| HỌC VIỆN KỸ THUẬT MẬT MÃ  **KHOA ATTT**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯ |
| --- |
| **CHỨNG THỰC ĐIỆN TỬ**  **TRIỂN KHAI HỆ THỐNG PKI ĐẢM BẢO AN TOÀN CHO DỊCH VỤ WEB VỚI PHẦN MỀM WINDOW CA** |
| *Nhóm sinh viên thực hiện*:  **Nguyễn Khánh Linh - AT180230**  **Lại Văn Hoàng - AT180220**  **Lê Xuân Phú - AT180239**    *Người hướng dẫn* :  **ThS. Đinh Tiến Thành**  Khoa Mật mã – Học viện Kỹ thuật mật mã |
| Hà Nội, 2025 |

# MỤC LỤC

[**MỤC LỤC 1**](#_heading=h.kdircjila85j)

[**DANH MỤC THUẬT NGỮ VIẾT TẮT 3**](#_heading=h.lutviis5os4)

[**DANH MỤC HÌNH VẼ 5**](#_heading=h.7qddeietvc6l)

[**LỜI NÓI ĐẦU 6**](#_heading=h.oti68xg20kyj)

[**CHƯƠNG 1. TỔNG QUAN VỀ CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI (PUBLIC KEY INFRASTRUCTURE – PKI) 7**](#_heading=h.fyox7gt2f1b9)

[1.1. Giới thiệu về cơ sở hạ tầng khóa công khai PKI 7](#_heading=h.fogqt36cn54g)

[1.1.1. Khái niệm 7](#_heading=h.yaj5mxysp4sl)

[1.1.2. Mục tiêu và chức năng 7](#_heading=h.x71zu0s8mafs)

[1.2. Các thành phần của PKI 8](#_heading=h.ughu7m3irz2u)

[1.2.1. Cơ quan chứng thực CA (Certification Authorities) 8](#_heading=h.5r9vaupb9b58)

[1.2.2. Trung tâm đăng ký RA (Registration Authorities) 9](#_heading=h.nro0es55bubl)

[1.2.3. Các thực thể đầu cuối (End Entities - EE) 9](#_heading=h.vau4mz2ikoqe)

[1.2.4. Kho lưu trữ các chứng chỉ (Certificate Repository – CR) 10](#_heading=h.4dv8hdebz12v)

[1.3. Một số kiến trúc PKI phổ biến 11](#_heading=h.vqbzmo769ld)

[1.3.1. Kiến trúc CA đơn 11](#_heading=h.g7357k93sjie)

[1.3.2. Kiến trúc phân cấp 11](#_heading=h.s6awy4y88ly)

[1.3.3. Kiến trúc mạng lưới 13](#_heading=h.7yk1eqpb56ge)

[1.3.4. Kiến trúc danh sách tin cậy mở rộng 14](#_heading=h.aqbj01itis6l)

[1.3.5. Kiến trúc chứng thực chéo 14](#_heading=h.gwvaw1afl941)

[1.3.6. Kiến trúc Bridge CA (BCA) 15](#_heading=h.dsc34eq2yere)

[1.4. Kết luận chương 1 16](#_heading=h.v340jvit0hm3)

[**CHƯƠNG 2. WINDOW CA TRONG BẢO MẬT DỊCH VỤ WEB 17**](#_heading=h.57qr2kavqh2d)

[2.1. Tổng quan về Windows Server 17](#_heading=h.igmts8z0l72r)

[2.1.1. Giới thiệu về Windows Server 17](#_heading=h.x4yji1x4ds4y)

[2.1.2. Một số tính năng nổi bật 17](#_heading=h.jpv02h5rlyjc)

[2.2. Dịch vụ Active Directory Certificate Services (AD CS) 19](#_heading=h.29xqdyxeg8sm)

[2.2.1. Khái niệm 19](#_heading=h.a7hr4egs9y57)

[2.2.2. Tính năng 19](#_heading=h.lf4v43y4pqec)

[2.2.2.1 .Cơ quan Chứng thực (CA): 19](#_heading=h.qrwu8njizd76)

[2.2.2.2. Đăng ký Web CA (Certification Authority Web Enrollment) 20](#_heading=h.6zjvfi3mt1zr)

[2.2.2.3. Trình Đáp ứng Trực tuyến (Online Responder) 20](#_heading=h.enbyx67sahox)

[2.2.2.4. Dịch vụ Đăng ký Thiết bị Mạng (Network Device Enrollment Service) 20](#_heading=h.n0zaz5ad3x72)

[2.2.2.5. Dịch vụ Web Đăng ký Chứng thư (Certificate Enrollment Web Service) 21](#_heading=h.rnz6lq2xfpkm)

[2.2.2.6. Dịch vụ Web Chính sách Đăng ký Chứng thư (Certificate Enrollment Policy Web Service) 21](#_heading=h.817t7v9rjkhp)

[2.2.3. Lợi ích 21](#_heading=h.9iadmmkt87qh)

[2.2.4. Nhược điểm 22](#_heading=h.3l4ekshr953s)

[2.3. Vai trò của Windows CA trong bảo vệ dịch vụ web 22](#_heading=h.k61cygjh0538)

[2.3.1. Giao thức HTTPS 22](#_heading=h.3jppsgrx8qb9)

[2.3.2. Giao thức SSL/TLS 23](#_heading=h.iio6zgstbe0j)

[2.3.3. Quá trình trình duyệt xác thực website thông qua CA 24](#_heading=h.91t3db1jbqd6)

[2.4. Kết luận chương 2 25](#_heading=h.gxkzh3kw9cye)

[**CHƯƠNG 3. TRIỂN KHAI THỰC NGHIỆM 26**](#_heading=h.ki9hlfiqvw9w)

[3.1. Mô tả bài toán 26](#_heading=h.ezytqteyy0cf)

[3.2. Triển khai thực nghiệm 26](#_heading=h.biq8rols0tff)

[3.2.1. Cấu hình địa chỉ IP 26](#_heading=h.daybryolspsb)

[3.2.2. Cài đặt DNS trên máy chủ Windows Server 2012 28](#_heading=h.8mitl5vtt8fj)

[3.2.3. Cài đặt dịch vụ web IIS trên máy chủ Windows Server 2012 37](#_heading=h.fn3mmuwlp0dr)

[3.2.4. Cài đặt dịch vụ Certification Authority (CA) 38](#_heading=h.p0m0wj7wcrf6)

[3.2.5. Cấu hình SSL cho dịch vụ Web 42](#_heading=h.1ssd9iokuan5)

[3.3. Kết luận chương 3 54](#_heading=h.qj7h8j769739)

[**KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 56**](#_heading=h.cogvi7r06y6c)

[1. Kết quả đạt được 56](#_heading=h.8a2qqumh8112)

[1.1. Về mặt lý thuyết 56](#_heading=h.qqog2idlwxgz)

[1.2. Về mặt thực nghiệm 56](#_heading=h.kp9a43xhougs)

[2. Hạn chế 56](#_heading=h.gw0bvok4mxzd)

[3. Hướng phát triển trong tương lai 57](#_heading=h.dnxk6fs28e4e)

[**TÀI LIỆU THAM KHẢO 58**](#_heading=h.q9xoh4y4pa20)

