

**BAN CƠ YẾU CHÍNH PHỦ  
HỌC VIỆN KỸ THUẬT MẬT MÃ**

**Module thực hành  
QUẢN TRỊ AN TOÀN HỆ THỐNG**

**ThS. Cao Minh Tuấn**

**HÀ NỘI, 2013**

## MỤC LỤC

MỤC LỤC.....	2
BÀI 1. THỰC HÀNH THIẾT LẬP SỬ DỤNG SSL ĐỂ MÃ HÓA CHO DỊCH VỤ WEB, MAIL.....	3
<b>1.1    Cấu hình sử dụng SSL/TLS để mã hóa cho dịch vụ web.....</b>	<b>3</b>
<i>1.1.1    Cài đặt DNS trên máy chủ Windows Server 2012.....</i>	<i>3</i>
<i>1.1.2    Cài đặt dịch vụ web IIS 8 trên máy chủ Windows Server 2012 ...</i>	<i>10</i>
<i>1.1.3    Cài đặt dịch vụ Certification Authority (CA) .....</i>	<i>14</i>
<i>1.1.4    Cấu hình SSL cho dịch vụ Web.....</i>	<i>16</i>
<b>1.2    Cấu hình sử dụng SSL/TLS để mã hóa cho dịch vụ Mail.....</b>	<b>21</b>
<i>1.2.1    Tạo bản ghi MX trong DNS, tắt tường lửa của Server 2012 .....</i>	<i>22</i>
<i>1.2.2    Cài đặt phần mềm Mdaemon, tạo tài khoản mail client .....</i>	<i>24</i>
<i>1.2.3    Cài đặt phần mềm Mail Client để gửi và nhận mail .....</i>	<i>26</i>
<i>1.2.4    Cấp chứng thư số cho người dùng user1 và user2.....</i>	<i>28</i>
<i>1.2.5    Gửi thư có mã hóa và ký số .....</i>	<i>34</i>
Tài liệu tham khảo.....	36

## **BÀI 1. THỰC HÀNH THIẾT LẬP SỬ DỤNG SSL ĐỂ MÃ HÓA CHO DỊCH VỤ WEB, MAIL**

### **1.1 Cấu hình sử dụng SSL/TLS để mã hóa cho dịch vụ web**

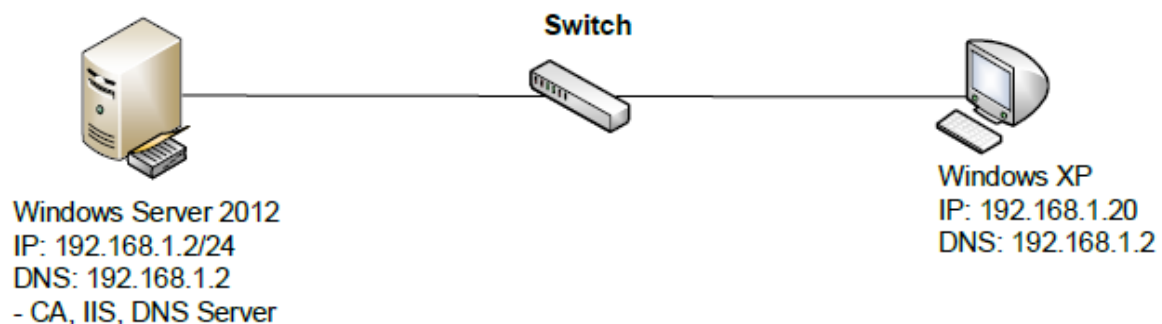
#### **Mục đích bài thực hành:**

Bài thực hành hướng dẫn sinh viên cài đặt, cấu hình các dịch vụ phân giải tên miền DNS, cài đặt và cấu hình cho dịch vụ Web IIS 8. Cài đặt dịch vụ cung cấp chứng thư số Certification Authority (CA). Xin chứng thư và cấu hình SSL cho dịch vụ web IIS. Nhằm mục đích bảo mật dữ liệu trên đường truyền giữa máy trạm web client và máy chủ web.

#### **Yêu cầu hệ thống:**

- 01 Máy chủ chạy hệ điều hành Windows Server 2012.
- 01 máy trạm chạy hệ điều hành Windows XP
- Cả 2 máy trên kết nối được với nhau.

#### **Mô hình triển khai:**



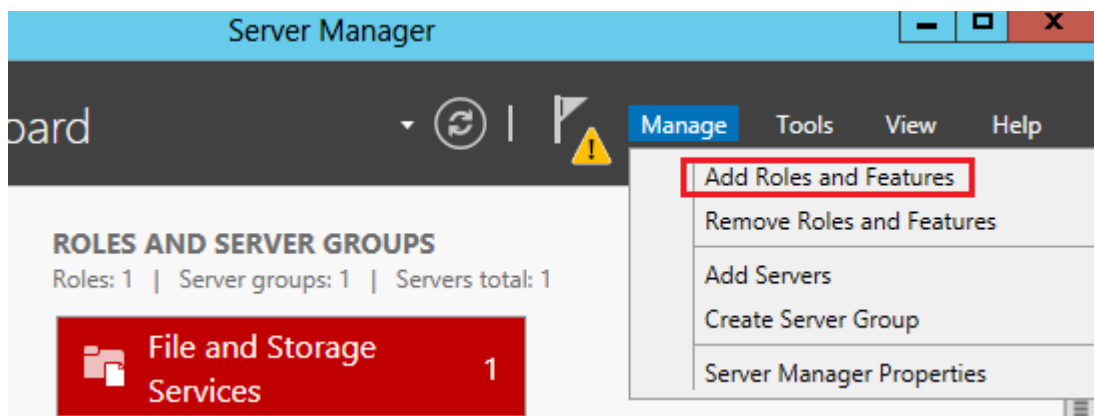
#### **Các bước triển khai:**

##### **1.1.1 Cài đặt DNS trên máy chủ Windows Server 2012**

**Bước 1:** Đăng nhập bằng tài khoản quản trị Administrator vào máy chủ Windows Server 2012.

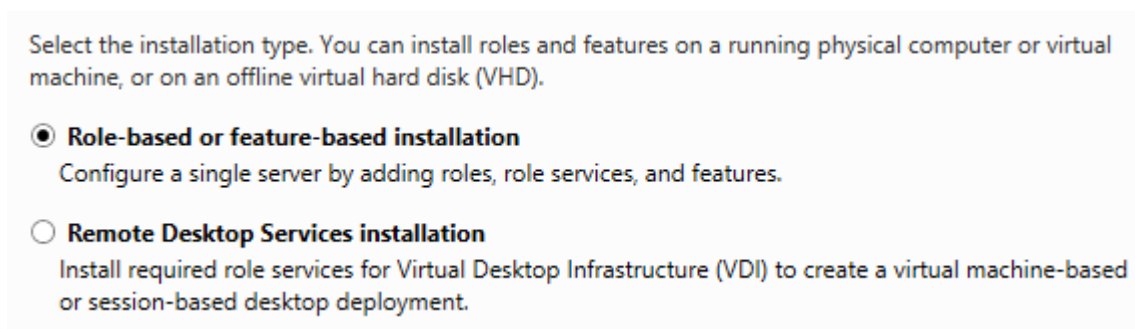
**Bước 2:** Truy cập theo đường dẫn để cài đặt dịch vụ DNS:

Server Manager → Manage → Add Roles and Features



**Bước 3:** Cửa sổ Add Roles and Features xuất hiện chọn Next để bắt đầu quá trình cài đặt.

Trong lựa chọn Select installation type → chọn Role-based or feature-based installation để cài đặt các dịch vụ và tính năng cho máy chủ.



Chọn Next để tiếp tục cài đặt.

Trong tùy chọn Select destination server → Chọn Select a server from the server pool.

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool  
☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
DC-KMA	192.168.1.2	Microsoft Windows Server 2012 Release Candidate Data

<  >

1 Computer(s) found

Chọn Next để tiếp tục cài đặt.

#### **Bước 4:** Lựa chọn dịch vụ

Trong tùy chọn Select server roles → tích vào dịch vụ DNS server

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☒ DNS Server
- ☐ Fax Server

Chọn Next để tiếp tục cài đặt.

Trong tùy chọn Select features để mặc định và chọn Next để tiếp tục.

Trong tùy chọn Confirm installation selection tích vào tùy chọn Restart the destination server automatically if required

To install the following roles, role services, or features on selected server, click Install.

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Chọn Install để cài đặt dịch vụ

View installation progress



Feature installation



Installation started on DC-KMA

DNS Server

Remote Server Administration Tools

Role Administration Tools

DNS Server Tools

Sau khi cài đặt thành công, trên giao diện Server Manager xuất hiện thêm chức năng giám sát dịch vụ DNS.

#### ROLES AND SERVER GROUPS

Roles: 2 | Server groups: 1 | Servers total: 1



DNS

1

1

Manageability

Events

Services

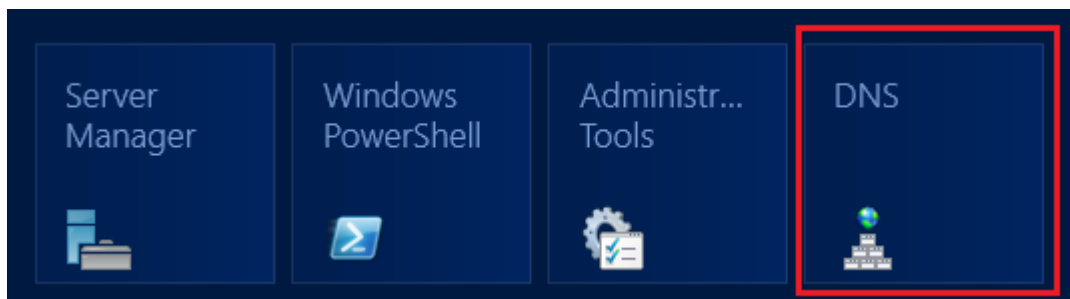
Performance

BPA results

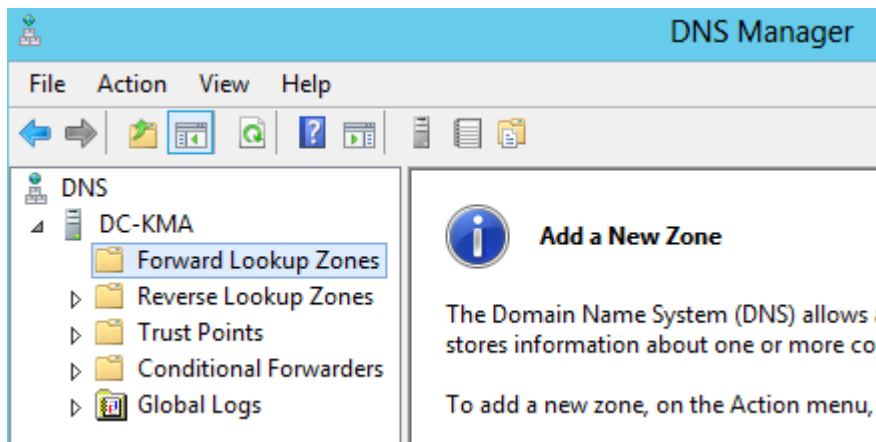
5/5/2014 9:13 PM

**Bước 5:** Cấu hình dịch vụ DNS để phân giải tên miền

Nhấn phím Start chọn DNS



Cửa sổ cấu hình DNS xuất hiện



**Bước 6:** Cấu hình phân giải xuôi:

Chuột phải vào mục Forward Lookup Zones → chọn New Zone

Trong mục Zone Type → chọn Primary zone

#### Zone Type

The DNS server supports various types of zones and storage.

