To replace the HTTP certification for DFL firewall

[Topology]

PC----------SW------(lan1)DFL
CA/DNS server--/

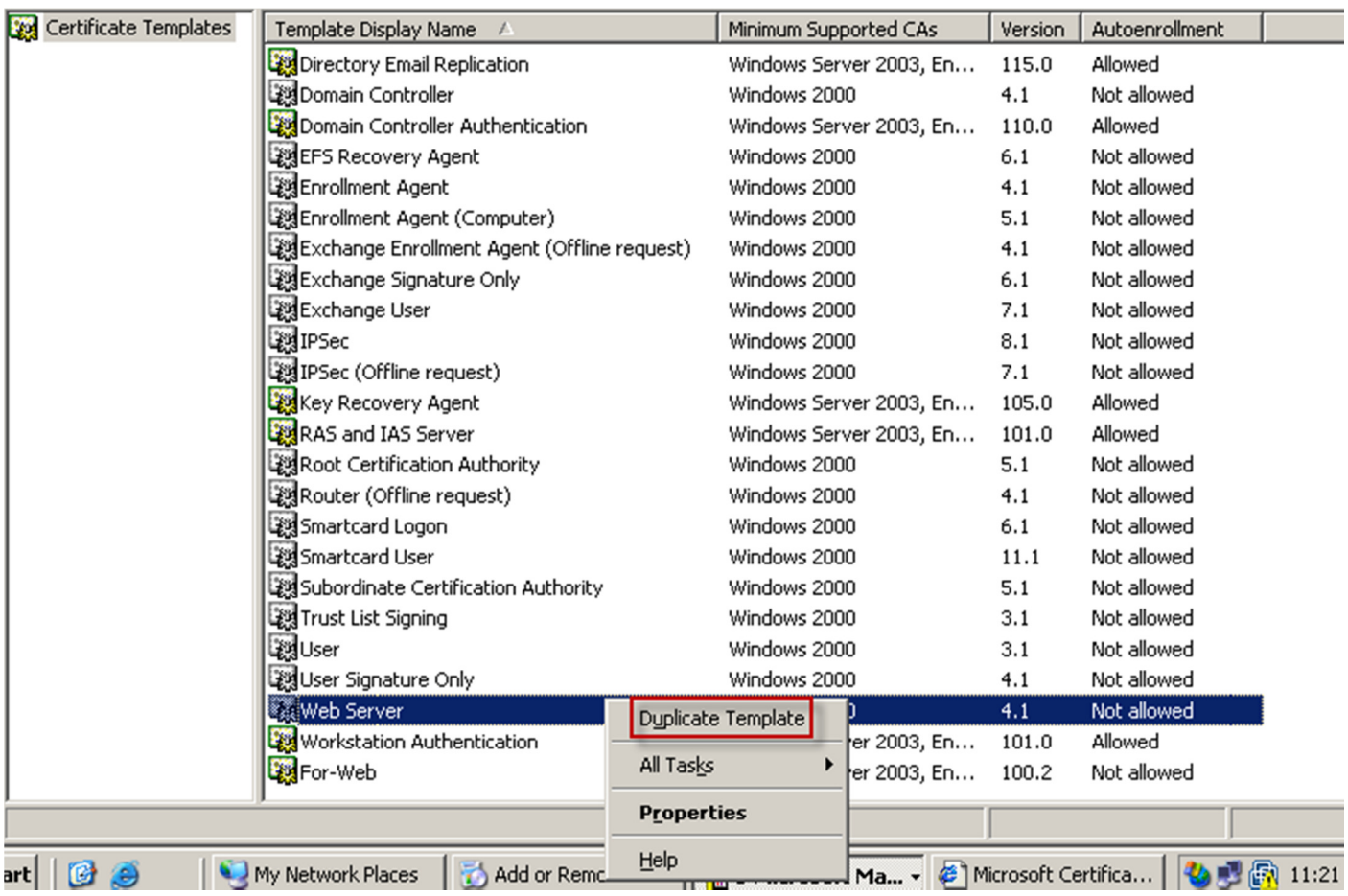
############################
CA/DNS server settings:
IP address: 192.168.1.200

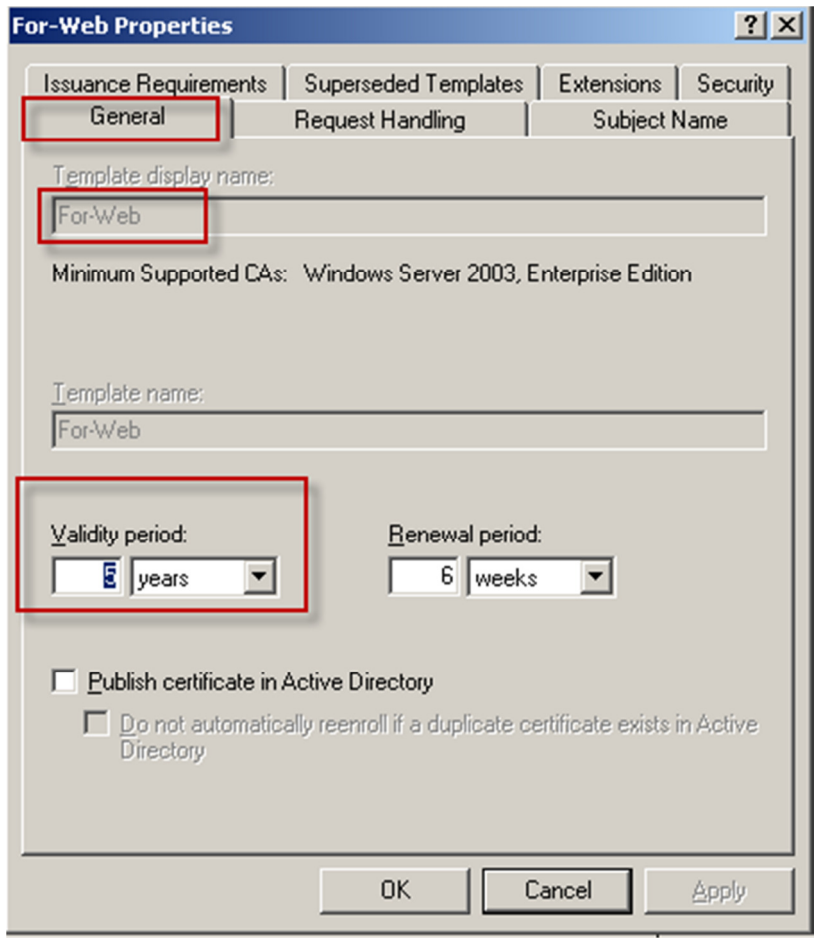
PC IP address: 192.168.1.58
PC DNS address: 192.168.1.200

