure 15 Portal Administrator Main Screen

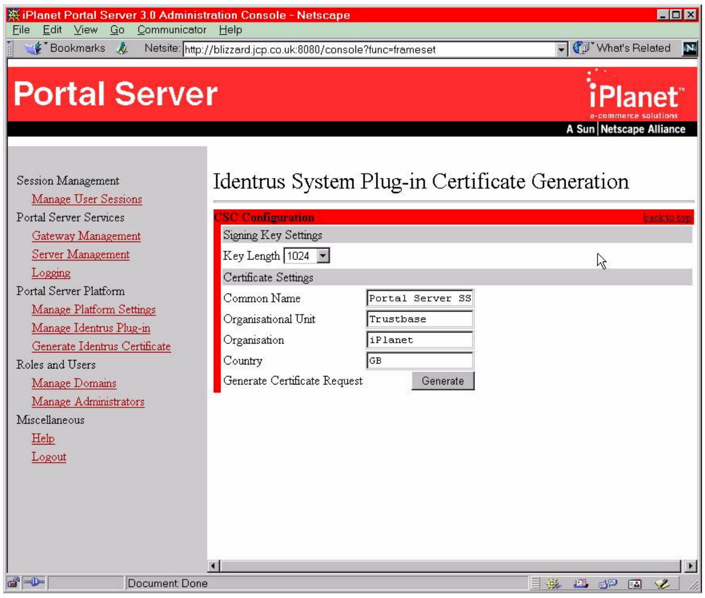


Session Servers

Server Name	Valid Sessions
firestorm.jcp.co.uk	1

- The following Certificate Settings must be supplied:

Figure 16 Generating a PKCS#10 certificate request



Identrus System Plug-in Certificate Generation

CSC Configuration

Signing Key Settings

Key Length 1024

Certificate Settings

Common Name	Portal Server SS
Organisational Unit	Trustbase
Organisation	iPlanet
Country	GB
Generate Certificate Request	Generate

- <Key length> (choice of 512 bit, 1024 bit[CB3]).

- <Common Name> is the Name to give the certificate e.g. Portal SSL Certificate.

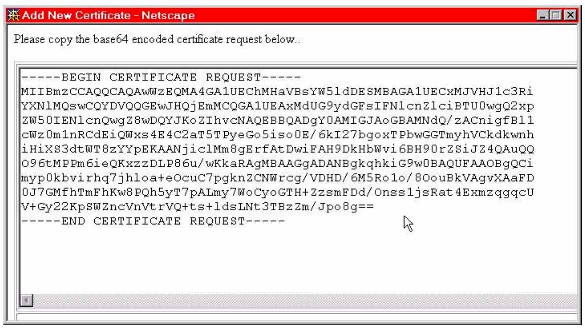
- <Organisation> the affiliation to which the user creating the certificate belongs e.g. iPlanet.

- <Organisational Unit> that represents the department or subsidiary of the organisation to which the user/entity belongs.

- <Country> that the user is based, as defined as ISO3611 standard http://www.iso.ch and X500 standard http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html e.g. GB.

- Generate a certificate request by selecting Generate This will cause a certificate request to be made. The request will be a base64 encoded PKCS 10 request.

Figure 17 Copying a PKCS10 request

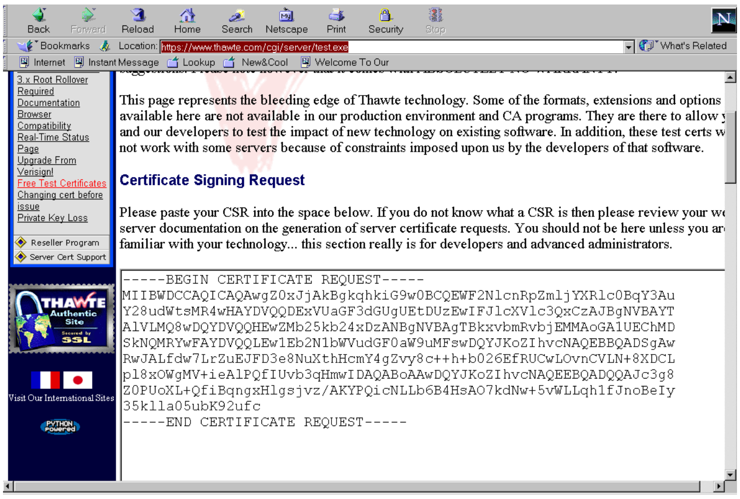


Please copy the base64 encoded certificate request below..

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBmzCCAQQCAQAwWzEQMA4GA1UEChMHaVBsYW5ldDESMBAGA1UECxMJVHJ1c3Ri
YXN1MQswCQYDVQQGEwJHQjEmMCQGA1UEAxMdUG9ydGFsIFNlcnZlciBTU0wgQ2xp
ZW50IENlcnQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMNdQ/zACnigfBl1
cWz0m1nRCdEiQWxs4E4C2aT5TPyeGo5iso0E/6kI27bgoxTPbwGGTmyhVCkdkwnh
iHiXS3dtWT8zYYpEKAANjiclMm8gErfAtDwiFAH9DkHbWvi6BH90rZSiJZ4QAuQQ
O96tMPPm6ieQKxzzDLP86u/wKkaRAgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQCi
myp0kbvirhq7jhloa+eOcuC7pgknZCNWrcg/VDHD/6M5Ro1o/8OouBkVAgvXAaFD
0J7GMfhTmFhKw8PQh5yT7pALmy7WoCyoGTH+ZzsmFDd/Onss1jsRat4ExmzqgqcU
V+Gy22KpSWZncVnVtrVQ+ts+ldsLNt3TBzZm/Jpo8g==
-----END CERTIFICATE REQUEST-----
```

- Go to a CA Web-site and search for the section that involves creating a Server Certificate and follow the instructions until it asks you to paste in the PKCS10 request.

Figure 18 Paste PKCS10 Request into CA Website



This page represents the bleeding edge of Thawte technology. Some of the formats, extensions and options available here are not available in our production environment and CA programs. They are there to allow y and our developers to test the impact of new technology on existing software. In addition, these test certs w not work with some servers because of constraints imposed upon us by the developers of that software.

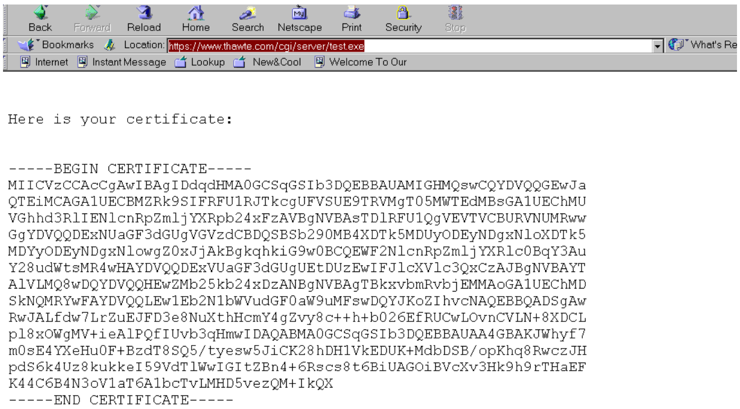
Certificate Signing Request

Please paste your CSR into the space below. If you do not know what a CSR is then please review your we server documentation on the generation of server certificate requests. You should not be here unless you ar familiar with your technology... this section really is for developers and advanced administrators.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBWDCCAQICAQAwgZ0xJjAkBgkqhkiG9w0BCQEWF2NlcnRpZmljYXRlc0BqY3Au
Y28udWtsMR4wHAYDVQQDExVUaGF3dGUgUEtDUzEwIFJlcXVlc3QxCzAJBgNVBAYT
AlVLMQ8wDQYDVQQHEwZMb25kb24xDzANBgNVBAgTBkxvbmRvbjEMMAoGA1UEChMD
SkNQMRYwFAYDVQQLEw1Eb2N1bWVudGF0aW9uMFswDQYJKoZIhvcNAQEBBQADSgAw
RwJALfdw7LrZuEJFD3e8NuXthHcmY4gZvy8c++h+b026EfRUCwLOvnCVLN+8XDCL
pl8xOWgMV+ieAlPQfIUvb3qHmwIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQAJc3g8
Z0PUoXL+QfiBqngxHlgsjvz/AKYPQicNLLb6B4HsAO7kdNw+5vWLLqh1fJnoBeIy
35klla05ubK92ufc
-----END CERTIFICATE REQUEST-----
```

- Collect the corresponding base64 encoded certificate response using cut and paste. When copying and pasting certificates use <Ctrl>C <Ctrl>V.

Figure 19 Copy base64 encoded Certificate response from CA



Here is your certificate:

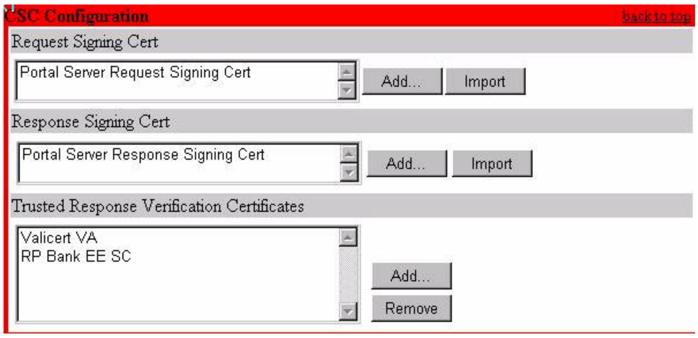
```
-----BEGIN CERTIFICATE-----
MIICVzCCAcCgAwIBAgIDdqdHMA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJa
QTEiMCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MWTEdMBsGA1UEChMU
VGhhd3RlIENlcnRpZmljYXRpb24xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRww
GgYDVQQDExNUaGF3dGUgVGVzdCBDQSBSb290MB4XDTk5MDUyODEyNDgxNloXDTk5
MDYyODEyNDgxNlowgZ0xJjAkBgkqhkiG9w0BCQEWF2NlcnRpZmljYXRlc0BqY3Au
Y28udWtsMR4wHAYDVQQDExVUaGF3dGUgUEtDUzEwIFJlcXVlc3QxCzAJBgNVBAYT
AlVLMQ8wDQYDVQQHEwZMb25kb24xDzANBgNVBAgTBkxvbmRvbjEMMAoGA1UEChMD
SkNQMRYwFAYDVQQLEw1Eb2N1bWVudGF0aW9uMFswDQYJKoZIhvcNAQEBBQADSgAw
RwJALfdw7LrZuEJFD3e8NuXthHcmY4gZvy8c++h+b026EfRUCwLOvnCVLN+8XDCL
pl8xOWgMV+ieAlPQfIUvb3qHmwIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAKJWhyf7
m0sE4YXeHu0F+BzdT8SQ5/tyesw5JiCK28hDH1VkEDUK+MdbDSB/opKhq8RwczJH
pdS6k4Uz8kukkeI59VdTlWwIGItZBn4+6Rscs8t6BiUAGOiBVcXv3Hk9h9rTHaEF
K44C6B4N3oV1aT6AlbcTvLMHD5vezQM+IkQX
-----END CERTIFICATE-----
```

- From iPlanet Portal Server main screen, select <Manage Identrus Plug-in>

- Select <CSC Configuration>

- Now Select <Add> from the diagram below

Figure 20 CSC Configuration



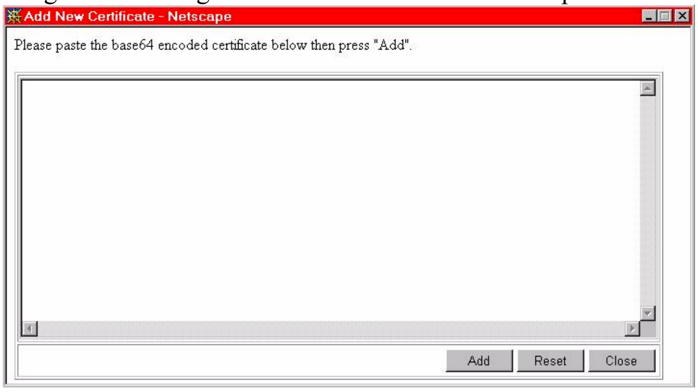
Portal Server Request Signing Cert

Portal Server Response Signing Cert

Valicert VA
RP Bank EE SC

- Certificates can be added by pasting in the resulting base64 encoded PKCS 7 response.

Figure 21 Pasting a base64 encoded Certificate response



Please paste the base64 encoded certificate below then press "Add".

- Select <Add>

- Alternatively the import feature Import, illustrated on the previous page, allows you to enter a PKCS7 response as a filename.

Removing a Certificate

Certificates can also be removed and in such cases will render users unable to send validated messages.

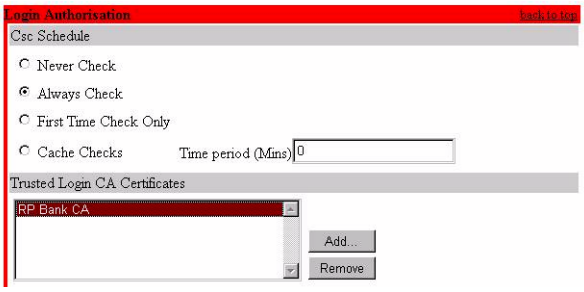
Note If in doubt, please consult your local product support representative on how to install your Certificate

Login Authorisation

This option allows you to decide what login security measures you want in place for your users when they log in. Allowed settings are:

- Never check certificate status at login
- Always check certificate status at login
- Check certificate status only at first login
- Positive certificate status checks are cached for the period (in minutes) given. If the user subsequently logs in within the cache period then the previously requested status is used. Note that negative (revoked/unknown) responses are *not* cached.

Figure 22 Login Authorisation Main Choices



Login Authorisation

Csc Schedule

○ Never Check

● Always Check

○ First Time Check Only

○ Cache Checks Time period (Mins) 0

Trusted Login CA Certificates

RP Bank CA

Enter the certificate of the Relying Participant's bank here. Any customers of this particular Identrus member bank can login to the Portal Sever. Trusted certificates can be added or removed accordingly. One or more base64-encoded certificates may be pasted into the configuration interface. For an identity certificate presented at login to be considered part of the scheme, one of these certificates must appear in its certificate chain.

