RALINK TECHNOLOGY, CORP.

802.1X INSTRUCTIONS ON MAC OS X

APPLICATION NOTE – VERSION 1.0

NOTE: THIS DOCUMENT CONTAINS SENSITIVE INFORMATION AND HAS RESTRICTED DISTRIBUTION.

Proprietary Notice and Liability Disclaimer

The confidential Information, technology or any Intellectual Property embodied therein, including without limitation, specifications, product features, data, source code, object code, computer programs, drawings, schematics, know-how, notes, models, reports, contracts, schedules and samples, constitute the Proprietary Information of Ralink (hereinafter "Proprietary Information")

All the Proprietary Information is provided "AS IS". No Warranty of any kind, whether express or implied, is given hereunder with regards to any Proprietary Information or the use, performance or function thereof. Ralink hereby disclaims any warranties, including but not limited warranties of non-infringement, merchantability, completeness, accuracy, fitness for any particular purpose, functionality and any warranty related to course of performance or dealing of Proprietary Information. In no event shall Ralink be liable for any special, indirect or consequential damages associated with or arising from use of the Proprietary Information in any way, including any loss of use, data or profits.

Ralink retains all right, title or interest in any Proprietary Information or any Intellectual Property embodied therein. The Proprietary Information shall not in whole or in part be reversed, decompiled or disassembled, nor reproduced or sublicensed or disclosed to any third party without Ralink's prior written consent.

Ralink reserves the right, at its own discretion, to update or revise the Proprietary Information from time to time, of which Ralink is not obligated to inform or send notice. Please check back if you have any question. Information or items marked as "not yet supported" shall not be relied on, nor taken as any warranty or permission of use.

Ralink Technology Corporation (Taiwan)

5F, No.36, Tai-Yuen Street,
ChuPei City
HsinChu Hsien 302, Taiwan, ROC
Tel +886-3-560-0868
Fax +886-3-560-0818

Sales Taiwan: Sales@ralinktech.com.tw
Technical Support Taiwan: FAE@ralinktech.com.tw

http://www.ralinktech.com/

TABLE OF CONTENTS

1 SUPPORTED AUTHENTICATION AND ENCRYPTION TYPES

The Ralink WLAN utility on Mac OS X supports WPA/802.1x with RADIUS server and Funk Odyssey server. The multiple supported security types are subsequently shown.

1.1 Radius Server

- PEAP
  - EAP-MSCHAP v2
  - EAP-TLS
  - Generic Token Card
- TLS
- MD5-Challenge

1.2 Funk Odyssey Server

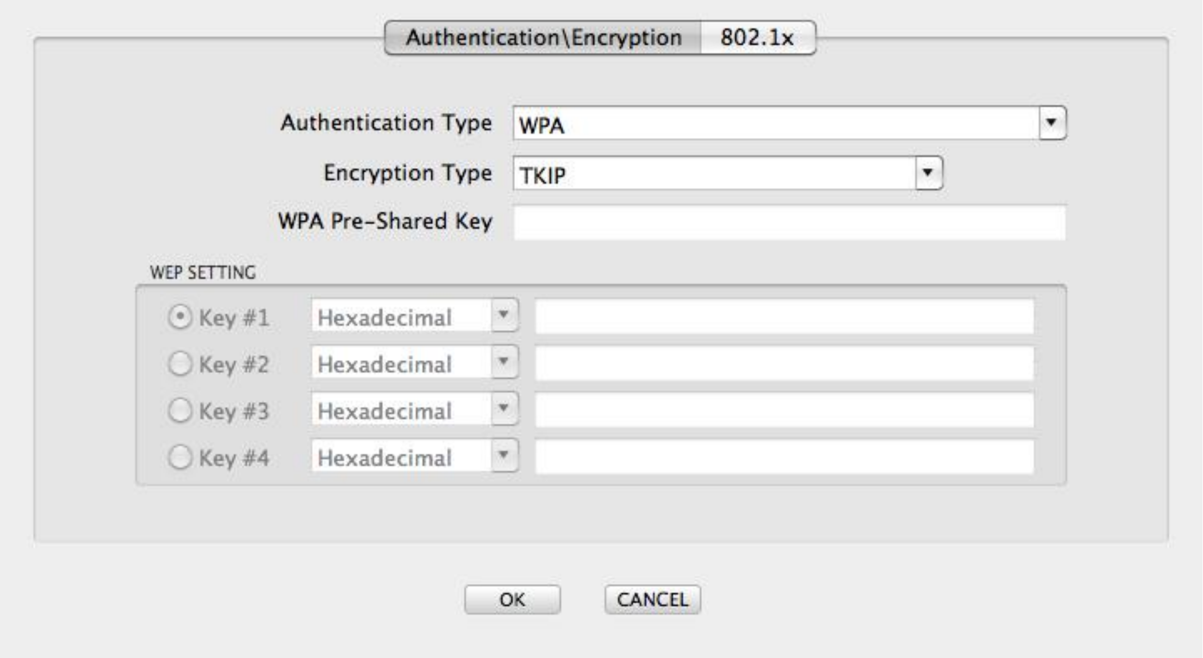
- PEAP
  - EAP-MSCHAP v2
  - EAP-TLS
  - Generic Token Card
- TLS
- TTLS
  - CHAP
  - MS-CHAP
  - MS-CHAP-V2
  - PAP
  - EAP-MD5
  - MD5-Challenge

1.3 Other

- WPA-PSK/TKIP
- WPA-PSK/AES
- WPA2-PSK/TKIP
- WPA2-PSK/AES
- LEAP (default on Cisco AP)

2 802.1x SETTING

The 802.1x setting dialog box is opened when the Authentication/Encryption type is set to WPA/TKIP, WPA/AES, WPA2/TKIP, WPA2/AES or open/WEP with checked 802.1x. The subsequent figures show the dialog box with different settings.



