



RSA Secured Implementation Guide For 3rd Party PKI Applications

Last Modified: December 11, 2007

Partner Information

Product Information	
Partner Name	Juniper Networks
Web Site	www.juniper.net
Product Name	Odyssey Access Client
Version & Platform	4.70.10539.0
Product Description	Juniper Networks Odyssey Access Client (OAC) is an enterprise-class 802.1X supplicant/access client, offering full support for the advanced protocols required for secure wired and wireless LAN access. OAC ensures that users can connect to authorized networks, where login credentials are not compromised, and data privacy is maintained. OAC is compatible and integrates with Juniper Networks' Unified Access Control (UAC) v2.x, a comprehensive network access control solution that combines powerful, standards-based user authentication and authorization with identity-based policy control and management, ensuring endpoint security intelligence to extend access control across an enterprise network.
Product Category	Networks and Communication



Solution Summary

The Juniper Odyssey Access Client (OAC) utilizes x.509 certificates that have been stored in the RSA Certificate Manager cryptographic service provider (CSP). Certificates stored in this CSP are accessible through both a Smart Card reader and Microsoft's CAPI, and are available for any application wishing to leverage the private key for use in authenticating to a networked security infrastructure.

Partner Integration Overview	
RSA Certificate Manager Interoperability	Y
Interoperable through RSA Authentication Utility	Y
Interoperable through RSA Sign-On Manager	Y
Pre-Boot Authentication	N
If Pre-Boot, which tokens are supported?	N/A

Product Requirements

Partner Product Requirements: Odyssey Access Client v 4.7 or higher	
CPU	Please refer to OAC minimum requirements
Memory	Please refer to OAC minimum requirements

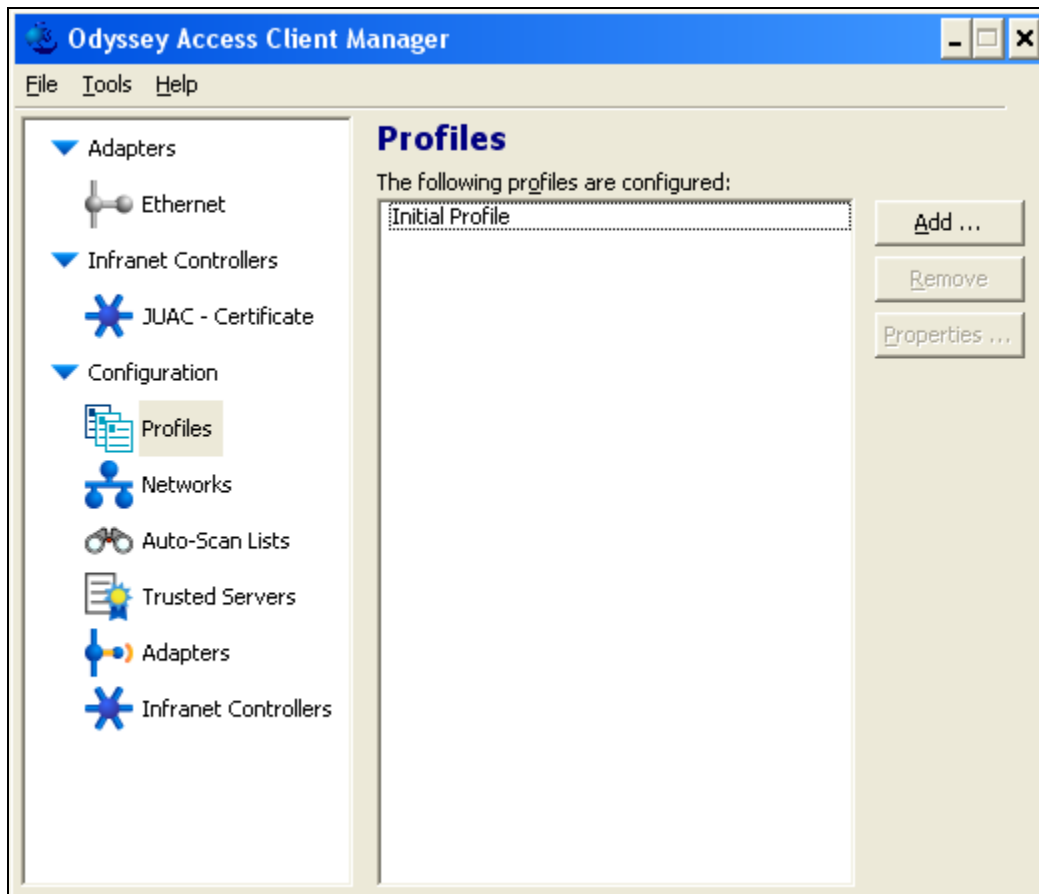
Operating System	
Platform	Required Patches
Windows XP	SP2