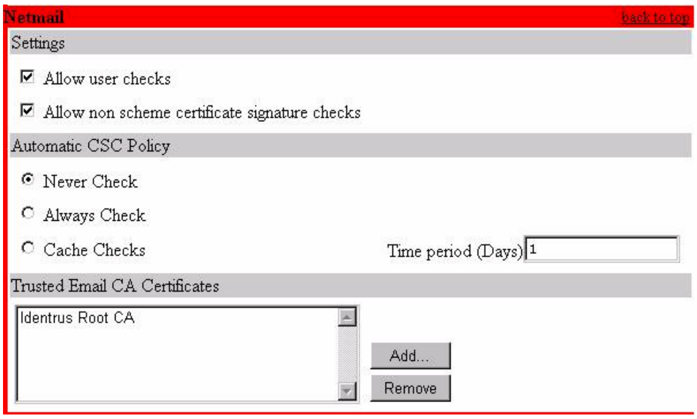
Note In order to obtain this certificate you should contact your CA administrator who, because you are already an Identrus member, will be in possession of both the Identrus root certificate and your relying participants certificate. If in doubt, please consult your local product support representative on how to install your Certificate. See also Section Adding a Certificate for Authentication and Authorisation purposes on page 31

Netmail Configuration

For billing reasons there are a number of scenarios for deciding whether you wish a Certificate Status check done automatically or manually. In the case where most of your users are known, Certificate Status Checks may not be necessary. There are three choices:

- Automatically perform CSC Check
- Allow Manual User checks
- Allow non-scheme certificate signature checks. If true then non-scheme signatures are checked and the relevant icon displayed; otherwise no signature checks are performed on messages signed by a non-scheme certificate.

Figure 23 Netmail Configuration Options



Netmail

Settings

☑ Allow user checks

☑ Allow non scheme certificate signature checks

Automatic CSC Policy

● Never Check

○ Always Check

○ Cache Checks Time period (Days) 1

Trusted Email CA Certificates

Identrus Root CA

Enter the Identrus root certificate here. Any email sent by any Identrus member can be verified. Other base64-encoded certificates may be pasted into this configuration interface. For an email-signing certificate to be considered part of the scheme, one of these certificates must appear in its certificate chain.

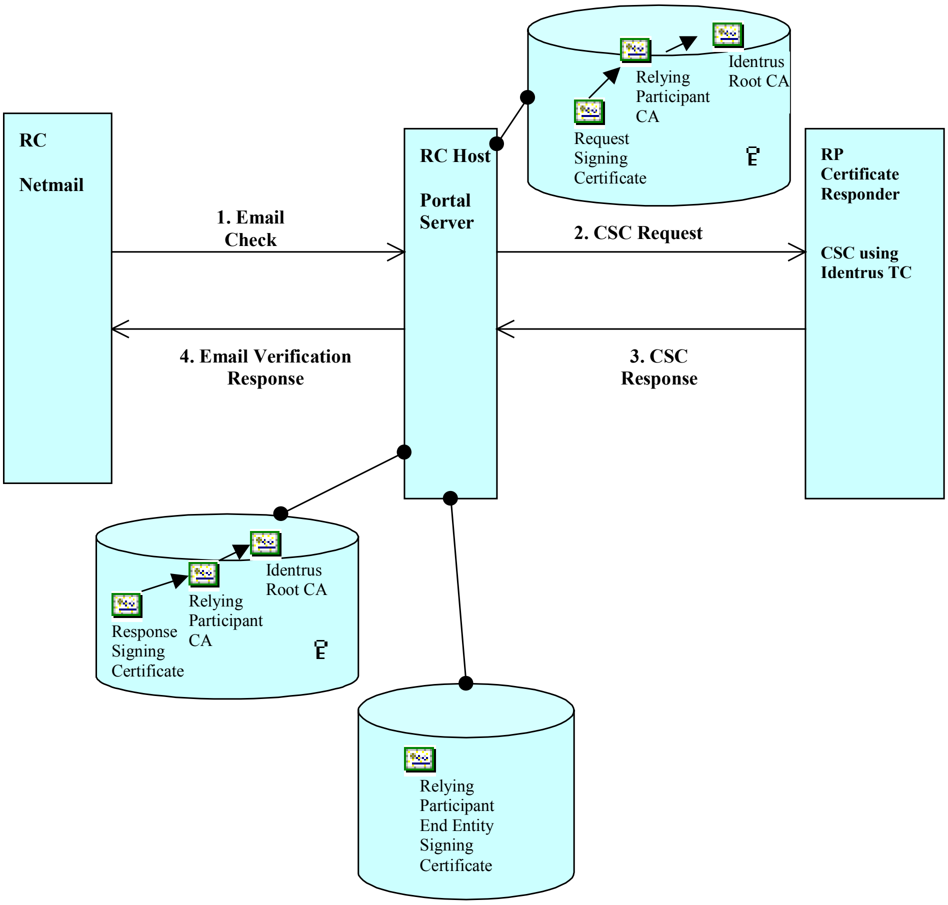
In order to obtain this certificate you should contact your CA administrator who, because you are already an Identrus member, will be in possession of both the Identrus root certificate and your relying participants certificate.

Note If in doubt, please consult your local product support representative on how to install your Certificate. See also Section Adding a Certificate for Authentication and Authorisation purposes on page 31

CSC Configuration

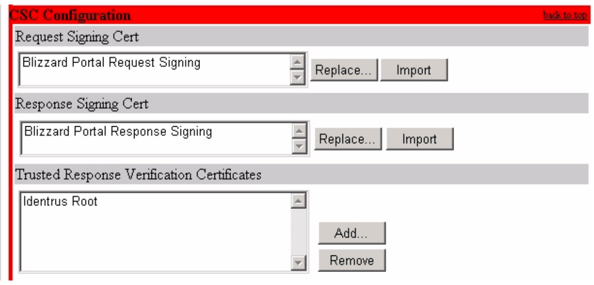
A Certificate Status Check allows you to check the status of any Identrus member certificate. The OCSP or Identrus CSC responder either responds to these requests by contacting its local responder, if this organisation issued a certificate or it forwards the request to another Responder whose organisation issued the certificate.

Figure 24 Example Identrus CSC Illustrating certificates needed to generate and verify messages



Before adding the Request/Response certificates, you will need to make sure the root certificate and its corresponding CA check has been configured. If you have the Certificate as an individual base64 encoded certificate it is recommended you add the root then <replace> it with the CA and then replace again with the corresponding Request and Response certificate. This has the effect of configuring the full Root/CA/Request or Response Certificate chain.

Figure 25 CSC Configuration



CSC Configuration

Request Signing Cert: Blizzard Portal Request Signing

Response Signing Cert: Blizzard Portal Response Signing

Trusted Response Verification Certificates: Identrus Root

The following certificates need to be configured in order for users to perform Certificate Status Checks.

- Request Signing Certificate. The signing key for CSC requests (sent from the RC host to RP) is held in a Hardware Security Module (HSM). All private key operations involving the signing key take place on the HSM. See Section Adding a Certificate for Signature purposes on page 33 on how to obtain this)

- Response Signing Certificate. The signing key for CSC responses (sent from the RC host to RC) is also held in a Hardware Security Module (HSM). Again, all private key operations involving the signing key take place on the HSM. See Section Adding a Certificate for Signature purposes on page 33 on how to obtain this)

- Trusted Response verification certificates. One or more base64-encoded certificates may be pasted into the configuration interface. For an OCSP responder or CSC responder to be trusted, one of these certificates must appear in the responder’s certificate chain. (See Section Adding a Certificate for Authentication and Authorisation purposes on page 31). This can be either a Certificate Authority that acts as an OCSP responder (e.g. the VA certificate) or in the case of Identrus the Relying Participant End Entity Signing certificate as illustrated in Figure 25 CSC Configuration.

Note If in doubt, please consult your local product support representative on how to install your Certificate. Before adding a Certificate you must get your certificate from an appropriate authority. See Section on page 30 for details on how to do this.

RC Host Configuration

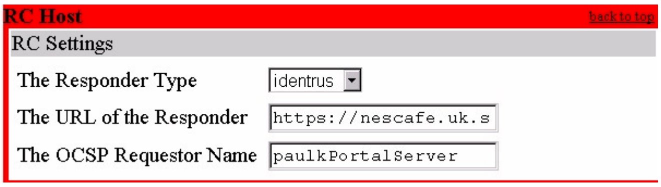
The following Relying Customer (RC) settings must be made:

- Responder types. There are two choices here: a) OCSP if you want to use an OCSP Responder. b) Identrus Certificate Status Check if you have a full Identrus implementation.

- Responder URLs e.g. ‘https://hailstorm.uk.sun.com:8080.

- The OCSP Requestor name. The name of the entity making an OCSP request needed when signed (usually a URL).

Figure 26 RC Host Configuration



RC Host

RC Settings

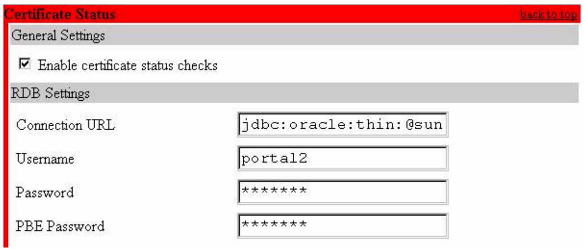
The Responder Type	identrus
The URL of the Responder	https://nescafe.uk.s
The OCSP Requestor Name	paulkPortalServer

Certificate Status

These settings define the system and whether or not Certificate Status Checks can be made for the system as a whole. They also define the database connection information used by the iPlanet Portal Server Plug-in for the Identrus System. Administrators wishing to view a Certificate Status Check made via the system will need to consult the audit log, see section Logging on page 44.

- Enable Certificate Status Checks.

Figure 27 Certificate Status Configuration



Certificate Status

General Settings

☑ Enable certificate status checks

RDB Settings

Connection URL	jdbc:oracle:thin:@sun
Username	portal2
Password	*******
PBE Password	*******

The following settings are required:

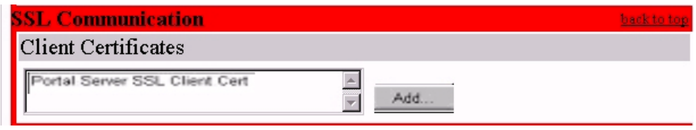
- <Connection URL> i.e. the location of your Oracle database.
- <Username> i.e. the username to allow you access onto the Oracle framework database
- <Password> i.e. the password to allow you access onto the Oracle framework database.
- <PBE Password> i.e. the password that allows you access to the encrypted data held within the certificate Storage locations running within the Oracle database.

SSL Communication

Certificates are required at the transport layer in order to allow SSL Handshaking to take place. The following Certificate options are needed:

- <Client Certificates>. i.e. those that sit on the portal server. This must be signed thus, See section Adding a Certificate for Signature purposes on page 33 for the procedure for obtaining this certificate.

Figure 28 SSL Communication Configuration



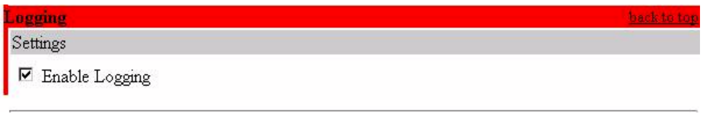
In order to obtain this certificate you should contact your CA administrator who, because you are already an Identrus member, will be in possession of both the Identrus root certificate and your relying participants certificate.

Logging

Configuration

The log can either be enabled or disabled. If the log is disabled then no new entries will be recorded in the view.

Figure 29 Configuring Logging



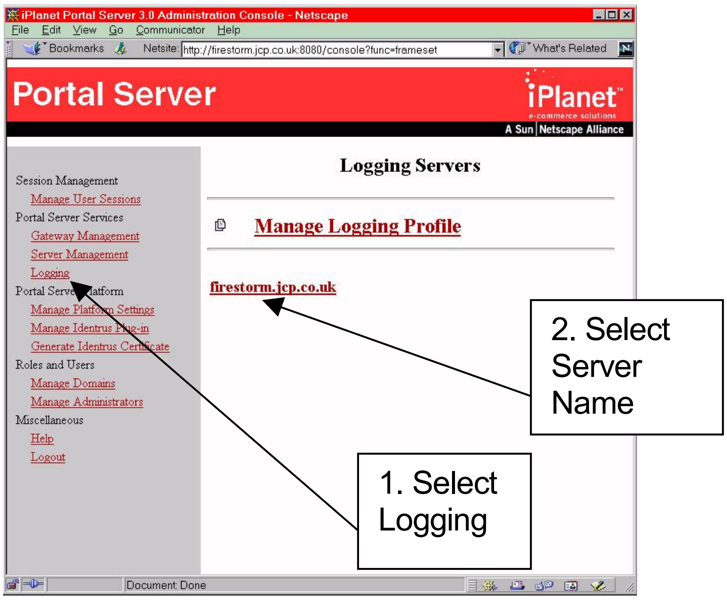
Settings

☑ Enable Logging

Viewing

From the main menu, Select <Logging> allows you to view aspects of the log.

Figure 30 Logging Main Menu



2. Select Server Name

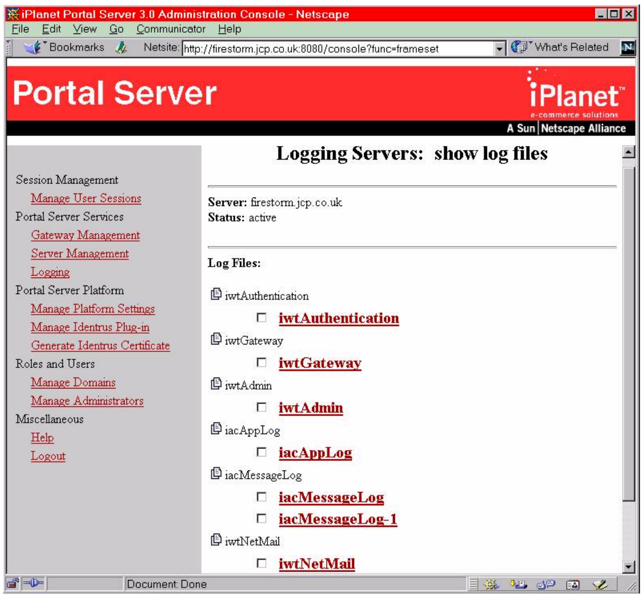
1. Select Logging

- A number of error logs can be viewed. By selecting your server e.g. firestorm.jcp.co.uk

- If you see the message “readExceedsMax” Error then the log file is too big to view on the screen. The files are still, however, viewable and can be found at the Portal default log directory

```
/var/opt/SUNWips/logs
```

Figure 31 Example Server log files



Logging Servers: show log files

Server: firestorm.jcp.co.uk
Status: active

Log Files:

iwtAuthentication
□ **iwtAuthentication**

iwtGateway
□ **iwtGateway**

iwtAdmin
□ **iwtAdmin**

iacAppLog
□ **iacAppLog**

iacMessageLog
□ **iacMessageLog**
□ **iacMessageLog-1**

iwtNetMail
□ **iwtNetMail**

There is an option also to delete specific log files if necessary. We now describe these log files.