# 

# DANH MỤC THUẬT NGỮ VIẾT TẮT

| **Từ viết tắt** | **Giải nghĩa đầy đủ** | **Tiếng Việt** |
| --- | --- | --- |
| AD CS | Active Directory Certificate Services | Dịch vụ chứng thực Active Directory |
| AI | Artificial Intelligence | Trí tuệ nhân tạo |
| BCA | Bridge Certificate Authority | Cơ quan chứng thực cầu nối |
| CA | Certification Authority | Tổ chức chứng thực |
| CMD | Command Prompt | Giao diện dòng lệnh Windows |
| CR | Certificate Repository | Kho lưu trữ chứng thư số |
| CRL | Certificate Revocation List | Danh sách thu hồi chứng thư số |
| CSP | Certification Service Provider | Nhà cung cấp dịch vụ chứng thực |
| CTS | Common Trust Store | Kho lưu trữ tin cậy chung |
| DNS | Domain Name System | Hệ thống phân giải tên miền |
| EE | End Entity | Thực thể cuối |
| EFS | Encrypting File System | Hệ thống mã hóa tệp tin |
| HTTPS | Hypertext Transfer Protocol Secure | Giao thức truyền siêu văn bản bảo mật |
| IE | Internet Explorer | Trình duyệt Internet Explorer |
| IIS | Internet Information Services | Dịch vụ máy chủ web của Microsoft |
| IP | Internet Protocol | Giao thức Internet |
| IPSec | Internet Protocol Security | Giao thức bảo mật tầng mạng IP |
| IoT | Internet of Things | Mạng lưới vạn vật kết nối Internet |
| MMC | Microsoft Management Console | Bảng điều khiển quản trị Microsoft |
| NAP | Network Access Protection | Cơ chế bảo vệ truy cập mạng |
| NDES | Network Device Enrollment Service | Dịch vụ đăng ký thiết bị mạng |
| NIST | National Institute of Standards and Technology | Viện Tiêu chuẩn và Công nghệ Quốc gia (Hoa Kỳ) |
| OCSP | Online Certificate Status Protocol | Giao thức kiểm tra trạng thái chứng thư số trực tuyến |
| P2P | Peer to Peer | Mô hình mạng ngang hàng |
| PKI | Public Key Infrastructure | Hạ tầng khóa công khai |
| POP | Proof of Possession | Bằng chứng sở hữu khóa |
| PTR | Pointer Record | Bản ghi con trỏ (trong phân giải DNS ngược) |
| RA | Registration Authority | Cơ quan đăng ký chứng thư số |
| RDS | Remote Desktop Services | Dịch vụ truy cập máy tính từ xa |
| SQL | Structured Query Language | Ngôn ngữ truy vấn có cấu trúc |
| SP | Special Publication | Ấn phẩm chuyên đề (thuộc NIST) |
| SSL | Secure Sockets Layer | Giao thức bảo mật tầng ổ cắm |
| URL | Uniform Resource Locator | Định danh tài nguyên thống nhất |
| VA | Validation Authority | Cơ quan xác thực chứng thư số |
| VPN | Virtual Private Network | Mạng riêng ảo |

# 

# DANH MỤC HÌNH VẼ

Hình 1.1. Các thành phần chính của PKI8

Hình 1.2. Kho lưu trữ các chứng chỉ10

Hình 1.3. Kiến trúc đơn11

Hình 1.4. Kiến trúc phân cấp12

Hình 1.5. Kiến trúc mạng lưới13

Hình 1.6. Kiến trúc danh sách tin cậy mở rộng14

Hình 1.7. Kiến thức chứng thực chéo15

Hình 1.8. Kiến trúc Bridge CA16

Hình 2.1. Giao diện của Microsoft Active Directory Certificate Services19

Hình 2.2. Giao thức HTTPS23

Hình 2.3. Website đang sử dụng TLS để bảo vệ thông tin24

# 

# LỜI NÓI ĐẦU

Trong kỷ nguyên số, khi các dịch vụ web ngày càng phổ biến, vấn đề bảo mật thông tin trở thành một trong những mối quan tâm hàng đầu. Việc đảm bảo tính toàn vẹn, tính xác thực và tính bí mật của dữ liệu trao đổi trên môi trường mạng không chỉ là yêu cầu kỹ thuật, mà còn là yếu tố then chốt để xây dựng niềm tin giữa các bên tham gia. Trong bối cảnh đó, cơ sở hạ tầng khóa công khai (Public Key Infrastructure – PKI) đã và đang khẳng định vai trò trọng yếu như một nền tảng công nghệ đảm bảo chứng thực điện tử an toàn và hiệu quả.

Với mong muốn tìm hiểu sâu hơn về lý thuyết và ứng dụng thực tiễn của PKI, nhóm chúng em thực hiện đề tài "Triển khai hệ thống PKI đảm bảo an toàn cho dịch vụ web với phần mềm Windows CA". Đề tài không chỉ dừng lại ở việc nghiên cứu các khái niệm và kiến trúc liên quan đến PKI, mà còn tập trung triển khai một hệ thống thực nghiệm sử dụng các dịch vụ sẵn có trên nền tảng Windows Server, qua đó thiết lập mô hình dịch vụ web được bảo vệ bằng chứng chỉ số SSL/TLS.

Báo cáo gồm ba chương chính:

Chương 1: Tổng quan về cơ sở hạ tầng khóa công khai (Public Key Infrastructure – PKI)

Chương 2: Windows CA trong việc bảo vệ dịch vụ Web

Chương 3: Triển khai thực nghiệm

# CHƯƠNG 1. TỔNG QUAN VỀ CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI (PUBLIC KEY INFRASTRUCTURE – PKI)

## 1.1. Giới thiệu về cơ sở hạ tầng khóa công khai PKI

### 1.1.1. Khái niệm

Trong mật mã học, hạ tầng khóa công khai (PKI) là một cơ chế để cho một bên thứ 3 (thường là nhà cung cấp chứng thực số) cung cấp và xác thực định danh các bên tham gia vào quá trình trao đổi thông tin. Cơ chế này cũng cho phép gán cho mỗi người sử dụng trong hệ thống một cặp khóa công khai/khóa bí mật. Các quá trình này thường được thực hiện bởi một phần mềm đặt tại trung tâm và các phần mềm phối hợp khác tại các địa điểm của người dùng. Khóa công khai thường được phân phối trong chứng thực khóa công khai.

Khái niệm cơ sở hạ tầng khóa công khai thường được dùng để chỉ toàn bộ hệ thống bao gồm nhà cung cấp chứng thực số (Certificate Authority) cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mã hóa khóa công khai trong trao đổi thông tin.

Ngoài ra, PKI còn được định nghĩa theo NIST SP 800-53, cơ sở hạ tầng khóa công khai là một bộ khung và các dịch vụ cung cấp khả năng tạo lập, phân phối, kiểm tra, kiểm soát và thu hồi các chứng thư khóa công khai. Các thành phần của cơ sở hạ tầng khóa công khai bao gồm con người, chính sách, quy trình, nền tảng máy chủ, phần mềm và máy trạm được sử dụng cho mục đích quản lý chứng thư số và các cặp khóa công khai - khóa riêng, bao gồm khả năng cấp phát, duy trì, khôi phục và thu hồi chứng thư khóa công khai.

### 1.1.2. Mục tiêu và chức năng

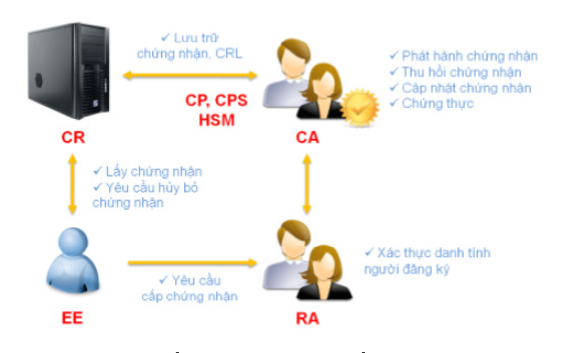
PKI cho phép những người tham gia xác thực lẫn nhau và sử dụng thông tin từ các chứng thư khóa công khai để mã hóa và giải mã thông tin trong quá trình trao đổi. PKI cho phép các giao dịch điện tử được diễn ra đảm bảo tính bí mật, toàn vẹn xác thực lẫn nhau và chống chối bỏ mà không cần phải trao đổi các thông tin mật từ trước.

* **Xác thực (Authentication):** Đảm bảo rằng một thực thể (người dùng, thiết bị, hệ thống) là đúng như họ khai báo.
* **Bí mật (Confidentiality):** Đảm bảo rằng dữ liệu chỉ có thể được đọc bởi những người hoặc hệ thống được ủy quyền.
* **Toàn vẹn (Integrity):** Đảm bảo rằng thông tin không bị sửa đổi hoặc giả mạo trong quá trình lưu trữ hoặc truyền tải.
* **Tính chống chối bỏ (Non-repudiation):** Ngăn chặn các bên liên quan từ chối hành vi đã thực hiện, như gửi hoặc nhận thông điệp.

PKI tận dụng cả mật mã đối xứng và phi đối xứng để để đạt được những tính năng cơ bản trên.