DFL LAN1 IP address: 192.168.1.1
############################

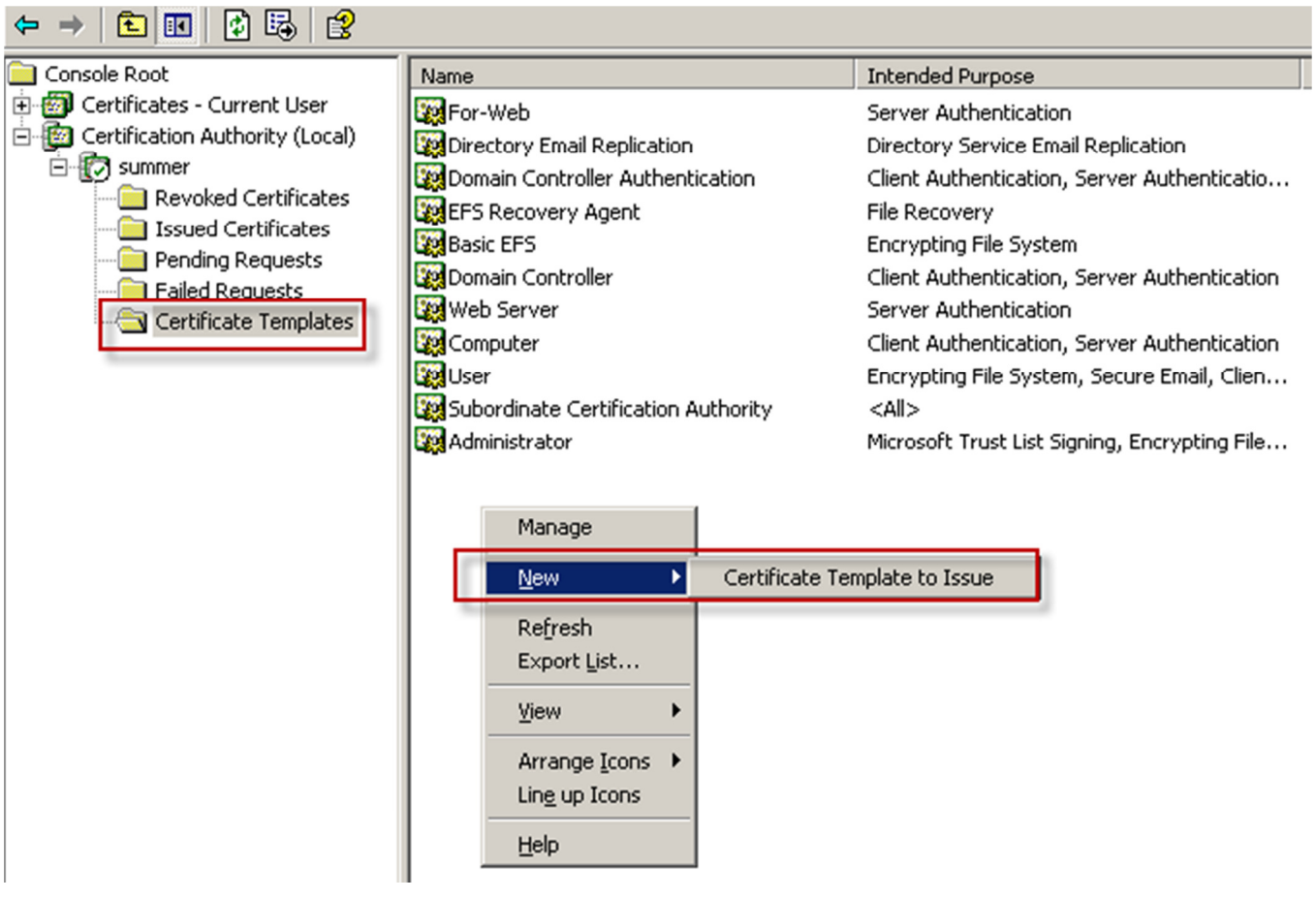
[Key points]
1. DFL needs to be installed a self-certification(including private and public key)
2. PC needs to be installed the CA-certification(Public key only) in the "Trusted certification authorities"

1. Build up a windows CA server. (Brief installation)
   a. Install DNS server
   b. Issue the command of "dcpromo".
   c. Install IIS
   d. Install CA server
   e. Create a CA template, name the template and allow its private key is exportable.

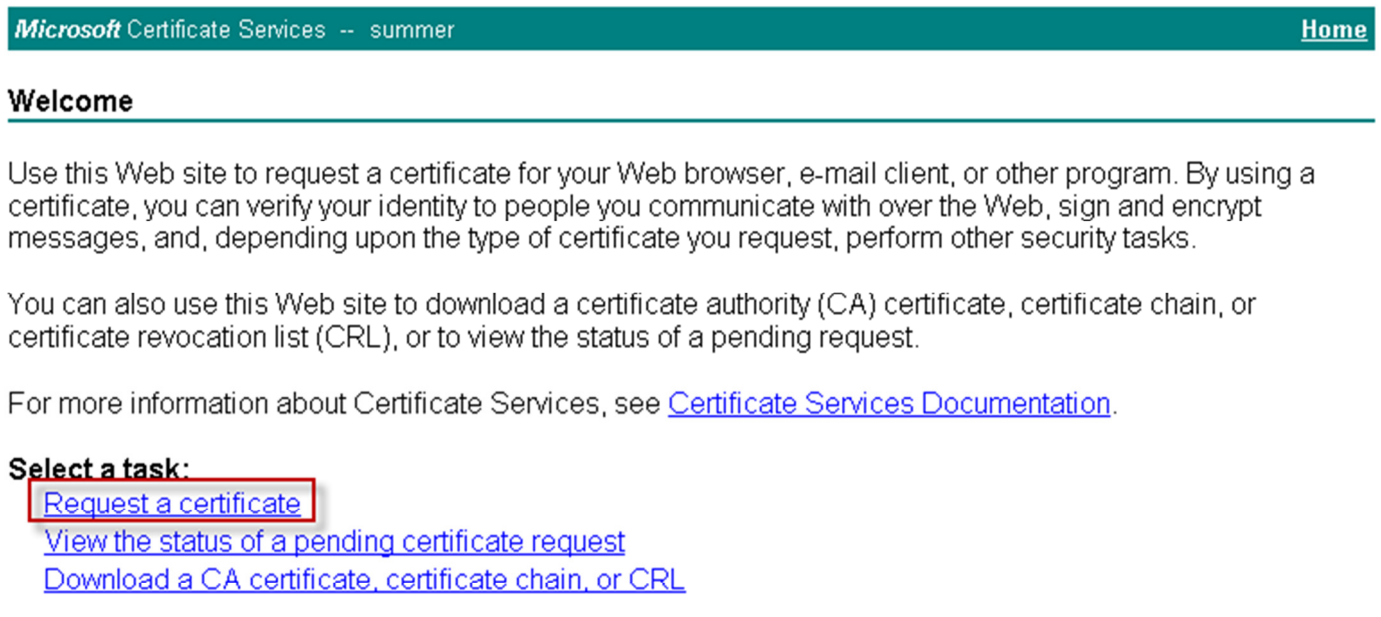




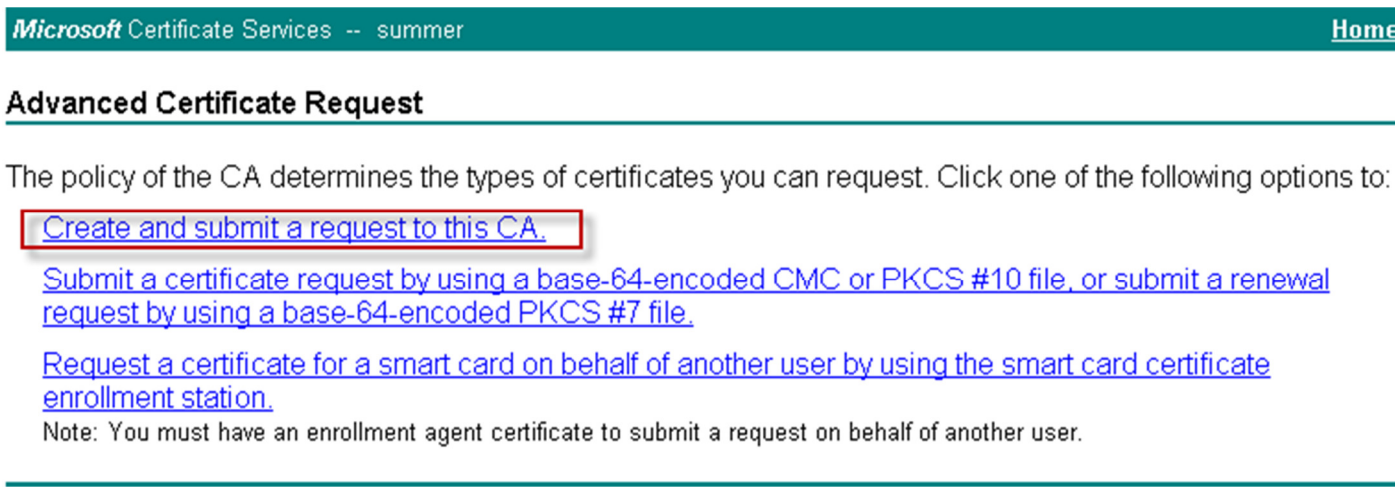
f. Publish the CA template(For-Web) created at step “e”.