- <iwtAuthentication>. Records all logon attempts, whether successful or failed. For the latter, the reason for logon failure will also be logged.
- <iwtGateway>. This is part of the standard Portal Server log and as such you should consult the Portal Administrator's guide for details about this.
- <iwtAdmin>. This is part of the standard Portal Server log and as such you should consult the Portal Administrator's guide for details about this.
- <iacMessageLog>. All certificate status check messages sent and received by the system are logged. Specifically, this includes:
  - CSC request received from RC
  - CSC request sent to RP
  - CSC response received from RP
  - CSC response sent to RC

- The following fields are included in the log record:
  - The raw message – this is always timestamped and signed by one of the RC, RC Host or CSC responder.
  - Requesting User – this allows determination of volume and type of request per requestor for profiling.
  - Subscribing Customer Certificate Chain
  - Date & Time – recorded to the nearest second. Timestamp format is YYYYMMDDhhmmss.
  - URL of responder – although the responder URL is fixed for the system for the time being, we log it in anticipation of a requirement to support multiple responders or if it changes over time.
  - Response Status – success, failure (with a record of the specific business or technical error causing the transaction's failure), timeout etc.
  - Certificate Status – valid, revoked, unknown.
  - Transaction ID
  - Complete response message
  - Context of request (currently mail check/login)
- <iacMessageLog-1> When a log file grows too large, it is renamed, and a new log file started in its place. This is a renamed iacMessageLog
- <iwtNetMail> This is part of the NetMail log and as such you should consult the Portal Administrator's guide for details about this.
- <iacAppLog> All errors are logged to an error log – this includes business, technical and implementation errors. The log entry includes
  - Date & Time – recorded to the nearest second. Timestamp format is YYYYMMDDhhmmss.
  - A unique identifier allowing the exact line of source code to be pinpointed.
  - A description of the error.
  - Data associated with the error where appropriate (e.g. a host name in the event of a connection failure)
  - Some kinds of errors may include a call-stack of any Java Exceptions

Note In some instances more information may be required. Under such circumstances, these logs are also expressed as text files that can be found in the following directory /var/opt/SUNWips/logs

Chapter 4

User

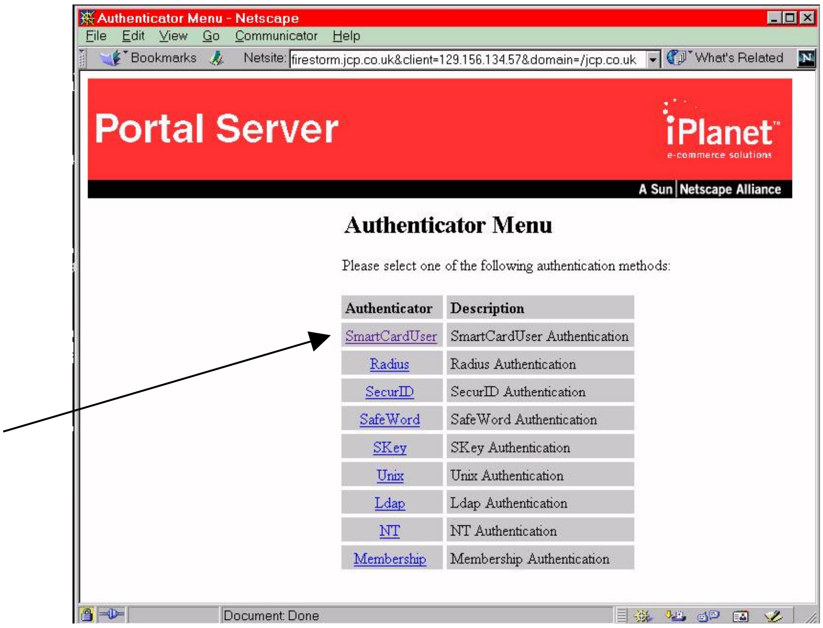
Having setup your digital certificates, you are now ready to use the iPlanet Portal Server Plug-in for the Identrus System. While using NetMail Lite you can , with confidence, choose to digitally sign messages that you wish to send and check the integrity and authenticity of messages that you receive. Thus, the objectives of this chapter are to cover the features that facilitate this:

- SmartCard Login Authorisation
- Email signing
- Viewing, Composing and Forwarding messages
- Message Verification Certificate Status logs
- Message Revocation
- Signature Validation

Smart Card Login

- From your browser enter the URL to access the Portal Server e.g. https://firestorm.jcp.co.uk:443

Figure 32 Login Main menu


Authenticator Menu - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: firestorm.jcp.co.uk&client=129.156.134.57&domain=/jcp.co.uk
What's Related
Portal Server
iPlanet
e-commerce solutions
A Sun | Netscape Alliance
Document: Done

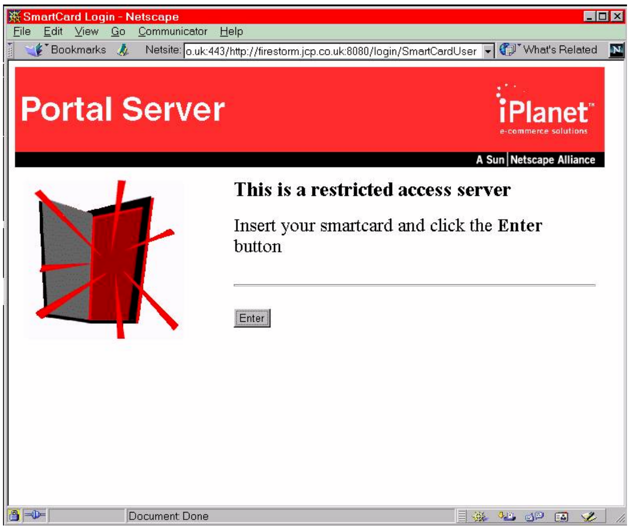
Authenticator Menu

Please select one of the following authentication methods:

Authenticator	Description
SmartCardUser	SmartCardUser Authentication
Radius	Radius Authentication
SecurID	SecurID Authentication
SafeWord	SafeWord Authentication
SKey	SKey Authentication
Unix	Unix Authentication
Ldap	Ldap Authentication
NT	NT Authentication
Membership	Membership Authentication

- Select <SmartCardUser>

Figure 33 Inserting your SmartCard

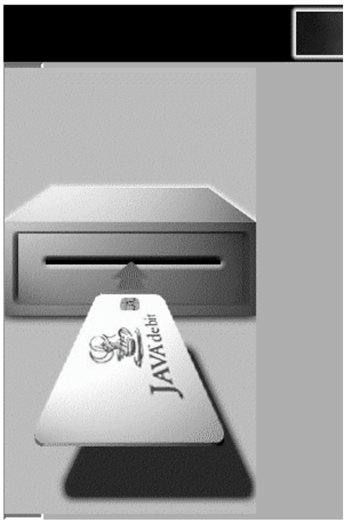

SmartCard Login - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: o.uk:443/http://firestorm.jcp.co.uk:8080/login/SmartCardUser
What's Related
Portal Server
iPlanet
e-commerce solutions
A Sun | Netscape Alliance
Enter
Document: Done

This is a restricted access server

Insert your smartcard and click the **Enter** button

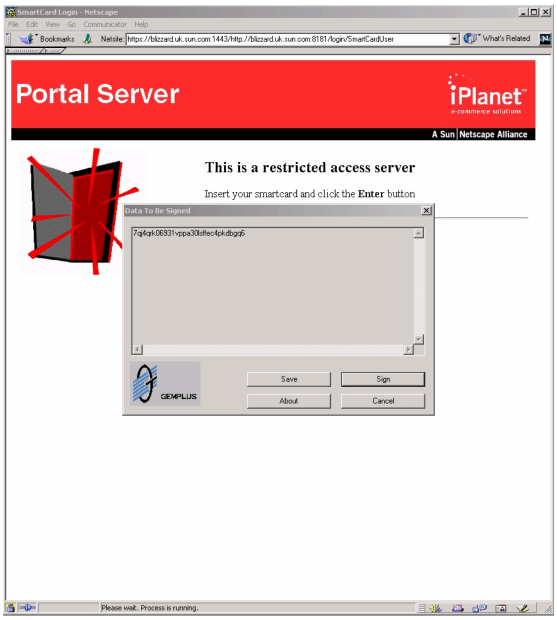
- Insert Smart Card into Card Reader

Figure 34 Inserting Smart Card into Card Reader



- On clicking the 'Enter' button, a dialog is displayed prompting the user to enter their SmartCard PIN.

Figure 35 Sign SmartCard Entry



https://blizzard.uk.sun.com:1443/http://blizzard.uk.sun.com:8181/login/SmartCardUser

This is a restricted access server

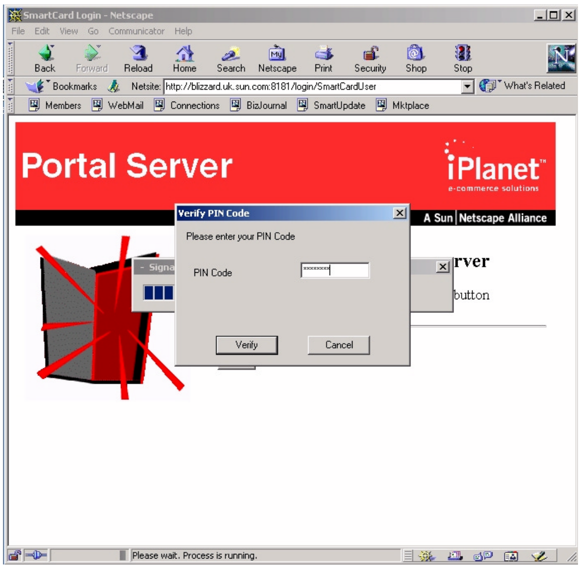
Insert your smartcard and click the **Enter** button

7qj4qrk06931vppa30lsffec4pkdbgq6

Please wait. Process is running.

- Select <Sign>

Figure 36 Entering a PIN Number for your SmartCard



SmartCard Login - Netscape

Netsite: http://blizzard.uk.sun.com:8181/login/SmartCardUser

Verify PIN Code

Please enter your PIN Code

PIN Code: ********

Please wait. Process is running.

- On entering the PIN and clicking <Verify> the login procedure is sent to the server. The user will be denied access and an appropriate message displayed if any of the following is true:

- No SmartCard was present in the reader

- The SmartCard PIN was entered incorrectly

- The SmartCard certificate chain is invalid

- The SmartCard certificate chain does not contain a trusted CA certificate

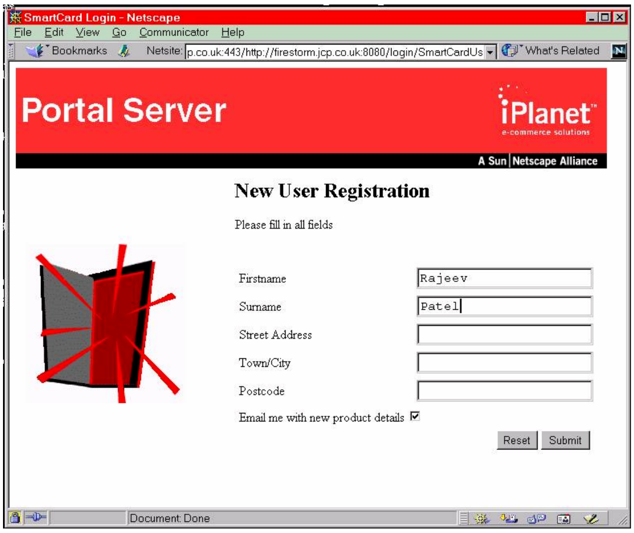
- The SmartCard certificate status is ‘unknown’ – i.e. the SmartCard was not issued under the ‘scheme’

- The SmartCard certificate status has been ‘revoked’

Note Your SmartCard third party vendor should supply your PIN number to you when they issue you with your SmartCard.

- When the user presses <Enter> on the SmartCard login page the login module will check the user's details (and verify its authenticity) and the user will then be presented with their user profile. If it’s the user’s first time entering into the system then they will be presented with the new user registration page. When this page is submitted the module will create and add the new user.

Figure 37 New User Registration



SmartCard Login - Netscape

File Edit View Go Communicator Help
Bookmarks
Netsite: p.co.uk:443/http://firestorm.jcp.co.uk:8080/login/SmartCardUs
What's Related

Portal Server

iPlanet™
e-commerce solutions
A Sun|Netscape Alliance

New User Registration

Please fill in all fields

Firstname	Rajeev
Surname	Patel
Street Address	
Town/City	
Postcode	

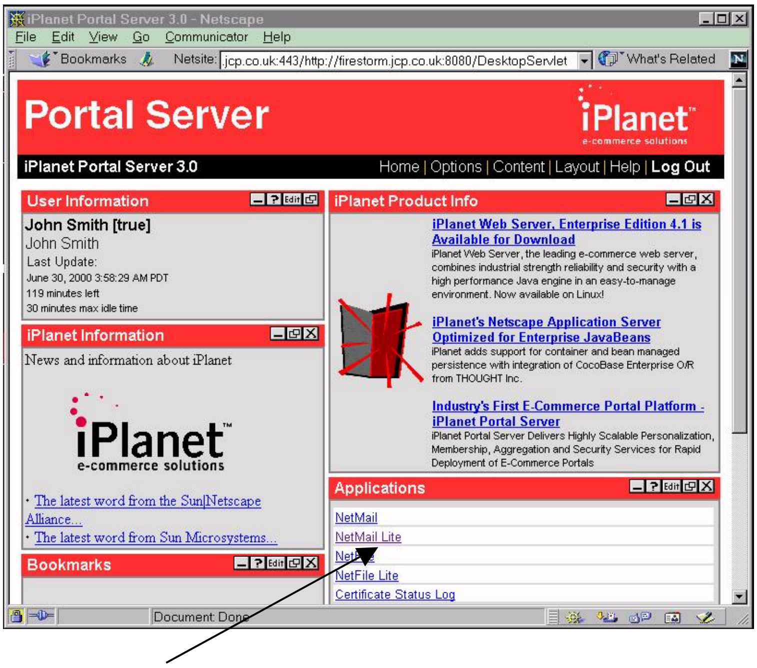
Email me with new product details ☑

Reset
Submit
Document: Done

- When you have entered your personal details select <Submit> This will then take you to the Portal Server main menu.

- The server performs Certificate Status Checks according to the security policy that your administrator has configured. Regardless of the Certificate Status Check policy in force, the validity of the signed response from the client is always verified and the signing certificate must be issued by a recognised source.