## 1.2. Các thành phần của PKI

PKI là cơ cấu tổ chức gồm con người, tiến trình, chính sách, thủ tục, phần cứng và phần mềm dùng để phát sinh, quản lý, lưu trữ, triển khai và thu hồi các chứng nhận khóa công khai.



Hình 1.1. Các thành phần chính của PKI

### 1.2.1. Cơ quan chứng thực CA (Certification Authorities)

Trong hạ tầng cơ sở khóa công khai, chứng chỉ có vai trò gắn kết giữa định danh với khoá công khai. Sự gắn kết này thể hiện trong dạng cấu trúc dữ liệu được ký số được đề cập đến như chứng chỉ đã được thảo luận ở phần trước. Một certificate authority (CA) là một thực thể PKI có trách nhiệm cấp chứng chỉ cho các thực thể khác trong hệ thống.

Cơ quan chứng thực - CA cũng được gọi là bên thứ ba được tin tưởng vì người sử dụng cuối tin tưởng vào chữ ký số của CA trên chứng chỉ trong khi thực hiện những hoạt động mã hoá khoá công khai cần thiết. Tổ chức cung cấp dịch vụ chứng thực – Certification Service Provider (CSP).

Thông thường, CA thực hiện chức năng xác thực bằng cách cấp chứng chỉ cho các CA khác và cho thực thể cuối (người giữ chứng chỉ) trong hệ thống. Nếu CA nằm ở đỉnh của mô hình phân cấp PKI và chỉ cấp chứng chỉ cho những CA ở mức thấp hơn thì chứng chỉ này được gọi là chứng chỉ gốc “root certificate”.

### 1.2.2. Trung tâm đăng ký RA (Registration Authorities)

Là cơ quan chịu trách nhiệm xác nhận về tính trung thực của yêu cầu sử dụng chứng thư số. RA không có trách nhiệm sinh và ký chứng thư. RA sau khi nhận yêu cầu sẽ chuyển sang CA để thực hiện. Kết quả của CA sẽ được chuyển tới người yêu cầu thông qua RA

Chức năng thực hiện của một RA cụ thể sẽ khác nhau tùy theo nhu cầu triển khai PKI nhưng chủ yếu bao gồm những chức năng sau:

* Xác thực cá nhân chủ thể đăng ký chứng chỉ.
* Kiểm tra tính hợp lệ của thông tin do chủ thể cung cấp.
* Xác nhận quyền của chủ thể đối với những thuộc tính chứng chỉ được yêu cầu.
* Kiểm tra xem chủ thể có thực sự sở hữu khoá riêng đang được đăng ký hay không, điều này thường được đề cập đến như sự chứng minh sở hữu (proof of possession - POP).

### 1.2.3. Các thực thể đầu cuối (End Entities - EE)

Thực thể cuối trong PKI có thể là con người, thiết bị, và thậm chí là một chương trình phần mềm nhưng thường là người sử dụng hệ thống.

Một EE có khả năng tham gia vào quá trình mã hóa và giải mã thông điệp. Nó sẽ sử dụng khóa công khai để mã hóa thông điệp và sử dụng khóa bí mật (private key) tương ứng để giải mã thông điệp đã được mã hóa.

Các thực thể đầu cuối đóng vai trò quan trọng trong việc xác thực và xác định danh tính của người dùng hoặc thiết bị trong hệ thống mật mã. Chúng cung cấp các chứng thư số (certificates) chứng minh rằng khóa công khai được liên kết với thực thể đầu cuối đó là hợp lệ và tin cậy.

Các thực thể đầu cuối thường được quản lý và phân phối chứng chỉ bởi một cơ quan tin cậy, như một cơ quan chứng thực (Certificate Authority - CA). Cơ quan này sẽ xác nhận danh tính của các EE và cung cấp chứng chỉ số cho họ, từ đó tạo ra một hạ tầng khóa công khai tin cậy và an toàn.

### 1.2.4. Kho lưu trữ các chứng chỉ (Certificate Repository – CR)

Hệ thống (có thể tập trung hoặc phân tán) lưu trữ chứng thư và danh sách các chứng thư bị thu hồi.

Cung cấp cơ chế phân phối chứng thư và danh sách thu hồi chứng thư (CRLs – Certificate Revocation Lists).

### 

Hình 1.2. Kho lưu trữ các chứng chỉ

(1) : Người dùng gửi yêu cầu phát hành thẻ chứng thư số và khóa công khai của nó đến RA;

(2) : Sau khi xác nhận tính hợp lệ định danh của người dùng thì RA sẽ chuyển yêu cầu này đến CA;

(3) : CA phát hành thẻ chứng thư số cho người dùng;

(4) : Sau đó người dùng “ký” thông điệp trao đổi với thẻ chứng thư số mới vừa nhận được từ CA và sử dụng chúng (thẻ chứng thực số + chữ ký số) trong giao dịch;

(5) : Định danh của người dùng được kiểm tra bởi đối tác thông qua sự hỗ trợ của VA; (VA (validation authority) : Cơ quan xác thực của bên thứ ba có thể cung cấp thông tin thực thể này thay mặt cho CA.)

(6) : Nếu chứng thư số của người dùng được xác nhận tính hợp lệ thì đối tác mới tin cậy người dùng và có thể bắt đầu quá trình trao đổi thông tin với nó (VA nhận thông tin về thẻ chứng thư số đã được phát hành từ CA (a))

## 

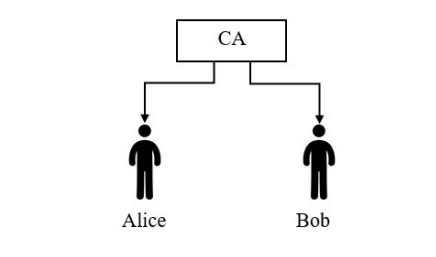
## 1.3. Một số kiến trúc PKI phổ biến

### 1.3.1. Kiến trúc CA đơn

Kiến trúc CA đơn là mô hình đơn giản nhất trong hệ thống hạ tầng khóa công khai (PKI). Trong mô hình này, chỉ có một CA (Certificate Authority) duy nhất đảm nhiệm việc cấp phát chứng thư số và phân phối danh sách thu hồi chứng thư (CRL). Tất cả các đối tượng trong hệ thống đều tin tưởng CA này và chỉ sử dụng chứng thư do nó cấp. Do chỉ có một CA tồn tại, nên không hình thành mối quan hệ tin cậy giữa các CA như trong các mô hình phức tạp khác. Đồng thời, mô hình này cũng không hỗ trợ thêm các CA mới vào hệ thống PKI.

Ưu điểm của kiến trúc CA đơn là dễ quản lý, vì toàn bộ hoạt động quản trị đều tập trung tại CA gốc (Root CA). Tuy nhiên, điểm yếu lớn nhất là nếu CA gặp sự cố, toàn bộ dịch vụ chứng thư sẽ bị gián đoạn: không thể cấp mới chứng thư, gia hạn hoặc cung cấp CRL cho đến khi CA được phục hồi.

Vì lý do đó, mô hình CA đơn thường chỉ phù hợp với các hệ thống đơn giản, ít phức tạp và yêu cầu chi phí triển khai thấp.