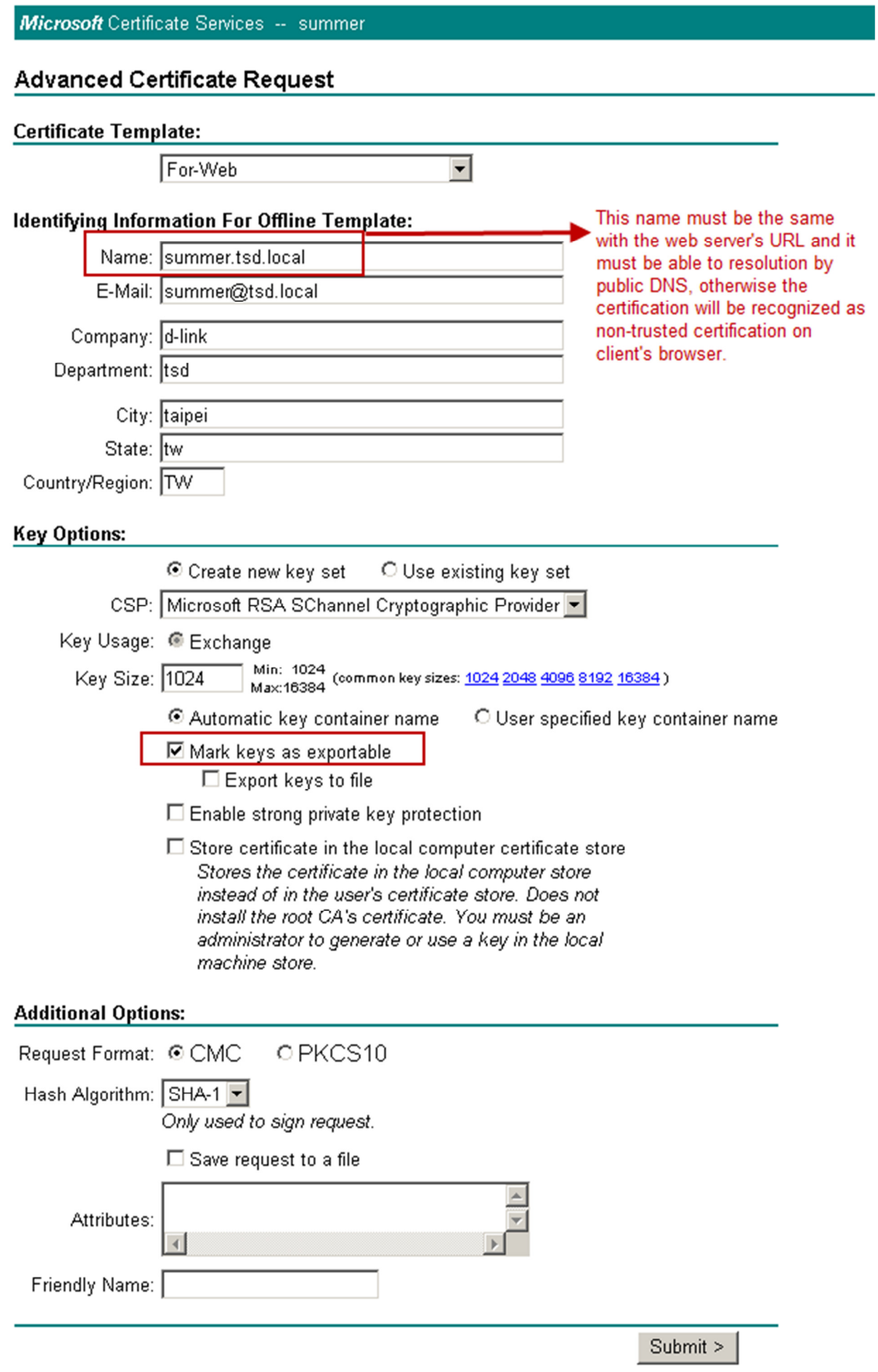


2. To apply a self-certification and download the CA server's certification.
    a. Connect to the web certificate service of CA server and request a certificate.

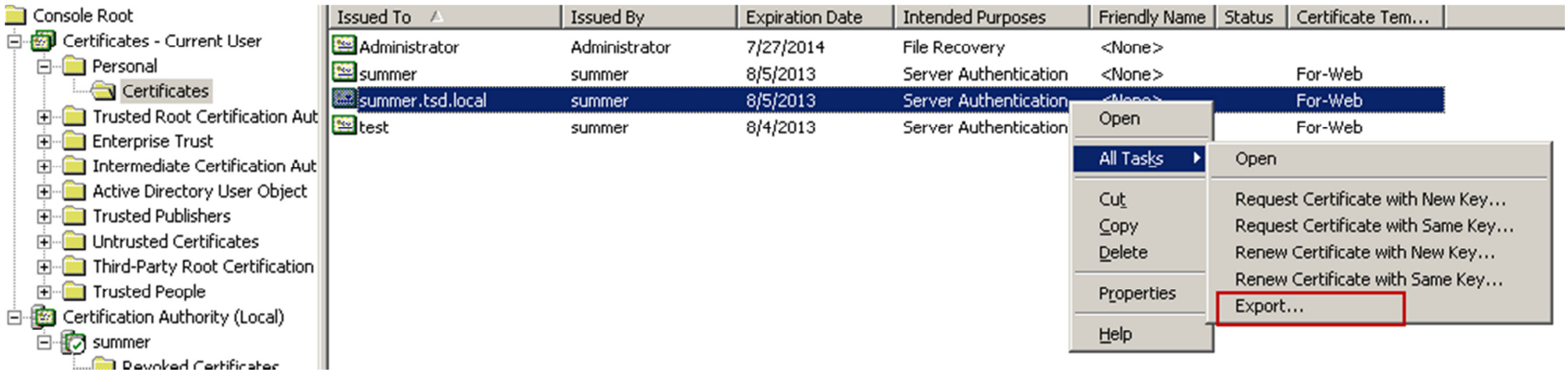


    b. Go to "advanced certificate request"