Additional Software Requirements	
Application	Additional Patches
RSA Authentication Client v2.0.0	Build 223 or higher
RSA SecurID Software Token v3.0.6	Build 254 or higher
RSA Smart Card 5200	
RSA or 3 rd party Smart Card reader	
Internet Explorer v6.0 or 3 rd party web browser	
Juniper Unified Access Control v2.0UAC2.0R2	Build 49383 or higher

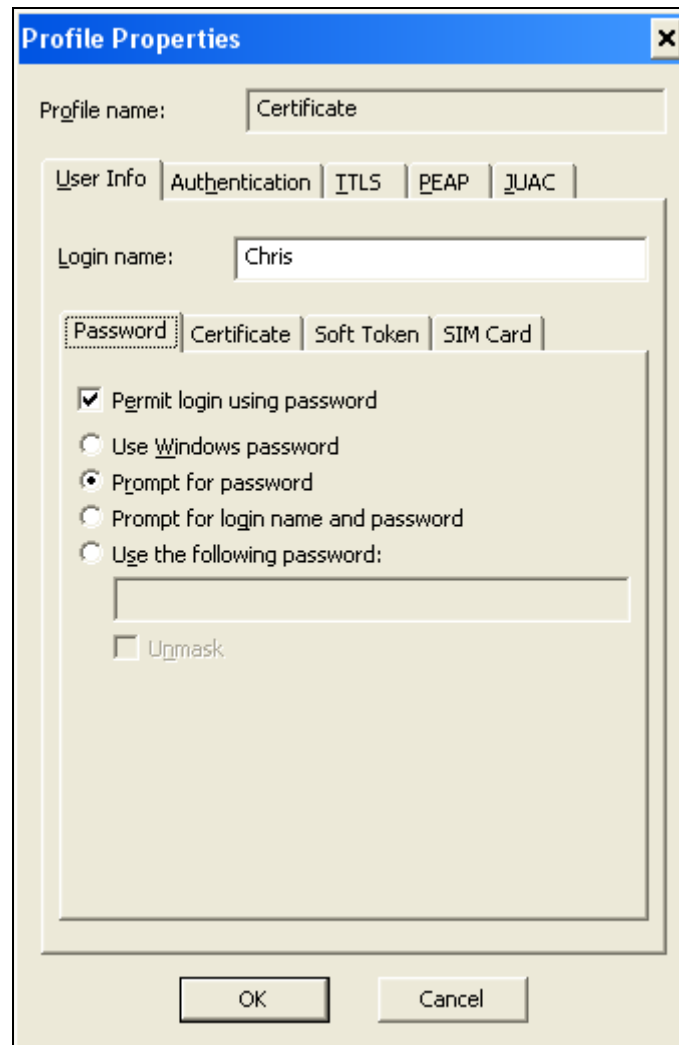
Product Configuration

Configuration of the Odyssey client is performed through the OAC User Interface. The following steps will outline profile and client configuration when authenticating using a client based Certificate. Please refer to the appropriate Juniper OAC documentation to obtain additional details on configuring wired and wireless infrastructures. Additionally, please refer to the appropriate documentation in enrolling for certificate based authentication.

1. Launch the OAC client, select **Profiles** and click **Add**.



2. For the **User Info** tab, enter a **Profile name** and **Login name** (for purposes of this certification, the username is not associated with the client side Certificate. Any **Login name** may be entered when following this guide)
3. Select the following under the **Password** tab:
 - Permit login using password
 - Prompt for password



The screenshot shows a 'Profile Properties' dialog box with a blue title bar and a close button. The 'Profile name' field contains 'Certificate'. Below it are tabs for 'User Info', 'Authentication', 'ITLS', 'PEAP', and 'UAC'. The 'User Info' tab is active, showing a 'Login name' field with 'Chris'. Below that are tabs for 'Password', 'Certificate', 'Soft Token', and 'SIM Card'. The 'Password' tab is active, showing a list of radio button options: 'Permit login using password' (checked), 'Use Windows password', 'Prompt for password', 'Prompt for login name and password', and 'Use the following password:'. Below these options is an empty text field and an unchecked 'Unmask' checkbox. At the bottom are 'OK' and 'Cancel' buttons.

