



RSA Keon Ready Implementation Guide For PKI 3rd Party Applications

Last Modified June 11, 2003

1. Partner Information

Partner Name	Funk Software
Web Site	www.funk.com
Product Name	Odyssey
Version & Platform	Odyssey Server v1.12 Odyssey Client v2.0
Product Description	Odyssey is a wireless LAN access control and security solution based on the IEEE security standard 802.1x. Odyssey provides strong security over the wireless link and can be easily and widely deployed and managed across an enterprise network. Odyssey includes client and server software. It secures the authentication and connection of WLAN users, ensuring that only authorized users can connect, that connection credentials will not be compromised, and that data privacy will be maintained.
Product Category	Wireless Communications
RSA product Interaction	RSA Keon Certificate Authority, RSA SecurID Passage



2. Contact Information

	Sales contact	Support Contact
Email	sales@funk.com	support@funk.com
Phone	(800) 828-4146	(617) 491-6503
Web	www.funk.com	www.funk.com

3. Product Requirements

Hardware Requirements

Component Name: Odyssey Server	
Wireless Access Point	The most recently updated compatibility list can be found on the Odyssey User Page located at: http://www.funk.com/radius/compatibility.asp

Component Name: Odyssey Client	
Wireless LAN Adapter Card	The most recently updated list of compatible adapter cards can be found on the Odyssey User Page located at: http://www.funk.com/radius/compatibility.asp

Software requirements

Component Name: Odyssey Server	
Operating System	Version (Patch-level)
Windows 2000 Server	Service Pack 2
Windows 2000 Advanced Server	Service Pack 2
Windows 2000 Professional	Service Pack 2
Windows XP Professional	
Web Browser:	MS Internet Explorer 5.5 or later

Component Name: Odyssey Client	
Operating System	Version (Patch-level)
Windows 2000 Server	Service Pack 2
Windows 2000 Advanced Server	Service Pack 2
Windows 2000 Professional	Service Pack 2
Windows XP Professional	
Windows XP Home	