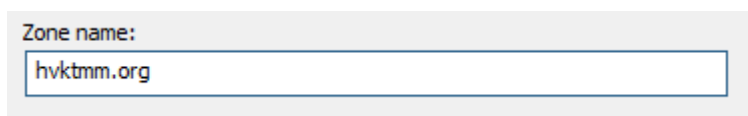
Select the type of zone you want to create:

☒ Primary zone

Creates a copy of a zone that can be updated directly on this server.

Chọn Next để tiếp tục

Trong mục Zone Name → điền tên miền: hvktmm.org



Trong mục Zone File để mặc định → Next

### Zone File


You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

☒ Create a new file with this file name:

Trong mục Dynamic Update → chọn Allow both nonsecure and secure dynamic update

☐ Allow only secure dynamic updates (recommended for Active Directory)  
This option is available only for Active Directory-integrated zones.

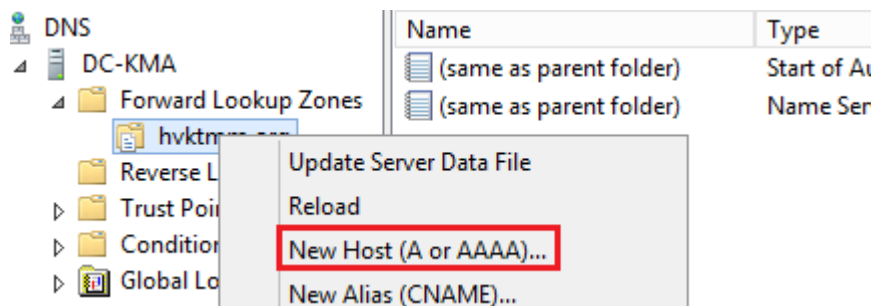
☒ Allow both nonsecure and secure dynamic updates  
Dynamic updates of resource records are accepted from any client.  
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.

☐ Do not allow dynamic updates  
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

Chọn Next → Finish

### Bước 7: Tạo bản ghi Host A (www)

Chuột phải vào mục hvktmm.org chọn New Host





**New Host**

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

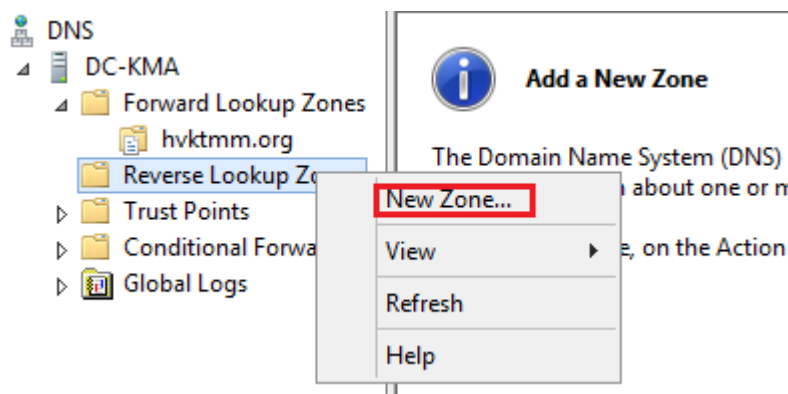
☒ Create associated pointer (PTR) record

Trong mục Name nhập www

Trong mục IP address nhập địa chỉ IP của Server → Add Host

### **Bước 8:** Cấu hình phân giải ngược

Chuột phải vào mục Reverse Lookup Zone chọn New Zone



Trong mục Zone Type → chọn Primary Zone

Trong mục Reverse Lookup Zone Name → chọn Ipv4 Lookup zone → Next

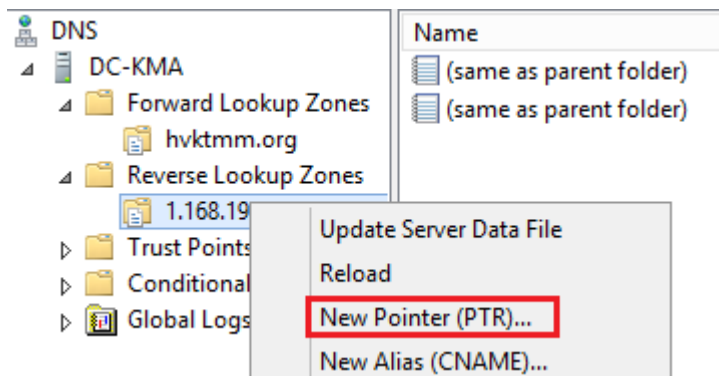
Trong mục Network ID nhập dải địa chỉ IP máy chủ sử dụng: 192.168.1 → Next

Trong mục Zone file để mặc định → Next

Trong mục Dynamic Update chọn Allow both nonsecure and secure dynamic update → Next → Finish

### **Bước 9:** Tạo bản ghi phân giải ngược PTR

Chuột phải vào dải IP đã khai báo chọn New Pointer



Nhập IP của Server (192.168.1.2)

Trở đến bản ghi Host A trong phân giải xuôi.

Nhấn OK → Finish

### **Bước 10:** Kiểm tra phân giải tên miền

Bật cửa sổ dòng lệnh CMD, sử dụng lệnh nslookup để kiểm tra

```
C:\Users\Administrator>nslookup
Default Server: www.hvktmm.org
Address: 192.168.1.2

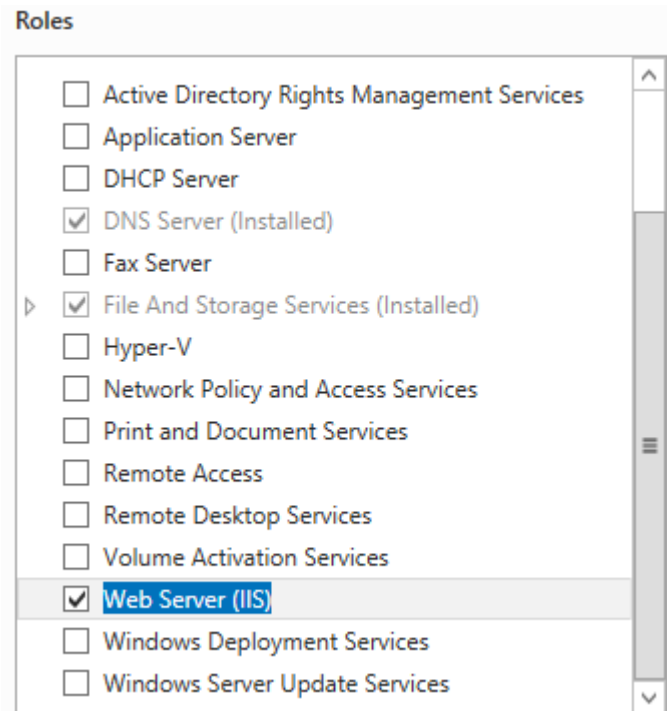
> www.hvktmm.org
Server: www.hvktmm.org
Address: 192.168.1.2

Name: www.hvktmm.org
Address: 192.168.1.2
```

Kết quả trả về đã có IP tương ứng với tên miền đã tạo.

#### *1.1.2 Cài đặt dịch vụ web IIS 8 trên máy chủ Windows Server 2012*

Thực hiện lại bước 2 và 3 trong mục 3.1.1 để vào mục Select server roles. Tích chọn dịch vụ Web server (IIS).

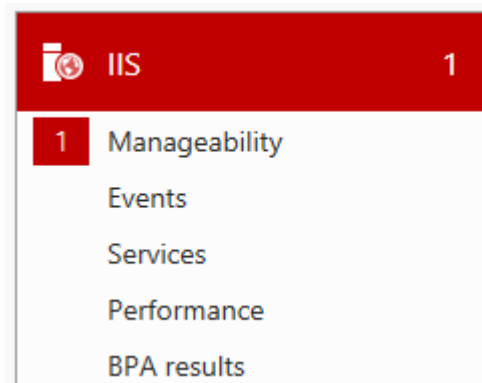


Chọn Next để tiếp tục.

Trong mục Select features để mặc định → chọn Next để tiếp tục.

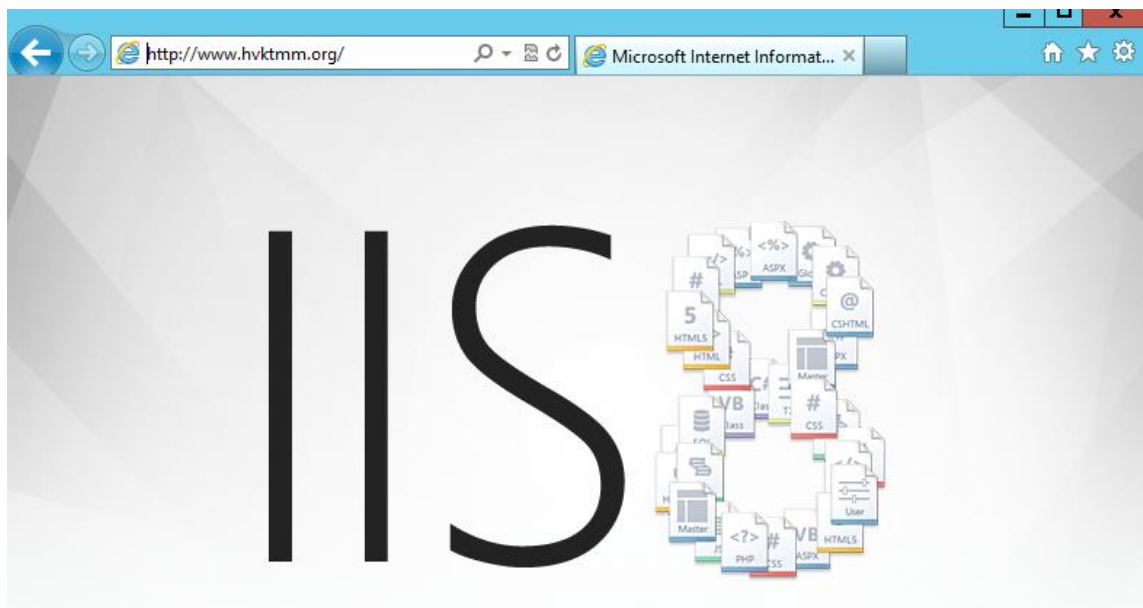
Các bước tiếp theo để mặc định → Install

Sau khi cài đặt thành công trong Server Manager xuất hiện giao diện giám sát dịch vụ IIS.