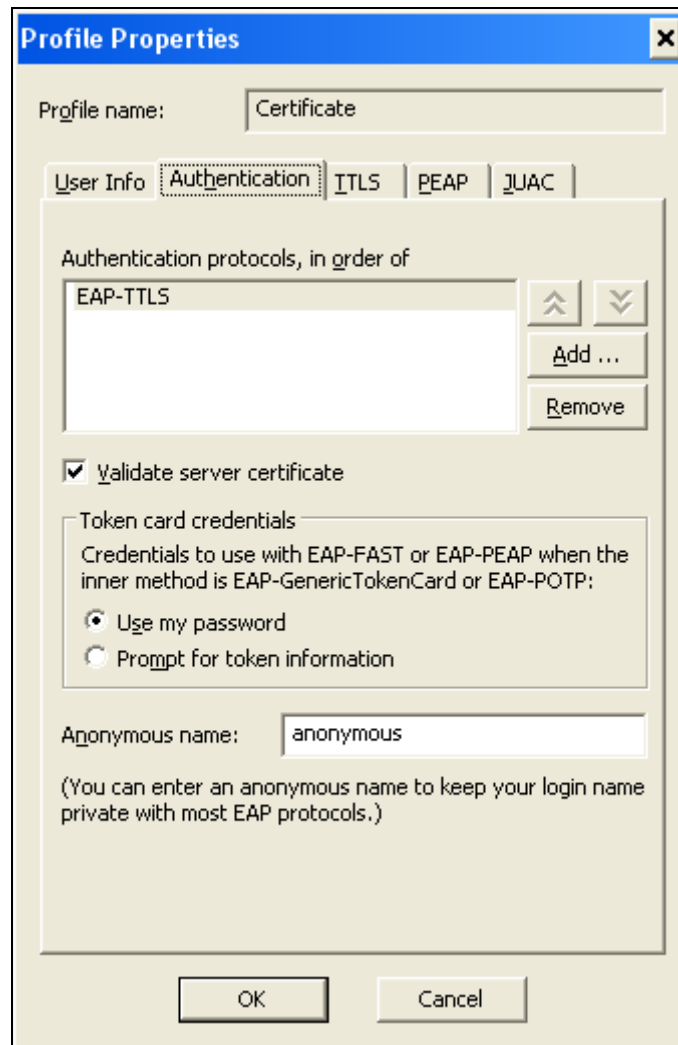
4. Click on the **Certificate** tab and select the following:

- Permit login using my certificate:
- Use the logon certificate from my smart card reader; **selecting the smart card reader from the drop down menu.**

The image shows a screenshot of the 'Profile Properties' dialog box, specifically the 'Certificate' tab. The dialog box has a blue title bar with the text 'Profile Properties' and a close button (X). Below the title bar, there is a text field for 'Profile name:' containing the text 'Certificate'. Below this, there are several tabs: 'User Info', 'Authentication', 'ITLS', 'PEAP', and 'Certificate'. The 'Certificate' tab is currently selected. Under the 'Certificate' tab, there is a text field for 'Login name:' containing the text 'Chris'. Below this, there are more tabs: 'Password', 'Certificate', 'Soft Token', and 'SIM Card'. The 'Certificate' tab is selected. In the main area of the dialog, there are three radio button options: 1. 'Permit login using my certificate:' which is checked. 2. 'Use automatic certificate selection' which is not checked. 3. 'Use the following certificate:' which is not checked. Below the third option is an empty text field and two buttons: 'View ...' and 'Browse ...'. Below these buttons, there is a radio button option 'Use the logon certificate from my smart card reader' which is checked. Below this option is a dropdown menu showing 'SCM Microsystems Inc. SCRx31 USB Smart Card F'. At the bottom of the dialog box, there are two buttons: 'OK' and 'Cancel'.