Figure 38 Portal Server Main menu Screen



iPlanet Portal Server 3.0 - Netscape

File Edit View Go Communicator Help
Bookmarks
Netsite: jcp.co.uk:443/http://firestorm.jcp.co.uk:8080/DesktopServlet
What's Related
Portal Server
iPlanet™
e-commerce solutions
iPlanet Portal Server 3.0
Home | Options | Content | Layout | Help | Log Out

User Information

John Smith [true]
John Smith
Last Update:
June 30, 2000 3:58:29 AM PDT
119 minutes left
30 minutes max idle time

iPlanet Information

News and information about iPlanet

- The latest word from the Sun|Netscape Alliance...
- The latest word from Sun Microsystems...

Bookmarks

iPlanet Product Info

iPlanet Web Server, Enterprise Edition 4.1 is Available for Download
iPlanet Web Server, the leading e-commerce web server, combines industrial strength reliability and security with a high performance Java engine in an easy-to-manage environment. Now available on Linux!

iPlanet's Netscape Application Server Optimized for Enterprise JavaBeans
iPlanet adds support for container and bean managed persistence with integration of CocoBase Enterprise O/R from THOUGHT Inc.

Industry's First E-Commerce Portal Platform - iPlanet Portal Server
iPlanet Portal Server Delivers Highly Scalable Personalization, Membership, Aggregation and Security Services for Rapid Deployment of E-Commerce Portals

Applications

NetMail
NetMail Lite
NetFile
NetFile Lite
Certificate Status Log

- Finally, select <NetMail Lite>

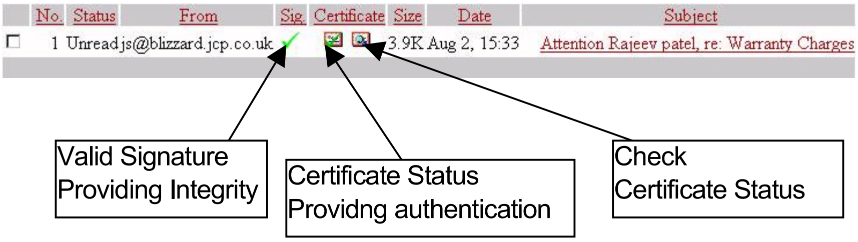
Overview of Message Verification

There are two options to verify your email messages:

- Viewing certificates that provide authentication
- Viewing signatures that provide integrity

Viewing Certificates

Figure 39 Example NetMail Lite Message Header



	No.	Status	From	Sig.	Certificate	Size	Date	Subject
□	1	Unread	js@blizzard.jcp.co.uk	✓		3.9K	Aug 2, 15:33	Attention Rajeev patel, re: Warranty Charges

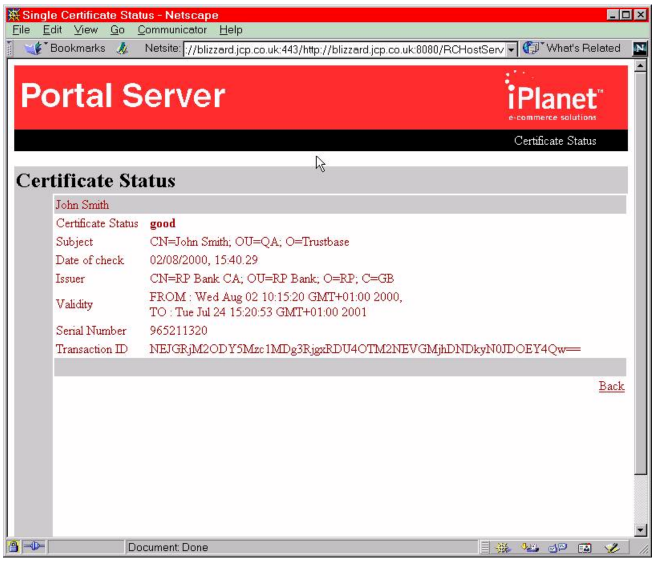
Valid Signature Providing Integrity
Certificate Status Providng authentication
Check Certificate Status

Clicking on the <certificate status> icon in any but the first two states displays a page showing the most recent status check details. If the system is configured to perform status checks automatically on receipt of messages, then the second state icon will never be displayed. This icon has five states, signifying:

- State 1. Message is not signed by a scheme certificate (blank space)
- State 2. Signing certificate has not yet been checked (blank space)
- State 3. Revoked certificate
- State 4. Verified certificate
- State 5. Unknown certificate or there was an error obtaining the status

The user may initiate a Certificate Status Check by clicking on the <check certificate> button. On clicking the button, a dialog is displayed informing the user that he is requesting a Certificate Status Check, and will be charged by his bank for this service. The user must insert his/her SmartCard and enter his/her PIN in order to confirm the request. On entering the PIN and clicking <OK>, a signed Certificate Status Check request is sent to the Portal Server. A few seconds later, on receipt of the response, a certificate status page is shown:

Figure 40 An example certificate status check


Single Certificate Status - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: ://blizzard.jcp.co.uk:443/http://blizzard.jcp.co.uk:8080/RCHostServ
What's Related
Portal Server
iPlanet™
e-commerce solutions
Certificate Status
Document: Done

Certificate Status

John Smith	
Certificate Status	**good**
Subject	CN=John Smith; OU=QA; O=Trustbase
Date of check	02/08/2000, 15:40.29
Issuer	CN=RP Bank CA; OU=RP Bank; O=RP; C=GB
Validity	FROM : Wed Aug 02 10:15:20 GMT+01:00 2000, TO : Tue Jul 24 15:20:53 GMT+01:00 2001
Serial Number	965211320
Transaction ID	NEJGRjM2ODY5Mzc1MDg3RjgxRDU4OTM2NEVGMjhDNDkyN0JDOEY4Qw==

Back

The RC host uses its response-signing certificate (configured in section RC Host Configuration on page 41) to sign the HTML source forming the displayed status information and includes the signature as base64 encoded hidden data elsewhere in the certificate status page HTML. The user may save the HTML page to his local disk to serve in case users need this information to verify for billing purposes.

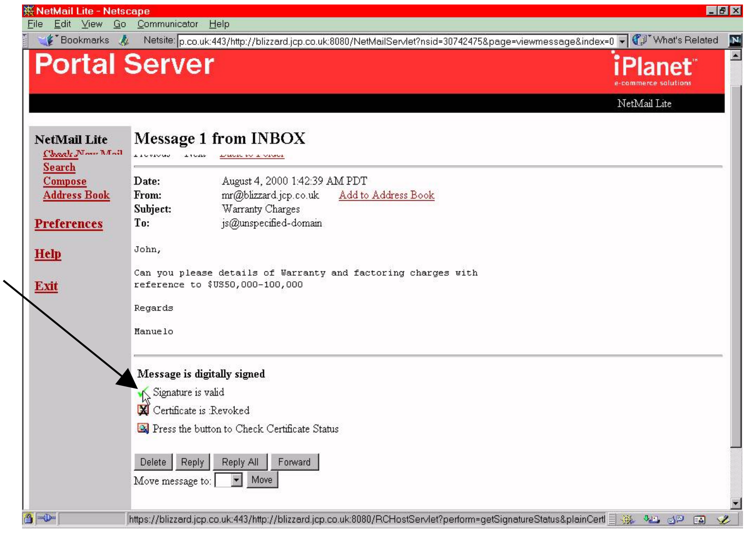
Viewing Signatures

Messages can have three states, signifying:

- State 1. Not signed (blank space)
- State 2. Invalid signature ✗
- State3. Valid signature ✓

The validity of the signature is independent of the certificate status. The signature validity icon will always appear for messages signed by a certificate belonging to the scheme. The system may be configured to optionally display the signature validity icon ✓ for messages signed by a non-scheme certificate.

Figure 41 Selecting Signature Details



Message 1 from INBOX

Date: August 4, 2000 1:42:39 AM PDT
From: mr@blizzard.jcp.co.uk Add to Address Book
Subject: Warranty Charges
To: js@unspecified-domain

```
John,

Can you please details of Warranty and factoring charges with
reference to $US50,000-100,000

Regards

Manuelo
```

Message is digitally signed

✓ Signature is valid

☒ Certificate is :Revoked

Press the button to Check Certificate Status

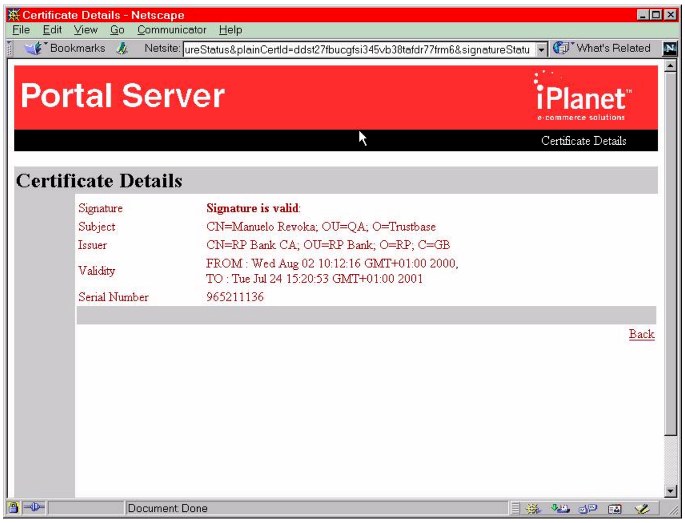
Delete
Reply
Reply All
Forward
Move message to:
Move
https://blizzard.jcp.co.uk:443/http://blizzard.jcp.co.uk:8080/RCHostServlet?perform=getSignatureStatus&plainCert

The signature details page shows details of the signature and the signing certificate. It is reached by clicking on the signature validity icon ✓ in either the message header page or the message page. On clicking on an icon ✓, the following information is displayed in the signature details Page:

- Subject. Distinguished name of the certificate holder
- Issuer. Distinguished name of the certificate issuer
- Validity. Start and end of the certificate's validity period
- Serial Number. The certificate serial number
- Signature Status. Either 'valid' or 'invalid', plus a summary of the meaning of signature status:

- Whether the contents have been altered since the message was signed
- Whether the signing certificate has expired
- Whether the signing certificate is a member of the scheme

Figure 42 Viewing a Signature


Certificate Details - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: ureStatus&plainCertId=ddst27fbucgfsi345vb38tafdr77frm6&signatureStatu
What's Related
Portal Server
iPlanet™
e-commerce solutions
Certificate Details
Document: Done

Certificate Details

Signature	**Signature is valid**:
Subject	CN=Manuelo Revoka; OU=QA; O=Trustbase
Issuer	CN=RP Bank CA; OU=RP Bank; O=RP; C=GB
Validity	FROM : Wed Aug 02 10:12:16 GMT+01:00 2000, TO : Tue Jul 24 15:20:53 GMT+01:00 2001
Serial Number	965211136

Back

Once checked certificates remain valid. If, however, the certificate expires a few days after the certificate status check has been performed the user still can perform an additional certificate status check to see whether or not the certificate status of the message still remains valid.

Email Signing Illustration

We now illustrate email messages using four users. The first three users are in possession of a valid certificate. The fourth user has a certificate that has been revoked and also tries to send a message signed outside the Identrus scheme.

- John Smith (Good certificate)
- Tom Jones (Good certificate)
- Rajeev Patel (Good certificate)
- Manuelo Revoka (Revoked certificate and sending an invalid signature)

The iPlanet Portal Server Plug-in for the Identrus System supports the following features

- Composing a signed message
- Forwarding a signed message
- Performing a certificate status request on the sender of a message
- Receiving a signed message
- Viewing the status of a signed message
- Viewing revoked certificates
- Viewing invalid signatures outside the Identrus Scheme

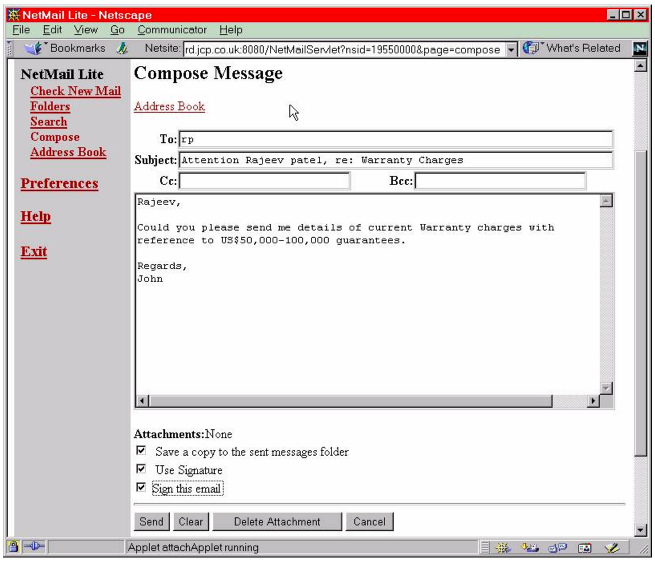
We now discuss these features in turn.

Composing a Signed Message

Messages can be sent using digital signatures allowing the recipient to attach integrity to messages.

- John Smith Logs onto NetMail Lite and sends a message to Rajeev Patel. He signs the message by selecting <sign this email>.

Figure 43 Composing a Message



Netsite: rd.jcp.co.uk:8080/NetMailServlet?nsid=19550000&page=compose

Compose Message

To: rp

Subject: Attention Rajeev patel, re: Warranty Charges

Cc:

Bcc:

```
Rajeev,

Could you please send me details of current Warranty charges with
reference to US$50,000-100,000 guarantees.

Regards,
John
```

Attachments:None

☑ Save a copy to the sent messages folder

☑ Use Signature

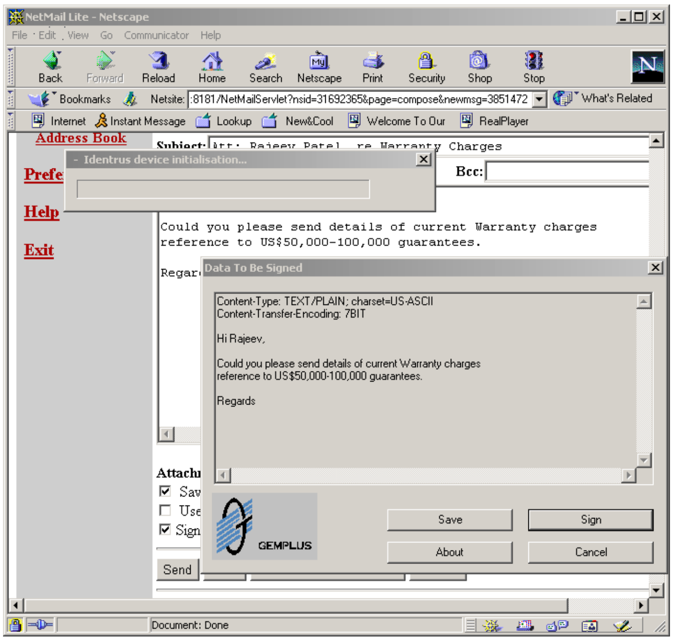
☑ Sign this email

Applet attachApplet running

- The iPlanet Portal Server Plug-in for the Identrus System, when composing a signed Message allows you to:
  - <Save a copy to the sent messages folder> i.e. Save a copy of your message
  - <Use Signature> Add some signature text at the end of your document. Select <Preferences> to establish a link to this text file.
  - <Sign this email> Digitally signing the message that has the effect of allowing its recipient to know that: the sender is who he/she says they are and that the message hasn't changed.