Bước 4: Kiểm tra hoạt động của web server

Bật trình duyệt web IE và gõ tên miền đã tạo ở trên: [www.hvktmm.org](http://www.hvktmm.org)



Giao diện xuất hiện trang web mặc định của IIS 8.

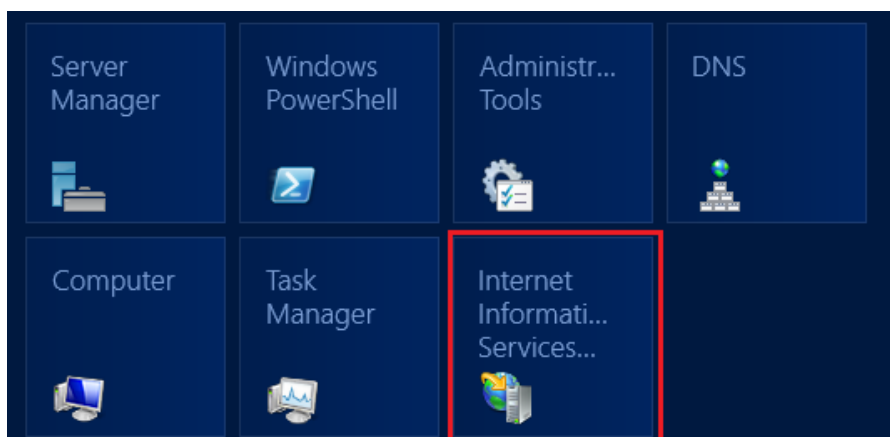
**Bước 5:** Tạo trang web riêng

Truy cập vào thư mục lưu trữ web của IIS theo đường dẫn: C:\inetpub\wwwroot

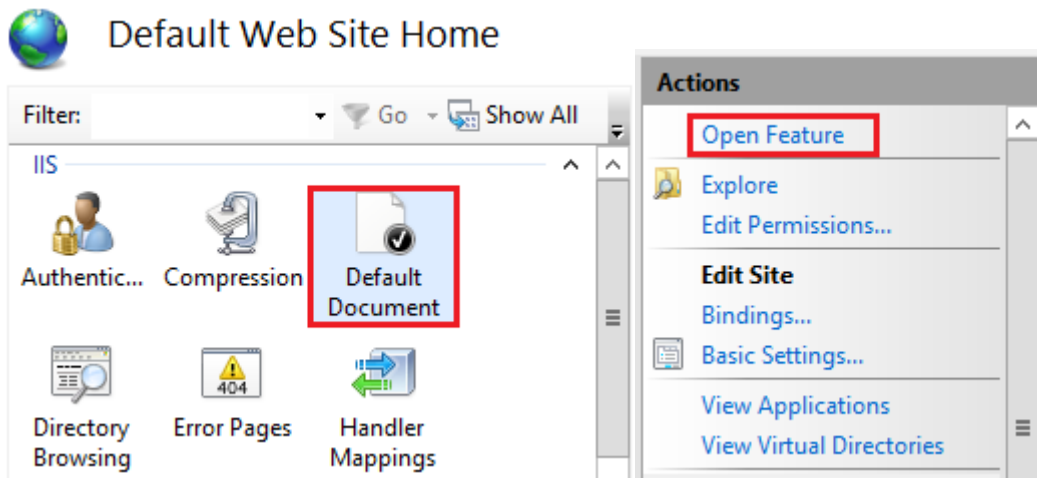
Tạo tệp tin mới có tên index.html, chỉnh sửa nội dung của file theo ý muốn.

**Bước 6:** Cấu hình để IIS nhận tệp tin index.html

Thực hiện theo đường dẫn: Start → Internet Information Service

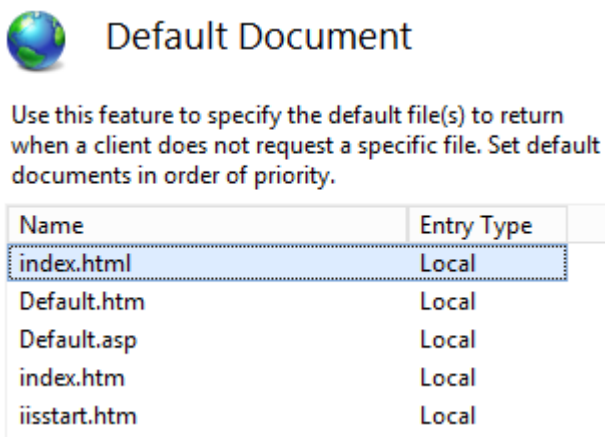


Truy cập vào website mặc định: Default Web Site



Chọn Default Document → Open feature.

Di chuyển vị trí của file index.html lên trên cùng như hình dưới đây:



OK.

**Bước 7:** Kiểm tra kết quả

Bật trình duyệt web IE và truy cập theo tên miền đã tạo ở trên.

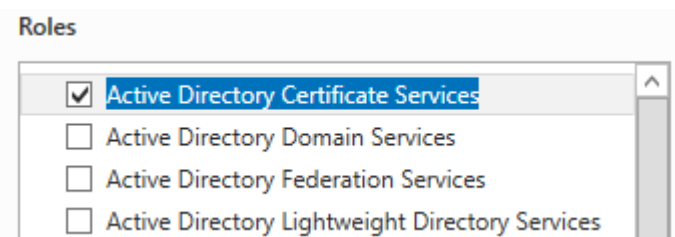


Trang web mặc định hiển thị trang index.html đã tạo ở trên.

### 1.1.3 Cài đặt dịch vụ Certification Authority (CA)

**Bước 1:** Thực hiện lại bước 2 và 3 trong mục 3.1.1 để truy cập đến các dịch vụ cần cài đặt.

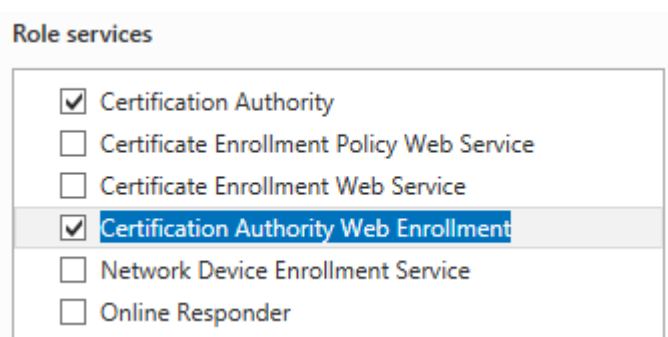
**Bước 2:** Tích chọn dịch vụ Active Directory Certificate Service



Chọn Next để tiếp tục.

Trong mục Select features để mặc định → Next

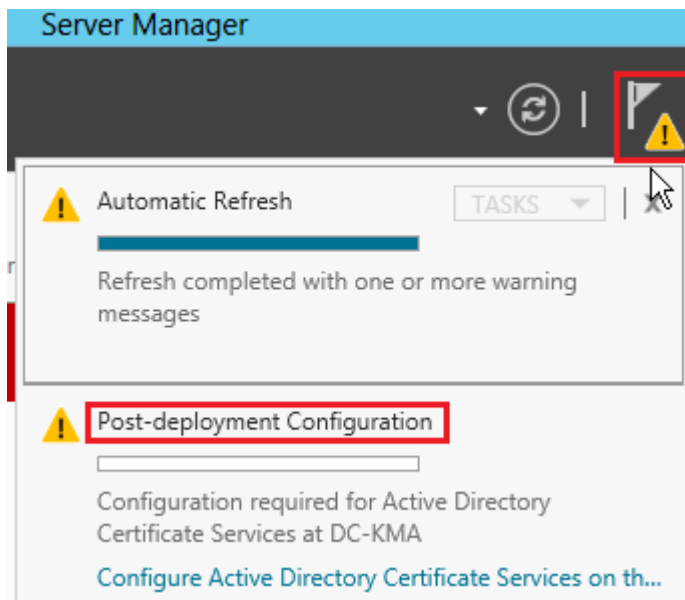
Trong mục Select role services chọn 2 dịch vụ: Certification Authority và Certification Authority Web Enrollment.



Chọn Next để tiếp tục, chọn Install để cài đặt dịch vụ.

**Bước 3:** Cấu hình dịch vụ CA

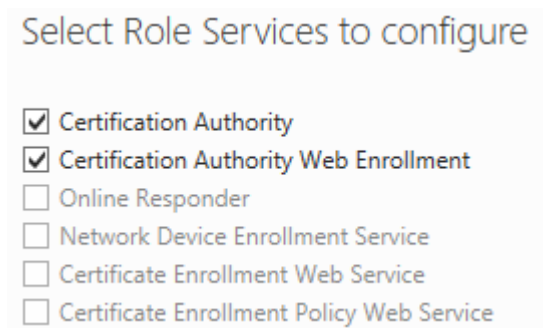
Sau khi cài đặt dịch vụ CA thành công, chúng ta phải cấu hình tiếp cho CA. Kích chọn vào biểu tượng hình lá cờ trong giao diện Server Manager như hình dưới đây:



Tiếp tục chọn Configure Active Directory Certificate Services

Trong giao diện Credential để mặc định → chọn Next

Trong giao diện Role Services tích chọn 2 tùy chọn Certification Authority và Certification Authority Web Enrollment.



Trong giao diện Setup Type chọn Standalone CA → Next.

Trong giao diện CA Type chọn Root CA → Next.

Trong giao diện Private Key chọn Create a new private key → Next.

Trong giao diện Cryptography for CA chọn mặc định → Next.

Trong giao diện CA Name đặt tên cho CA → Next.