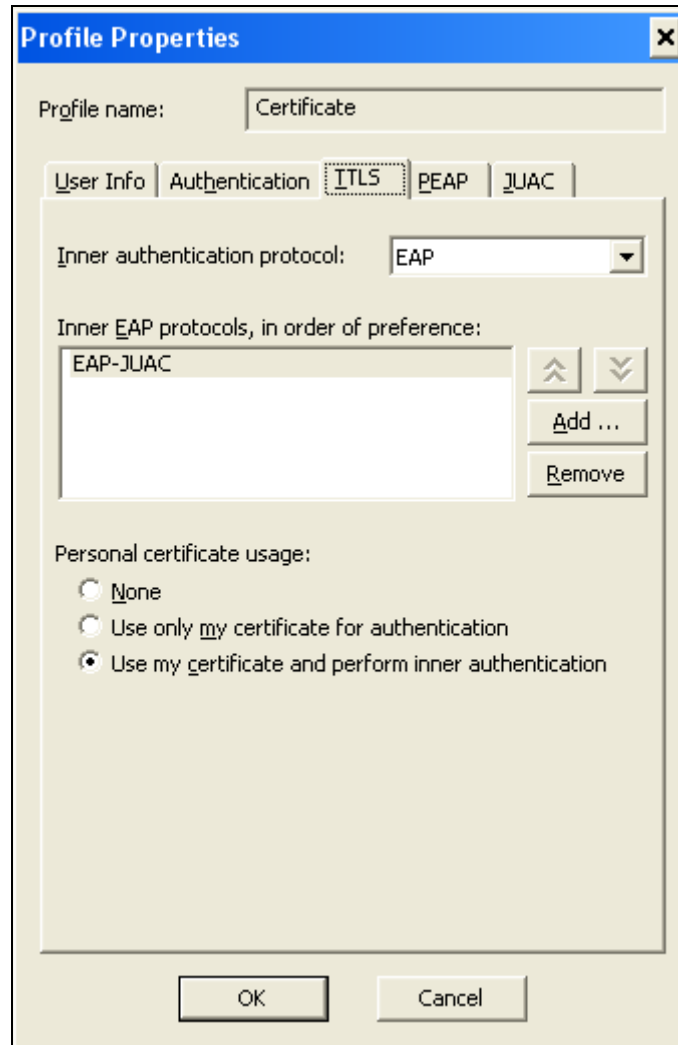
5. Next, click on the **Authentication** tab and verify/select the following:

- EAP-TTLS is in the list of Authentication protocols
- Validate server certificate
- Use my password
- Anonymous name: **anonymous**



6. Next, click on the **TTLS** tab and select the following:

- Inner authentication protocol: EAP
- EAP-JUAC for Inner EAP protocols **list (click Add if not in list)**
- Use my certificate and perform inner authentication



The image shows a screenshot of the "Profile Properties" dialog box, specifically the "TTLS" tab. The "Profile name" field is set to "Certificate". The "Inner authentication protocol" is set to "EAP". Under "Inner EAP protocols, in order of preference", "EAP-JUAC" is listed. The "Personal certificate usage" section has three radio buttons: "None", "Use only my certificate for authentication", and "Use my certificate and perform inner authentication", with the last one selected. The dialog has "OK" and "Cancel" buttons at the bottom.

Profile name: Certificate

User Info Authentication **TTLS** PEAP JUAC

Inner authentication protocol: EAP

Inner EAP protocols, in order of preference:

EAP-JUAC

Personal certificate usage:

None

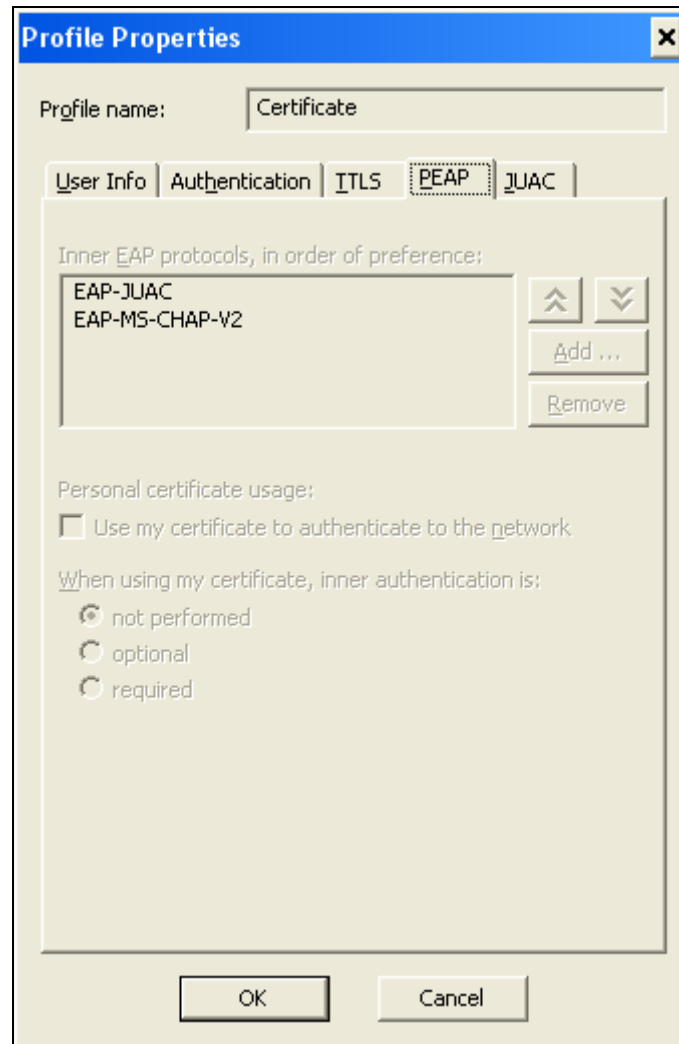
Use only my certificate for authentication

Use my certificate and perform inner authentication


OK Cancel

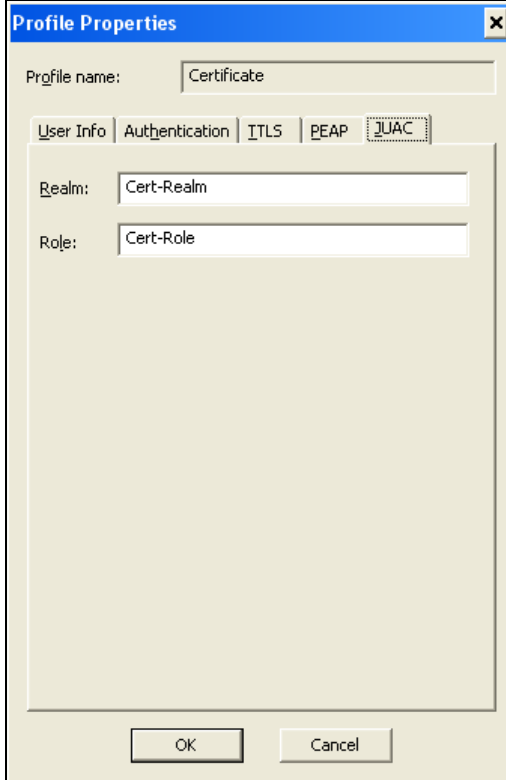
7. Click on the **PEAP** tab and verify the following protocols are in the list (click **Add** if not in list)

- EAP-JUAC
- EAP-MS-CHAP-V2



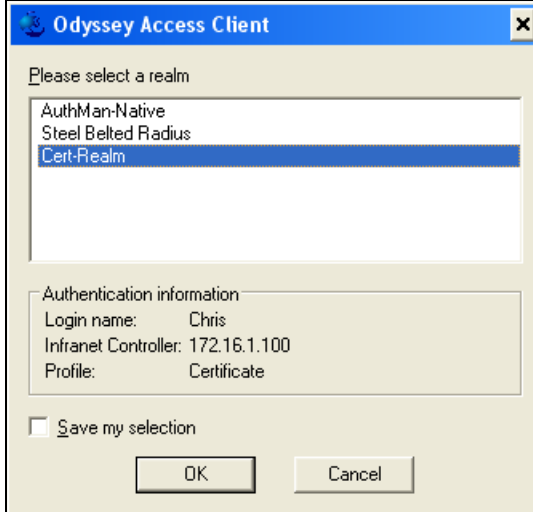
8. Click on the **JUAC** tab and enter the appropriate **Realm** and **Role**.