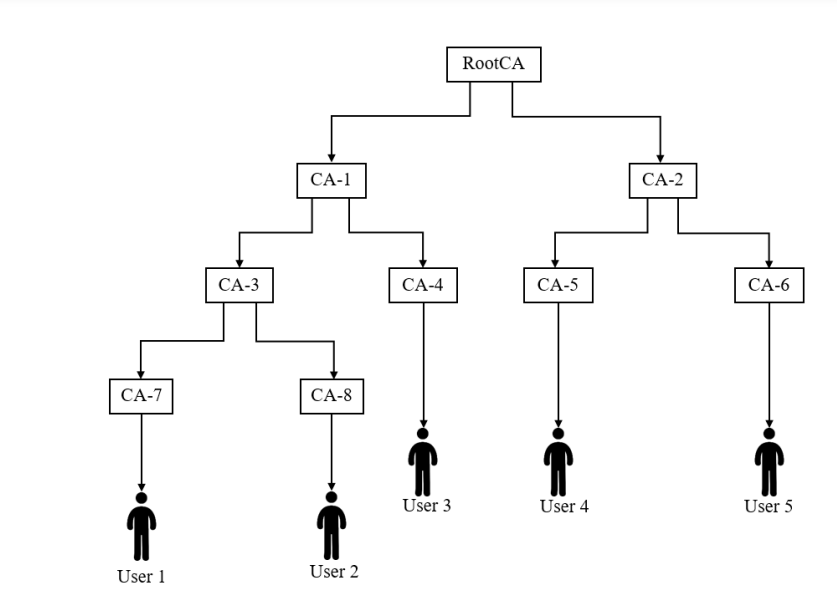


Hình 1.3. Kiến trúc đơn

### 1.3.2. Kiến trúc phân cấp

Kiến trúc CA phân cấp là một mô hình tổ chức hệ thống chứng thực số được sử dụng rộng rãi trong các tổ chức lớn. Trong mô hình này, toàn bộ hệ thống được tổ chức theo dạng hình cây, với một Root CA (CA gốc) nằm ở đỉnh, đóng vai trò là trung tâm tin cậy tuyệt đối. Phía dưới Root CA là một hoặc nhiều lớp CA cấp dưới (Subordinate CAs), có nhiệm vụ cấp phát và quản lý chứng chỉ cho các thực thể như người dùng, máy tính, thiết bị và các đơn vị RA (Registration Authority).

Điểm đặc trưng của mô hình phân cấp là mỗi CA cấp dưới chỉ có một CA cấp trên, tạo thành một chuỗi tin cậy rõ ràng và dễ quản lý. Mọi thực thể trong hệ thống đều đặt niềm tin vào khóa công khai của Root CA, vì tất cả các chứng chỉ đều xuất phát gián tiếp hoặc trực tiếp từ Root CA thông qua quy trình ký xác thực. Root CA không trực tiếp cấp chứng chỉ cho người dùng cuối; thay vào đó, vai trò này được giao cho các Subordinate CA, giúp phân tán trách nhiệm và tăng cường bảo mật cho Root CA.



Hình 1.4. Kiến trúc phân cấp

Một ưu điểm quan trọng của mô hình này là khả năng áp dụng thống nhất các chính sách bảo mật, tiêu chuẩn và quy trình quản lý trong toàn bộ hệ thống PKI. Việc phân cấp rõ ràng giúp tổ chức dễ dàng mở rộng hệ thống: có thể bổ sung CA mới tại bất kỳ cấp nào phù hợp với nhu cầu thay đổi hoặc phát triển cấu trúc tổ chức. Mô hình này tương tự như cách tổ chức hệ thống tên miền (DNS) trên Internet — có sự phân tầng và quản lý phân cấp rõ ràng.

Tuy nhiên, giống như bất kỳ hệ thống nào, kiến trúc CA phân cấp cũng tiềm ẩn những rủi ro nhất định. Nếu một Subordinate CA bị xâm nhập hoặc thỏa hiệp, CA cấp trên của nó phải thu hồi chứng chỉ đã cấp và tạm ngưng hoạt động của CA đó cho đến khi vấn đề được khắc phục. Sau khi được khôi phục an toàn, Subordinate CA sẽ được cấp lại chứng chỉ mới để tiếp tục hoạt động.

### 1.3.3. Kiến trúc mạng lưới

Trong mô hình này, mỗi người dùng trong mạng lưới có thể lựa chọn tin tưởng vào một CA bất kỳ, không yêu cầu toàn bộ người dùng phải chia sẻ cùng một nguồn tin cậy. Việc xác thực phụ thuộc vào việc người dùng tin tưởng vào CA nào, và chỉ cần tin vào một CA là có thể chấp nhận các chứng chỉ do CA đó phát hành.

# 

Hình 1.5. Kiến trúc mạng lưới

Các CA trong mạng lưới thiết lập mối quan hệ tin cậy lẫn nhau bằng cách trao đổi và xác thực chéo chứng chỉ. Khi hai CA cùng cấp chứng chỉ cho nhau, một liên kết tin cậy hai chiều được hình thành. Việc mở rộng mạng lưới được thực hiện bằng cách thêm các CA mới thông qua quá trình xây dựng các mối quan hệ tin cậy lẫn nhau với các CA hiện có trong hệ thống.

Do không có một điểm trung tâm duy nhất, kiến trúc này giảm thiểu rủi ro tập trung so với mô hình phân cấp. Khi một CA trong hệ thống bị xâm phạm, hệ thống không bị sụp đổ hoàn toàn. Các CA khác trong mạng có thể chủ động thu hồi các chứng chỉ đã cấp cho CA bị ảnh hưởng. Chỉ khi CA bị xâm phạm được khôi phục và xây dựng lại niềm tin với các CA khác, nó mới có thể tiếp tục hoạt động và cấp phát chứng chỉ trở lại.

### 1.3.4. Kiến trúc danh sách tin cậy mở rộng

Kiến trúc danh sách tin cậy mở rộng là một mô hình mở rộng từ kiến trúc danh sách tin cậy, nhằm hỗ trợ các đường dẫn chứng thực dài hơn một hệ thống tin cậy đơn (CTS). Trong mô hình này, thực thể cuối (như người dùng hoặc thiết bị) sẽ duy trì một danh sách các điểm tin cậy – là nơi bắt đầu cho quá trình xác thực chứng chỉ. Mỗi điểm tin cậy có thể là một cơ quan chứng thực đơn (CA đơn), một hệ thống PKI phân cấp, hoặc một mạng lưới PKI. Nhờ đó, hệ thống có thể liên kết các tổ chức khác nhau thông qua các mối quan hệ tin cậy được thiết lập trước, cho phép các thực thể từ các tổ chức khác nhau xác thực lẫn nhau một cách an toàn và linh hoạt.

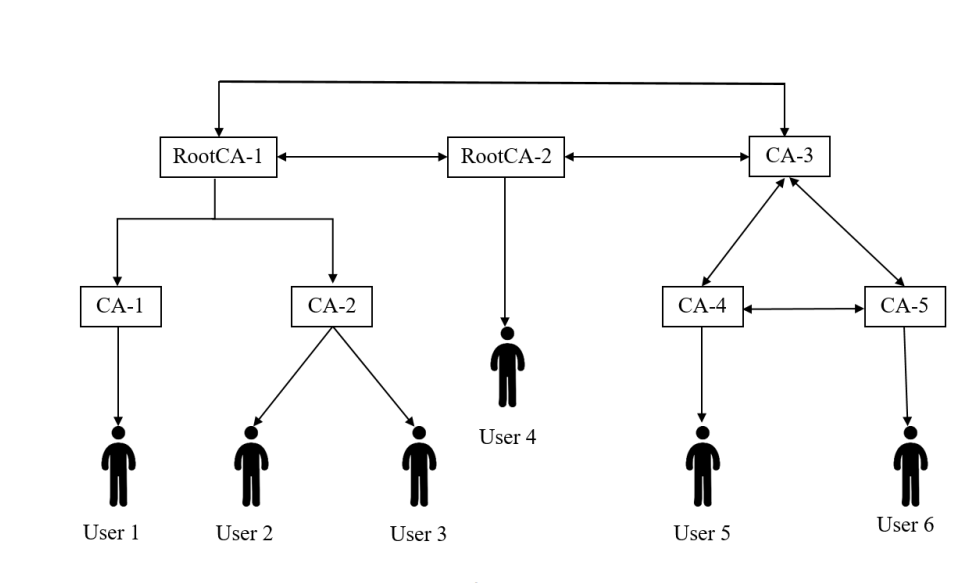
Cấu trúc này phù hợp với các mô hình lớn, phức tạp, đòi hỏi sự liên kết chặt chẽ giữa nhiều hệ thống PKI độc lập hoặc bán độc lập.

# 

Hình 1.6. Kiến trúc danh sách tin cậy mở rộng

### 1.3.5. Kiến trúc chứng thực chéo

Trong kiến trúc xác thực chéo, CA gốc hoặc CA cấp dưới của một PKI cụ thể sẽ thiết lập mối quan hệ ngang hàng với CA gốc hoặc CA cấp dưới của PKI khác.