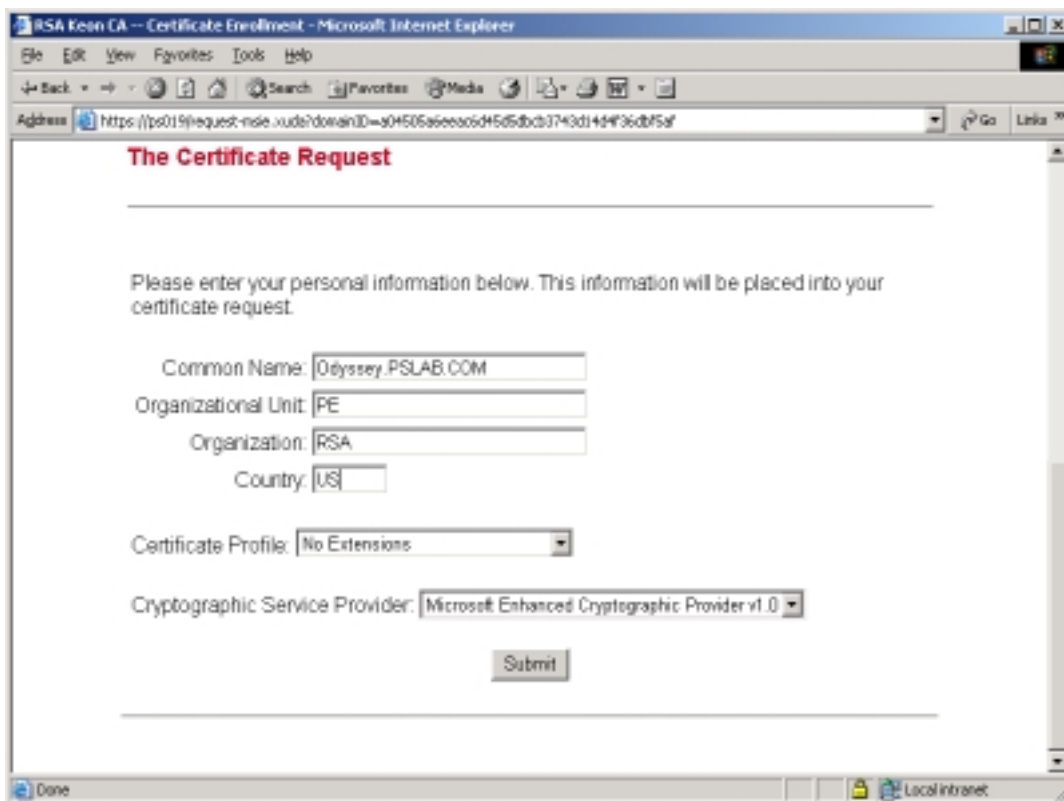
4. Product Configuration

Overview

The scope of this guide is to show how to setup and configure Odyssey Server and Odyssey client for EAP-TLS to be used in an RSA Keon Certificate authenticated WLAN environment. For a more in depth explanation of how to configure your wireless hardware, please refer to the documentation provided by your hardware vendor. This document assumes you have installed and configured a wireless access point for 802.1x authentication against an Odyssey server. For more information on installation and configuration, please see Tech Notes: http://www.funk.com/subsections/tec_ody.asp

Odyssey server Configuration:

1. Connect to the RSA Keon Certificate Authority and make an End-Entity request for the Odyssey server. The common name must be the fully qualified domain name of the Odyssey server.

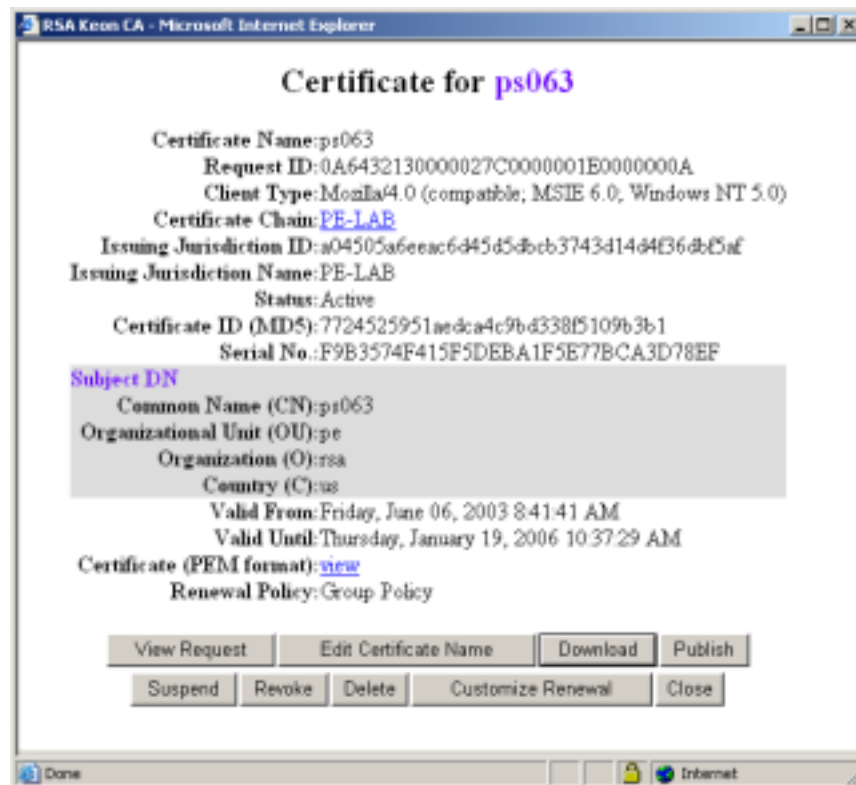


The screenshot shows a Microsoft Internet Explorer browser window titled "RSA Keon CA - Certificate Enrollment". The address bar contains a URL starting with "https://ps015/request-noie...". The main content area is titled "The Certificate Request" and contains a form for entering personal information. The form fields are as follows:

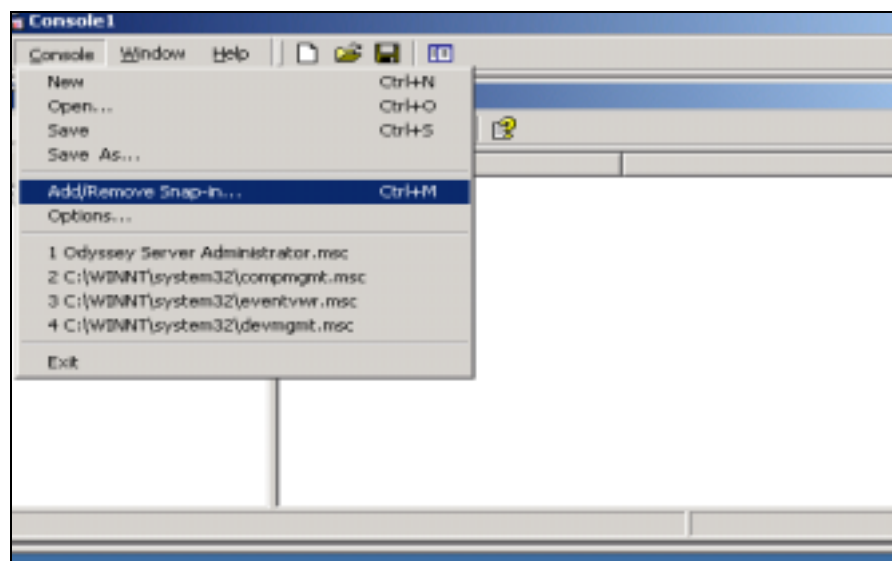
- Common Name: Odyssey.PSLAB.COM
- Organizational Unit: PE
- Organization: RSA
- Country: US
- Certificate Profile: No Extensions
- Cryptographic Service Provider: Microsoft Enhanced Cryptographic Provider v1.0

A "Submit" button is located below the form fields. The browser's status bar at the bottom shows "Done" and "Local intranet".

2. Upon approval, download certificate to the local Odyssey server.

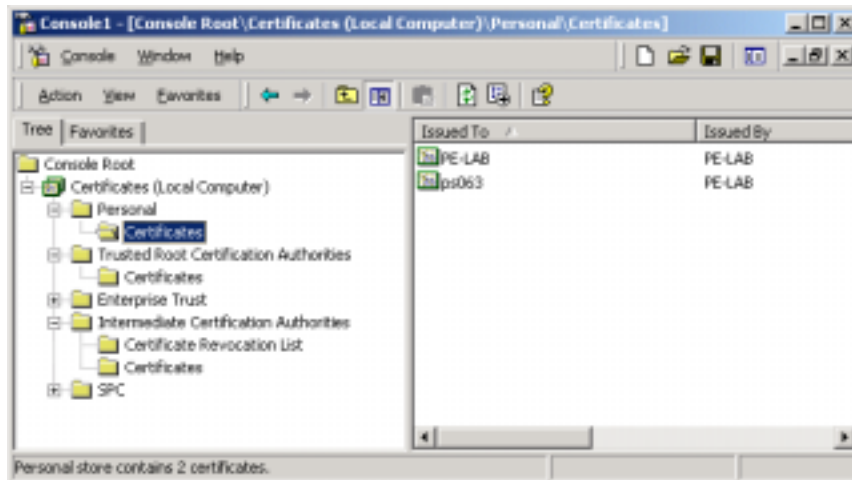


3. Install the certificate in the Personal Folder of the local machine's certificate store:
 - a. From the Windows desktop: Start, Run, "MMC" (this will bring up a Microsoft Management Console screen).
 - b. Select Console, Add/remove Snap-in.

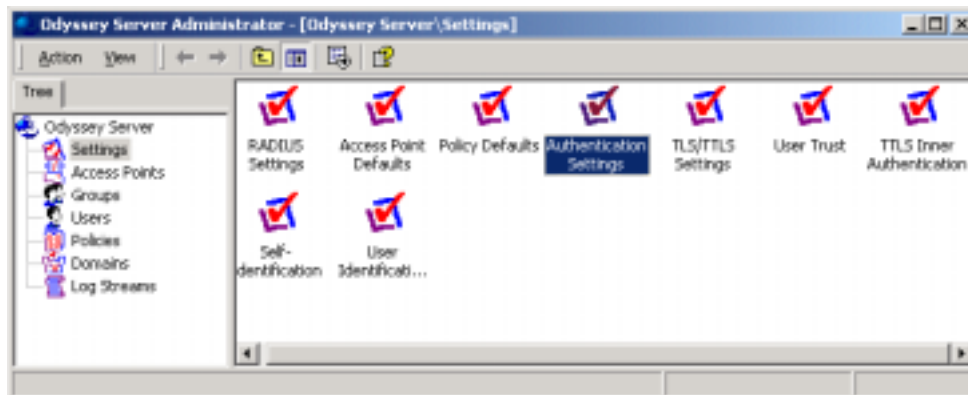


- c. Click Add, and double click on Certificates (this will bring up the certificates snap-in window).