 The Realm and Role are configured on the Unified Access Control (UAC) device or other network device. Check with your Administrator for these parameters. If these parameters are not defined, the user will be presented a list of Realm(s) to choose from. (see Screen Shot “List” below)



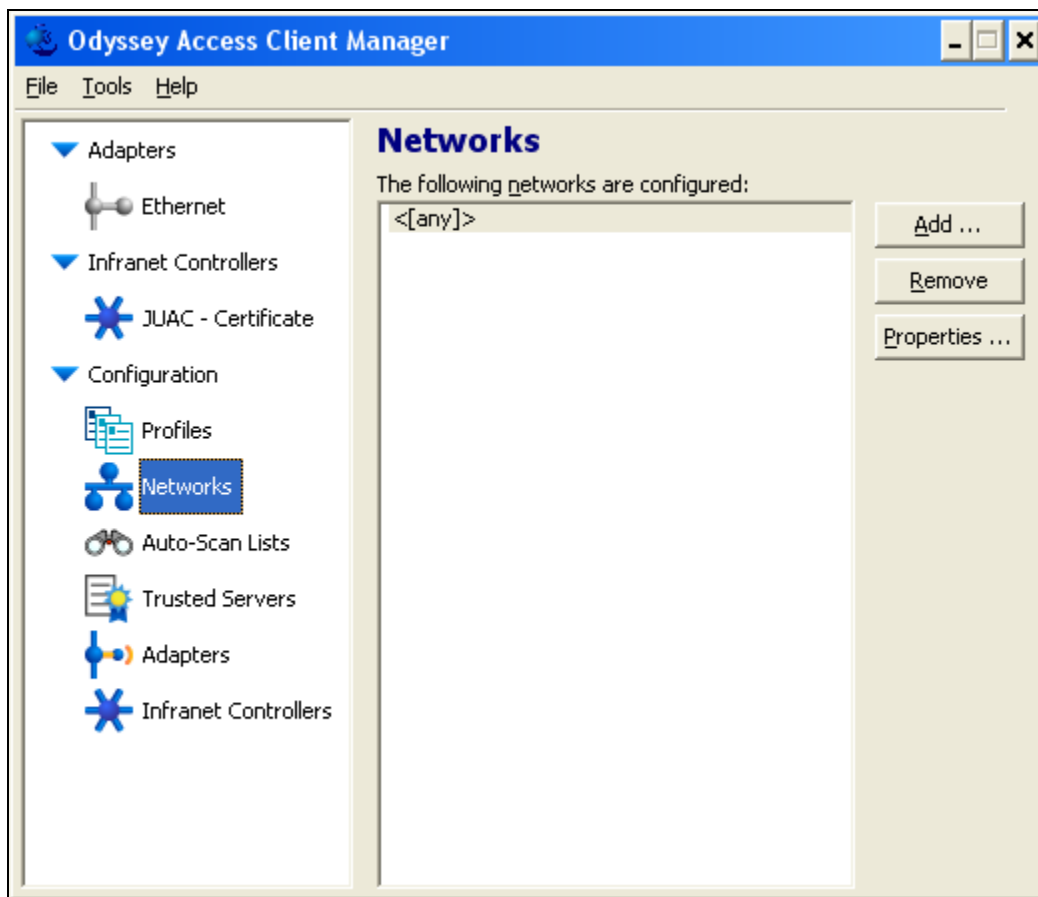
The screenshot shows a dialog box titled "Profile Properties" with a close button (X) in the top right corner. The "Profile name" field contains "Certificate". Below this are five tabs: "User Info", "Authentication", "ITLS", "PEAP", and "JUAC". The "JUAC" tab is selected. Under the "JUAC" tab, there are two text input fields: "Realm:" with the value "Cert-Realm" and "Role:" with the value "Cert-Role". At the bottom of the dialog are "OK" and "Cancel" buttons.