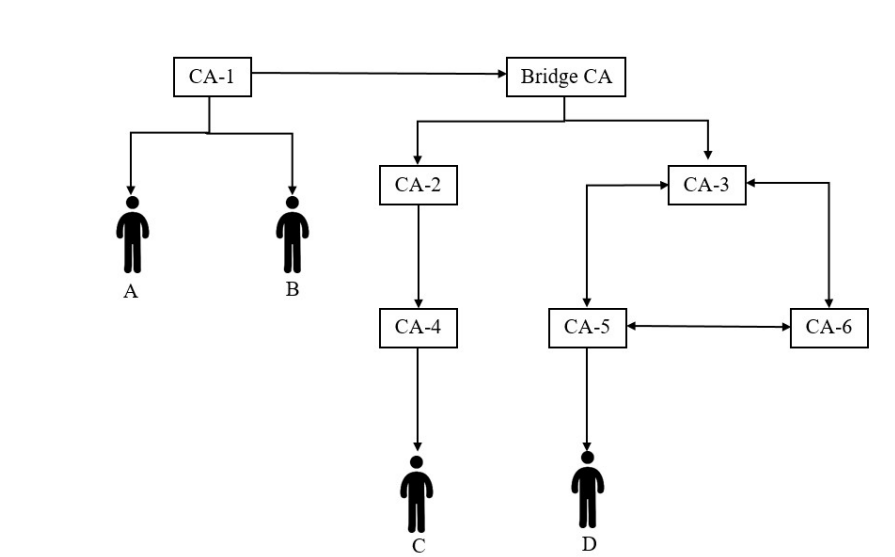


Hình 1.7. Kiến thức chứng thực chéo

Mỗi người dùng sẽ có một điểm tin cậy riêng. Mối quan hệ xác thực chéo giữa các doanh nghiệp là mối quan hệ ngang hàng. Mỗi CA được xác thực chéo với nhau, các đối tượng của họ có thể xác thực các đối tượng trong PKI khác. Do đó, một hành động duy nhất có thể cho phép liên lạc an toàn giữa tất cả người dùng chéo trong các PKI. Kiến trúc này phù hợp cho một số nhỏ doanh nghiệp PKI cần thiết lập mối quan hệ tin cậy.

### 1.3.6. Kiến trúc Bridge CA (BCA)

Bridge CA được thiết kế để giải quyết các thiếu sót trong các kiến trúc PKI cơ bản và tạo kết nối các PKI khác nhau. Bridge CA không cấp chứng thư cho người dùng và chúng không phải là nguồn tin cậy. Thay vào đó, Bridge CA sẽ thiết lập mối quan hệ tin cậy peer to peer (P2P) giữa các cộng đồng người dùng khác nhau và làm giảm nhẹ vấn đề cấp phát chứng thư giữa các tổ chức trong khi đó lại cho phép người dùng giữ được nguồn tin cậy.



Hình 1.8. Kiến trúc Bridge CA

Trong kiểu kiến trúc này, Bridge CA sẽ cung cấp một cái cầu tin cậy (thông qua cặp chứng thực chéo) giữa các cơ sở hạ tầng khóa công khai phân cấp và cơ sở hạ tầng khóa công khai chứng thực chéo. Độ phức tạp của mô hình này khá cao và có thể phải điều chỉnh các module PKI của người dùng cuối. Mỗi một mối quan hệ tin cậy Bridge CA được thể hiện bằng một cặp chứng thư, một được cấp phát bởi BCA.

## 1.4. Kết luận chương 1

Trong chương này, chúng ta đã khám phá tổng quan về cơ sở hạ tầng khóa công khai (PKI) – một thành phần cốt lõi trong hệ thống bảo mật thông tin hiện đại. PKI đóng vai trò nền tảng trong việc thiết lập môi trường trao đổi thông tin an toàn bằng cách cung cấp các cơ chế xác thực, mã hóa và quản lý khóa công khai – khóa bí mật.

Các thành phần như cơ quan chứng thực (CA), trung tâm đăng ký (RA), thực thể đầu cuối (EE) và kho lưu trữ chứng chỉ phối hợp với nhau để đảm bảo các nguyên tắc bảo mật: xác thực, toàn vẹn, bí mật và chống chối bỏ. Ngoài ra, chương cũng trình bày các mô hình kiến trúc PKI tiêu biểu như mô hình CA đơn, phân cấp, mạng lưới, Bridge CA và xác thực chéo, cho phép triển khai linh hoạt tùy theo quy mô và nhu cầu bảo mật của từng tổ chức.

# CHƯƠNG 2. WINDOW CA TRONG BẢO MẬT DỊCH VỤ WEB

## 2.1. Tổng quan về Windows Server

### 2.1.1. Giới thiệu về Windows Server

Windows Server là một dòng hệ điều hành chuyên dụng do Microsoft phát triển, được thiết kế đặc biệt để vận hành trên máy chủ. Máy chủ là những cỗ máy mạnh mẽ, hoạt động liên tục để cung cấp tài nguyên và dịch vụ cho các máy tính khác trong mạng.

Chức năng chính của Windows Server bao gồm chia sẻ dịch vụ, lưu trữ dữ liệu, vận hành ứng dụng và quản lý tài nguyên cho doanh nghiệp. Do đó, đối tượng sử dụng chủ yếu của Windows Server là các doanh nghiệp và tổ chức cần một nền tảng mạnh mẽ và ổn định để quản lý hạ tầng công nghệ thông tin của họ. Người dùng máy tính thông thường hiếm khi tiếp xúc hoặc cần sử dụng đến Windows Server.

### 2.1.2. Một số tính năng nổi bật

Windows Server không chỉ là một hệ điều hành thông thường chúng ta thường gặp trên máy tính cá nhân, mà còn là một nền tảng mạnh mẽ được thiết kế đặc biệt để đáp ứng nhu cầu quản lý, bảo mật và triển khai các tài nguyên mạng và hạ tầng trong môi trường doanh nghiệp. Dưới đây là một cái nhìn chi tiết về những tính năng nổi bật của Windows Server:

* Quản lý Tài Nguyên Mạng và Hạ Tầng:
* Windows Server cho phép quản lý các tài nguyên mạng như máy tính, máy in, thiết bị lưu trữ và dịch vụ mạng một cách hiệu quả.
* Tạo và quản lý các tài khoản người dùng, nhóm và cơ cấu tổ chức với mục tiêu tăng tính quản lý và bảo mật.
* Triển Khai Ứng Dụng và Dịch Vụ:
* Hỗ trợ triển khai và quản lý các ứng dụng doanh nghiệp như máy chủ web (IIS), cơ sở dữ liệu (SQL Server), dịch vụ email (Exchange Server) và ứng dụng đám mây.
* Cung cấp tính năng tối ưu hóa hiệu suất và bảo mật cho các ứng dụng quan trọng của tổ chức.
* Quản Lý Cơ Sở Dữ Liệu:
* Cung cấp dịch vụ quản lý cơ sở dữ liệu với hỗ trợ đặc biệt cho các hệ quản lý cơ sở dữ liệu như SQL Server.
* Lưu trữ, quản lý và bảo mật dữ liệu kinh doanh quan trọng của tổ chức.
* Bảo Mật Hệ Thống:
* Sở hữu cơ chế bảo mật mạnh mẽ, bao gồm xác thực người dùng, kiểm soát truy cập và mã hóa dữ liệu.
* Tính năng như Windows Defender và Windows Firewall giúp bảo vệ máy chủ khỏi các mối đe dọa bảo mật.
* Quản Lý Quyền và Chính Sách:
* Cho phép xác định và quản lý quyền truy cập của người dùng vào các tài nguyên và dịch vụ.
* Thiết lập chính sách bảo mật để đảm bảo tuân thủ các quy định và yêu cầu an ninh.
* Quản Lý và Điều Khiển Từ Xa:
* Cung cấp công cụ quản lý từ xa, cho phép quản trị viên kiểm soát và giám sát máy chủ từ xa.
* Remote Desktop Services (RDS) tạo điều kiện cho người dùng truy cập máy chủ để làm việc từ xa.
* Ảo Hoá Máy Chủ:
* Hỗ trợ ảo hóa máy chủ, cho phép tạo và quản lý các máy chủ ảo trên một máy chủ vật lý duy nhất.
* Hyper-V là một ví dụ về nền tảng ảo hóa tích hợp trong Windows Server.
* Quản Lý Chuỗi Cung Ứng và Công Nghệ Đám Mây:
* Tích hợp Kubernetes để hỗ trợ triển khai và quản lý các ứng dụng dựa trên container.
* Xây dựng môi trường đám mây riêng (private cloud) để quản lý tài nguyên và dịch vụ.
* Tích Hợp Công Nghệ Mới:
* Liên tục cập nhật để tích hợp các công nghệ mới như trí tuệ nhân tạo (AI), Internet of Things (IoT), và tích hợp các tính năng đám mây như Azure.