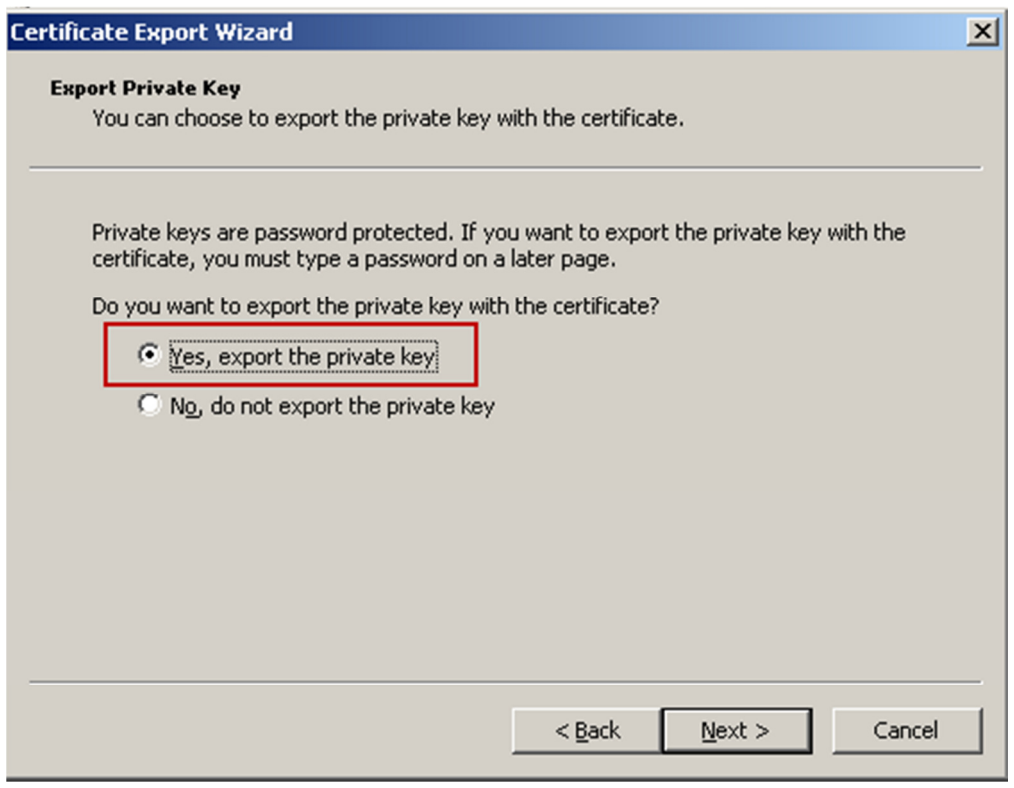


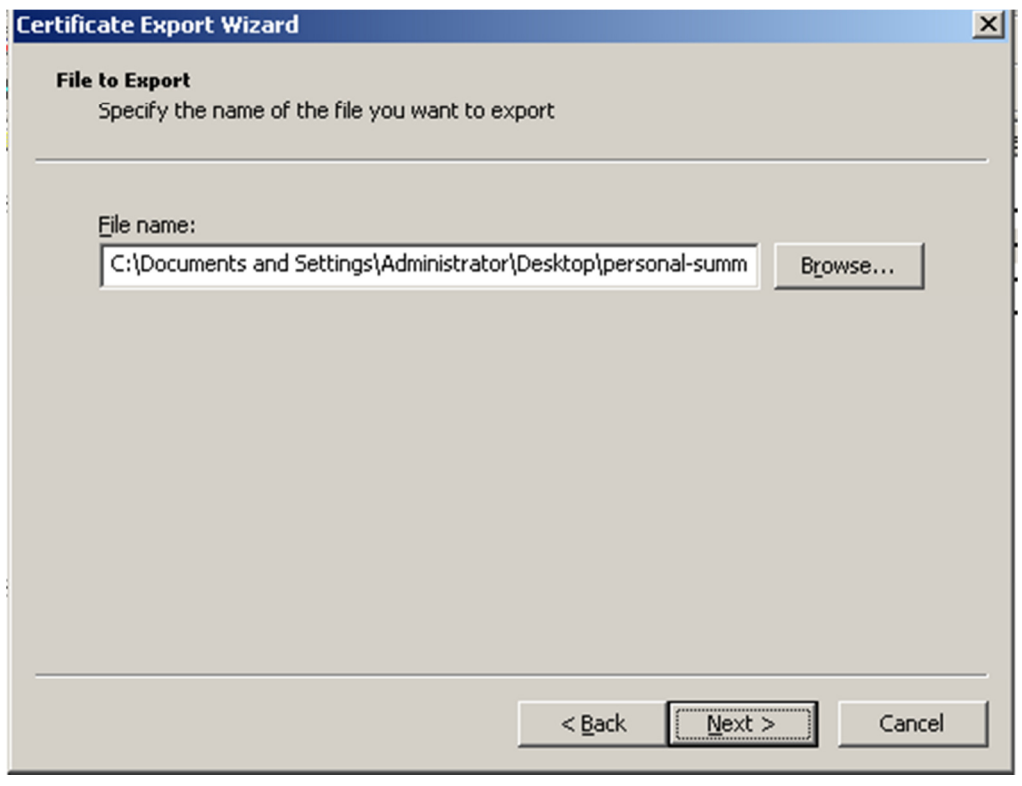


c. Export the self-certification.



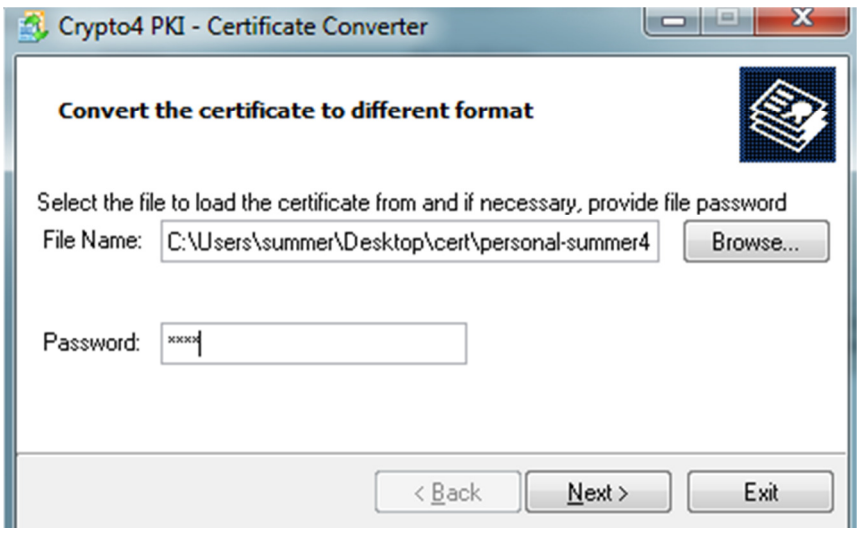

Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

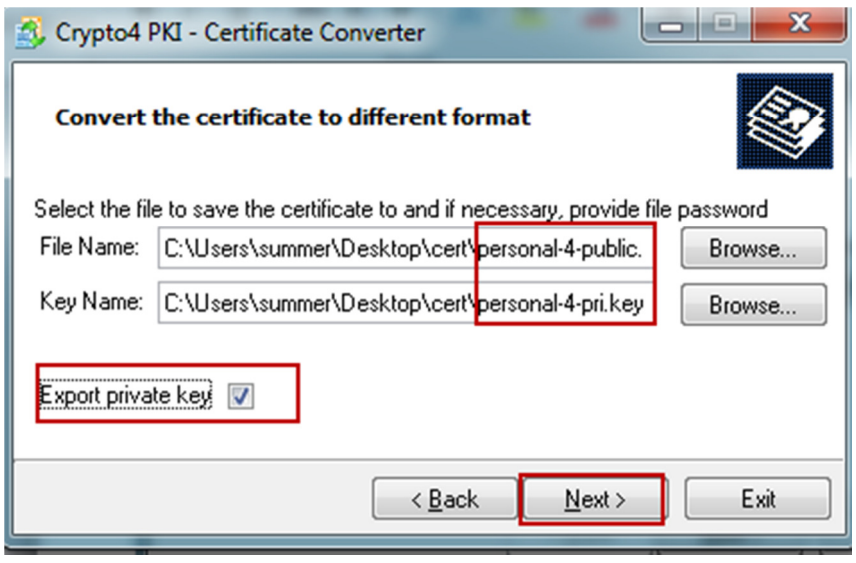

Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
No, do not export the private key
< Back
Next >
Cancel


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
C:\Documents and Settings\Administrator\Desktop\personal-summ
Browse...
< Back
Next >
Cancel

d. The self-certification exports from Microsoft windows will be the format of “PFX”, we have to convert the file to the format of x.509 by the tool of “CryptTo4”


Package





e. Upload the self-certification to DFL.

Certificate

An X. 509 certificate is used to authenticate a VPN client or gateway when establishing an IPsec tunnel.