Authentication Type: WPA

Encryption Type: TKIP

WPA Pre-Shared Key:

WEP SETTING

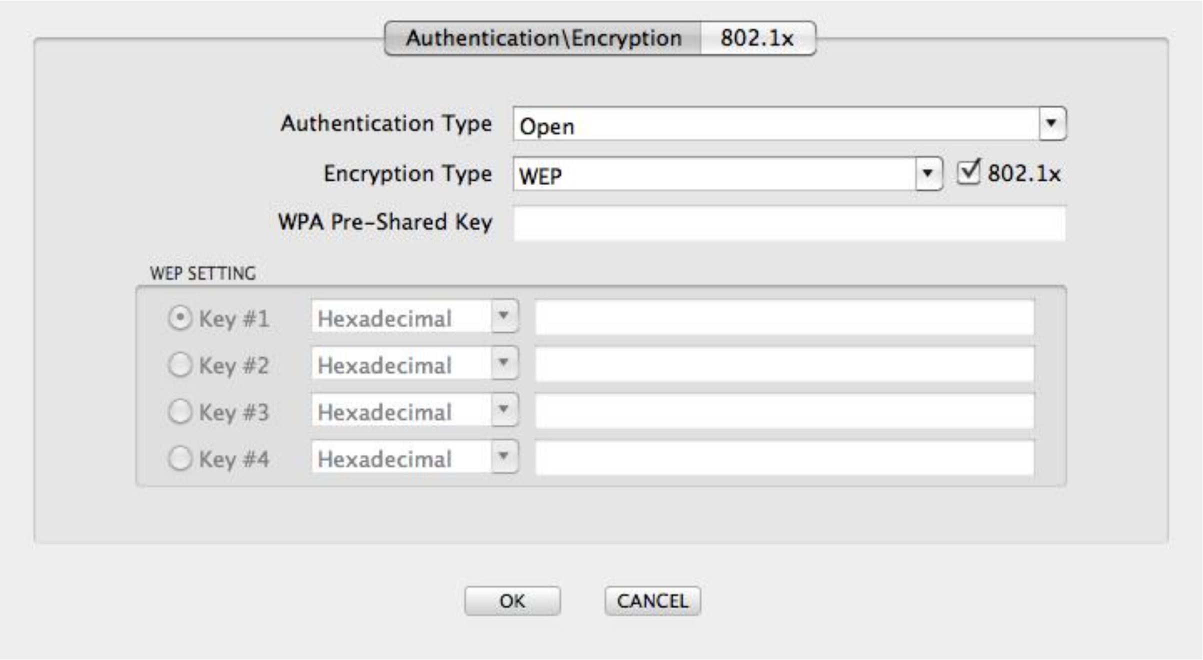
● Key #1 Hexadecimal

○ Key #2 Hexadecimal

○ Key #3 Hexadecimal

○ Key #4 Hexadecimal

Figure 1 802.1x Setting Dialog Box - Authentication Type = WPA/WPA2



Authentication Type: Open

Encryption Type: WEP ☑ 802.1x

WPA Pre-Shared Key:

WEP SETTING

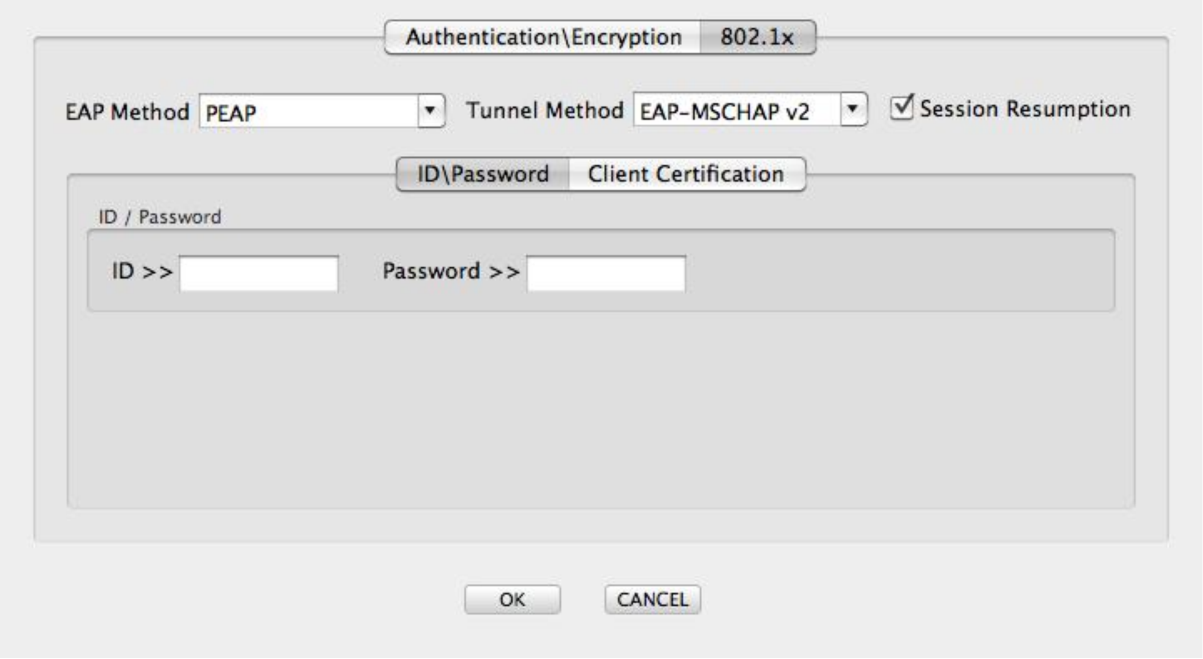
● Key #1 Hexadecimal

○ Key #2 Hexadecimal

○ Key #3 Hexadecimal

○ Key #4 Hexadecimal

Figure 2 802.1x Setting Dialog Box - Authentication Type = Open, Encryption Type = WEP, 802.1x checked



EAP Method: PEAP

Tunnel Method: EAP-MSCHAP v2

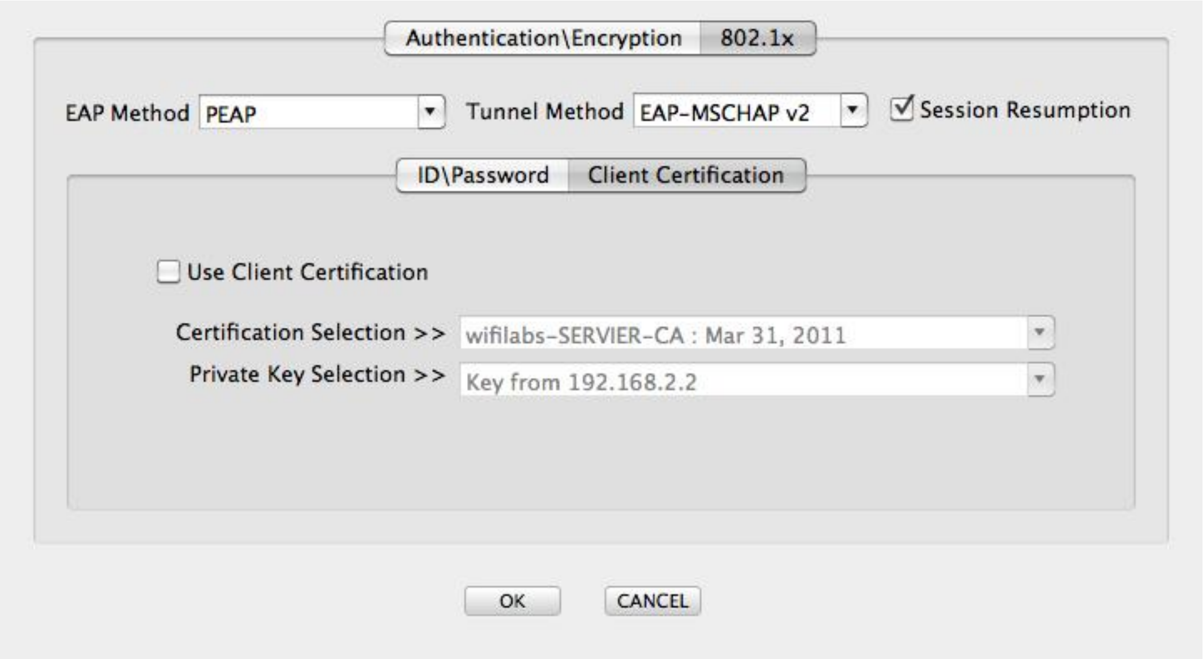
☑ Session Resumption

ID / Password

ID >>

Password >>

Figure 3 802.1x setting page overview



EAP Method: PEAP

Tunnel Method: EAP-MSCHAP v2

☑ Session Resumption

□ Use Client Certification

Certification Selection >> wifilabs-SERVIER-CA : Mar 31, 2011

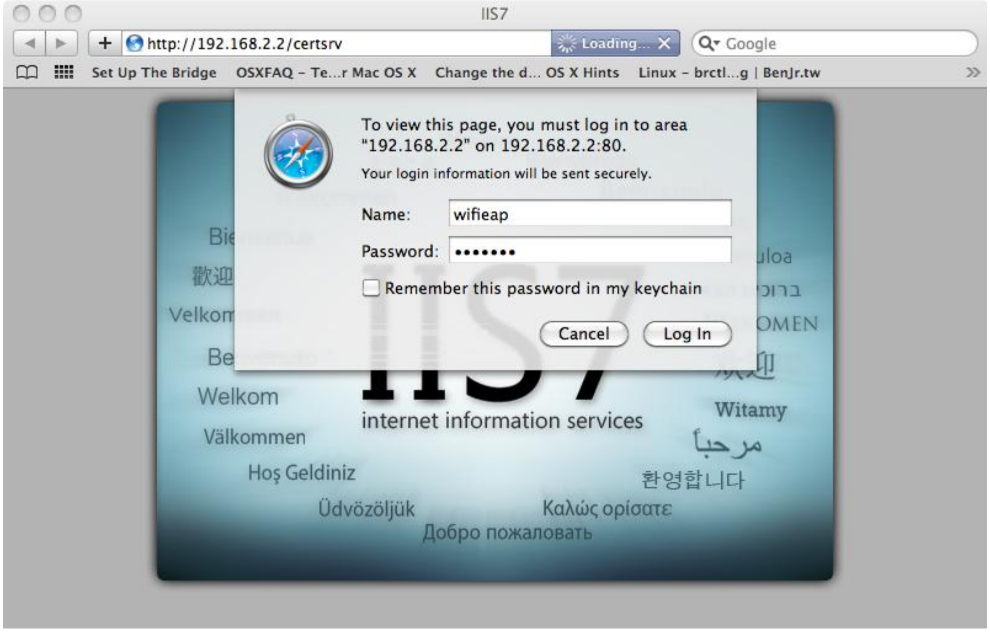
Private Key Selection >> Key from 192.168.2.2