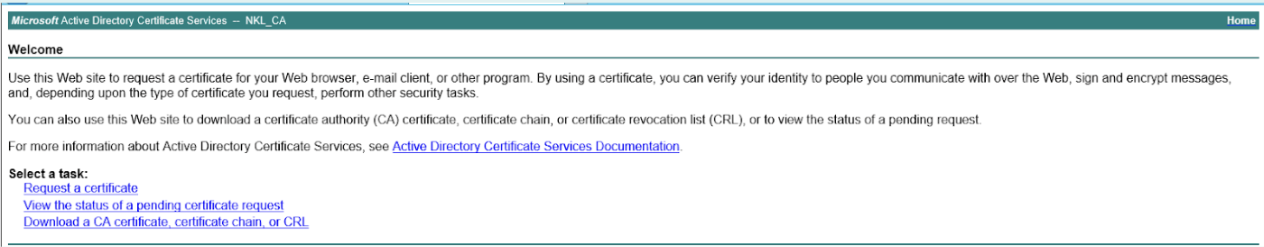
Windows Server mang đến một giải pháp toàn diện, đáp ứng đa dạng nhu cầu của doanh nghiệp trong việc quản lý và phát triển hạ tầng mạng của họ.

## 2.2. *Dịch vụ Active Directory Certificate Services (AD CS)*

### 2.2.1. Khái niệm

Microsoft Active Directory Certificate Services (AD CS) là một trong các vai trò máy chủ được giới thiệu trong Windows Server 2008, cung cấp cho người dùng các dịch vụ tùy chỉnh để tạo và quản lý chứng thư Hạ tầng khóa công khai (PKI), có thể sử dụng để mã hóa và ký số điện tử các tài liệu, email, và tin nhắn.

Các ứng dụng được hỗ trợ bởi AD CS bao gồm mạng không dây bảo mật, Mạng riêng ảo (VPN), Bảo mật Giao thức Internet (IPSec), Bảo vệ Truy cập Mạng (NAP), Hệ thống Mã hóa Tệp (EFS), đăng nhập bằng thẻ thông minh, và nhiều hơn nữa.



Hình 2.1. Giao diện của Microsoft Active Directory Certificate Services

### 2.2.2. Tính năng

Microsoft Active Directory Certificate Services có nhiều tính năng để phục vụ cho các kịch bản triển khai khác nhau:

#### 2.2.2.1 .Cơ quan Chứng thực (CA):

Cơ quan Chứng thực trong AD CS chủ yếu quản lý và phát hành chứng thư khóa công khai. Nhiều CA có thể được liên kết để tạo thành một PKI. Một PKI điển hình là sự kết hợp của phần mềm, phần cứng, tiêu chuẩn, dịch vụ và chính sách để quản lý các chứng thư số sử dụng trong PKI. CA có thể là hai loại:

* **CA Doanh nghiệp:** Phải là thành viên của Domain và có thể phát hành chứng thư cho chữ ký số, xác thực truy cập các trình duyệt web bảo vệ, và bảo mật giao dịch email.
* **CA Độc lập:** Không yêu cầu Active Directory Domain Services, có thể hoạt động ngoại tuyến và không nên kết nối với mạng.

#### 2.2.2.2. Đăng ký Web CA (Certification Authority Web Enrollment)

Đăng ký Web CA trong AD CS cho phép các khách hàng bên ngoài, không thuộc mạng miền, kết nối với CA qua trình duyệt Internet. Đăng ký Web CA chỉ hỗ trợ các yêu cầu tương tác mà người yêu cầu thực hiện và tải lên thủ công qua trang web. Chứng thư có thể được tải xuống từ trình duyệt sau khi CA phát hành chứng thư. Dịch vụ này cũng có thể được sử dụng để yêu cầu Danh sách Thu hồi Chứng thư (CRL), bao gồm tất cả các chứng thư đã hết hạn hoặc bị thu hồi trong PKI.

Đối với người dùng thuộc miền, mối quan hệ tin cậy cho phép CA phát hành chứng thư một cách an toàn. Đăng ký web cho phép các khách hàng bên ngoài yêu cầu và thu hồi chứng thư từ CA. Việc đăng ký cũng có thể được thực hiện giữa các rừng, nghĩa là các khách hàng trong một rừng có thể nhận chứng thư từ một CA trong rừng khác. Để sử dụng đăng ký giữa các rừng, bạn phải thiết lập mối quan hệ tin cậy giữa tất cả các rừng liên quan và mức độ tin cậy và cấp độ rừng phải được thiết lập ở Windows Server 2008 R2 hoặc các phiên bản liên quan khác.

#### 

#### 2.2.2.3. Trình Đáp ứng Trực tuyến (Online Responder)

Trình Đáp ứng Trực tuyến là một dịch vụ Windows của Microsoft chạy trên máy chủ OCSP với các đặc quyền Dịch vụ Mạng. Trong AD CS, trình đáp ứng trực tuyến nhận và xử lý các yêu cầu về trạng thái của chứng thư. Tính hợp lệ của chứng thư và chữ ký số được xác minh để xác định chứng thư có hợp lệ hay không. Ngoài ra, chứng thư được kiểm tra xem có thuộc Danh sách Thu hồi Chứng thư (CRL) hay không.

Do nhiều lý do, chứng thư có thể bị thu hồi tạm thời hoặc bị tước quyền vĩnh viễn trước khi hết hạn bởi CA và các chứng thư này được liệt kê trong CRL. Ngoài CRL, việc kiểm tra thu hồi cũng có thể được thực hiện bởi phản hồi Giao thức Trạng thái Chứng thư Trực tuyến (OCSP). OCSP kiểm tra trạng thái của trang web bằng cách gửi URL tới Cơ quan Chứng thực. Cơ quan Chứng thực cung cấp phản hồi có chữ ký chứa trạng thái của chứng thư được yêu cầu.

#### 

#### 2.2.2.4. Dịch vụ Đăng ký Thiết bị Mạng (Network Device Enrollment Service)

Dịch vụ Đăng ký Thiết bị Mạng (NDES) trong AD CS có khả năng phát hành chứng thư cho các thiết bị mạng quản lý lưu lượng như bộ định tuyến, tường lửa và chuyển mạch. Các thiết bị này không phải là thành viên miền Active Directory và do đó không có thông tin đăng nhập độc quyền của Active Directory. NDES cấp mật khẩu đăng ký một lần cho các thiết bị mạng này. Các yêu cầu mật khẩu này sau đó được gửi tới CA để xử lý và chứng thư nhận từ CA được chuyển tiếp tới thiết bị. Do đó, NDES được các quản trị viên sử dụng để xác thực các thiết bị mạng như vậy.

#### 

#### 2.2.2.5. Dịch vụ Web Đăng ký Chứng thư (Certificate Enrollment Web Service)

Dịch vụ Web Đăng ký Chứng thư trong AD CS cho phép người dùng và máy tính đăng ký và gia hạn chứng thư sử dụng giao thức HTTPS. Một thành viên/người dùng không thuộc doanh nghiệp bên ngoài ranh giới bảo mật của miền có thể sử dụng dịch vụ này. Dịch vụ Web Đăng ký Chứng thư tập trung chủ yếu vào các yêu cầu khách hàng tự động và xử lý các yêu cầu chứng thư với sự trợ giúp của khách hàng bản địa.