Trong giao diện Validity Period để mặc định là 5 năm → Next.

Trong giao diện CA database để mặc định

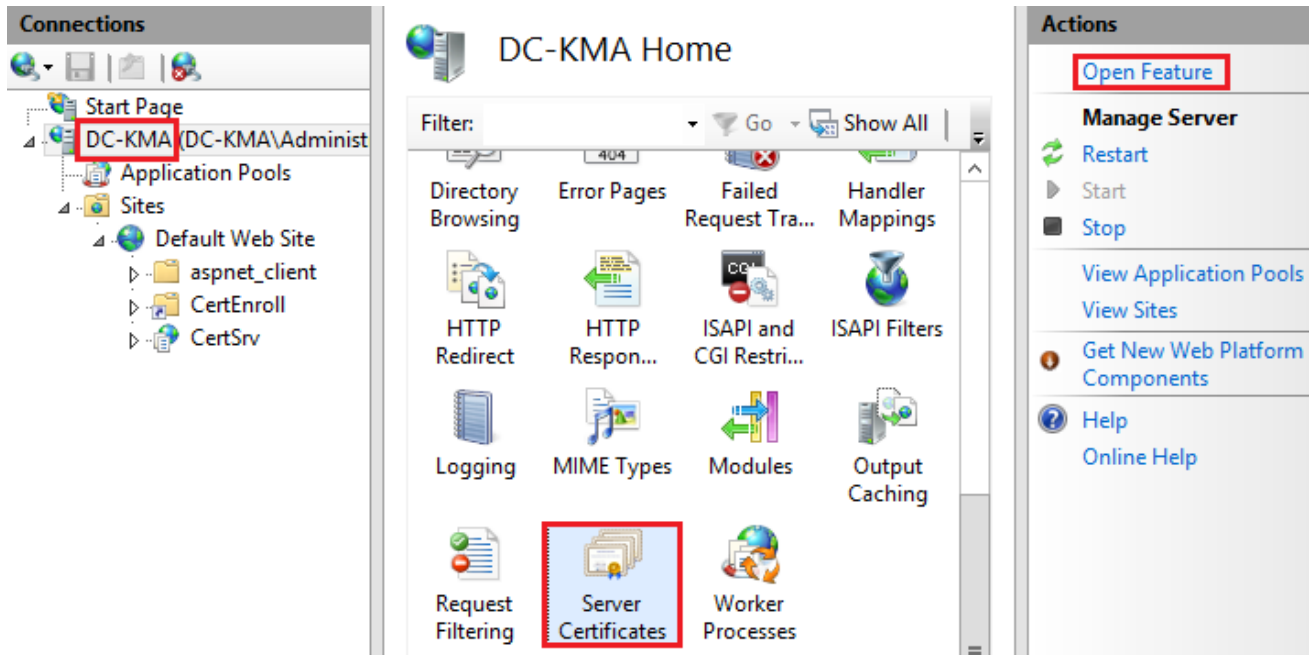
Cuối cùng chọn Configure → Finish

Hoàn tất quá trình cài đặt và cấu hình dịch vụ cung cấp chứng thư số CA.

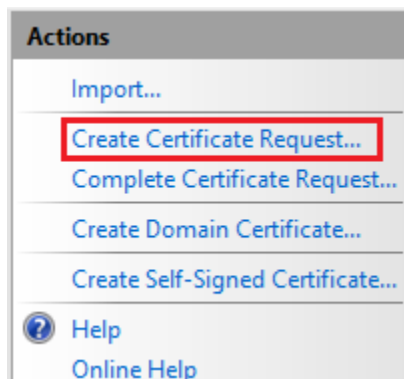
#### 1.1.4 Cấu hình SSL cho dịch vụ Web

**Bước 1:** IIS gửi yêu cầu chứng thư số tới CA

Bật dịch vụ IIS lên, chọn tên của máy chủ web (DC-KMA), trong giao diện ở giữa DC-KMA Home tìm đến dịch vụ Server Certificates → Open feature



Trong giao diện của Server Certificates, ở cột Action chọn Create Certificate Request



Trong giao diện tiếp theo nhập các thông tin về máy chủ IIS. Đặc biệt trong mục Common name phải nhập tên chính xác của tên miền web.



Common name:	<input type="text" value="www.hvktmm.org"/>
Organization:	<input type="text" value="kma"/>
Organizational unit:	<input type="text" value="kma"/>
City/locality	<input type="text" value="ha noi"/>
State/province:	<input type="text" value="ha noi"/>
Country/region:	<input type="text" value="VN"/>

Chọn Next để tiếp tục.

Trong giao diện tiếp theo tùy chọn của độ dài khóa mã, mặc định là 1024 bit.

Trong giao diện tiếp theo File Name, trở đến nơi lưu trữ file và đặt tên cho file. File này lưu trữ thông tin về khóa.

Specify a file name for the certificate request:

Chọn Finish để kết thúc.

## Bước 2: Gắn thông tin về khóa với chứng thư số

- Bật trình duyệt Web IE lên và truy cập theo tên miền vào đường đường dẫn của CA:

<http://www.hvktmm.org/certsrv>

- Chọn tùy chọn Request a Certificate → Advanced certificate request → Submit a certificate request by using...

- Mở file key1.txt vừa tạo ở trên, copy nội dung của file và dán vào ô Saved Request

### Saved Request:

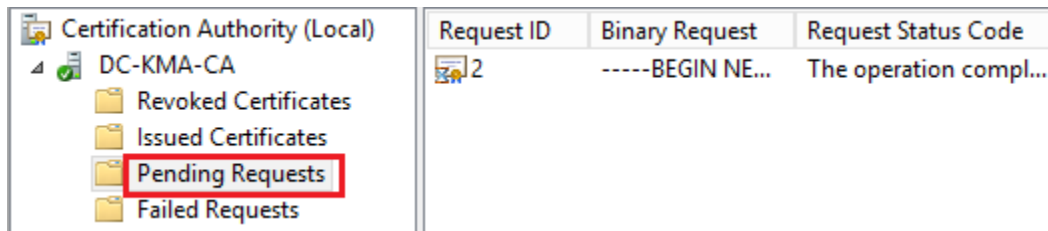
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	<pre> BBYEFBOJgBvPTW7SiXjG++30V39hFbCvMA0GCSqG: s8RKDULsdPv3xGWWja1xX+vxG1F6XUnJdJ7OX6aq: //uWDBqlFAhlwc+GWDp93AQQDxCcab+nS29rx05ml DZSWF5M6ihuO2PkesedXgRBgcohBax9nGnmI -----END NEW CERTIFICATE REQUEST----- </pre>
---	---

Chọn Submit.

Yêu cầu chứng thư số kèm với thông tin của khóa mã đã được gửi tới CA.

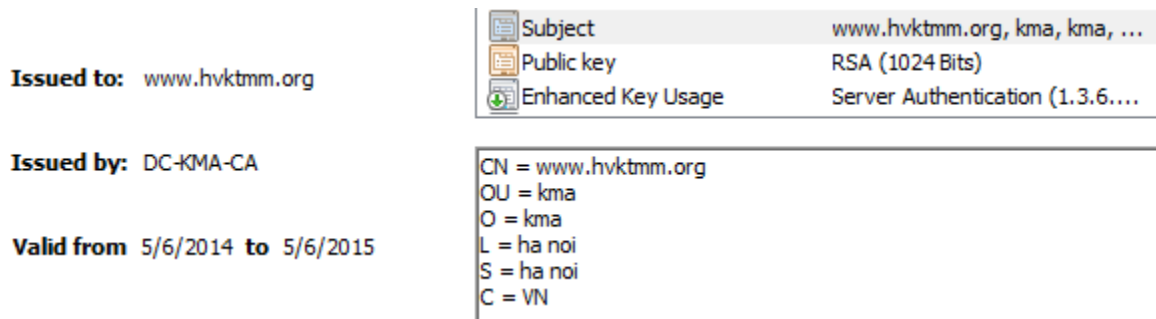
## Bước 3: Cấp chứng thư số cho IIS

- Bật dịch vụ CA lên, truy cập vào mục Pending Requests, thấy có 1 chứng thư đang chờ đợi duyệt của CA.



- Chuột phải vào chứng thư số có ID là 2 và chọn All Tasks → Issue

Bây giờ trong mục Issued Certificates thấy có chứng thư ID 2 đã được cấp với các thông tin như đã khai báo lúc yêu cầu.



- Tiếp tục thực hiện như ở bước 2, truy cập IE theo đường dẫn:

<http://www.hvktmm.org/certsrv>

- Chọn tùy chọn View the status of a pending certificate request

**Select a task:**

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Kích vào đường dẫn Saved-Request Certificate để lưu chứng thư.

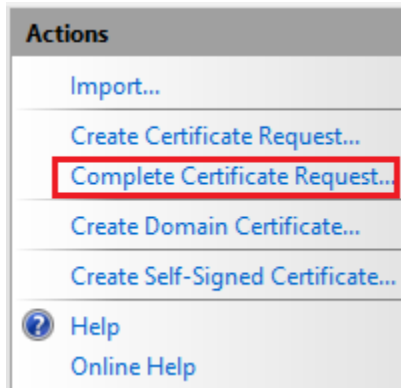
### View the Status of a Pending Certificate Request

Select the certificate request you want to view:

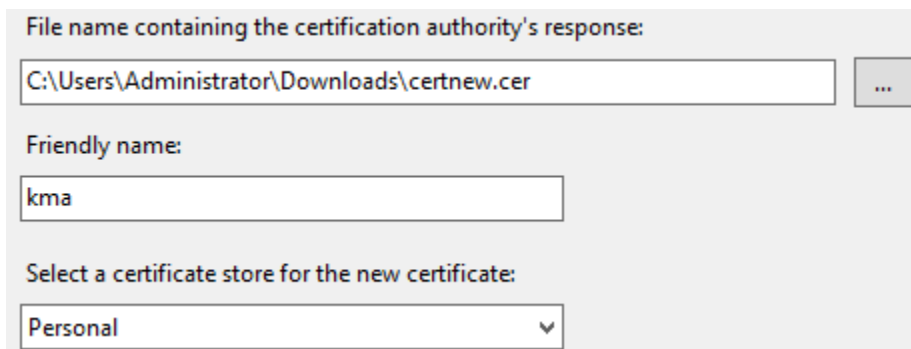
[Saved-Request Certificate \(Tuesday May 6 2014 8:34:15 PM\)](#)

**Bước 4:** Cài đặt chứng thư cho máy chủ IIS

- Bật dịch vụ IIS, chọn máy chủ IIS, chọn Server Certificates, trong mục Action chọn Open feature
- Chọn Complete Certificate Request