Figure 4 802.1x setting page overview 2

3 INSTALL CERTIFICATE

The Install certificate procedure on the Mac OS X is different from the install certificate procedure on the Windows OS. When authentication with the certificated server is successful on the Windows OS, IE automatically installs the certificate on the OS. On Mac OS X, the certificated server sends a certificate as a file and the user must install it manually. Please obey the subsequent steps to complete the installation of the certificate on Mac OS X.

1. Login to the certificated server. The Keychain Access will keep a private key and public key if the login is successful. The keys are shown in step 8.



IIS7
http://192.168.2.2/certsrv
Loading...
Google
Set Up The Bridge
OSXFAQ – Te...r Mac OS X
Change the d... OS X Hints
Linux – brctl...g | BenJr.tw

To view this page, you must log in to area "192.168.2.2" on 192.168.2.2:80.

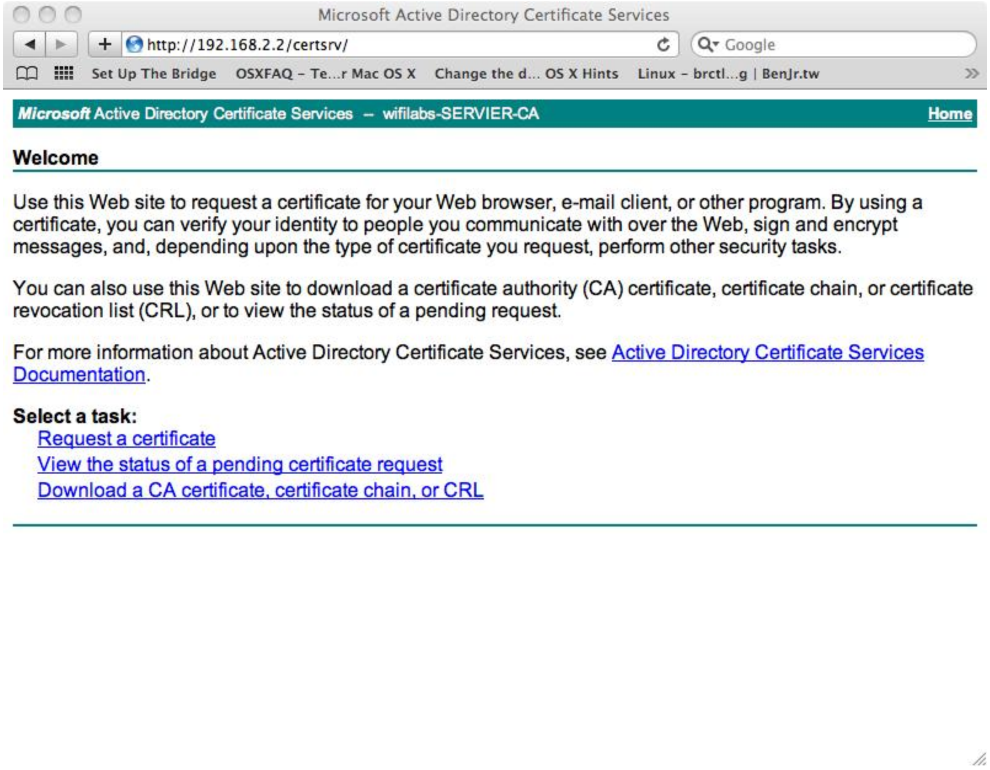
Your login information will be sent securely.

Name: wifieap

Password: •••••••

□ Remember this password in my keychain

2. Click “Request a certificate”.



Microsoft Active Directory Certificate Services
http://192.168.2.2/certsrv/
Google
Set Up The Bridge
OSXFAQ – Te...r Mac OS X
Change the d... OS X Hints
Linux – brctl...g | BenJr.tw