#### 

#### 2.2.2.6. Dịch vụ Web Chính sách Đăng ký Chứng thư (Certificate Enrollment Policy Web Service)

Dịch vụ Web Chính sách Đăng ký Chứng thư trong AD CS cho phép máy tính và người dùng truy xuất thông tin về chính sách đăng ký chứng thư của họ. Chính sách đăng ký chứng thư cung cấp vị trí chính xác của các CA và các loại chứng thư được yêu cầu từ chúng. Cùng với Dịch vụ Web Đăng ký Chứng thư, dịch vụ này sẽ cho phép đăng ký web dựa trên chính sách cho một khách hàng không thuộc doanh nghiệp hoặc thành viên bên ngoài miền. Chính sách đăng ký có thể được kích hoạt bằng cách sử dụng cài đặt chính sách nhóm hoặc áp dụng riêng cho các máy tính khách hàng. Do đó, AD CS chứng tỏ là một phương pháp hiệu quả để quản lý cơ sở hạ tầng chứng thư cho bất kỳ thực thể nào trong mạng miền Windows.

### 2.2.3. Lợi ích

AD CS có thể được các tổ chức sử dụng để tăng cường bảo mật bằng cách liên kết danh tính của một người, thiết bị hoặc dịch vụ với khóa riêng tương ứng. AD CS cũng cung cấp cho các doanh nghiệp một cách quản lý chứng thư hiệu quả, an toàn và tiết kiệm chi phí.

AD CS cung cấp cho tổ chức PKI cần thiết để sử dụng chứng thư số nhằm bảo mật máy chủ web (SSL/TLS), xác thực dựa trên chứng thư, chữ ký số cho tài liệu, mã hóa email (S/MIME), và nhiều ứng dụng khác. Nếu không có AD CS, tổ chức sẽ phải dựa vào bên thứ ba để cung cấp các dịch vụ này hoặc không thể triển khai chứng thư.

### 

### 2.2.4. Nhược điểm

Việc triển khai và quản lý một CA của Microsoft không phải là nhiệm vụ dễ dàng. Bạn sẽ cần một đội ngũ chuyên môn có kinh nghiệm về PKI để triển khai suôn sẻ. Sau khi thiết lập, đội ngũ của bạn cần phải cập nhật liên tục các thực hành tốt nhất về PKI để duy trì thời gian hoạt động và độ tin cậy.

Chi phí có thể cao với các chi phí liên quan đến phần cứng, triển khai và bảo trì bởi một đội ngũ chuyên gia.

AD CS gặp vấn đề tương thích với các thiết bị MAC OS.

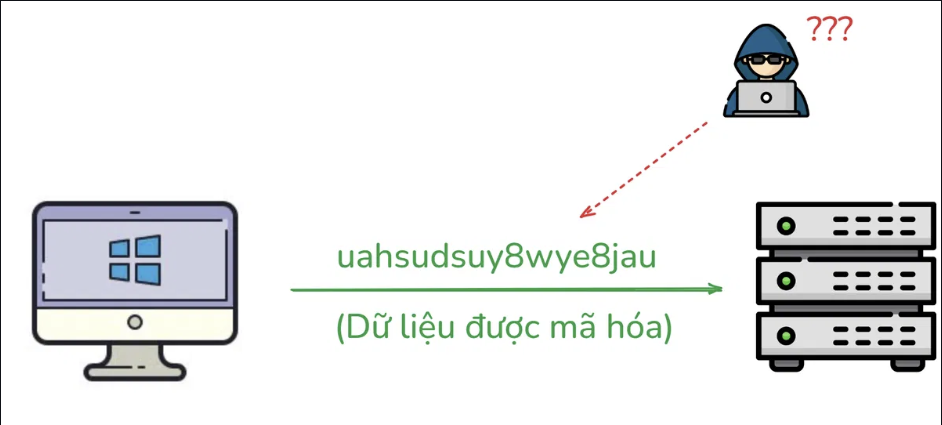
Các cuộc tấn công XSS hoặc Cross-site scripting có thể xảy ra trong AD CS vì Web Enrollment không lọc đầu vào người dùng đúng cách, dẫn đến việc không kiểm tra đầu vào người dùng trước khi lưu trữ vào cơ sở dữ liệu. Đầu vào không được lọc kỹ càng cũng có thể dẫn đến các cuộc tấn công SQL injection.

## 2.3. Vai trò của Windows CA trong bảo vệ dịch vụ web

Trong bối cảnh các dịch vụ web ngày càng trở thành mục tiêu tấn công của nhiều loại hình tin tặc, việc bảo vệ kết nối và thông tin truyền tải giữa người dùng và máy chủ trở nên vô cùng cấp thiết. Một trong những phương pháp bảo mật phổ biến và hiệu quả là sử dụng chứng chỉ số SSL/TLS được cấp bởi một tổ chức chứng thực (CA). Windows CA trong môi trường nội bộ có thể đóng vai trò như một CA tin cậy, giúp bảo vệ các dịch vụ web thông qua hạ tầng PKI.

### 2.3.1. Giao thức HTTPS

HTTPS (HyperText Transfer Protocol Secure - Giao thức truyền siêu văn bản bảo mật), là phiên bản nâng cấp và an toàn hơn của HTTP. Sự khác biệt nằm ở chữ "S" - Secure, đại diện cho lớp bảo mật được bổ sung. Nó hoạt động như một lớp mã hóa, bảo vệ thông tin trao đổi giữa trình duyệt của bạn và máy chủ website, giúp ngăn chặn việc nghe lén, đánh cắp hoặc thay đổi dữ liệu.



Hình 2.2. Giao thức HTTPS

HTTPS sử dụng một giao thức mã hóa gọi là SSL/TLS để mã hóa thông tin trao đổi giữa trình duyệt và máy chủ web. Điều này đồng nghĩa với việc:

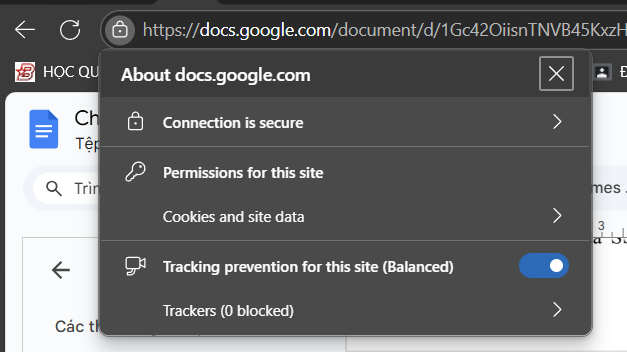
* **Dữ liệu được mã hóa:** Thông tin truyền giữa trình duyệt và máy chủ web sẽ được mã hóa thành một chuỗi ký tự ngẫu nhiên, và chỉ có thể được giải mã bằng một khóa mã hóa tương ứng, ngăn chặn việc đọc lén.
* **Kết nối được xác thực:** HTTPS đảm bảo rằng bạn đang kết nối với đúng máy chủ web mà bạn muốn, chứ không phải một trang web giả mạo. Việc này được thực hiện thông qua chứng chỉ SSL, tương tự như một "hộ chiếu" điện tử xác nhận danh tính của trang web.
* **Dữ liệu được bảo toàn:** HTTPS đảm bảo thông tin không bị thay đổi hoặc giả mạo trong quá trình truyền tải.

### 2.3.2. Giao thức SSL/TLS

SSL (Secure Sockets Layer) là một giao thức bảo mật được phát triển để thiết lập một kết nối mã hóa giữa máy chủ và máy khách. SSL được Netscape phát triển lần đầu tiên vào năm 1995 với mục đích đảm bảo quyền riêng tư, tính xác thực và tính toàn vẹn của dữ liệu trong truyền thông Internet.Tuy nhiên, giống như bất kỳ công nghệ nào, SSL cũng bộc lộ những hạn chế về bảo mật theo thời gian. Các phiên bản SSL 2.0 và 3.0 dần trở nên lỗi thời, tạo cơ hội cho các lỗ hổng bảo mật bị khai thác.

Nhận thức được những hạn chế của SSL, TLS (Transport Layer Security) ra đời như một phiên bản nâng cấp, kế thừa những ưu điểm và khắc phục những lỗ hổng của SSL. Năm 1999, IETF đề xuất một bản cập nhật cho SSL. TLS được xây dựng dựa trên nền tảng của SSL 3.0, đồng thời được bổ sung thêm nhiều tính năng bảo mật tiên tiến, đảm bảo an toàn cho dữ liệu trong môi trường Internet ngày càng phức tạp. Ngày nay, TLS đã thay thế hoàn toàn SSL, trở thành tiêu chuẩn bảo mật không thể thiếu cho các website và ứng dụng trực tuyến.