List

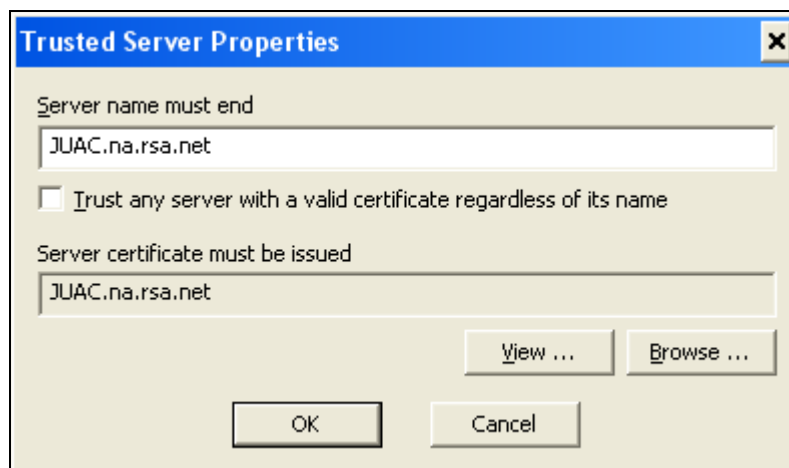


The screenshot shows a dialog box titled "Odyssey Access Client" with a close button (X) in the top right corner. The text "Please select a realm" is displayed above a list box. The list box contains three items: "AuthMan-Native", "Steel Belted Radius", and "Cert-Realm", with "Cert-Realm" selected and highlighted in blue. Below the list box is a section titled "Authentication information" containing the following text: "Login name: Chris", "Infranet Controller: 172.16.1.100", and "Profile: Certificate". At the bottom left is a checkbox labeled "Save my selection" which is currently unchecked. At the bottom center are "OK" and "Cancel" buttons.

9. Click on **Networks** and verify that <[any]> is in the list.



10. Next, click on **Trusted Servers** and enter either the fully qualified domain name or IP address of the network device you will be connecting to.