Microsoft Active Directory Certificate Services -- wifilabs-SERVIER-CA Home

Welcome

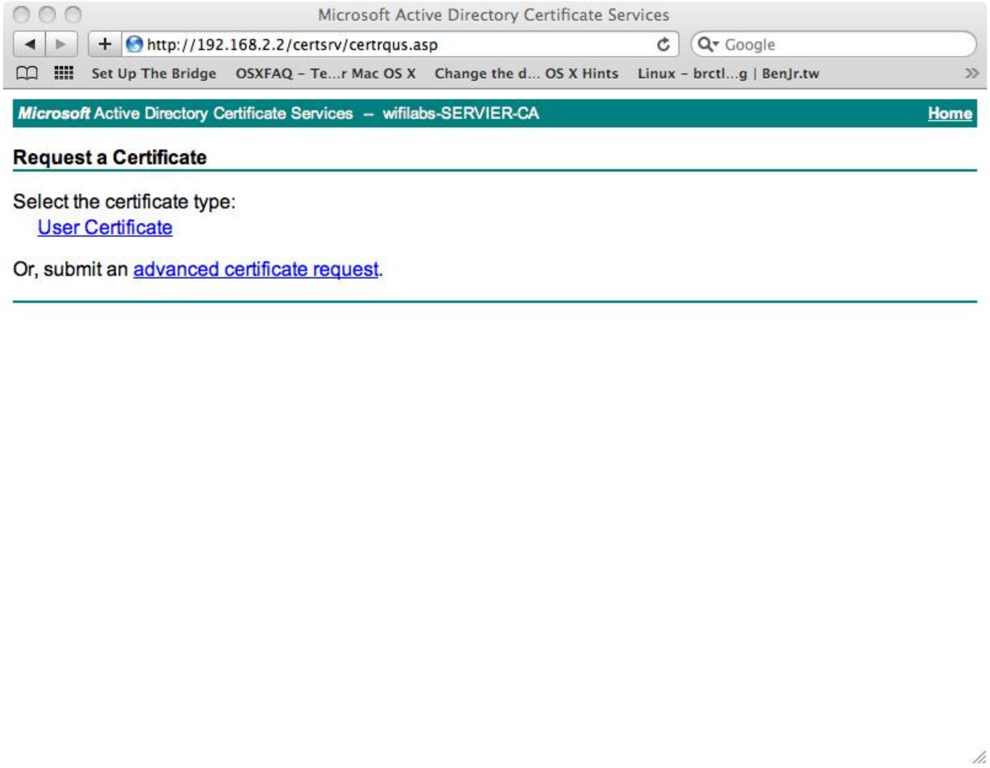
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

3. Click “User Certificate”.



Microsoft Active Directory Certificate Services
http://192.168.2.2/certsrv/certrqus.asp
Google
Set Up The Bridge
OSXFAQ – Te...r Mac OS X
Change the d... OS X Hints
Linux – brctl...g | BenJr.tw

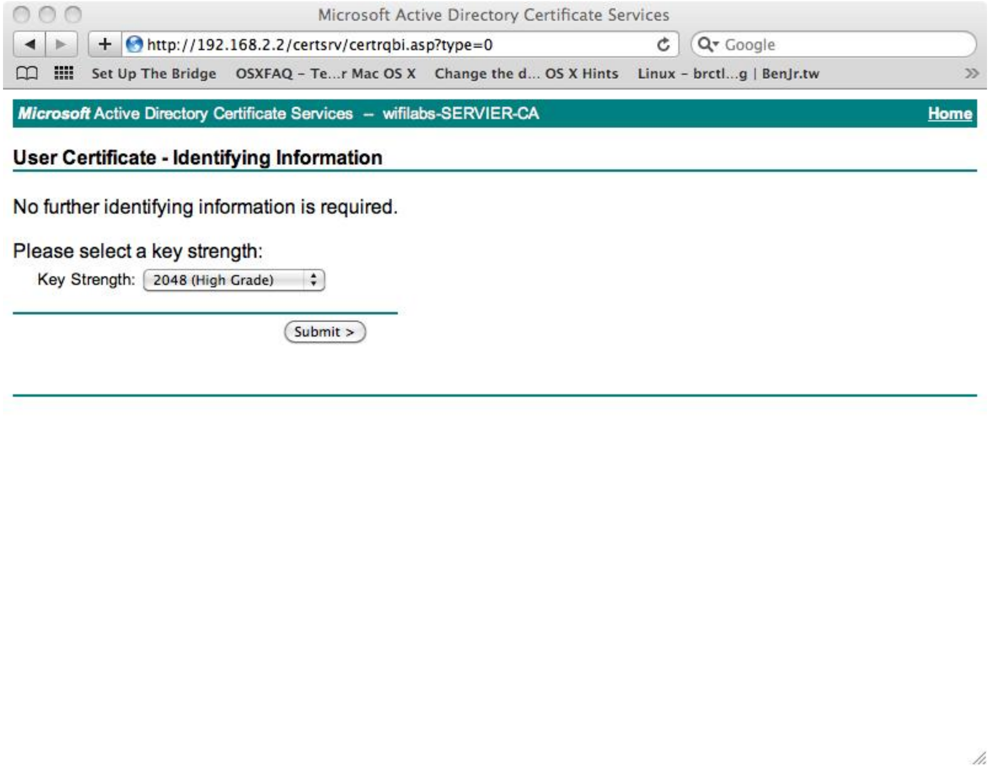
Microsoft Active Directory Certificate Services -- wifilabs-SERVIER-CA Home

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

4. Click "Submit" without changing anything.



Microsoft Active Directory Certificate Services
http://192.168.2.2/certsrv/certrqbi.asp?type=0
Google
Set Up The Bridge
OSXFAQ – Te...r Mac OS X
Change the d... OS X Hints
Linux – brctl...g | BenJr.tw
Home