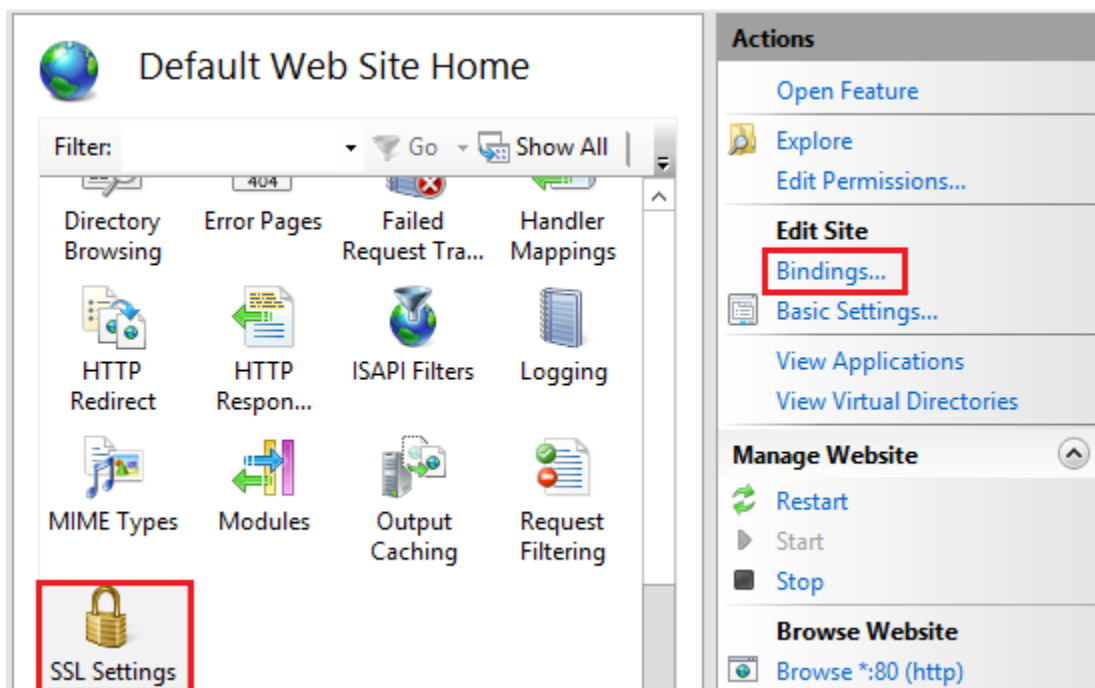
Tiếp tục trở đến nơi lưu trữ chứng thư đã tải về từ bước 3.

A screenshot of the 'Import and Export Wizard' dialog box. The 'File name containing the certification authority's response:' field is filled with 'C:\Users\Administrator\Downloads\certnew.cer'. The 'Friendly name:' field is filled with 'kma'. The 'Select a certificate store for the new certificate:' dropdown is set to 'Personal'.

Nhấn OK để kết thúc.

### **Bước 5:** Cấu hình để máy chủ IIS chạy dịch vụ SSL

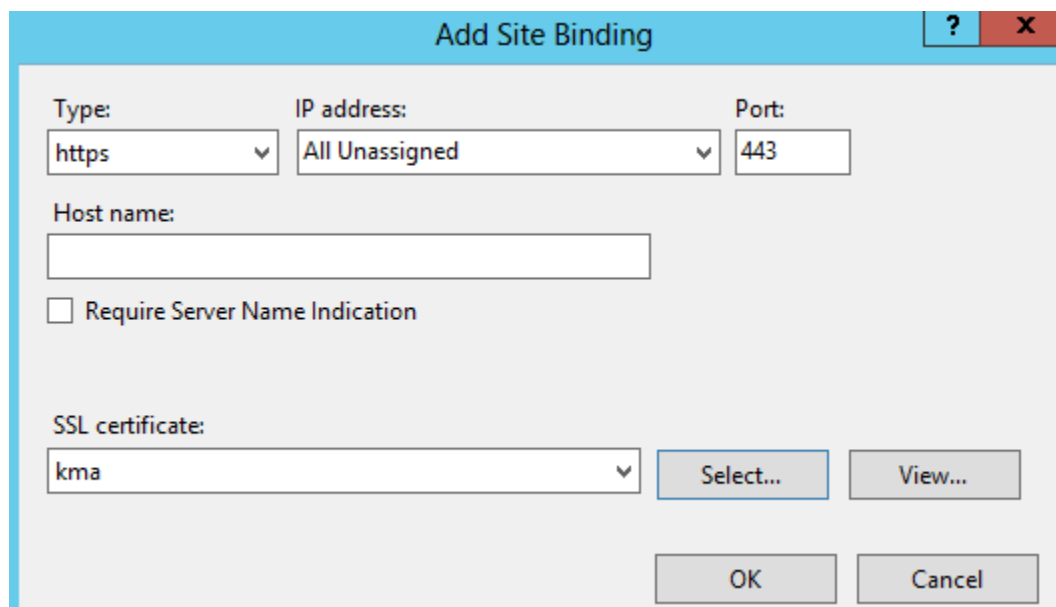
- Từ giao diện quản trị của IIS truy cập tới Sites → Default Web Site, trong các chức năng ở cột giữa Default Web Site Home tìm đến chức năng SSL setting
- Trong mục Action chọn Bindings...



- Giao diện Site Bindings chọn Add

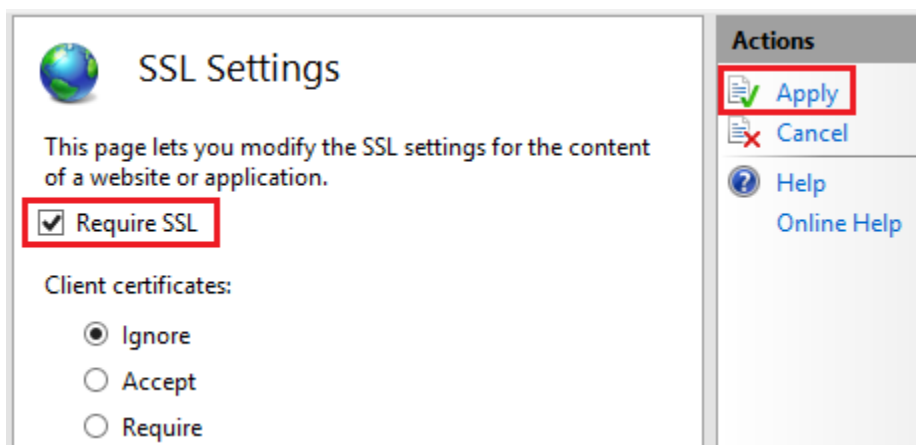
Trong mục Type chọn https : Port 443

Trong mục SSL Certificate → Select → chọn chứng thư đã cài đặt



Chọn OK để kết thúc.

- Trở lại giao diện Default Web Site Home chọn SSL Settings, mục Action chọn Open feature. Tích chọn vào yêu cầu SSL, mục Action chọn Apply



Kết thúc cài đặt và cấu hình SSL.

Bước 6: Kiểm thử

- Bật trình duyệt web IE và gõ tên miền với https



→ Thành công.

- Từ một máy tính chạy hệ điều hành XP kết nối vào mạng của máy chủ IIS và truy cập tên miền với https



→ Thành công.

## 1.2 Cấu hình sử dụng SSL/TLS để mã hóa cho dịch vụ Mail

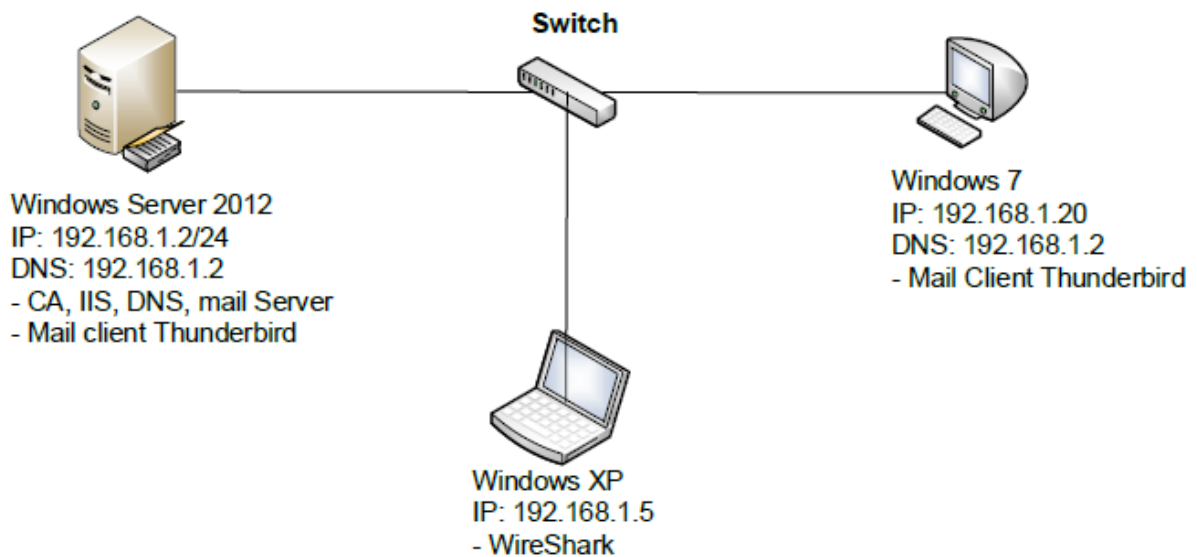
### Mục đích bài thực hành:

Bài thực hành hướng dẫn sinh viên cài đặt và cấu hình máy chủ dịch vụ mail MDaemon V10, cài đặt và cấu hình phần mềm mail client Thunderbird, xin và cấp chứng thư số cho các tài khoản mail client sử dụng CA, cấu hình các chứng thư số tương ứng để người dùng mã hóa và ký số mail khi gửi từ người dùng này đến người dùng khác. Nhằm mục đích đảm bảo tính bí mật và toàn vẹn nội dung mail khi gửi trên đường truyền.

## **Yêu cầu hệ thống:**

- Máy chủ chạy hệ điều hành Windows Server 2012. Đã cài đặt các dịch vụ:
  - Dịch vụ phân giải tên miền DNS.
  - Dịch vụ cấp chứng thư số Certification Authority.
  - Dịch vụ Web IIS.
- Phần mềm máy chủ dịch vụ mail server MDAemon V10.
- Phần mềm máy trạm mail Thunderbird Setup 24.5.0.
- Phần mềm phân tích lưu lượng mạng Wireshark-win32-1.8.6.
- Máy trạm chạy hệ điều hành Windows 7, Windows XP kết nối với máy chủ Windows Server 2012.