- Having sent the message, the system asks you to verify how you wish the message to be signed. Select <sign > and as before enter your SmartCard PIN Number. Make sure your SmartCard has been entered into your SmartCard Reader.

Figure 44 Digitally signing a Message



Netsite: :8181/NetMailServlet?nsid=31692365&page=compose&newmsg=3851472

Subject: Att: Rajeev Patel re Warranty Charges

Bcc:

Could you please send details of current Warranty charges reference to US$50,000-100,000 guarantees.

Regar

Content-Type: TEXT/PLAIN; charset=US-ASCII
Content-Transfer-Encoding: 7BIT

Hi Rajeev,

Could you please send details of current Warranty charges reference to US$50,000-100,000 guarantees.

Regards

☑ Sav
□ Use
☑ Sign

Receiving a Signed Message

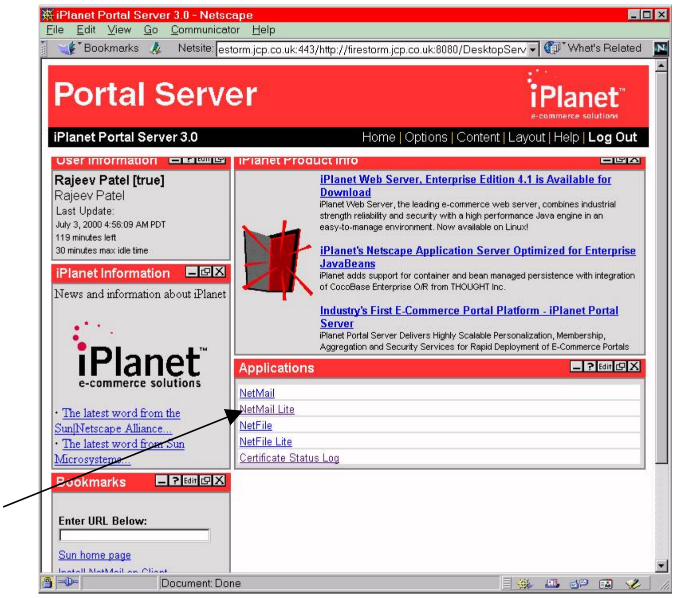
Message Headers illustrate which messages have been digitally signed and also those that require a Certificate Status Check should you wish to validate the sender of the message. There are two main aspects to this:

- The recipient of the message can verify who the sender is. Clicking on this icon requests the system to perform a Certificate Status Check. This feature can be set automatically (Consult your administrator).

- The recipient of the message can know whether or not what is being said in a message is valid and has not changed. Under such circumstances, the signature icon will appear as a tick ✓

- Rajeev Patel logs into NetMail Lite to read his email.

Figure 45 User Rajeev Patel's Portal Homepage


iPlanet Portal Server 3.0 - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: estorm.jcp.co.uk:443/http://firestorm.jcp.co.uk:8080/DesktopServ
What's Related
Portal Server
iPlanet™ e-commerce solutions
iPlanet Portal Server 3.0
Home | Options | Content | Layout | Help | Log Out
User Information
iPlanet Product Info
iPlanet Information
Applications
Bookmarks
Edit
Document: Done

Rajeev Patel [true]
Rajeev Patel
Last Update:
July 3, 2000 4:56:09 AM PDT
119 minutes left
30 minutes max idle time

News and information about iPlanet

- The latest word from the Sun|Netscape Alliance...
- The latest word from Sun Microsystems...

iPlanet Web Server, Enterprise Edition 4.1 is Available for Download
iPlanet Web Server, the leading e-commerce web server, combines industrial strength reliability and security with a high performance Java engine in an easy-to-manage environment. Now available on Linux!

iPlanet's Netscape Application Server Optimized for Enterprise JavaBeans
iPlanet adds support for container and bean managed persistence with integration of CocoBase Enterprise O/R from THOUGHT Inc.

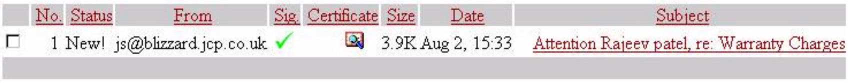
Industry's First E-Commerce Portal Platform - iPlanet Portal Server
iPlanet Portal Server Delivers Highly Scalable Personalization, Membership, Aggregation and Security Services for Rapid Deployment of E-Commerce Portals

NetMail
NetMail Lite
NetFile
NetFile Lite
Certificate Status Log

Enter URL Below:
Sun home page
Install NetMail on Client

- Rajeev Patel views the message header from John Smith.

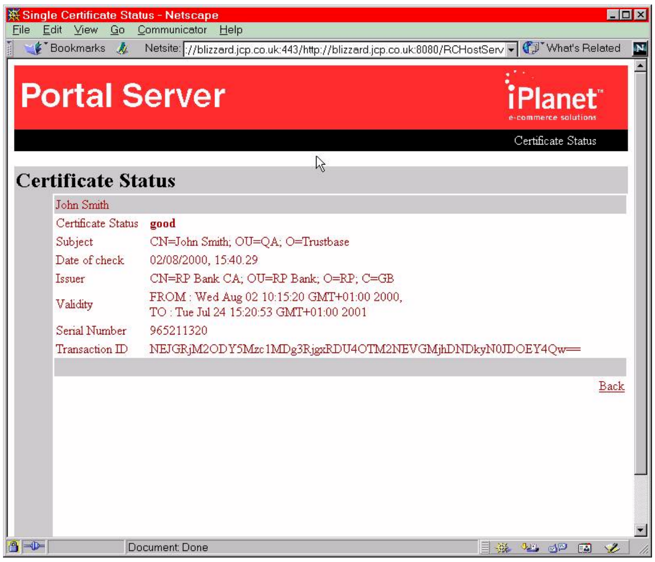
Figure 46 Rajeev Patel's message NetMail Lite Message Headers



	No.	Status	From	Sig.	Certificate	Size	Date	Subject
□	1	New!	js@blizzard.jcp.co.uk	✓	🔍	3.9K	Aug 2, 15:33	Attention Rajeev patel, re: Warranty Charges

- Selecting the <Check Certificate> icon , determines whether or not John Smith's certificate is good or has been revoked:

Figure 47 Certificate Status Check on John Smith



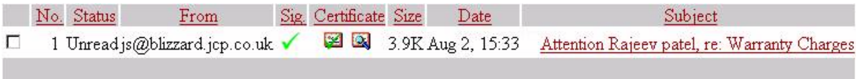
Single Certificate Status - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: ://blizzard.jcp.co.uk:443/http://blizzard.jcp.co.uk:8080/RCHostServ
What's Related
Portal Server
iPlanet™
e-commerce solutions
Certificate Status
Back
Document: Done

Certificate Status

John Smith	
Certificate Status	**good**
Subject	CN=John Smith; OU=QA; O=Trustbase
Date of check	02/08/2000, 15:40.29
Issuer	CN=RP Bank CA; OU=RP Bank; O=RP; C=GB
Validity	FROM : Wed Aug 02 10:15:20 GMT+01:00 2000, TO : Tue Jul 24 15:20:53 GMT+01:00 2001
Serial Number	965211320
Transaction ID	NEJGRjM2ODY5Mzc1MDg3RjgxRDU4OTM2NEVGMjhDNDkyN0JDOEY4Qw==

- On completion of a Certificate Status Check a certificate Icon appears in the message header as illustrated below:

Figure 48 Rajeev Patel's Message Headers illustrating a Manual Certificate Status Check



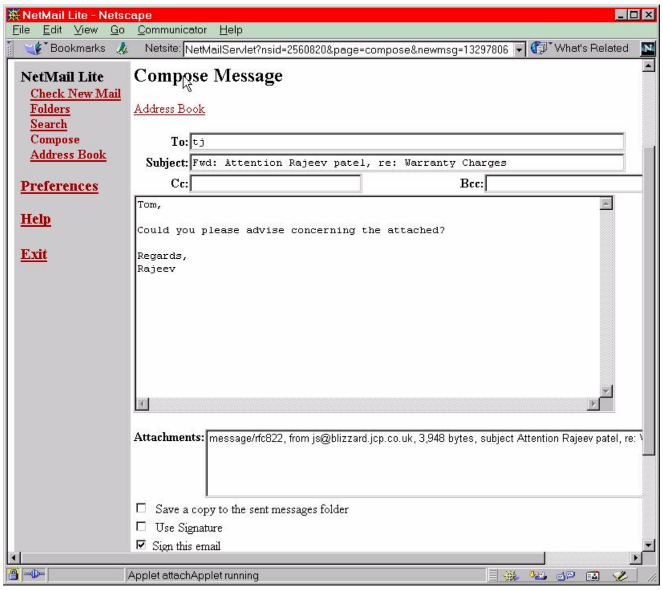
	No.	Status	From	Sig.	Certificate	Size	Date	Subject
□	1	Unread	js@blizzard.jcp.co.uk	✓		3.9K	Aug 2, 15:33	Attention Rajeev patel, re: Warranty Charges

Forwarding a Signed Message

Forwarding messages are also possible indicating the status of a message; whether it be signed or have its certificate status checked. Under such circumstances, it is up to the user to interpret situations involving some but not all of the hierarchy of forwarded messages that may or may not have unsigned signatures or revoked certificates. There is no limit to the number of forwarded embedded messages allowed.

- Rajeev Patel forwards the message to Tom Jones for further clarification.

Figure 49 Forwarding a message


NetMail Lite - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: NetMailServlet?nsid=2560820&page=compose&newmsg=13297806
What's Related
NetMail Lite
Check New Mail
Folders
Search
Compose
Address Book
Preferences
Help
Exit
Applet attachApplet running

Compose Message

Address Book

To: tj

Subject: Fwd: Attention Rajeev patel, re: Warranty Charges

Cc:

Bcc:

```
Tom,

Could you please advise concerning the attached?

Regards,
Rajeev
```

Attachments: message/rfc822, from js@blizzard.jcp.co.uk, 3,948 bytes, subject Attention Rajeev patel, re: W

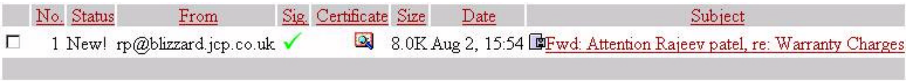
☐ Save a copy to the sent messages folder

☐ Use Signature

☑ Sign this email

- Tom Jones Logs into NetMail Lite to view his messages

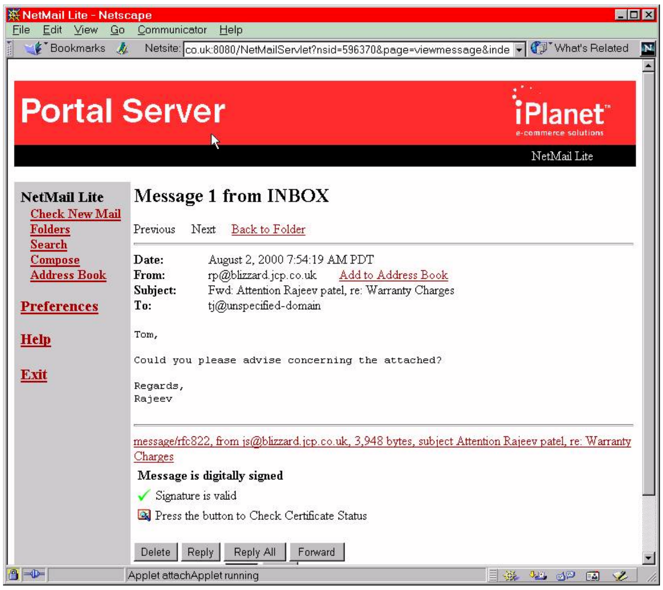
Figure 50 Message headers for Tom Jones



	No.	Status	From	Sig	Certificate	Size	Date	Subject
☐	1	New!	rp@blizzard.jcp.co.uk	✓		8.0K	Aug 2, 15:54	Fwd: Attention Rajeev patel, re: Warranty Charges

On receiving a forwarded message the user simply clicks on the forwarded attachment to see whether or not the forwarded message was digitally signed.

Figure 51 A forwarded Message



Message 1 from INBOX

Date: August 2, 2000 7:54:19 AM PDT
From: rp@blizzard.jcp.co.uk
Subject: Fwd: Attention Rajeev patel, re: Warranty Charges
To: tj@unspecified-domain

```
Tom,

Could you please advise concerning the attached?

Regards,
Rajeev
```

message/rfc822, from js@blizzard.jcp.co.uk, 3,948 bytes, subject Attention Rajeev patel, re: Warranty Charges

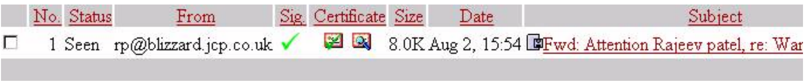
Message is digitally signed

✓ Signature is valid

Press the button to Check Certificate Status

- Select <Check New Mail> and the Certificate checked icon appears.

Figure 52 Certificate status check performed on Forwarded message



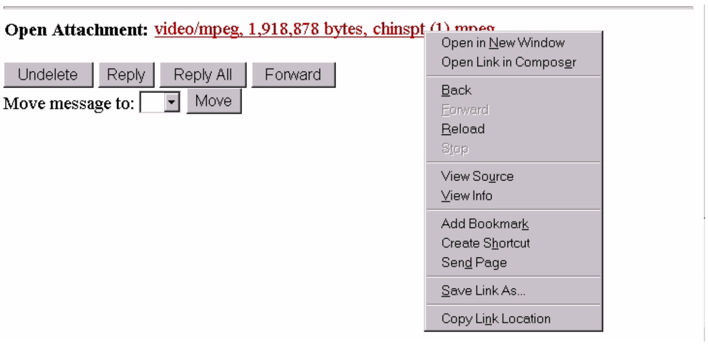
	No.	Status	From	Sig.	Certificate	Size	Date	Subject
☐	1	Seen	rp@blizzard.jcp.co.uk	✓		8.0K	Aug 2, 15:54	Fwd: Attention Rajeev patel, re: War

Forwarding messages can be useful when you need to provide non-repudiable evidence that a message instruction took place. Forwarding the message to an independent party that is part of the Identrus network achieves such an aim. If, on opening the message, the certificate status has been revoked then it would be necessary to go back to when the original certificate status was made. This can be done, by viewing the certificate status log, or if necessary the user can save the certificate status log view as an HTML file locally.