Microsoft Active Directory Certificate Services – wifilabs-SERVIER-CA

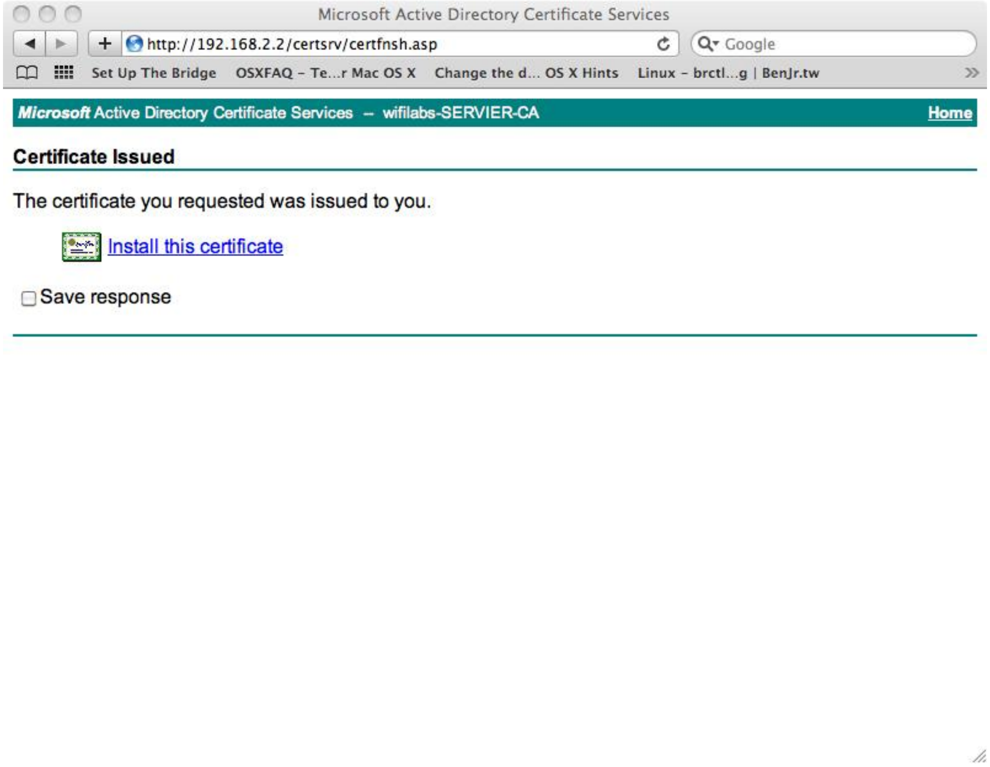
User Certificate - Identifying Information

No further identifying information is required.

Please select a key strength:

Key Strength: 2048 (High Grade)

5. Click "Install the certificate".



Microsoft Active Directory Certificate Services
http://192.168.2.2/certsrv/certfnsh.asp
Google
Set Up The Bridge
OSXFAQ – Te...r Mac OS X
Change the d... OS X Hints
Linux – brctl...g | BenJr.tw
Home

Microsoft Active Directory Certificate Services – wifilabs-SERVIER-CA

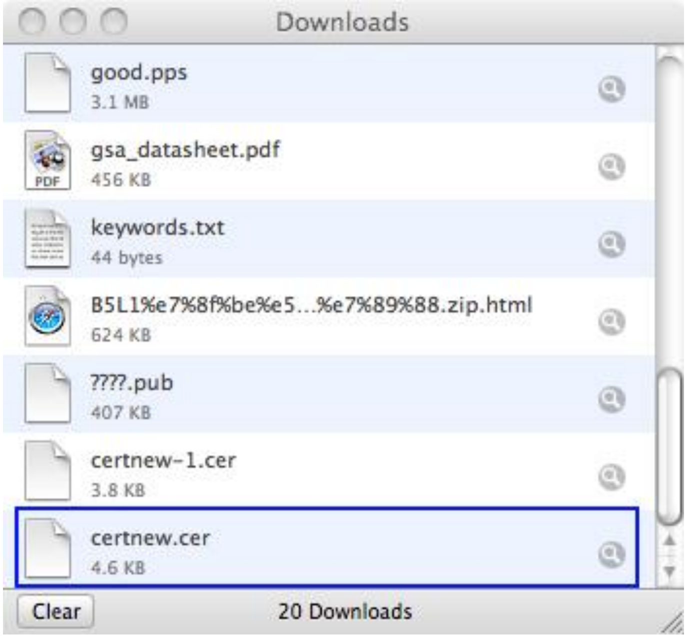
Certificate Issued

The certificate you requested was issued to you.