## **Mô hình mạng:**



## **Các bước thực hiện:**

### *1.2.1 Tạo bản ghi MX trong DNS, tắt tường lửa của Server 2012*

#### **Bước 1:** Tạo bản ghi MX để xác định máy chủ mail

- Bật dịch vụ DNS và tạo bản ghi Host A với tên mail:

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

☒ Create associated pointer (PTR) record

- Tiếp tục tạo bản ghi MX

Mail Exchanger (MX)

Host or child domain:

By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank.

Fully qualified domain name (FQDN):

Fully qualified domain name (FQDN) of mail server:

Mail server priority:

Nhấn OK để kết thúc.

**Bước 2:** Tắt tường lửa của Windows để cho phép dịch vụ mail kết nối tới máy chủ mail.

- Bật dịch vụ Server Manager truy cập theo đường dẫn: Tools → Windows Firewall with Advanced Security
- Click vào chức năng Windows Firewall Properties

**Public Profile is Active**

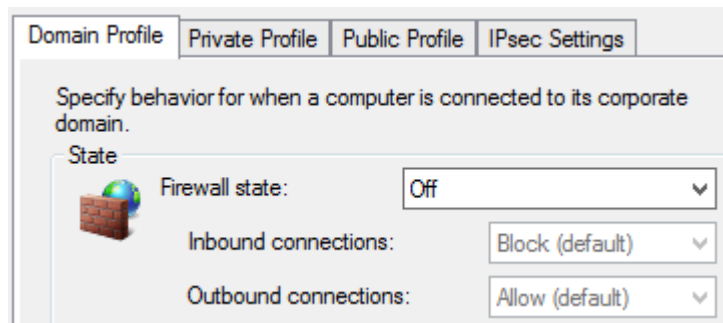
☒ Windows Firewall is on.

☐ Inbound connections that do not match a rule are blocked.

☒ Outbound connections that do not match a rule are allowed.

☒ [Windows Firewall Properties](#)

- Trong các Tab Domain Profile, Private Profile, Public Profile chuyển sang trạng thái Firewall state: Off



Apply → OK → Kết thúc cấu hình tường lửa.

### 1.2.2 Cài đặt phần mềm Mdaemon, tạo tài khoản mail client

Bài thực hành này vẫn kế thừa một số thiết lập ở bài 3.1 như: sử dụng CA, DNS, IIS và vẫn sử dụng https để truy cập tên miền.

#### **Bước 1:** Cài đặt phần mềm MDAemon V10 làm máy chủ mail

- Copy phần mềm MDAemon V10 vào máy chủ Windows Server 2012 và tiến hành cài đặt.
- Quá trình cài đặt Mdaemon cần một số thiết lập như sau:

Nhập thông tin đăng ký phần mềm:

- Trong mục Domain Name nhập: hvktnm.org
- Thiết lập First Account:



Full name (ex: Frank Thomas)

Mailbox (ex: Frank - don't include a domain name)

Password (ex: SwordFish - no spaces)

- Thiết lập DNS là địa chỉ của DNS server:

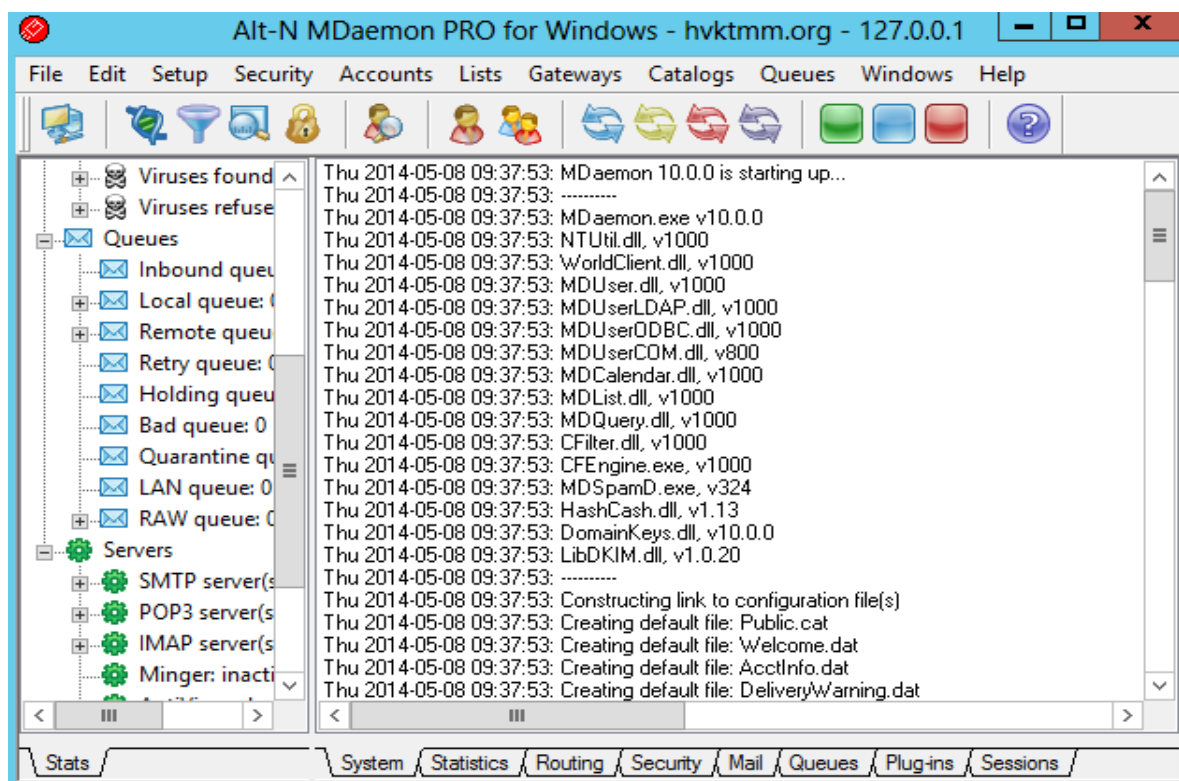
☒ Use Windows DNS settings

Primary DNS IP Address  (optional)

Backup DNS IP Address  (optional)

- Next → Finish

Sau khi cài đặt xong và bật máy chủ mail hoạt động



## Bước 2: Thiết lập tài khoản mail cho người dùng

Truy cập giao diện quản trị mail server và theo đường dẫn như sau:

Main menu → Tab Account → New Account

Trong giao diện tạo tài khoản mới hiện ra, nhập thông tin cho tài khoản, ví dụ:

Chọn OK để kết thúc.

Tương tự tạo tiếp tài khoản có tên là user2.

### 1.2.3 Cài đặt phần mềm Mail Client để gửi và nhận mail

#### Bước 1: Cài đặt tại máy chủ Windows Server 2012

- Copy phần mềm Thunderbird Setup 24.5.0 vào máy chủ Windows Server và tiến hành cài đặt theo chỉ dẫn mặc định.
- Sau khi cài đặt và khởi động phần mềm Thunderbird sẽ hỏi người dùng thiết lập tài khoản. Click vào tùy chọn use my existing email:

- Nhập các thông tin về tài khoản của người dùng user1:

Chọn Continue để tiếp tục. Thunderbird sẽ truy vấn đến tên miền tìm địa chỉ mail đã khai báo.

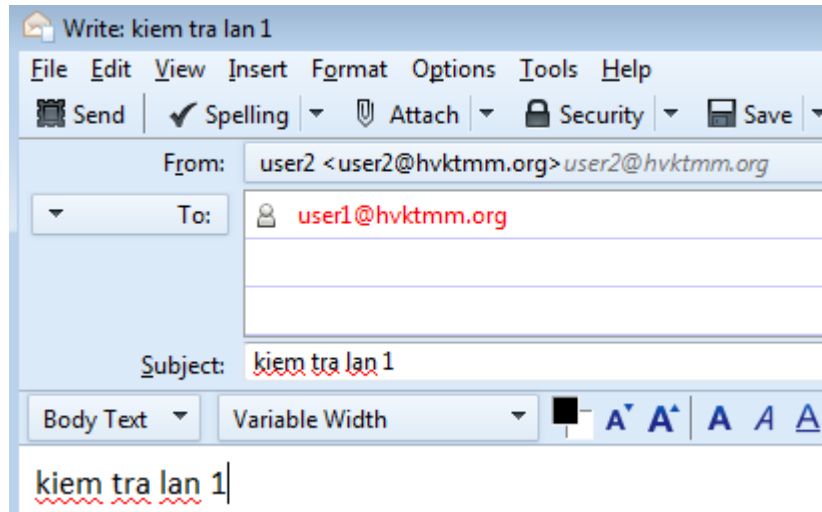
- Kết quả như sau:

Nhấn Done để kết thúc cấu hình.

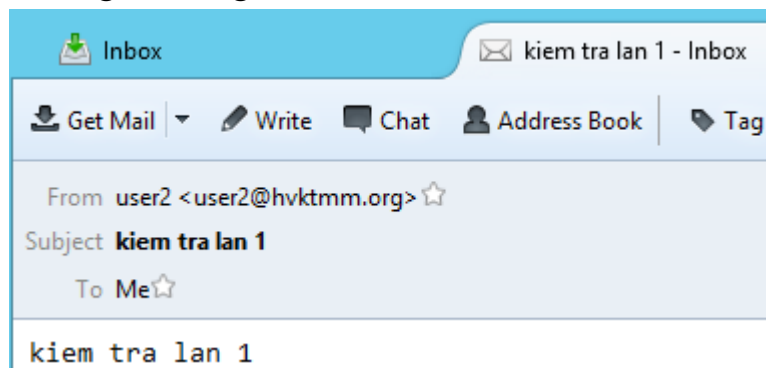
**Bước 2:** Thực hiện tương tự như bước 1 nhưng cài đặt trên máy Windows 7 và tài khoản là của user2.