General

General

Name: for-web4

Disable CRLs (Certificate Revocation Lists)

Certificate Information

Certificate type: N/A

Public Key Algorithm: Unknown

Options

Don't upload anything

Don't upload anything right now

Upload X.509 Certificate

Upload a previously created X.509 Certificate, along with its private key.

Upload a remote certificate

Upload a certificate belonging to a remote peer or a CA server

Upload X.509 certificate

Upload a previously created X.509 Certificate

General

C:\Users\summer\Desktop\cert\personal-4-public.cer Browse...

Upload X.509 certificate

Upload X.509 private key

Now upload a private key matching the newly uploaded certificate

General

C:\Users\summer\Desktop\cert\personal-4-pri.key Browse...

Upload X.509 private key

Home | Configuration | Tools | Status | Maintenance

- DFL-2560G
  - System
    - Date and Time
    - DNS
    - Remote Management
    - Log and Event Receivers
    - DHCP
    - High Availability
    - Misc. Clients
    - Hardware Monitoring

Remote Management

Setup and configure methods and permissions for remote management of this system.

Add | Advanced Settings

#	Name	Type	Mode	Interface	Network
1	RemoteMgmtHTTP	HTTP/HTTPS Management	Admin: HTTPS	lan1	lan1net

Remote Management Settings

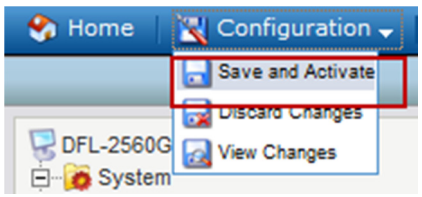
Setup and configure methods and permissions for remote management of this system.

General

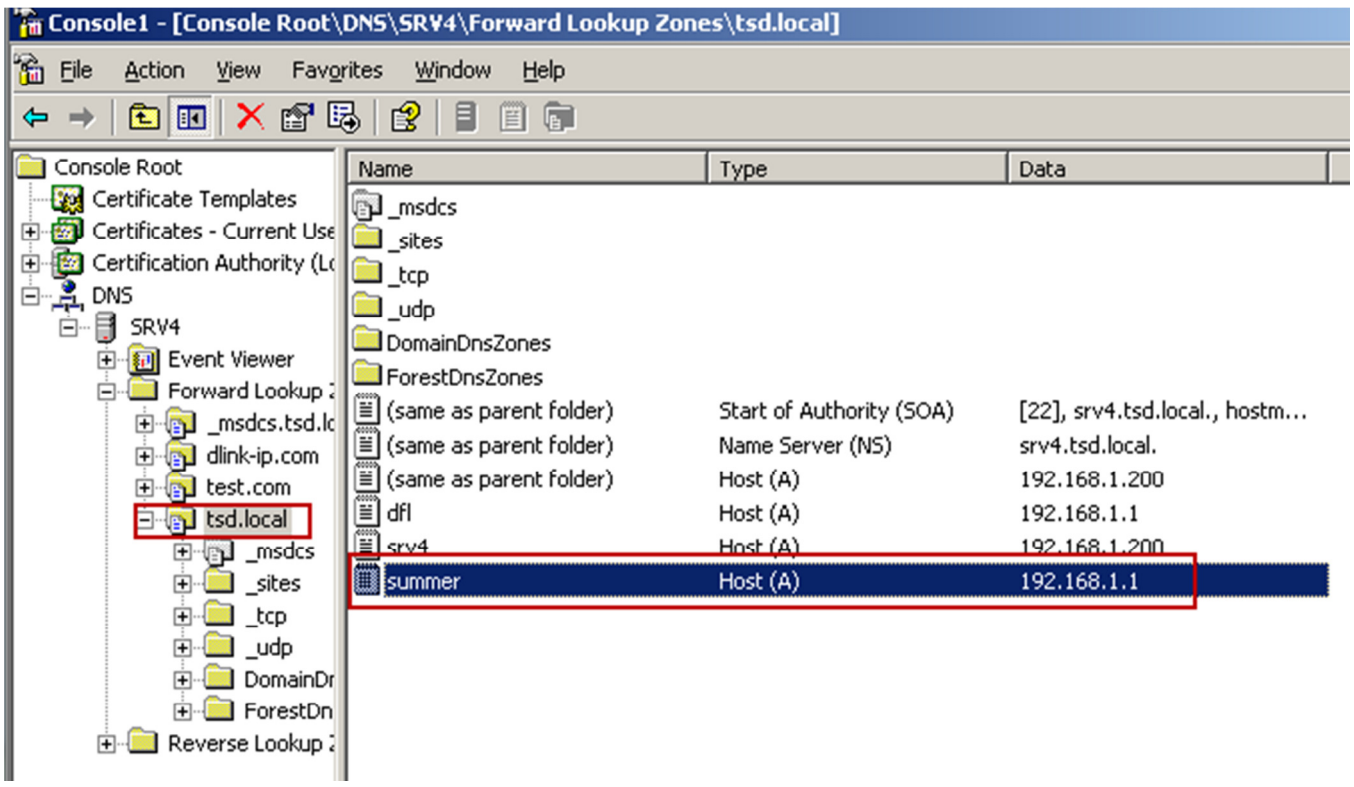
General

SSH Before Rules:	☑	Enable SSH traffic to the security gateway regardless of configured IP Rules.
WebUI Before Rules:	☑	Enable HTTP(S) traffic to the security gateway regardless of configured IP Rules.
WebUI Idle timeout:	900	Number of seconds of inactivity until the HTTP(S) session is closed.
Local Console Timeout:	900	Number of seconds of inactivity until the local console user is automatically logged out.
Validation Timeout:	30	Specifies the amount of seconds to wait for the administrator to log in before reverting to the previous configuration.
WebUI HTTP port:	80	Specifies the HTTP port for the web user interface.
WebUI HTTPS port:	443	Specifies the HTTP(S) port for the web user interface.
HTTPS Certificate:	for-web4	Specifies which certificate to use for HTTPS traffic. Only RSA certificates are supported.