Install this certificate

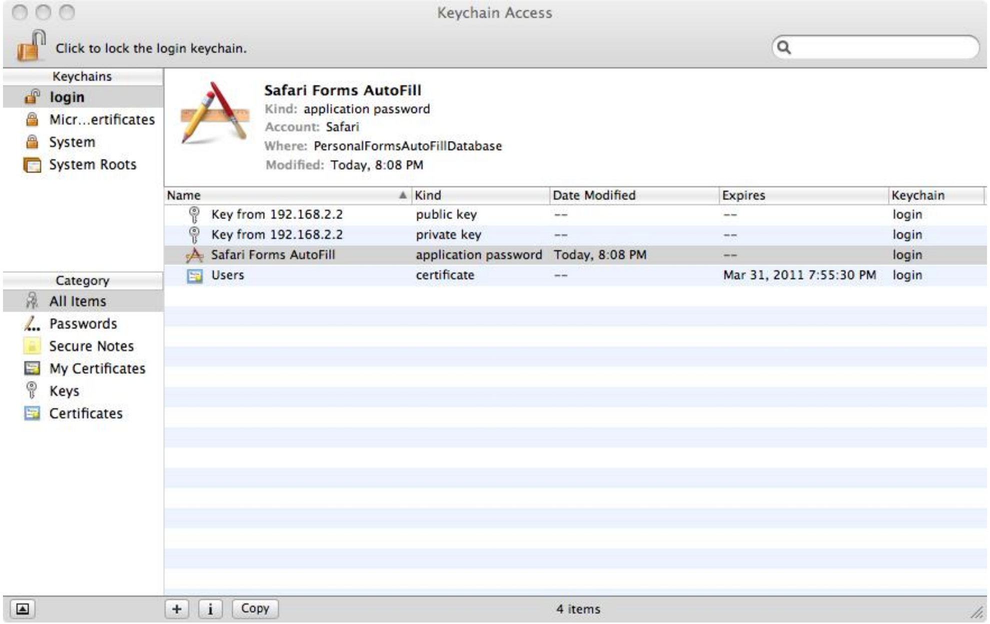
□ Save response

6. A certificate is sent from the certificated server. Find the certificate and double click it to install it to the Mac OS X Keychain Access.



good.pps	3.1 MB
gsa_datasheet.pdf	456 KB
keywords.txt	44 bytes
B5L1%e7%8f%be%e5...%e7%89%88.zip.html	624 KB
????.pub	407 KB
certnew-1.cer	3.8 KB
certnew.cer	4.6 KB

7. A private key, a public key and a certificate are now put in Keychain Access. The private key and the certificate are used to connect with an 802.1x AP.



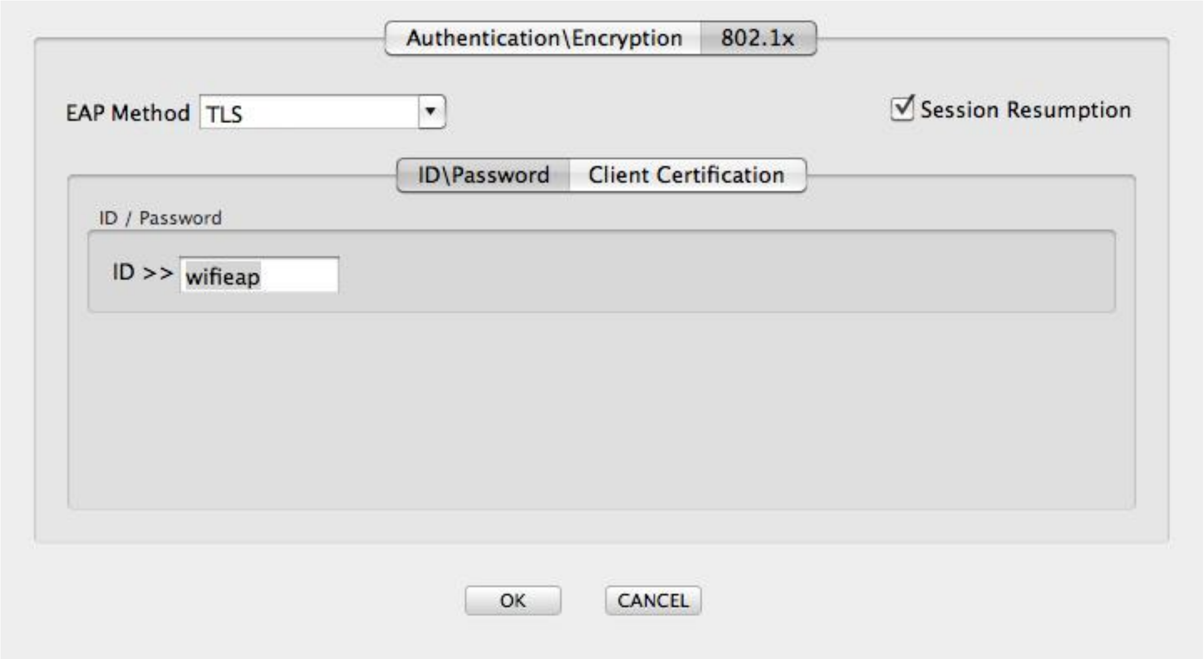
Safari Forms AutoFill
Kind: application password
Account: Safari
Where: PersonalFormsAutoFillDatabase
Modified: Today, 8:08 PM

Name	Kind	Date Modified	Expires	Keychain
Key from 192.168.2.2	public key	--	--	login
Key from 192.168.2.2	private key	--	--	login
Safari Forms AutoFill	application password	Today, 8:08 PM	--	login
Users	certificate	--	Mar 31, 2011 7:55:30 PM	login

4 TLS SETTING SAMPLE

A TLS connected setting sample is subsequently shown.