- d. Select Computer account, click Next.
- e. Click Finish (make no changes on this screen!).
- f. Click Close, Click OK.
- g. You will now see, in the MMC console, the entry for Certificates (Local Computer).
- h. Expand this view and click on the Personal folder.
- i. Right click on the Personal folder.
- j. From the pop-up menu select All Tasks, Import (this will bring up the certificate import wizard).
- k. Click Next.
- l. Browse for the certificate, Click Next.
- m. *Optional (if a password was used to export the certificate) - Enter the password for the certificate, and check the box for "Mark key as exportable", Click Next.
- n. Select "Place certificate in the following store", choosing "Personal".
- o. Click Next.
- p. Confirm details and Click Finish.
- q. You will now see your imported certificate in the "Certificates" Personal\Certificates folder.



4. From the Odyssey Server Administrator, click on Settings and double-click on Authentication Settings in the right hand pane.



5. If TLS is not present, click on Add.
6. Select TLS from the list.
7. Click OK and then click OK again to close.



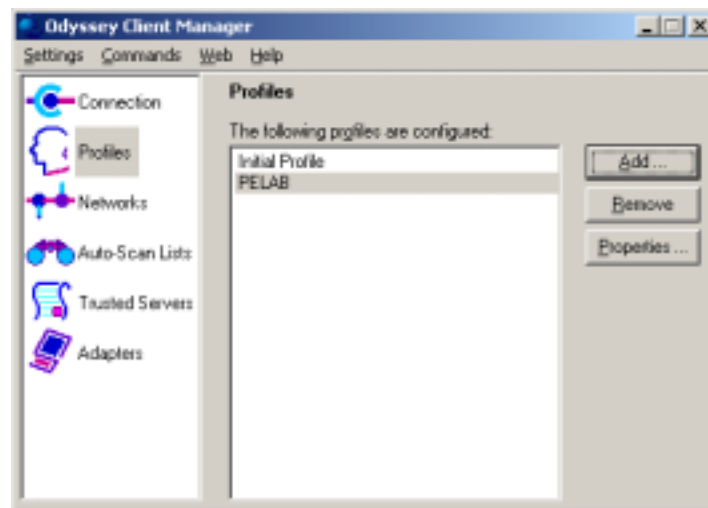
8. Double-click on User Trust from the right hand pane.
9. Click on Add Certificate.
10. Click on the Trusted Root tab and browse to the certificate for your CA, where you enrolled for the server certificate, select it and click OK.
11. Select your CA from the certificates list and click on Add Identity.
12. Check the box "Any user or CA certificate issued by parent" and click OK. This states that any certificate from the same CA will be trusted. Click OK.



13. Double-click User Identification by Certificate.
14. Select the appropriate criteria for validating user certificates and click OK.
15. From the Odyssey Server Administrator ensure your access points, domain(s), groups, and users are configured properly. Authorization is based on Windows users and groups; the server must match the certificate to a particular user to be able to authorize the user. Therefore, a user validated by certificate MUST have a valid Windows account.

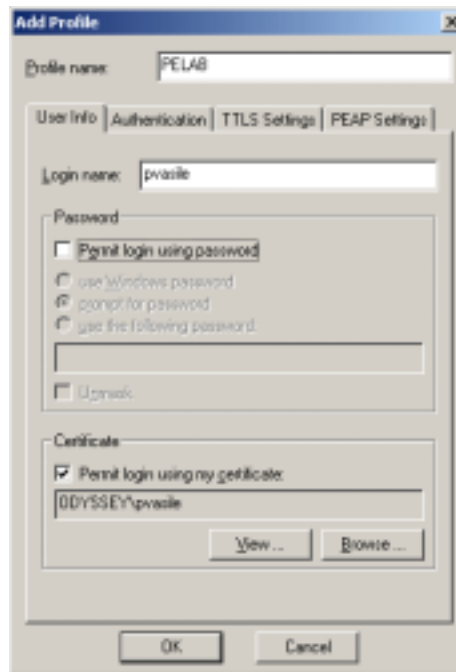
Wireless client Configuration:

1. Connect to the RSA Keon Certificate Authority and make an End-Entity request for the Wireless LAN user. The common name must adhere to the criteria configured in step #11 under the section "Odyssey Server Configuration".
2. Upon approval, install the certificate on WLAN PC.
3. Install the Trusted Root CA Certificate for the CA that issued the server certificate that will be presented by the Odyssey Server for authentication.
* NOTE - A Trusted Root CA Certificate needs to be installed to the Current User's Trusted Root Certificate Store on the client machine prior to installing the Odyssey client.
4. Verify that the Wireless Network card is properly installed, and that the proper drivers and firmware for this card have been installed. Make sure that the card is inserted into the PC, and that the adapter is "Enabled" by the operating system.
5. Run the Odyssey Client installer.
6. Upon successful completion of Odyssey Client install, launch the Odyssey Client Manager and select Profiles from the left hand pane. Click Add.



7. Type a name for your Profile in the Profile name box.
8. Type the correct login name in Login name box.
9. Uncheck the box for Permit login using password.

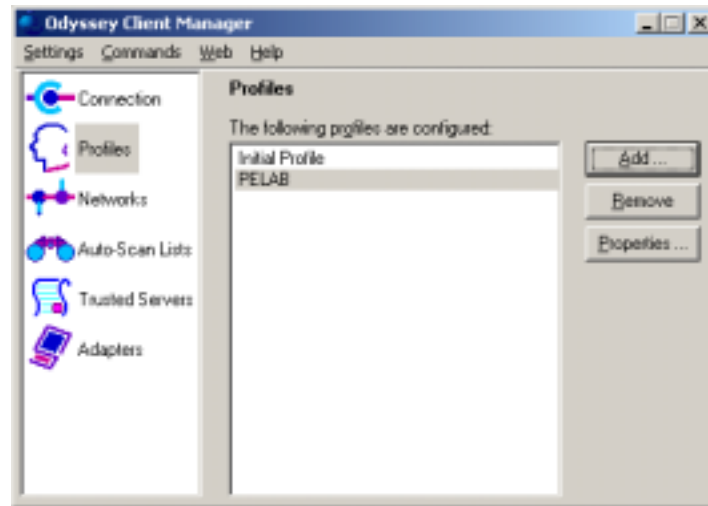
10. Check the box for Permit login using my certificate and then click Browse. Select the user's personal certificate from the list and click OK. You should now see your certificate listed in the box below.



11. Click on the Authentication tab. Click Add.
12. Select EAP-TLS from the list of EAP Protocols. Click OK.
13. Check the box for Validate server certificate. Click OK.