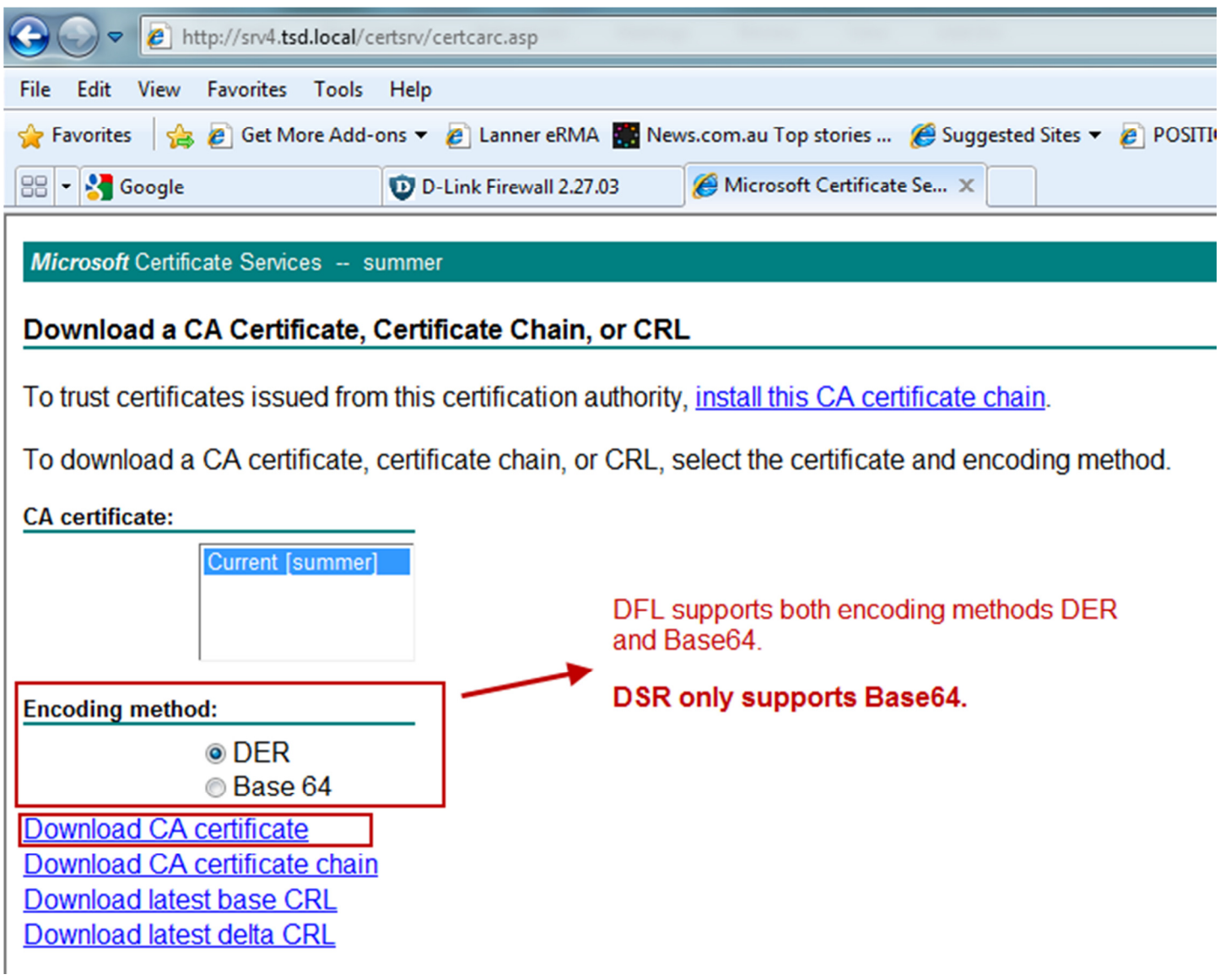
SNMP

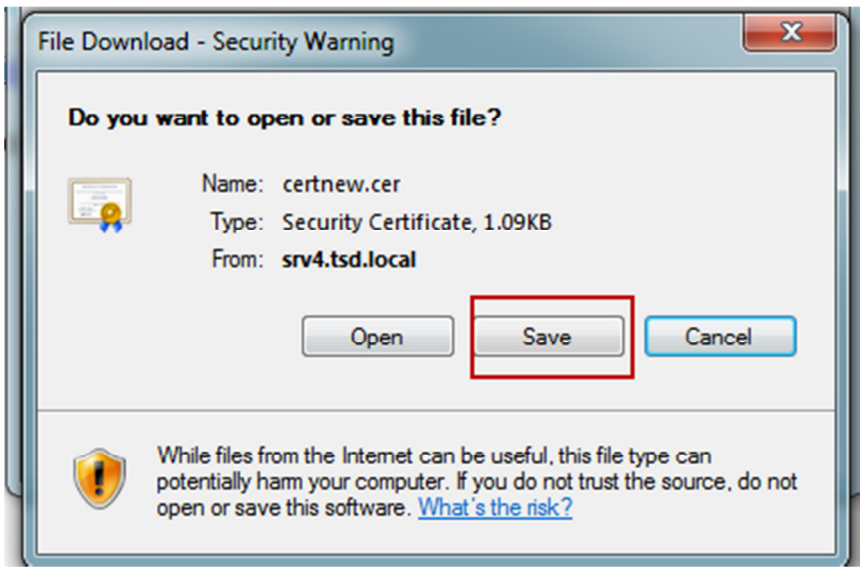


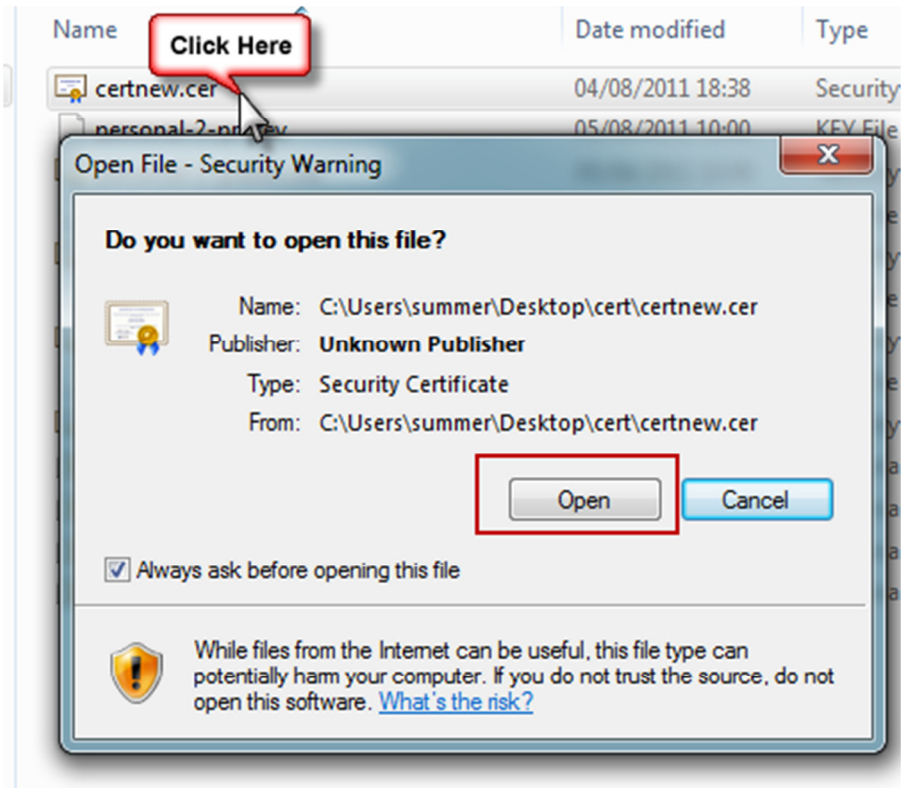
f. On the DNS server, make sure the DNS resolution is work without problem.