Saving an Attachment

This can be achieved by highlighting the link. <right-click> link and selecting <Save Link as> as illustrated below:

Figure 53 Saving an Attachment



Open Attachment: video/mpeg, 1,918,878 bytes, chinspt (1).mpeg

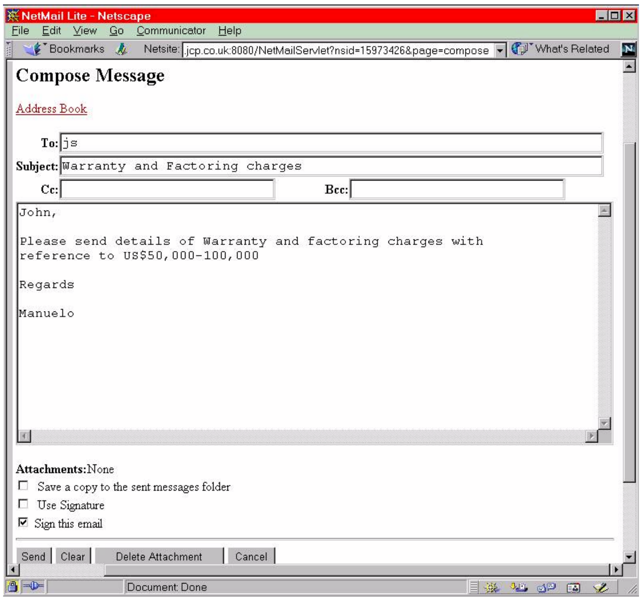
Move message to:

Revoked Messages

In certain circumstances, employees leave companies or certificates that were once valid in the past may expire or be revoked.

- Manuelo Revoka Logs onto NetMail Lite to send a message to John Smith using a revoked certificate.

Figure 54 Sending an email message using a revoked certificate



Compose Message

To: js

Subject: Warranty and Factoring charges

Cc:

Bcc:

```
John,

Please send details of Warranty and factoring charges with
reference to US$50,000-100,000

Regards

Manuelo
```

Attachments:None

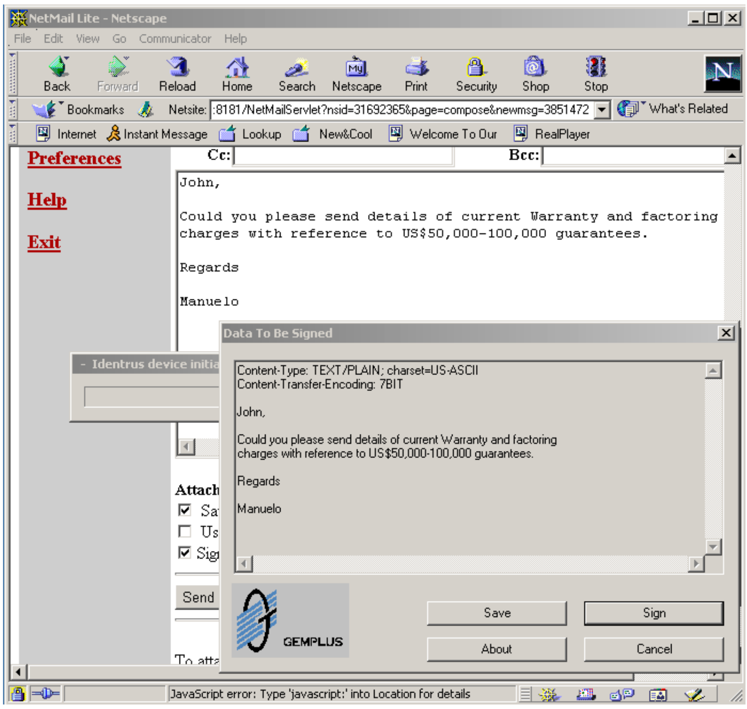
☐ Save a copy to the sent messages folder

☐ Use Signature

☑ Sign this email

- He signs the message with his revoked certificate

Figure 55 Signing a message with a revoked certificate



Netsite: :8181/NetMailServlet?nsid=31692365&page=compose&newmsg=3851472

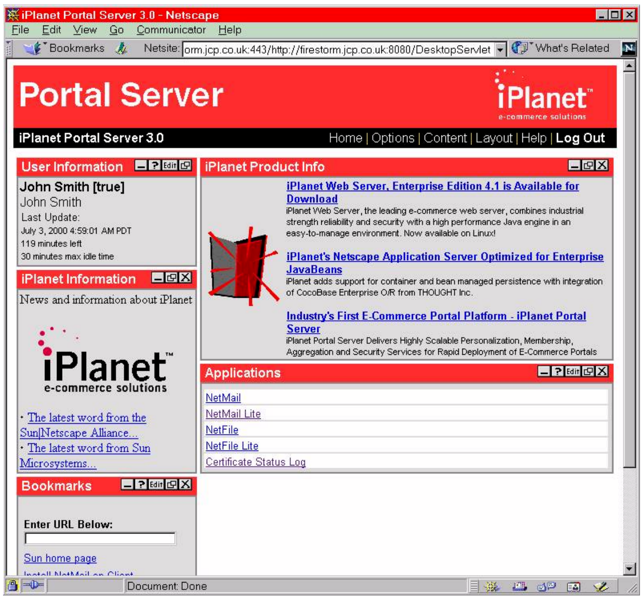
```
John,

Could you please send details of current Warranty and factoring
charges with reference to US$50,000-100,000 guarantees.

Regards

Manuelo
```

```
Content-Type: TEXT/PLAIN; charset=US-ASCII
Content-Transfer-Encoding: 7BIT

John,

Could you please send details of current Warranty and factoring
charges with reference to US$50,000-100,000 guarantees.

Regards

Manuelo
```

JavaScript error: Type 'javascript:' into Location for details

- John Smith Logs onto NetMail Lite to check his email.

Figure 56 John Smith's Portal User Screen



Netsite: orm.jcp.co.uk:443/http://firestorm.jcp.co.uk:8080/DesktopServlet

John Smith [true]
John Smith
Last Update:
July 3, 2000 4:59:01 AM PDT
119 minutes left
30 minutes max idle time

News and information about iPlanet

- The latest word from the Sun|Netscape Alliance...
- The latest word from Sun Microsystems...

Enter URL Below:

Sun home page

Install NetMail on Client

iPlanet Web Server, Enterprise Edition 4.1 is Available for Download
iPlanet Web Server, the leading e-commerce web server, combines industrial strength reliability and security with a high performance Java engine in an easy-to-manage environment. Now available on Linux!

iPlanet's Netscape Application Server Optimized for Enterprise JavaBeans
iPlanet adds support for container and bean managed persistence with integration of CocoBase Enterprise O/R from THOUGHT Inc.

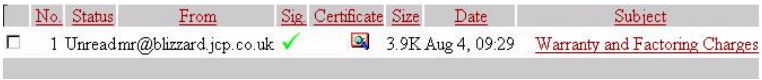
Industry's First E-Commerce Portal Platform - iPlanet Portal Server
iPlanet Portal Server Delivers Highly Scalable Personalization, Membership, Aggregation and Security Services for Rapid Deployment of E-Commerce Portals

NetMail
NetMail Lite
NetFile
NetFile Lite
Certificate Status Log

Document: Done

- John Smith checks his Mail to see the message from Manuela Revoka

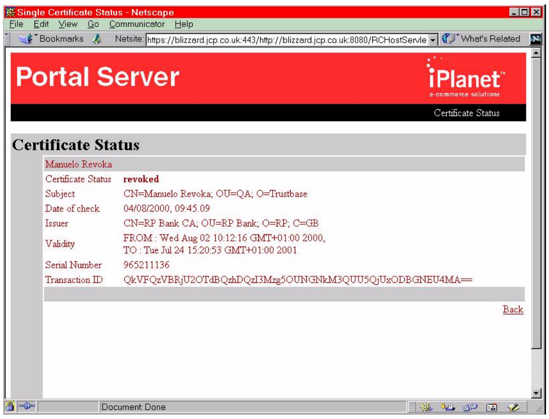
Figure 57 John Smith's Message Header



	No.	Status	From	Sig.	Certificate	Size	Date	Subject
☐	1	Unread	mr@blizzard.jcp.co.uk	✓	🔍	3.9K	Aug 4, 09:29	Warranty and Factoring Charges

- He performs a Manual Certificate Status Check by clicking on the <check certificate> icon 🔍.

Figure 58 Message Header Details containing a revoked Certificate



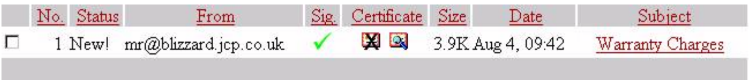
Single Certificate Status - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: https://blizzard.jcp.co.uk:443/http://blizzard.jcp.co.uk:8080/RCHostServle
What's Related
Portal Server
iPlanet™
e-commerce solutions
Certificate Status

Certificate Status

Manuelo Revoka	
Certificate Status	**revoked**
Subject	CN=Manuelo Revoka; OU=QA; O=Trustbase
Date of check	04/08/2000, 09:45.09
Issuer	CN=RP Bank CA; OU=RP Bank; O=RP; C=GB
Validity	FROM : Wed Aug 02 10:12:16 GMT+01:00 2000, TO : Tue Jul 24 15:20:53 GMT+01:00 2001
Serial Number	965211136
Transaction ID	QkVFQzVBRjU2OTdBQzhDQzI3Mzg5OUNGNkM3QUU5QjUxODBGNEU4MA==

- The certificate icon ☒ indicates that it has been revoked. The text of the message and its sender, however, still has integrity.

Figure 59 Message Header Overview containing a revoked certificate



	No.	Status	From	Sig.	Certificate	Size	Date	Subject
☐	1	New!	mr@blizzard.jcp.co.uk	✓	☒ 🔍	3.9K	Aug 4, 09:42	Warranty Charges

Invalid Signatures

Invalid signatures can occur for a number of reasons:

- The signature is outside the Certificate Scheme that your Administrator has configured for you. This is normally The Identrus Scheme. If you have any doubts you should refer this to your Administrator

- Somebody has tampered with the message. In this case somebody has managed to hack into the system and change the contents of your message. This is highly unlikely and as such you should report this to your Systems administrator immediately.

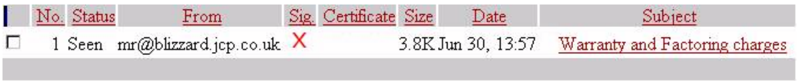
- The certificate of the signature has expired. Under such circumstance you should request that the sender renew his/her signing certificate and transmit the message again.

- The email address of the sender must be the same as the subject of the certificate. This is intuitively obvious but can occur if the sender tries to sign a message with the certificate of somebody else within the certificate scheme.

Invalid Signature Example

- Manuelo Revoka sends a message to Tom Jones and signs it with a certificate that is outside the certificate scheme

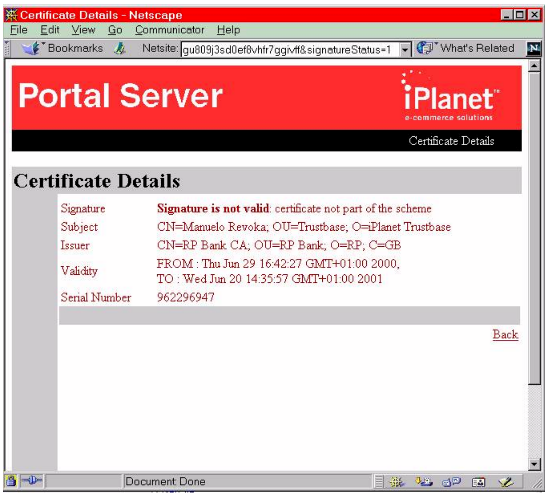
Figure 60 Example Invalid Digital Signature in Message Header



	No.	Status	From	Sig.	Certificate	Size	Date	Subject
□	1	Seen	mr@blizzard.jcp.co.uk	✗		3.8K	Jun 30, 13:57	Warranty and Factoring charges

- Tom Jones selects the icon ✗ to view why the Signature is invalid.

Figure 61 Invalid Signature Details



Certificate Details - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: gu809j3sd0ef8vhfr7ggivff&signatureStatus=1
What's Related
Portal Server
iPlanet™
e-commerce solutions
Certificate Details

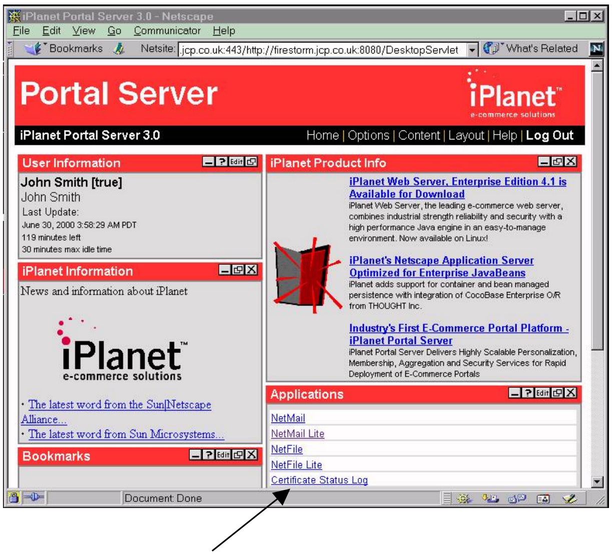
Certificate Details

Signature	**Signature is not valid**: certificate not part of the scheme
Subject	CN=Manuelo Revoka; OU=Trustbase; O=iPlanet Trustbase
Issuer	CN=RP Bank CA; OU=RP Bank; O=RP; C=GB
Validity	FROM : Thu Jun 29 16:42:27 GMT+01:00 2000, TO : Wed Jun 20 14:35:57 GMT+01:00 2001
Serial Number	962296947

Certificate Status Log

The user will be able to view a log of all of the certificate status checks he has made. This log is accessible from a link in the ‘Applications’ list on the main iPlanet Portal Server page (see Figure 62 below). Clicking on the link <Certificate Status Log> causes the log page to appear in a new browser window.