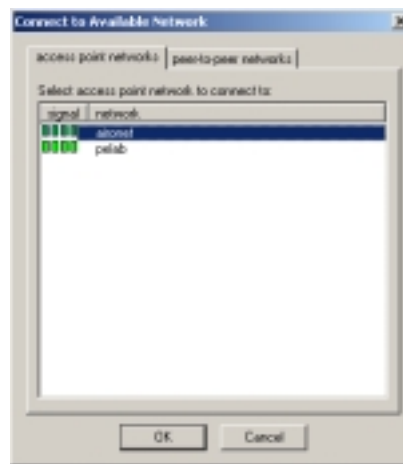


14. Your profile should now be listed in the Profiles window.

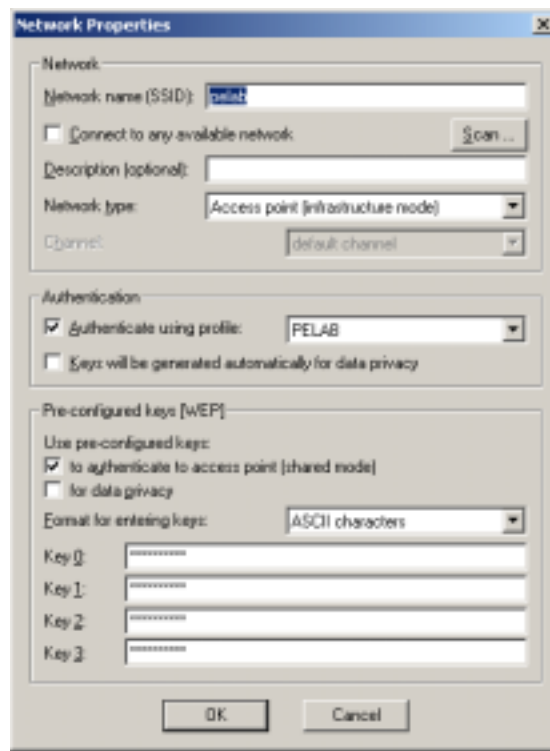


15. Select Networks from the left pane of the Odyssey Client Manager window.

16. Click Add. Enter the SSID of your WLAN or click Scan and choose your WLAN from the list of access point networks.



17. Check the box for Authenticate using profile and select your profile from the pull-down menu.
18. Enter the proper WEP settings for your WLAN and click OK when finished.

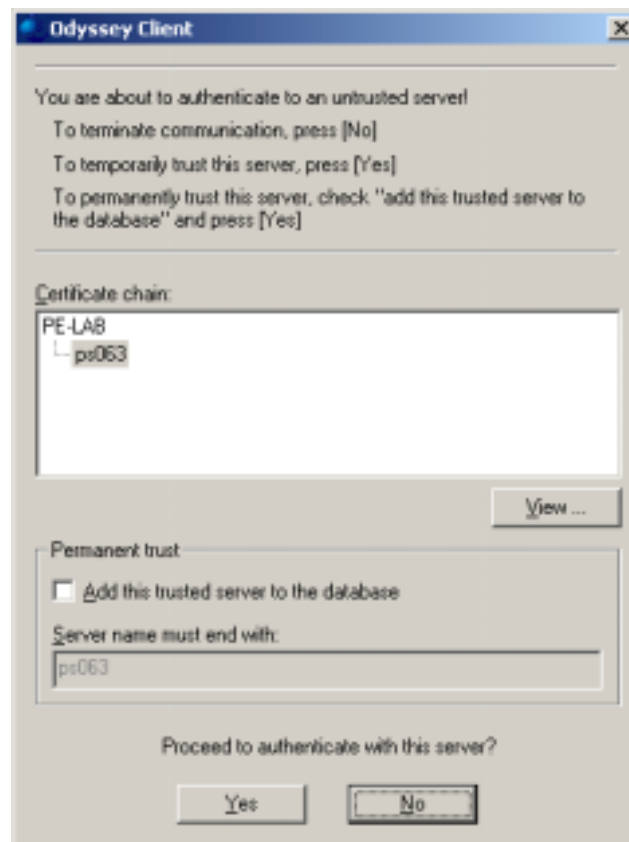


19. Click on Connection from the left pane of the Odyssey Client Manager window.
20. You should see your wireless adapter listed in the adapter box. Ensure the "Connect to Network" box is checked and the proper SSID for your WLAN is displayed.
21. The Odyssey client is now configured to authenticate with the Odyssey server via EAP-TLS.