**Bước 3:** Kiểm tra gửi và nhận mail giữa 2 người dùng user1 và user2.

- Từ người dùng user2 soạn mail và gửi cho user1



- Bên người dùng user1 đã nhận được mail:



**Bước 4:** Chặn bắt thông tin truyền

- Từ máy chạy Windows XP cài phần mềm WireShark chặn bắt thông tin không được mã hóa giữa người dùng user1 gửi cho user2.
- Kết quả chặn bắt

```

MAIL FROM:<user2@hvktmm.org> SIZE=377
250 <user2@hvktmm.org>, Sender ok
RCPT TO:<user1@hvktmm.org>
250 <user1@hvktmm.org>, Recipient ok
DATA
354 Enter mail, end with <CRLF>.<CRLF>
Message-ID: <536BD69E.1050005@hvktmm.org>
Date: Thu, 08 May 2014 12:10:22 -0700
From: user2 <user2@hvktmm.org>
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101
MIME-Version: 1.0
To: user1@hvktmm.org
Subject: kiểm tra lần 2
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit

kiểm tra lần 2
.
250 ok, message saved <Message-ID: 536BD69E.1050005@hvktmm.org>

```

Kết quả chặn bắt cho thấy kẻ tấn công có thể biết được người gửi và người nhận, tiêu đề của mail, và quan trọng là biết được nội dung của mail.

#### 1.2.4 Cấp chứng thư số cho người dùng user1 và user2

**Bước 1:** Cấp chứng thư số cho người dùng user1 trên máy chủ Windows Server 2012

- Bật trình duyệt web IE và truy cập theo đường dẫn  
<https://www.hvktmm.org/certsrv>
- Trong giao diện web xuất hiện chọn Request a certificate:  
**Select a task:**  
[Request a certificate](#)  
[View the status of a pending certificate request](#)  
[Download a CA certificate, certificate chain, or CRL](#)
- Tiếp tục chọn Advanced certificate request.
- Tiếp tục chọn Create and submit a request to this CA.
- Trong mục Identifying Information: Nhập thông tin của user1
- Trong mục Type of Certificate Needed: chọn E-mail protection certificate
- Trong mục Key options: tích chọn Mark keys as exportable

### Identifying Information:

Name:	user1
E-Mail:	user1@hvktmm.org
Company:	kma
Department:	ha noi
City:	ha noi
State:	ha noi
Country/Region:	vn

### Type of Certificate Needed:

E-Mail Protection Certificate ▼

### Key Options:

☒ Create new key set   ☐ Use existing key set

CSP: Microsoft Enhanced RSA and AES Cryptographic Provider

Key Usage: ☐ Exchange   ☐ Signature   ☒ Both

Key Size: 1024   Min: 384   Max: 16384   (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

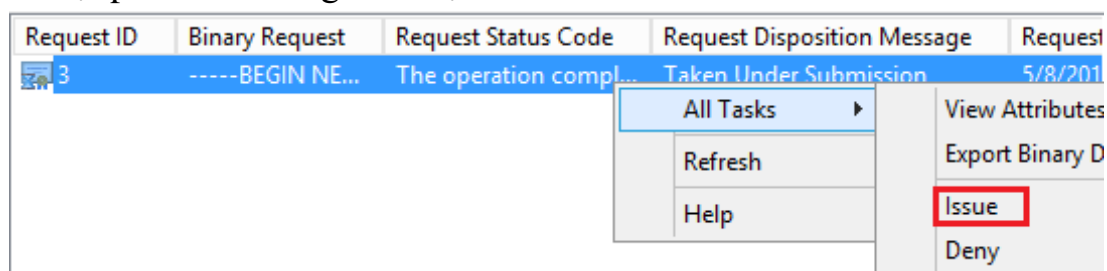
☒ Automatic key container name   ☐ User specified key container name

☒ Mark keys as exportable

- Nhấn Submit để gửi yêu cầu tới CA.

**Bước 2:** Truy cập vào dịch vụ CA để cấp phát chứng thư cho người dùng user1

- Truy cập vào mục Pending requests ta thấy có 1 chứng thư đang chờ đợi đồng ý.
- Chuột phải vào chứng thư chọn All Tasks → Issue



- Như vậy chứng thư đã được cấp cho người dùng user1

**Bước 3:** Cài đặt chứng thư của user1 vào máy chủ Windows Server 2012

- Truy cập vào trình duyệt web IE theo đường dẫn:  
<https://www.hvktmm.org/certsrv>
- Trong mục Select a task chọn View the status of a pending certificate request:

**Select a task:**

[Request a certificate](#)

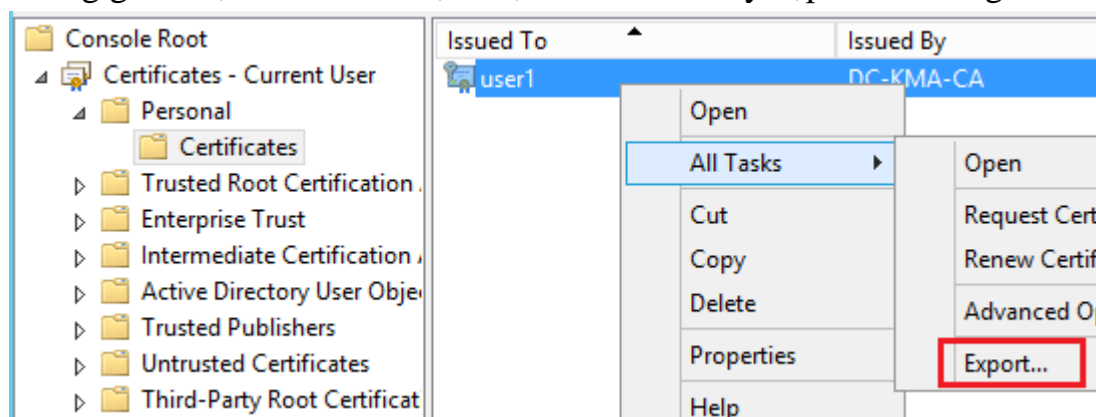
[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

- Chọn E-Mail Protection Certificate.
- Tiếp tục chọn Install this certificate.

**Bước 4:** Trích xuất chứng thư của người dùng user1 thành 2 định dạng để import vào phần mềm Thunderbird.

- Bật công cụ MMC từ Run.
- Chọn File → Add/Remove Snap-in → Certificates → Add (My user account) → OK
- Trong giao diện MMC với dịch vụ Certificate truy cập theo đường dẫn:



Chuột phải vào chứng thư của user1 chọn All Tasks → Export.

- Giao diện truy xuất chứng thư xuất hiện chọn Next để tiếp tục.
- Giao diện tiếp theo chọn No, do not export the private key:

Do you want to export the private key with the certificate?

- ☐ Yes, export the private key
- ☒ No, do not export the private key

Chọn Next để tiếp tục.

- Trong định dạng của chứng thư chọn encoded binary X.509:

Select the format you want to use:

- ☒ DER encoded binary X.509 (.CER)
- ☐ Base-64 encoded X.509 (.CER)
- ☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

- Chọn Next để tiếp tục, chọn nơi lưu trữ file và đặt tên chứng thư là user1.cer
- Tiếp tục lại quá trình trích xuất chứng thư của user1 nhưng lần này trích xuất cả khóa bí mật của user1:

Do you want to export the private key with the certificate?



- ☒ Yes, export the private key  
☐ No, do not export the private key

- Định dạng:

- ☒ Personal Information Exchange - PKCS #12 (.PFX)  
☒ Include all certificates in the certification path if possible  
☐ Delete the private key if the export is successful  
☐ Export all extended properties

- Trong mục Security: nhập mật khẩu để bảo vệ khóa.
- Tiếp tục chọn nơi lưu và đặt tên cho chứng thư.

Kết thúc quá trình trích xuất chứng thư với 2 định dạng là user1.cer, và user1-key.pfx

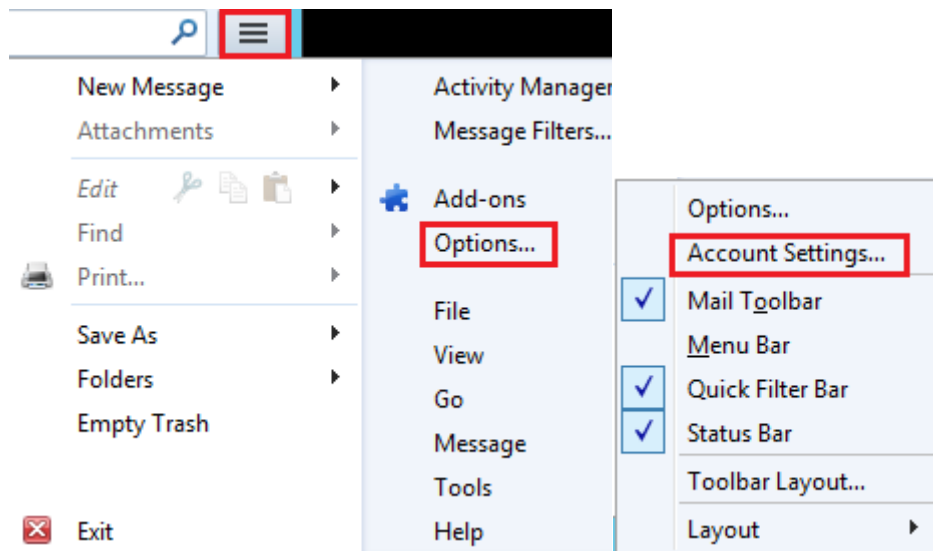
Name	Date modified	Type	Size
 user1.cer	5/8/2014 11:00 AM	Security Certificate	1 KB
 user1-key.pfx	5/8/2014 11:05 AM	Personal Informati...	3 KB

### **Bước 5:** Trích xuất chứng thư của CA để Import vào Thunderbird

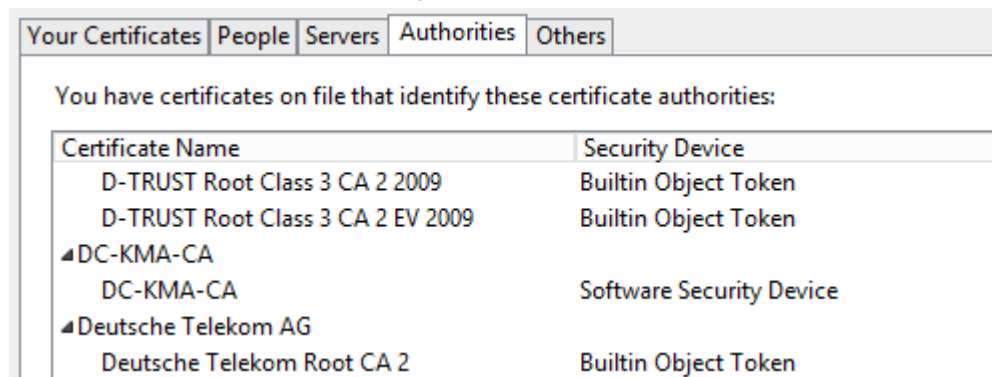
- Trong giao diện MMC Console Root → Trusted Root Certification Authorities chọn chứng thư của CA → All Tasks → Export
- Đặt tên cho chứng thư là CA.cer và chọn nơi lưu trữ.