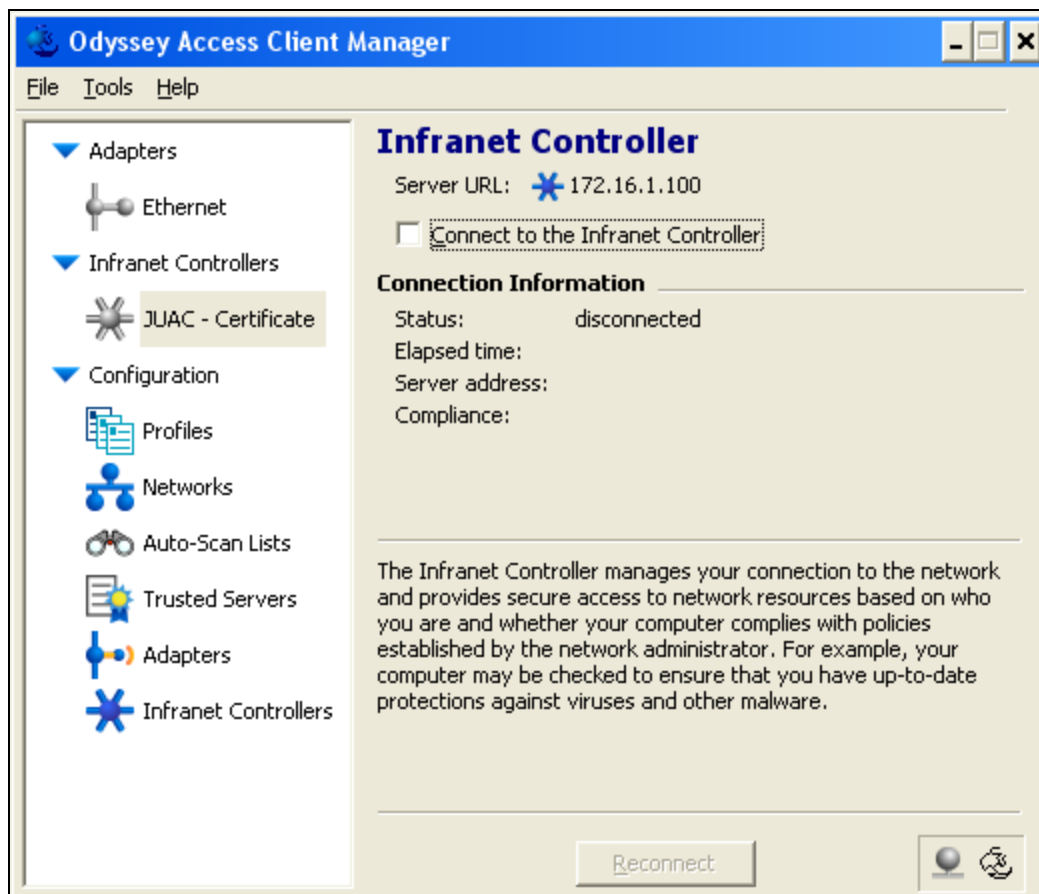


11. Click on **Infranet Controllers** and enter/configure the following:

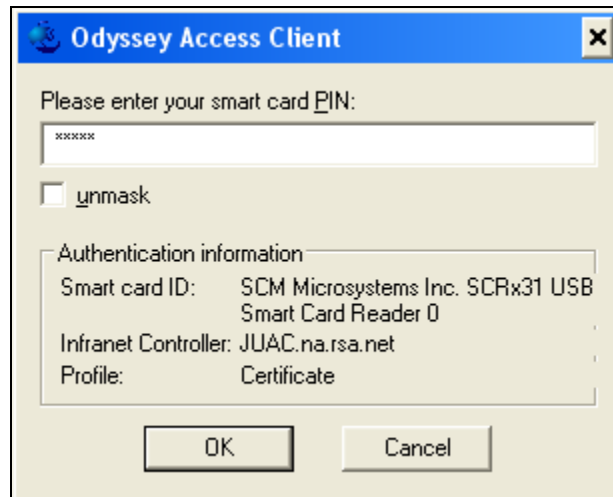
- Infranet Controller name:
- Server URL: (**either FQDN or IP address**)
- Authentication Profile: (**previously configured in step 2**)



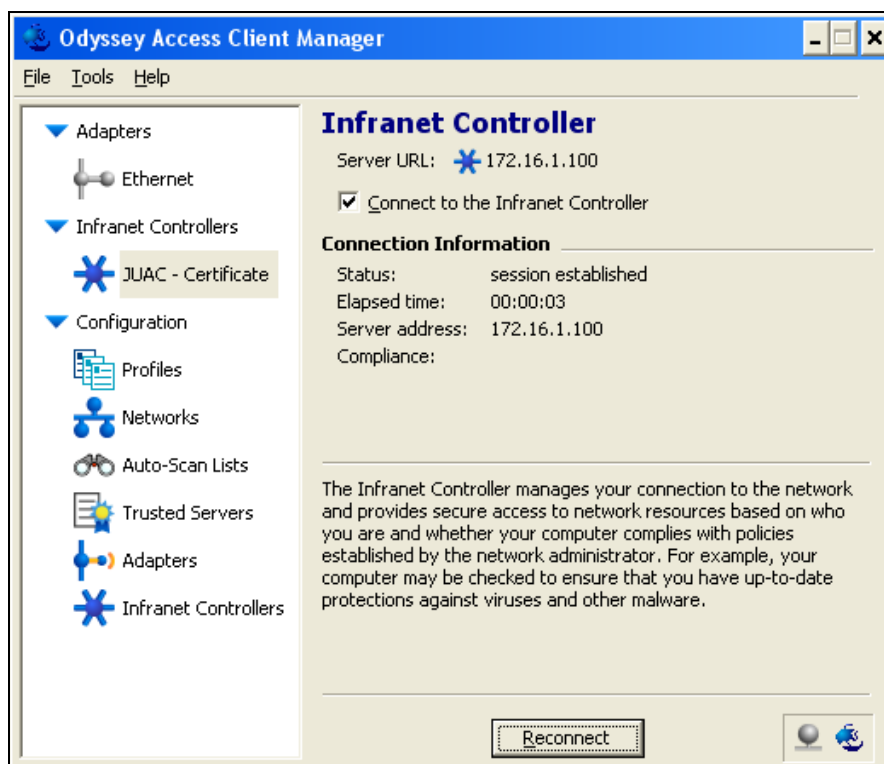
12. Select **Infranet Controllers** and select the device previously configured and click **Connect to the Infranet Controller**.



13. Enter **smart card PIN** when prompted. (this PIN is configured via the RSA Authentication Client software utility)



Session established



Certification Checklist for 3rd Party Applications

Date Tested: December 11, 2007

Product	Operating System	Tested Version
RSA Certificate Manager	Windows 2003	v6.7
RSA Remote Authentication Client	Windows XP	v2.0.0 (build 223)
RSA SecurID Software Token	Windows XP	V3.0.6 (build 254)
Odyssey Access Client	Windows XP	v4.60.494855.0
RSA Smart Card	USB	5200

Test Case	Results		
Certificate Enrollment			
P10 Certificate Request			✓
P7 Response installed correctly			✓
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			✓
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			✓
Certificate Usage			
S/MIME	Sign	Encrypt	SSL
Document and Files	N/A	N/A	
SSL Client Authentication	N/A	N/A	✓
LDAP Support			
Name lookup			Results
Certificate retrieval			N/A
Status Check of Certificate			
Success with a valid certificate	OCSP	CRL	Other
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 Remote Authentication Client / RSA Sign-On Manager			
Access certificates via MS CAPI (Internet Explorer)		RAC	SOM
		✓	N/A

CMY / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function