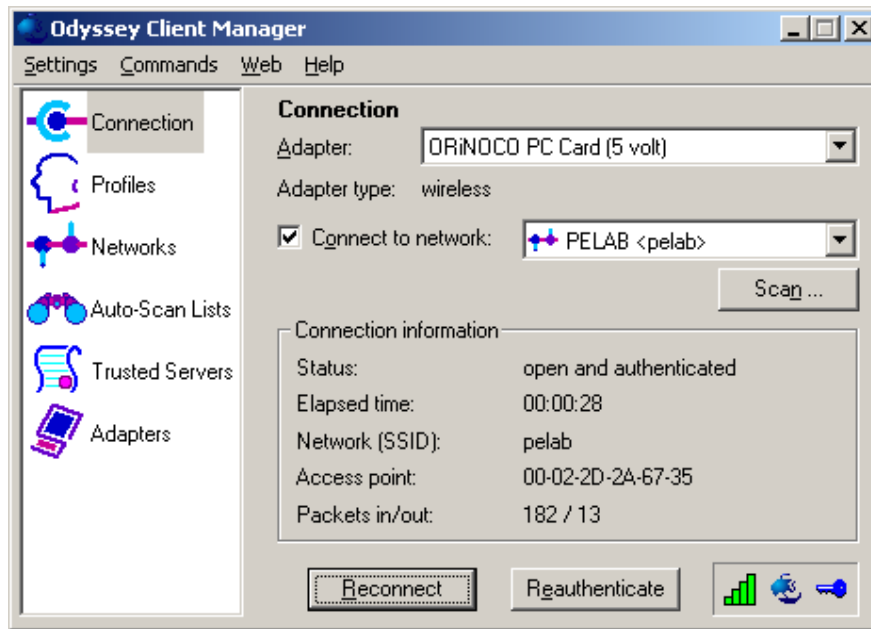
5. Product Operation

To connect to the Wireless LAN, click the Reconnect button on the Odyssey Client Manager.

You may receive a message that you are about to authenticate with an untrusted server. Check the credentials of the server (it should be your Odyssey server) and if all is correct check the box to Add this trusted server to the database.



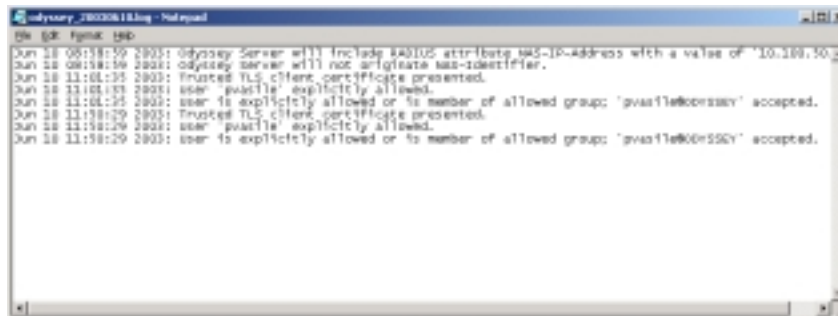
You should now be authenticated on the wireless LAN via certificate. Odyssey Client Manager status should be Open and authenticated.



Upon successful configuration of the WLAN to authenticate via EAP-TLS, operation should be seamless. After all certificates have been vetted, authentication is processed in the background.

The Odyssey client authenticates with the server automatically when the WLAN user logs onto their PC.

A typical log entry from the Odyssey server showing successful authentication:



6. Certification Checklist

Date Tested: June 9, 2003

Product	Tested Version
RSA Keon Certificate Authority	6.5
RSA SecurID Passage	3.4
Odyssey Server	1.12
Odyssey Client	2.0

Test Case	Result		
Certificate Enrollment			
P10 Certificate Request	P		
P7 Response installed correctly	P		
CMP Certificate Request	N/A		
CMP Response installed correctly	N/A		
SCEP Certificate Request	N/A		
SCEP Response installed correctly	N/A		
Import Certificate			
Import PKCS#12 envelope	P		
Import via cut & paste	N/A		
Install Root Certificate via cut/paste	N/A		
Install SubCA Certificate via cut/paste	N/A		
Install Root Certificate via SCEP	N/A		
Install SubCA Certificate via SCEP	N/A		
Verify Certificate chain is installed	P		
Certificate Usage			
S/MIME	Sign N/A	Encrypt N/A	SSL N/A
Document and Files	N/A	N/A	N/A
SSL Client Authentication	N/A	N/A	N/A
LDAP Support			
Name lookup	N/A		
Certificate retrieval	N/A		
Status Check of Certificate			
Success with a valid certificate	OCSP N/A	CRL N/A	Other N/A
Fails with a revoked certificate	N/A	N/A	N/A
Fails with a suspended certificate	N/A	N/A	N/A
Pass with a re-instated certificate	N/A	N/A	N/A
RSA Keon Web Passport / RSA SecurID Passage Support			
Access certificates via MS CAPI (Internet Explorer)	Passage P		KWP N/A
Access certificates via PKCS#11 (Netscape)	N/A		N/A

PJV

*P=Pass or Yes F=Fail N/A=Non-available function

7. Known Issues

There are no known issues.