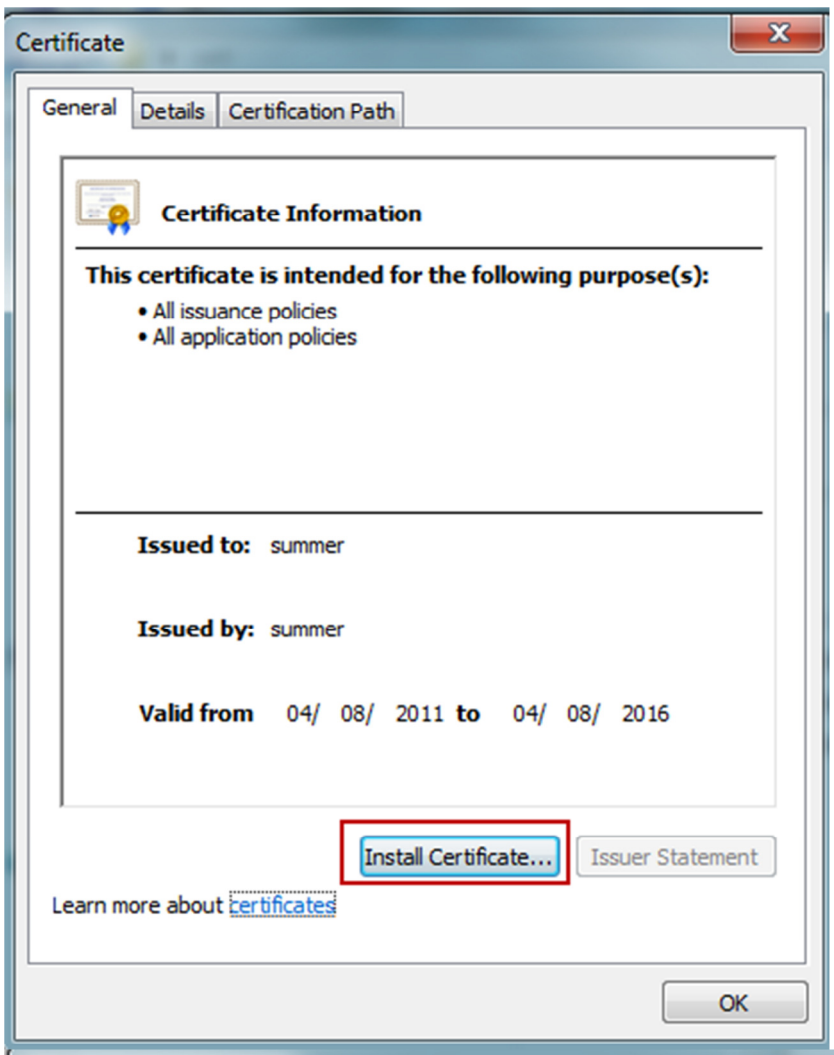


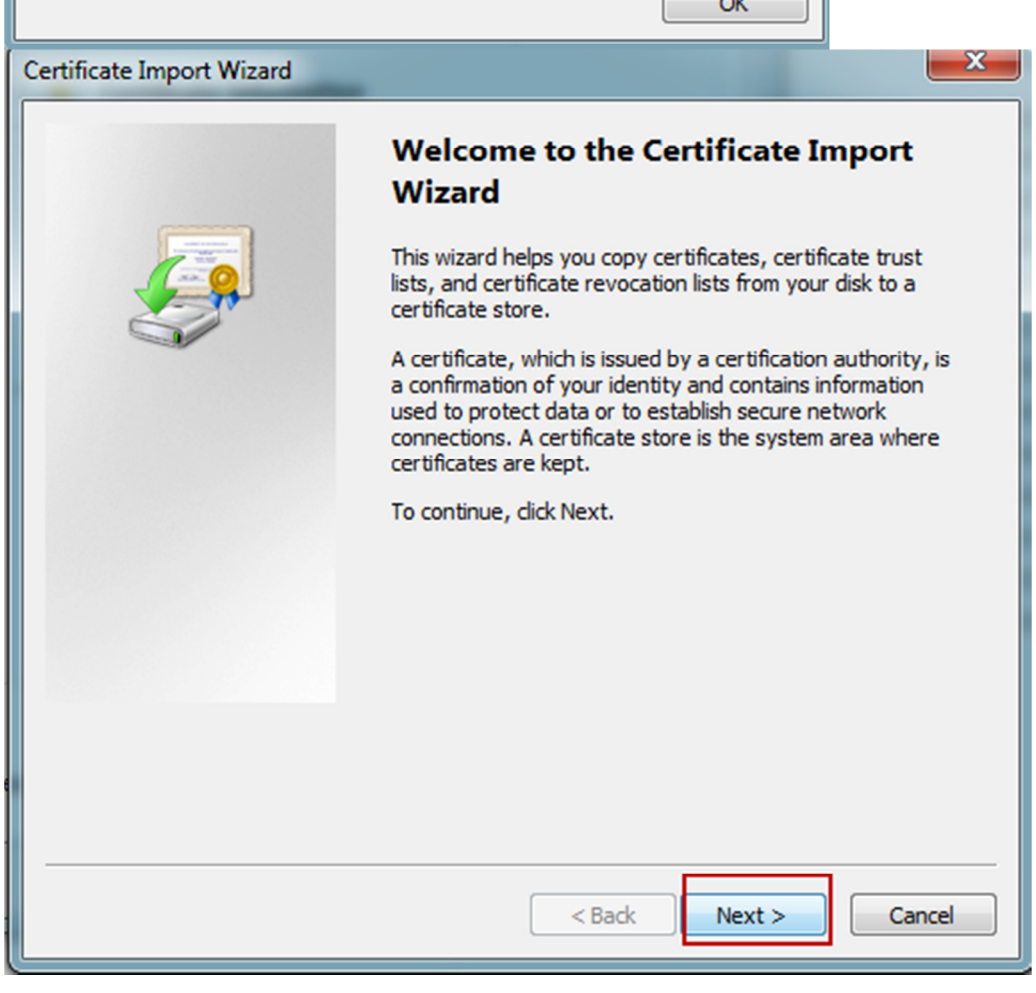
g. PC downloads CA server's certification, and install it into "trusted root certification authorities".