Figure 62 Main iPlanet Portal Server Page



jcp.co.uk:443/http://firestorm.jcp.co.uk:8080/DesktopServlet

John Smith [true]
John Smith
Last Update:
June 30, 2000 3:58:29 AM PDT
119 minutes left
30 minutes max idle time

News and information about iPlanet

- The latest word from the Sun|Netscape Alliance...
- The latest word from Sun Microsystems...

iPlanet Web Server, Enterprise Edition 4.1 is Available for Download
iPlanet Web Server, the leading e-commerce web server, combines industrial strength reliability and security with a high performance Java engine in an easy-to-manage environment. Now available on Linux!

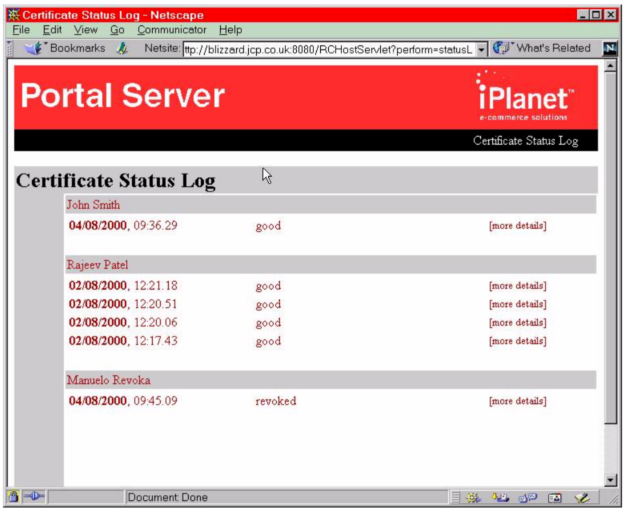
iPlanet's Netscape Application Server Optimized for Enterprise JavaBeans
iPlanet adds support for container and bean managed persistence with integration of CocoBase Enterprise O/R from THOUGHT Inc.

Industry's First E-Commerce Portal Platform - iPlanet Portal Server
iPlanet Portal Server Delivers Highly Scalable Personalization, Membership, Aggregation and Security Services for Rapid Deployment of E-Commerce Portals

NetMail
NetMail Lite
NetFile
NetFile Lite
Certificate Status Log

This page shows the list of Certificate Status Checks performed by a user, ordered by time, the most recent first.

Figure 63 Certificate Status Log


Certificate Status Log - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: ttp://blizzard.jcp.co.uk:8080/RCHostServlet?perform=statusL
What's Related
Portal Server
iPlanet™
e-commerce solutions
Certificate Status Log
Document: Done

Certificate Status Log

John Smith

04/08/2000, 09:36.29	good	[more details]

Rajeev Patel

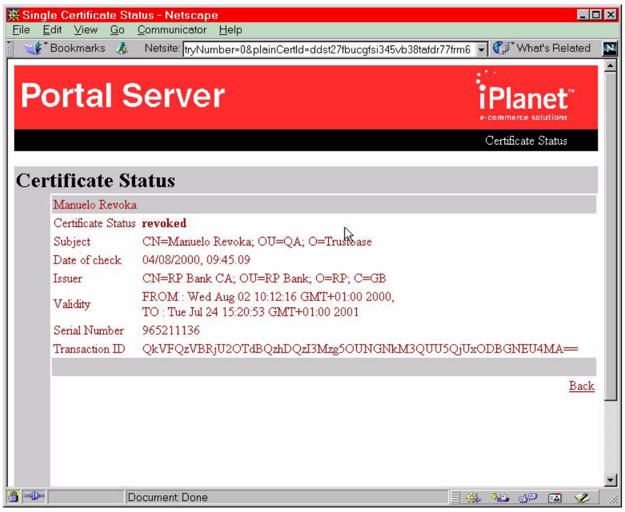
02/08/2000, 12:21.18	good	[more details]
02/08/2000, 12:20.51	good	[more details]
02/08/2000, 12:20.06	good	[more details]
02/08/2000, 12:17.43	good	[more details]

Manuelo Revoka

04/08/2000, 09:45.09	revoked	[more details]

- The following data is shown for each entry:
  - Subject. Common name of the certificate holder
  - Certificate Status. Result of Certificate Status Check – one of “Good”, “Revoked” or “Unknown”
  - Date of Check. Time and date of the Certificate Status Check
- The user (in this case John Smith) may click on <[more details]> to access the certificate status page for that entry.

Figure 64 Certificate Status Details


Single Certificate Status - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: tryNumber=0&plainCertId=ddst27fbucgfsi345vb38tafdr77frm6
What's Related
Portal Server
iPlanet™
e-commerce solutions
Certificate Status
Back
Document: Done

Certificate Status

Manuelo Revoka

Certificate Status	**revoked**
Subject	CN=Manuelo Revoka; OU=QA; O=Trustbase
Date of check	04/08/2000, 09:45.09
Issuer	CN=RP Bank CA; OU=RP Bank; O=RP; C=GB
Validity	FROM : Wed Aug 02 10:12:16 GMT+01:00 2000, TO : Tue Jul 24 15:20:53 GMT+01:00 2001
Serial Number	965211136
Transaction ID	QkVFQzVBRjU2OTdBQzhDQzI3Mzg5OUNGNkM3QUU5QjUxODBGNEU4MA==

Chapter 5

Deploying Applications

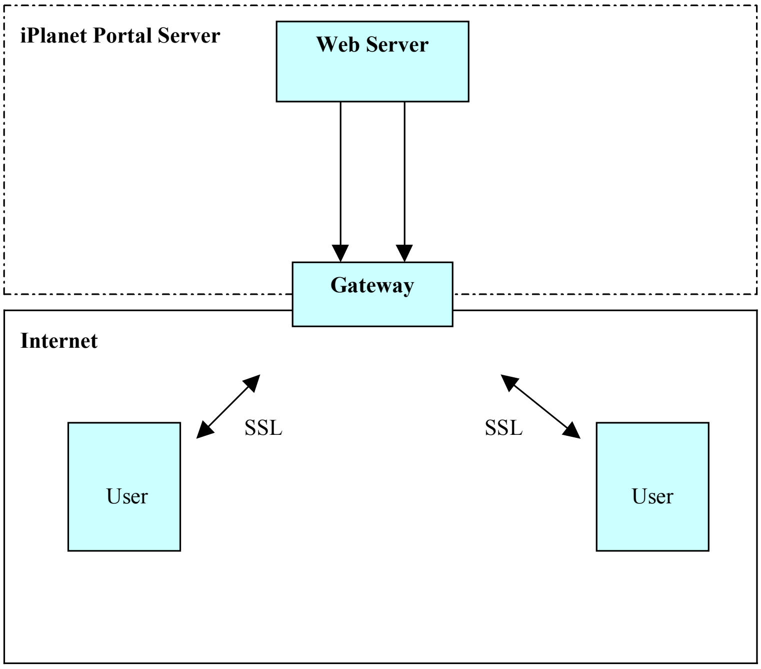
Developing the iPlanet Portal Server Plug-in for the Identrus System involves understanding how to perform a Certificate Status check using the Identrus enabled four corner model. The objectives of this chapter are to cover:

- How to set up a Development Environment
- How to start and stop the Portal Server
- The interface packages X509Certificate, CertStatusChecker, CertID and CertMapStore
- How to compile and run the source sampleCSC.java code supplied

Introduction

IPlanet Portal Server Plug-in for the Identrus System comes with an API and a Sample Java Source code designed to help you integrate your own applications within the Portal Server that are Identrus enabled.

Figure 65 Portal Server Hardware Overview



Normally the portal is deployed over a server and gateway and as such Java needs to be installed on both these machines. In order to assimilate this environment the following procedure must be adopted.

Installing the Development Environment

Sample Source code and API

The source code, that illustrates how Identrus enabled applications might be deployed, can be found in the following directory:

```
<portal_install_directory>/SUNWpin/sample/src/com/iplanet/sample/Samp
leCSC.java
```

The API suitable for deploying applications that are Identrus enabled can be found in the following directory:

```
<portal_install_directory>/SUNWpin/apidocs/helper/index.html
<portal_install_directory>/SUNWpin/apidocs/plugin/index.html
```

The API covering Java Security can be found within the Java 2 documentation at the following websites

```
http://java.sun.com/j2se/1.3/docs/api/
http://java.sun.com/security/JCE1.2/spec/apidoc/
```

The HTML source screens can be found on:

```
<portal_install_directory>SUNWips/public_html
```

The API package com.iplanet.portalserver can be found in

```
<portal_install_directory>/SUNWips/public_html/docs/en_US/javadocs/co
m/iplanet/portalserver
```

Information about how to deploy the Portal API package `com.iplanet.portalserver` can be found in

```
http://docs.iplanet.com/docs/manuals/portal/30/progref/
```

Creating two Java virtual machines

Download JDK from the website and put in a temporary directory in for instance /app

```
http://java.sun.com
```

Copy into an appropriate directory as follows:

```
cd/app
mkdir java1.2.2_06
cp -r java1.2/* java1.2.2_06/
```

Starting the Portal Server

The following Script illustrates how to start the portal server

```
#!/bin/sh
LD_LIBRARY_PATH=/app/SUNWips/lib
export LD_LIBRARY_PATH
/app/SUNWips/bin/ipsserver start debug > ipsserver.out
JAVA_HOME=/app/java1.2.2_06
export JAVA_HOME
/app/SUNWips/bin/ipsgateway start
tail -f ipsserver.out
```

Stopping the Portal Server

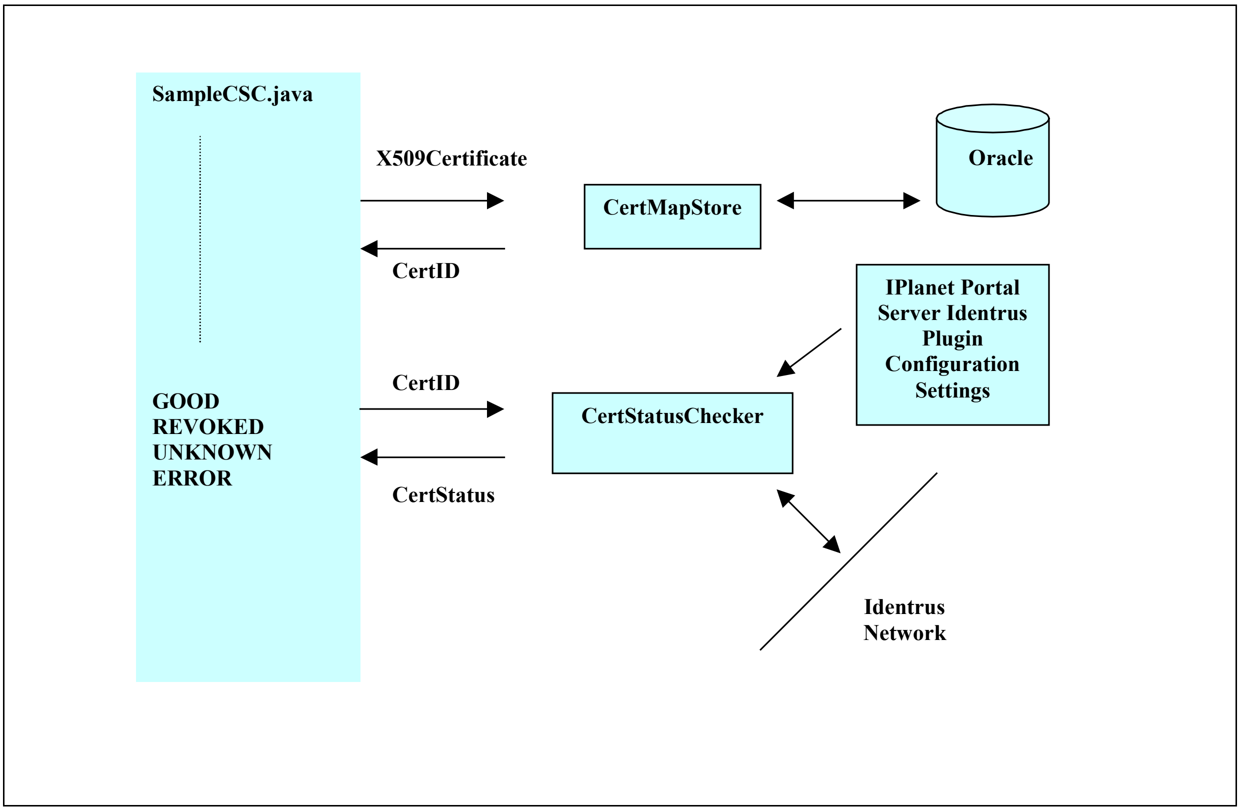
The following Script illustrates how to stop the Portal Server:

```
/app/SUNWips/bin/ipsserver stop
/app/SUNWips/bin/ipsgateway stop
```

Certificate Status Check

Performing a Certificate Status Check involves the following interface packages

Figure 66 Performing a CSC using the interface packages



Performing a CSC Check

The CertStatusChecker provides the means to get the status for a given CertID. This is deployed using checkStatus(CertID). From the properties object returned you can retrieve : The Request Time, Certificate Status, Response Status and Transaction ID . Calling .checkStatus(CertID) will cause a certificate status check using the certificate id presented. For this to be successful the responder URL, and the signing certificate will need to have been correctly set-up, within portal server. This is done via the admin server typically on http://127.0.0.1:8080/console. The following configuration settings must be made

- CSC Configuration Request Signing Certificate, Response Signing Certificate and Trusted Response Verification Certificates
- RC Host
- RC Settings : The Responder Type, The URL of the Responder and The OCSP Requestor Name
- Organisation Details : Organisation ID, Legal Name, Short Name, The URL of the logo, Postal Address and Contact Informtaion

The following code fragment illustrates this:

```
   CertStatusChecker statusChecker =
SingletonCertStatusChecker.getChecker( mySessionID );
    Properties certProps = statusChecker.checkStatus( myCertID );
    //Get the Certificate Status
   String certStatus = certProps.getProperty(
CertStatusChecker.CERT_STATUS );
      if (certStatus.equals ( CertStatusChecker.GOOD ) )
   {System.out.println("Certificate is trusted.");}
   else if (certStatus.equals ( CertStatusChecker.REVOKED ) )
   {System.out.println("Certificate has been revoked.");}
   else if (certStatus.equals ( CertStatusChecker.UNKNOWN ) )
   {System.out.println("The certificate status is not known by the
CSC.");}
   else if (certStatus.equals ( CertStatusChecker.ERROR ) )
   {System.out.println("There was an error getting the certificate
status.");}
    //Get request time
   String requestTime = certProps.getProperty(
CertStatusChecker.REQUEST_TIME );
    System.out.println("The request was made at" + requestTime);
    //Get response status
   // The response code is used to provide more detail of an error if
the cert status was ERROR.
   String requestStatus = certProps.getProperty(
CertStatusChecker.RESPONSE_STATUS );
    System.out.println("The request status is " + requestStatus);
    //Get Transaction ID
   String transID = certProps.getProperty( CertStatusChecker.TX_ID );
    System.out.println("The transaction ID is " + transID);
```