### **Bước 6:** Import 2 chứng thư của user1 vào Thunderbird

- Bật Thunderbird lên và thực hiện theo đường dẫn: chọn biểu tượng 3 dấu gạch ngang ở phía góc của Thunderbird → Chọn Options, thanh công cụ hiện ra chọn Account Settings



- Trong giao diện Account Setting chọn tab Security
- Trong mục Certificates chọn View certificate
- Giao diện Certificate Manager xuất hiện chọn Tab Authorities → Chọn Import và trở đến nơi lưu trữ chứng thư của CA đã trích xuất ở bước 5.

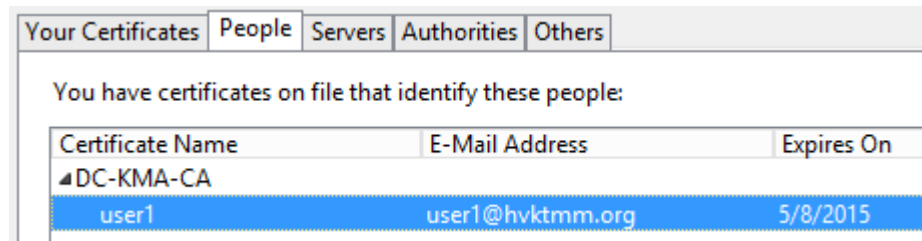




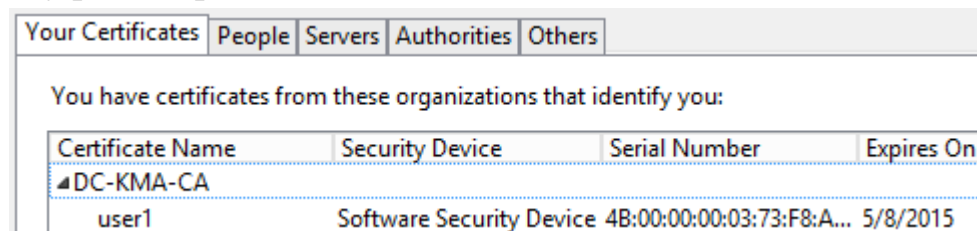


Chọn OK

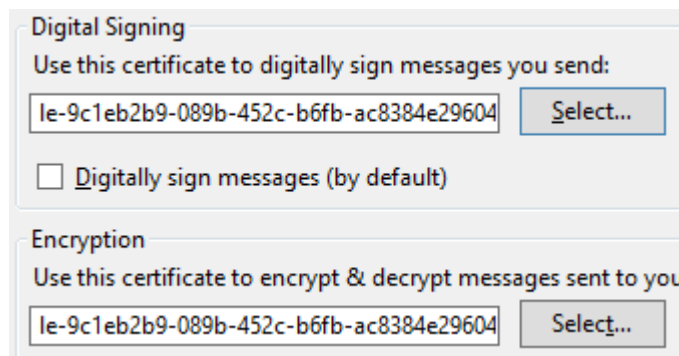
- Trong Tab People Import chứng thư của user1 với định dạng user1.cer



- Trong Tab People Import chứng thư của user2 với định dạng user2.cer (sau khi đã trình xuất ở phần sau)
- Trong Tab Your Certificates Import chứng thư của user1 với định dạng user1-key.pfx, nhập mật khẩu bảo vệ:



- Nhấn OK để kết thúc.
- Từ giao diện Account Setting trong mục Digital Signing và Encryption trở đến chứng thư đã Import:



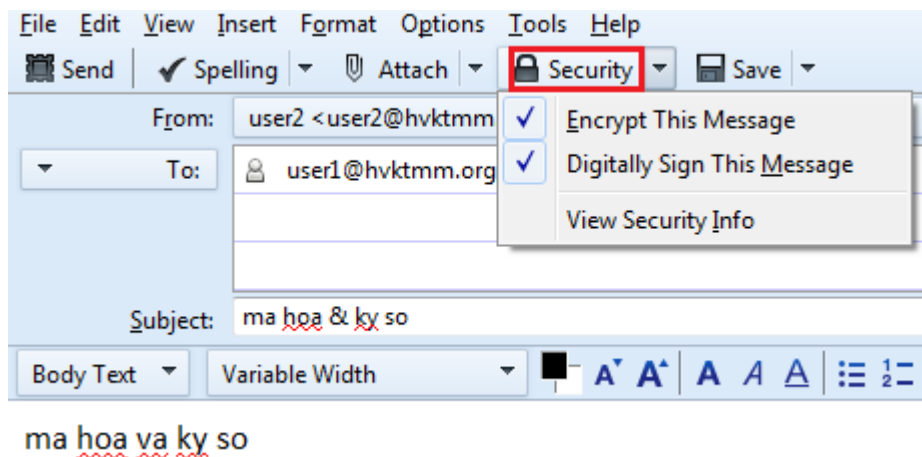
- Nhấn OK để kết thúc cấu hình chứng thư cho người dùng user1.

**Bước 7:** Cấp chứng thư, cài đặt chứng thư và Import chứng thư của người dùng user2 vào Thunderbird trên máy Windows 7

- Các bước thực hiện tương tự từ bước 1 đến bước 6 cho người dùng user1 trên máy chủ Windows Server 2012.
- Import thêm chứng thư của người dùng user1 với định dạng user1.cer vào Tab People

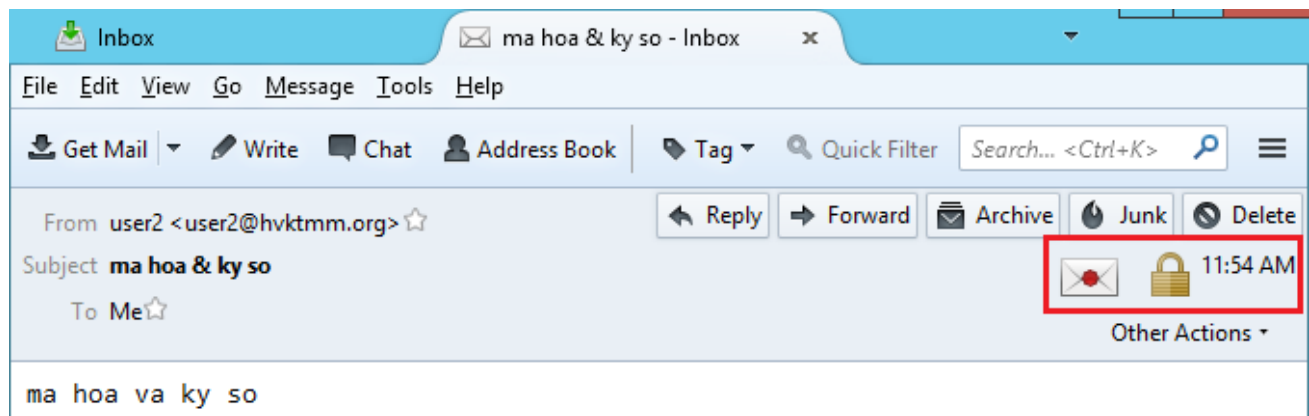
### 1.2.5 Gửi thư có mã hóa và ký số

**Bước 1:** Từ người dùng user2 soạn thư có mã hóa và ký số gửi cho user1



Gửi cho user1

**Bước 2:** chuyển sang tài khoản của user1 để kiểm tra kết quả



Kết quả người dùng user1 đã nhận được mail, trong mail có 2 biểu tượng ký số và mã hóa.

### Bước 3: Chặn bắt thông tin truyền

- Từ một máy chạy hệ điều hành XP và cài phần mềm Wireshark để chặn bắt thông tin truyền giữa máy Windows 7 và Windows Server 2012.
- Kết quả chặn bắt và phân tích thông tin.

```

Message-ID: <536BD4AE.1080709@hvktmm.org>
Date: Thu, 08 May 2014 12:02:06 -0700
From: user2 <user2@hvktmm.org>
User-Agent: Mozilla/5.0 (windows NT 6.1; rv:24.0) Gecko/20100101 Thunderb
MIME-Version: 1.0
To: user1@hvktmm.org
Subject: ky so & ma hoa
Content-Type: application/pkcs7-mime; name="smime.p7m"; smime-type=envelo
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: S/MIME Encrypted Message

MIAGCSqGSIb3DQEHA6CAMIACAQAxgGKMIHCAgEAMCswFDESMBAGA1UEAXMJREMTS01BLUNB
AhNLAAAAA3P4pgpgHZMMAAAAAAADMA0GCSqGSIb3DQEBAQUABIGASH4OXH19LcC5d4pQytPV
wfUPPGCAKKJhvexkrALT02Quu+UexREFKml6hiy5wv5lGphHts2GctHa0Qhq33QgKRijcwjN
OnP8HAXPJW5aTaqeZkhXctU+jD77CY2YJPLGx06U6lDc7E7GeCLYd1113jgchfADh1J19P58
73Cs ch8wgCICAQAwKZAUMRIWEAYDVQQDEW1EQY1LTUetQ0ECE0sAAAAEtfXddPgmaCAAAAA

```

Trong kết quả chặn bắt này, kẻ tấn công có thể biết được người gửi và người nhận, tiêu đề của mail, nhưng không biết được nội dung của mail, bởi vì đã được mã hóa.

## **Tài liệu tham khảo**

- [1] Microsoft. Windows Server 2012: Evaluation Guide. Năm 2012.
  - [2] Microsoft Official. Administering Windows Server 2012. Wiley. Năm 2013.
  - [3] Tom Adelstein, Bill Lubanovic. Linux System Administration. O'Reilly Media. Năm 2007.
  - [4] Remo Suppi Boldrito, Josep Jorba Esteve. GNU/Linux Advanced Administration. Năm 2008.
  - [5] Daniel P. Bovet, Marco Cesati. Understanding the Linux Kernel, 3rd Edition. O'Reilly Media. Năm 2005.
  - [6] Juliet Kemp. Linux System Administration Recipes: A Problem-Solution Approach. Apress. Năm 2009.
  - [7] Evi Nemeth, Garth Snyder. UNIX and Linux System Administration Handbook (4th Edition). Prentice Hall. Năm 2010.
  - [8] Configure the GRUB boot loader.
- Website:<http://www.tldp.org/HOWTO/Remote-Serial-Console-HOWTO/configure-boot-loader-grub.html>