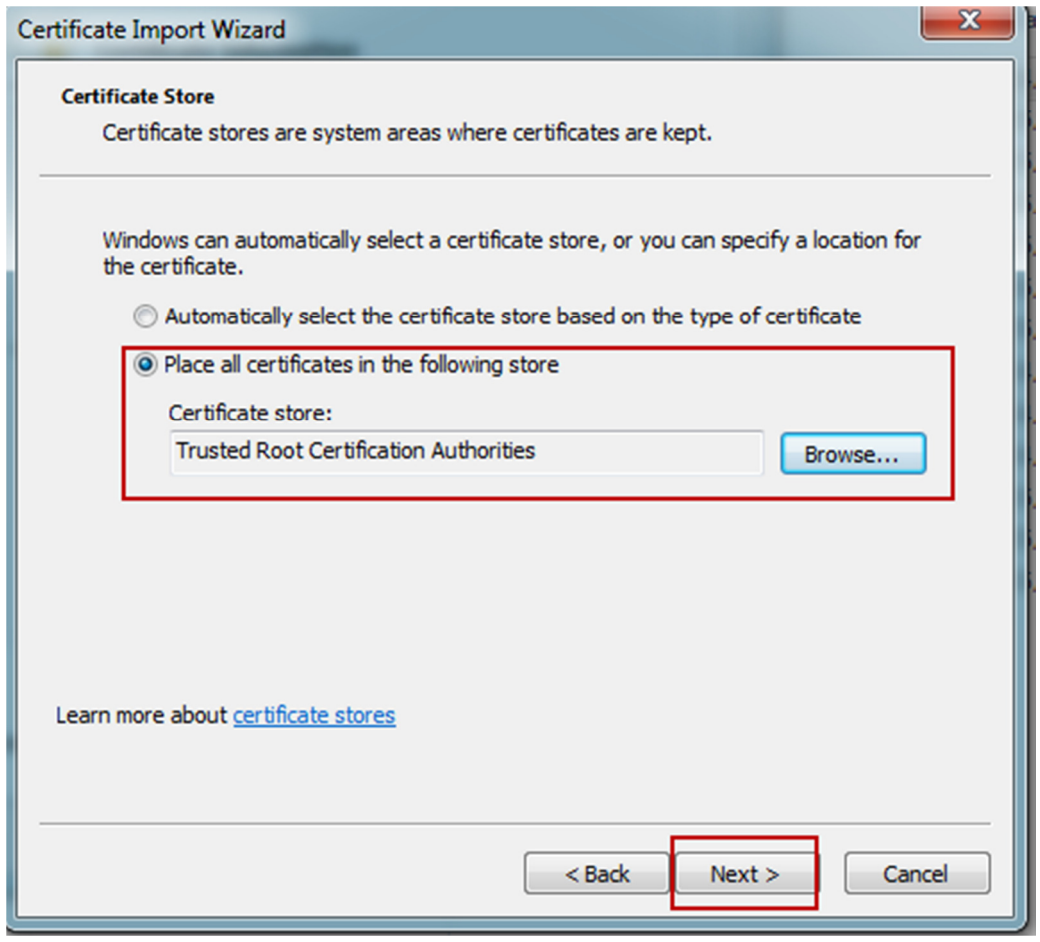




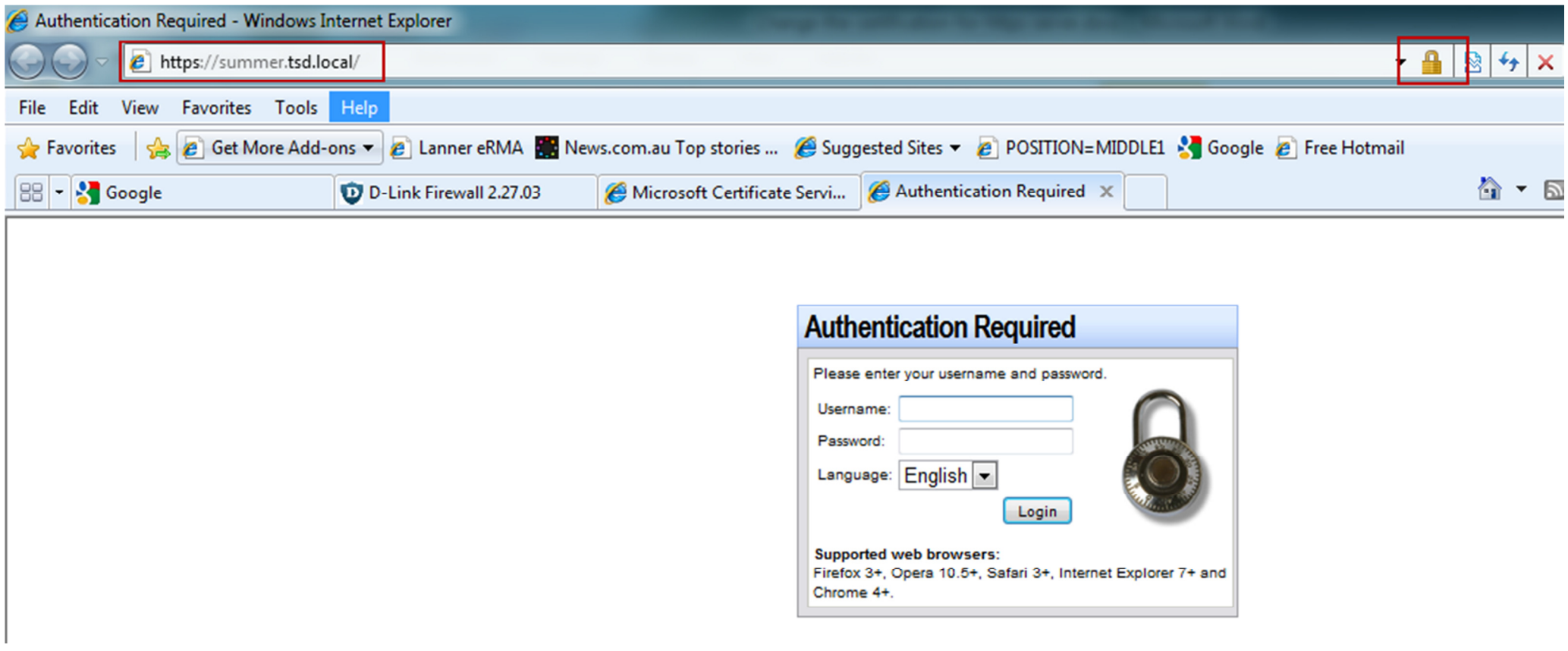

Name
Date modified
Type
Click Here
certnew.cer
04/08/2011 18:38
Security
Open File - Security Warning
Do you want to open this file?
Name: C:\Users\summer\Desktop\cert\certnew.cer
Publisher: Unknown Publisher
Type: Security Certificate
From: C:\Users\summer\Desktop\cert\certnew.cer
Open
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

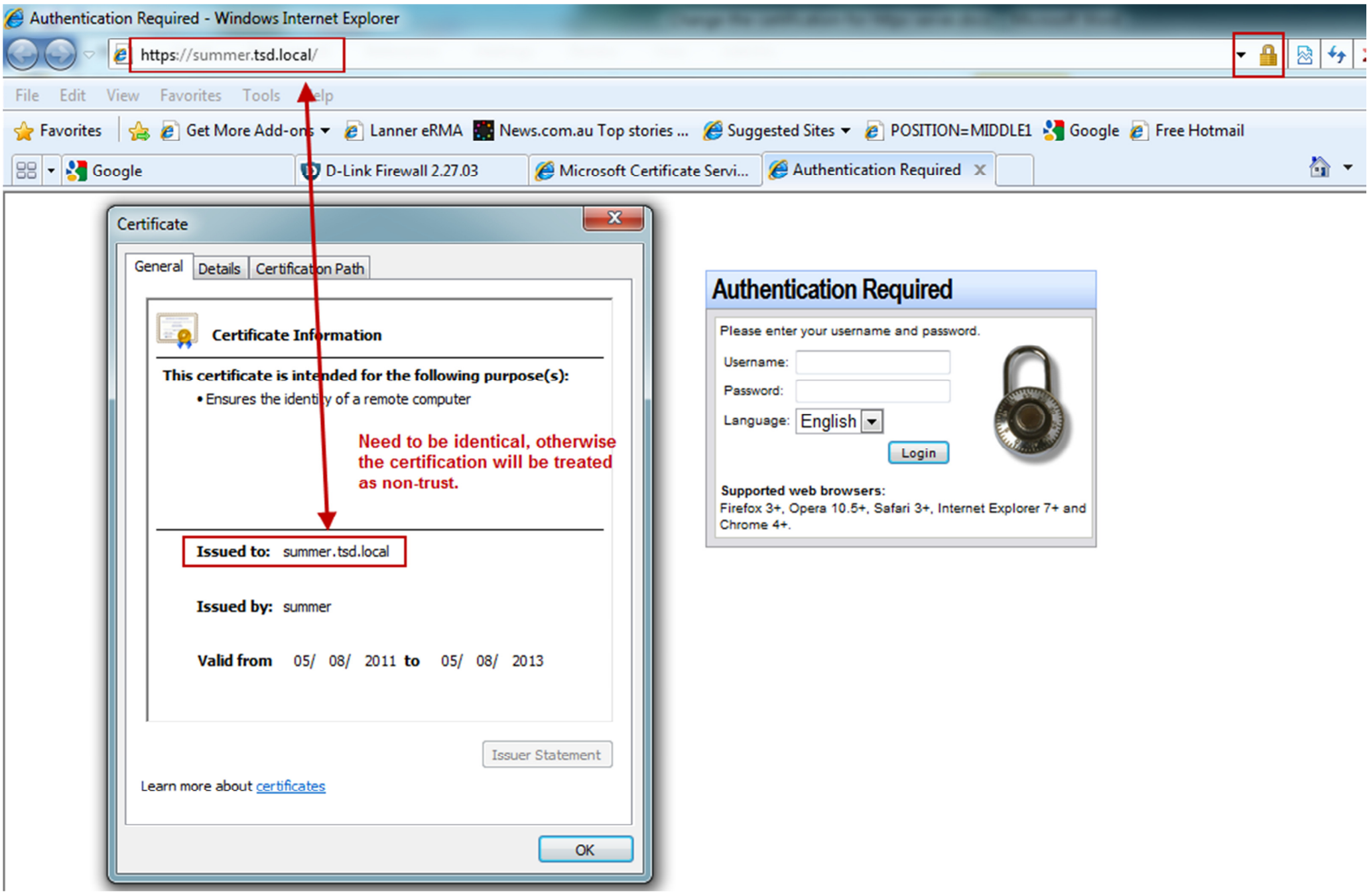

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: summer
Issued by: summer
Valid from 04/ 08/ 2011 to 04/ 08/ 2016
Install Certificate...
Issuer Statement
Learn more about certificates
OK


Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel



h. Now, double check the DNS settings of PC is set correctly, then connect to DFL via domain name (summer.tsd.local).





End of document.

Author: Summer Chang. 2011/08/05