Note Developers should consult:
<portal_install_directory>/SUNWpin/apidocs/com/iplanet/portalserver/identrus/statuscheck/CertStatusChecker.html
Configuration settings are described in the Administrator Chapter 3

Mapping the Certificate Store

CertMapStore's are used to access Certificates and CertIDs. CertIDs are used by the Portal Server CSC libraries to identify certificates which are present within the CertMapStore. The following fragment illustrates how it might typically be used:

```
 CertMapStore certStore =
SingletonStatusStoreRegistry.getCertMapStore( mySessionID );

 //Example 1 : a single certificate, may-be presented as base64

 X509Certificate aPKCS7Cert = convertSomePKCS7DataFromSomeSource (
pkcs7data ) ;

 CertID certID = certStore.getCertID ( aPKCS7Cert ) ;

 performCSCCode ( certID ); //see CertStatusChecker for more details
```

Note Details of how to access X509Certificate can be found at http://java.sun.com/j2se/1.3/docs/api/java/security/cert/X509Certificate.html

Details about the interface CertMapStore can be found at <portal_install_directory>/SUNWpin/apidocs/com/iplanet/portalserver/identrus/statuscheck/CertMapStore.html

Compiling the sample program

All the libraries needed to develop CSC applications can be found in:

```
<Portal_install_directory>/SUNWips/lib
```

This directory includes all portal server libraries as well as all the Plugin libraries. The following script illustrates how to run and compile the sample program, from MSDOS:

```
cd <Portal_install_directory>/SUNWips/lib
set
CLASSPATH=sample.jar:activation.jar:asn1.jar:config.jar:ipspin.jar:ds
ms.jar:jndi.jar:jaas.jar:jss21.jar:ldapbp.jar:jsskeystore.jar:ldapfil
t.jar:ldap.jar:ocsp.jar:ldapjdk_debug.jar:mail.jar:servlet.jar:pkcs.j
ar:tbmail.jar:providerutil.jar:tbutil.jar:ssl.jar:x509v1.jar:tokenkey
store.jar:country.zip:xml.jar:identrus_update.zip:xml4j.jar:utiloverr
ide.zip:identrus.zip:oracle-jdbc-815.zip:
 tbextlibrary.zip: tblibrary.zip: ips_services.jar: trustbase.zip
export CLASSPATH
javac
<Portal_install_directory>/SUNWpin/sample/src/com/iplanet/sample/Samp
leCSC.java
cd <Portal_install_directory>/SUNWpin/sample/src
jar cvf <Portal_install_directory>/SUNWpin/sample/src
/com/iplanet/sample/sample.jar com/iplanet/sample/SampleCSC.class
```

Once the program has been compiled and loaded into the jar file sample.jar it must be copied into the jar directory where the portal server was installed:

```
<portal_install_directory>/SUNWips/lib/sample.jar
```

Running the sample program

In order to run the program the following conditions must be met

- The CSC must be setup, see earlier chapter on administration

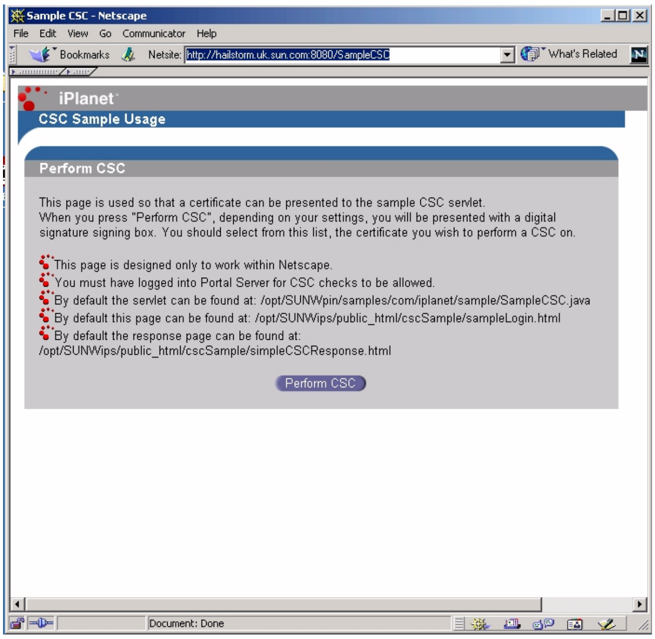
- The user must be logged in either as a SmartCard User or from the Administration console.

To run the sample program, type the following:

```
http://hailstorm.uk.sun.com:8080/SampleCSC
```

The following screen should appear:

Figure 67 Sample Certificate Status Check Main Screen


Sample CSC - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: http://hailstorm.uk.sun.com:8080/SampleCSC
What's Related
iPlanet
Document: Done

CSC Sample Usage

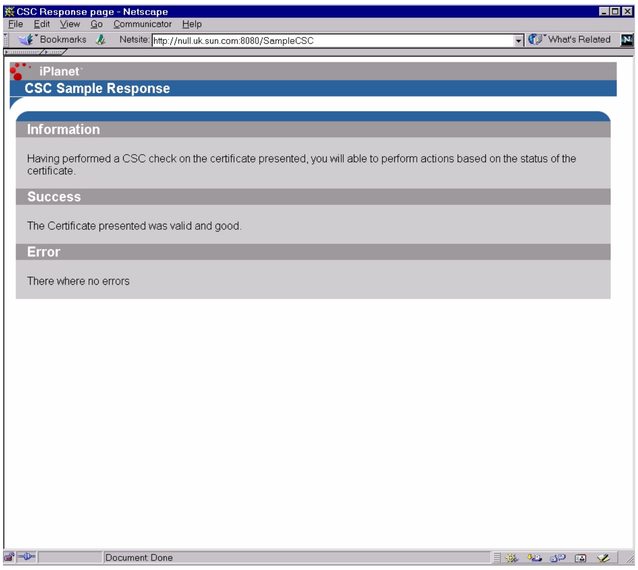
Perform CSC

This page is used so that a certificate can be presented to the sample CSC servlet. When you press "Perform CSC", depending on your settings, you will be presented with a digital signature signing box. You should select from this list, the certificate you wish to perform a CSC on.

This page is designed only to work within Netscape.
You must have logged into Portal Server for CSC checks to be allowed.
By default the servlet can be found at: /opt/SUNWpin/samples/com/iplanet/sample/SampleCSC.java
By default this page can be found at: /opt/SUNWips/public_html/cscSample/sampleLogin.html
By default the response page can be found at: /opt/SUNWips/public_html/cscSample/simpleCSCResponse.html

- Select <Perform CSC> and the following output should appear:

Figure 68 Sample Certificate Status Check Output


CSC Response page - Netscape
File Edit View Go Communicator Help
Bookmarks
Netsite: http://null.uk.sun.com:8080/SampleCSC
What's Related
iPlanet
Document: Done

CSC Sample Response

Information

Having performed a CSC check on the certificate presented, you will able to perform actions based on the status of the certificate.

Success

The Certificate presented was valid and good.

Error

There where no errors

Chapter 6

Glossary and References

The objectives of this chapter are to cover

- Software Platform
- Protocol
- Glossary

Software Platform

Java Development Kit 1.2.1

http://java.sun.com/products/jdk/

Java

http://www.javasoft.com

Java interface

http://java.sun.com/products/jndi/index.html

Host iPlanet Portal Server 3.0

http://www.iplanet.com/products/infrastructure/portal/index.html

Hardware Security nCipher KeySafe 1.0 and CAFast

http://www.ncipher.com

Oracle 8I

http://www.oracle.com

GemSAFE IS SmartCard tool

http://www.gemplus.com

Protocol

S/MIME Version 1

http://www.ietf.org/rfc.html (see RFC2045, 2046, 2047, 2048 and 2049)

http://www.imc.org/ietf-smime

http://www.ietf.org/rfc/rfc2311.txt

OCSP

http://www.imc.org/ietf-pkix/

http://www.ietf.org/rfc/rfc2560.txt

IMAP

http://www.cis.ohio-state.edu/htbin/rfc/rfc1730.html
http://www.cis.ohio-state.edu/htbin/rfc/rfc2060.html

SMTP

http://www.imc.org/ietf-smtp/

http://www.cis.ohio-state.edu/htbin/rfc/rfc2156.html

ftp://ftp.isi.edu/in-notes/rfc821.txt client protocol specified in RFC 821 and RFC 822

SmartCard Standard

http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-11.html

Certificate requests and responses

PKCS10 requests RFC2314 can be found in http://www.ietf.org/rfc.html

PKCS7 responses RFC2315 can be found in http://www.ietf.org/rfc.html

HTML

HTML 3.2 as specified in http://www.w3.org/TR/REC-html32.html

HTTP

HTTP/1.0 or 1.1 protocol http://www.w3.org/Protocols/rfc1945/rfc1945.txt

Identrus

http://www.identrus.com

LDAP

LDAP client protocol specified in RFC 1777 and RFC 1778, as supported by the JNDI API http://www.cis.ohio-state.edu/htbin/rfc/rfc1777.html

Glossary

AIA Authority Information Access

Application protocol. An application protocol is a protocol that normally layers directly on top of the transport layer (e.g., TCP/IP). Examples include HTTP, TELNET, FTP, and SMTP.

ASN.1. Abstract Syntax Notation One.

Authentication. Authentication is the ability of one entity to determine the identity of another entity. i.e. in the case of NetMail Lite, you know who your email message came from.

base64. A representation of characters in digital format using a 65 character subset of U.S. ASCII.

BBS. A random number generating algorithm.

BER. Basic encoding Rules used with X509.

Block cipher. A block cipher is an algorithm that operates on plaintext in groups of bits, called blocks. 64 bits is a typical block size.

Bulk cipher. A symmetric encryption algorithm used to encrypt large quantities of data.

CA Certificate Authority

Cipher Block Chaining Mode (CBC). CBC is a mode in which every plaintext block encrypted with the block cipher is first eXclusive-OR-ed with the previous ciphertext block (or, in the case of the first block, with the initialisation vector).

Certificate. As part of the X.509 protocol (a.k.a. ISO Authentication framework), certificates are assigned by a trusted Certificate Authority and provide verification of a party's identity and may also supply its public key.

Certificate Authority. An organisation authorised to issue certificates (as in CA).

Client. The application entity that initiates a connection to a server.

CN Common Name See for instance http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html for definition.

Connection. A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer to peer relationships. The connections are transient. Every connection is associated with one session.

CRL Certificate Revocation List. A list of certificates that have been declared invalid by their issuing CA before their expiry dates

CSC Certificate Status Check

Data Encryption Standard (DES). DES is a very widely used symmetric encryption algorithm. DES is a block cipher.

3DES. Similar to DES.

DER. Distinguished Encoding rules used in X509.

DH. A public-key cryptographic algorithm for encrypting and decrypting data.

Digital Signature Standard (DSS). A standard for digital signing, including the Digital Signing Algorithm, approved by the National Institute of Standards and Technology, defined in NIST FIPS PUB 186, "Digital Signature Standard," published May, 1994 by the U.S. Dept. of Commerce.

Digital signatures. Digital signatures utilise public key cryptography and one-way hash functions to produce a signature of the data that can be authenticated, and is difficult to forge or repudiate.

DN Distinguished Name. See for instance http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html or http://search.ietf.org/internet-drafts/draft-zeilenga-ldapv3bis-rfc2253-00.txt for definition.

DSA. Digital Signature Algorithm.

EE. End Entities are customers. i.e. the last person in the certificate chain.

Handshake. An initial negotiation between client and server that establishes the parameters of their transactions.

HSM Hardware Security Module.

HTML HyperText Markup Language.

IDEA. A 64-bit block cipher designed by Xuejia Lai and James Massey.

Integrity i.e. You know your email message has not changed.

IP Issuing Participant Bank (or other financial institution) issuing smart cards containing private keys and certificates to Subscribing Customers.

IR Identrus Root

key. The key used to encrypt data written by the client.

LDAP Lightweight Directory Access Protocol

Message Authentication Code (MAC). A Message Authentication Code is a one-way hash computed from a message and some secret data. Its purpose is to detect if the message has been altered.

MD5. MD5 is a secure hashing function that converts an arbitrarily long data stream into a digest of fixed size.

MIME. MultiPURPOSE Internet Mail Extension

Non-repudiation A process set up to ensure that the sender cannot disavow a message

OCSP Online Certificate Status Protocol

OU Organisation Unit See for instance http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html or http://search.ietf.org/internet-drafts/draft-zeilenga-ldapv3bis-rfc2253-00.txt for definition.

PBE. Password based encryption

PEM. Privacy enhanced mail

Public Key Infrastructure (PKI). Defines protocols to support online interaction.

Public key cryptography. A class of cryptographic techniques employing two-key ciphers. Messages encrypted with the public key can only be decrypted with the associated private key. Conversely, messages signed with the private key can be verified with the public key.

OSI. Open Systems Inter-Connection.

RC2, RC4. Proprietary ciphers from RSA Data Security, Inc. RC2 is block cipher and RC4 is a stream cipher.

RC Relying Customer Party with whom the Subscribing Customer initiates a signed transaction.

RC Host Server software that performs the role of the RC in the identrus certificate status check scheme. In the case of this document this is the portal server.

RC NetMail Lite or RC Mail. The client software interface that a customer uses to send and receive messages. In the case of this document this is NetMail Lite.

RP Relying Participant Bank with which the Relying Customer communicates to obtain some level of trust in the signed data received from the Subscribing Customer.

RSA. A very widely used public-key algorithm that can be used for either encryption or digital signing.

Server. The server is the application entity that responds to requests for connections from clients. The server is passive, waiting for requests from clients.

SC Subscribing Customer. Member of the Issuing Participant bank authorised to participate in Identrus activities.

Session. A SSL session is an association between a client and a server. Sessions are created by the handshake protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

SmartCard A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.

SHA. The Secure Hash Algorithm is defined in FIPS PUB 180-1. It produces a 20-byte output.

SSL. Secure sockets layer

Stub The Java interface to support communication with the CAFast hard server

TC Transaction Co-ordinator

X509. An authentication framework based on ASN.1 BER and DER and base64.

Index