1. Key-in the ID.

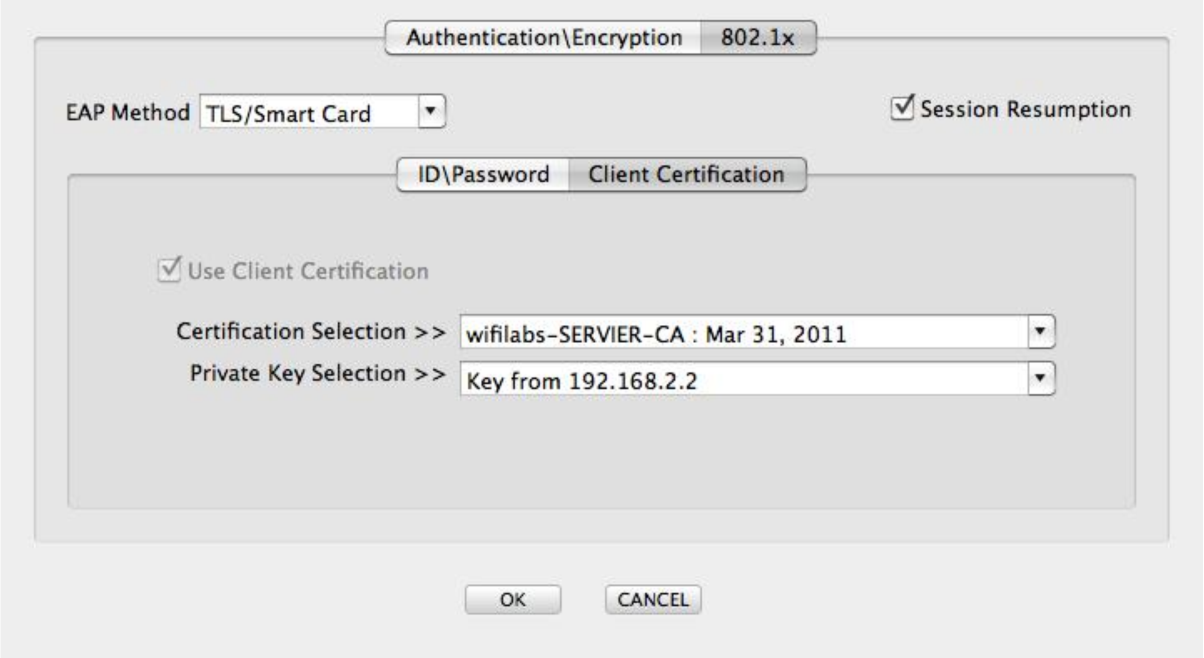


EAP Method TLS

☑ Session Resumption

ID >> wifieap

2. Certification Selection and Private Key Selection. The correct private key and certificate must be used. There may be many pairs, but only one private key can decrypt the related certificate.



EAP Method TLS/Smart Card

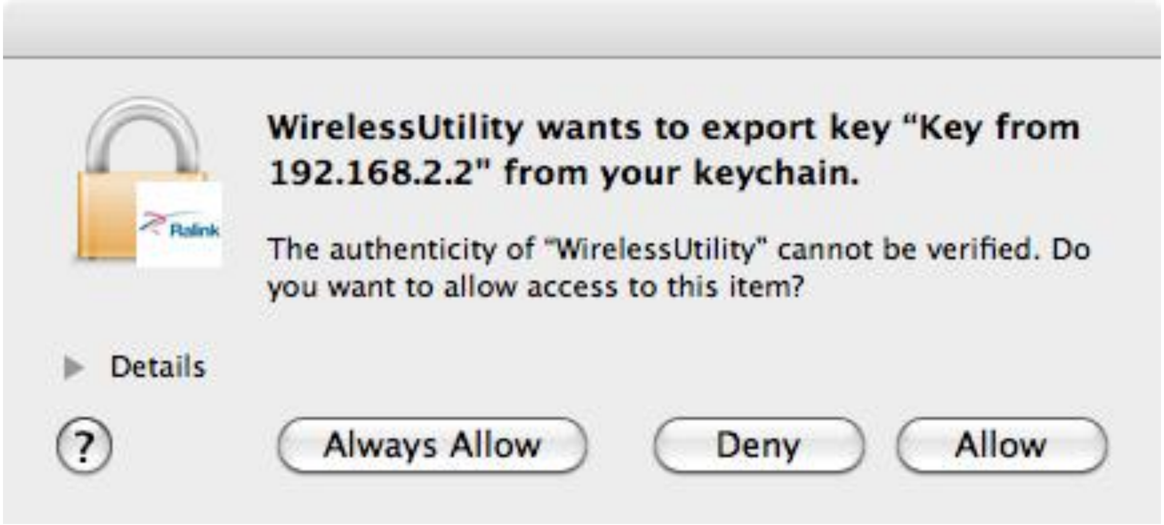
☑ Session Resumption

☑ Use Client Certification

Certification Selection >> wifilabs-SERVIER-CA : Mar 31, 2011

Private Key Selection >> Key from 192.168.2.2

3. Click the “Always Allow” button. It will not be shown next time.



WirelessUtility wants to export key “Key from 192.168.2.2" from your keychain.

The authenticity of "WirelessUtility" cannot be verified. Do you want to allow access to this item?

5 DOCUMENT REVISION HISTORY

Version	Date	Change
1.0	April. 1, 2010	Initial release