Khi truy cập một website, hãy chú ý đến biểu tượng ổ khóa trên thanh địa chỉ, đó chính là dấu hiệu cho thấy website đó đang sử dụng TLS để bảo vệ thông tin của bạn.



Hình 2.3. Website đang sử dụng TLS để bảo vệ thông tin

### 

### 2.3.3. Quá trình trình duyệt xác thực website thông qua CA

Khi người dùng truy cập một trang web qua HTTPS, trình duyệt sẽ thực hiện một loạt kiểm tra để xác thực tính hợp lệ của chứng chỉ:

* Kiểm tra xem chứng chỉ có được ký bởi một CA nằm trong danh sách tin cậy hay không.
* Kiểm tra thời gian hiệu lực của chứng chỉ.
* Kiểm tra xem tên miền trong chứng chỉ có khớp với địa chỉ trang web hay không.
* Kiểm tra trạng thái thu hồi của chứng chỉ thông qua CRL hoặc OCSP.

Nếu chứng chỉ được phát hành bởi Windows CA và CA đó đã được thêm vào kho tin cậy (Trusted Root Certification Authorities) của thiết bị, quá trình xác thực sẽ diễn ra suôn sẻ. Người dùng sẽ thấy biểu tượng ổ khóa hiển thị trên trình duyệt, xác nhận rằng kết nối đã được mã hóa và chứng thực đầy đủ. Trong các hệ thống nội bộ, quản trị viên có thể đẩy CA nội bộ vào thiết bị người dùng thông qua Group Policy để đảm bảo mọi thiết bị đều tin cậy CA nội bộ.

## 2.4. Kết luận chương 2

Chương 2 đã cung cấp một cái nhìn toàn diện về Windows Server và vai trò của dịch vụ Active Directory Certificate Services (AD CS) trong việc thiết lập hạ tầng bảo mật dựa trên chứng chỉ số. Với khả năng quản lý tài nguyên mạng, triển khai ứng dụng và đảm bảo an toàn hệ thống, Windows Server là nền tảng không thể thiếu trong các tổ chức hiện đại. Bên cạnh đó, AD CS đóng vai trò then chốt trong việc xây dựng và quản lý hệ thống PKI nội bộ, cung cấp các chứng chỉ số để đảm bảo tính xác thực, tính toàn vẹn và tính bảo mật cho các dịch vụ mạng, đặc biệt là các dịch vụ web sử dụng giao thức HTTPS và SSL/TLS.

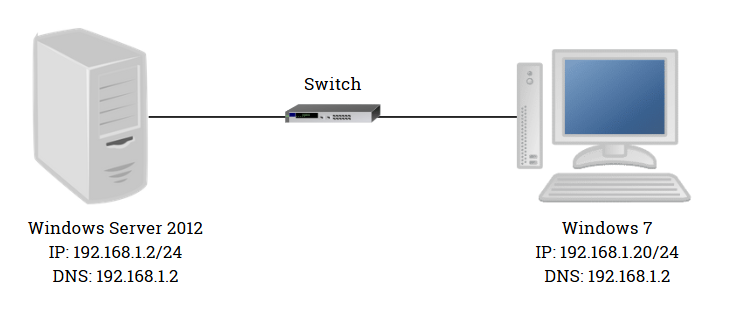
Thông qua việc tích hợp Windows CA, các tổ chức có thể chủ động phát hành và kiểm soát chứng chỉ số, giảm sự phụ thuộc vào bên thứ ba, đồng thời nâng cao hiệu quả quản lý bảo mật trong môi trường nội bộ.

# 

# CHƯƠNG 3. TRIỂN KHAI THỰC NGHIỆM

## 3.1. Mô tả bài toán

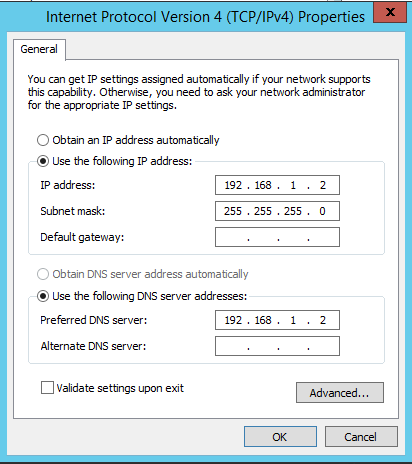
* **Mục tiêu:** Cài đặt và cấu hình hệ thống dịch vụ mạng bao gồm: DNS để phân giải tên miền, IIS để cung cấp dịch vụ web, và Certification Authority (CA) để cấp phát chứng thư số. Sau đó, thực hiện yêu cầu chứng thư số từ CA và cấu hình giao thức bảo mật SSL trên IIS nhằm mã hóa dữ liệu truyền tải, đảm bảo tính bảo mật và toàn vẹn thông tin giữa máy khách và máy chủ web.
* **Mô hình triển khai:**

****

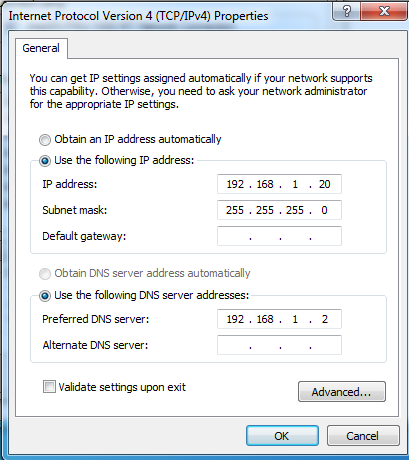
## 3.2. Triển khai thực nghiệm

### 3.2.1. Cấu hình địa chỉ IP

* Cấu hình địa chỉ IP trên máy Windows Server 2012

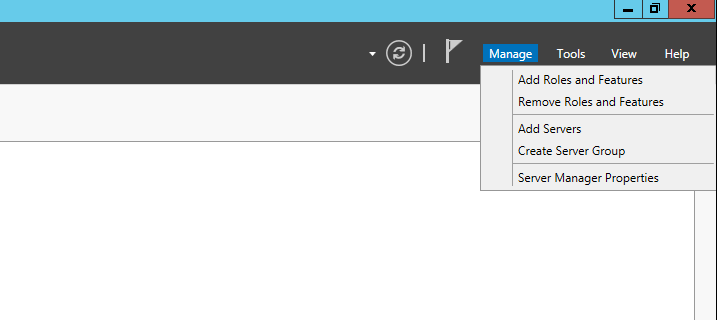


* Cấu hình địa chỉ IP trên máy Windows 7

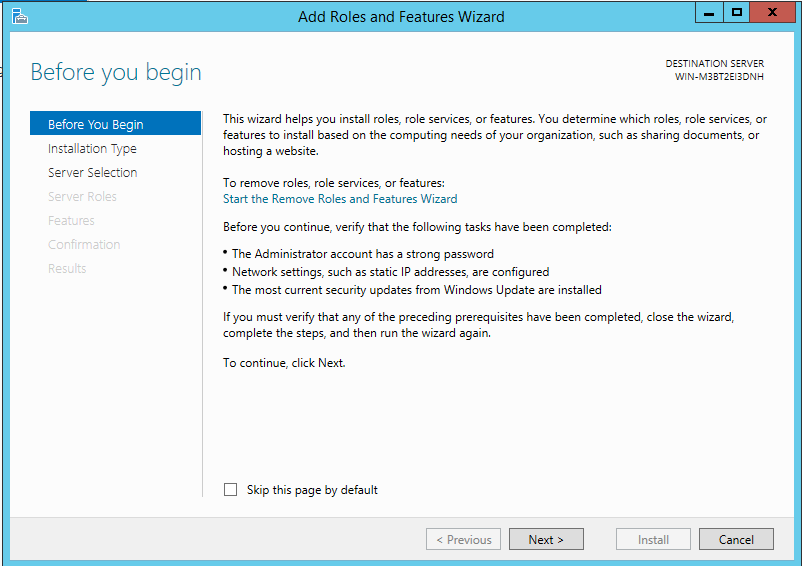


### 3.2.2. Cài đặt DNS trên máy chủ Windows Server 2012

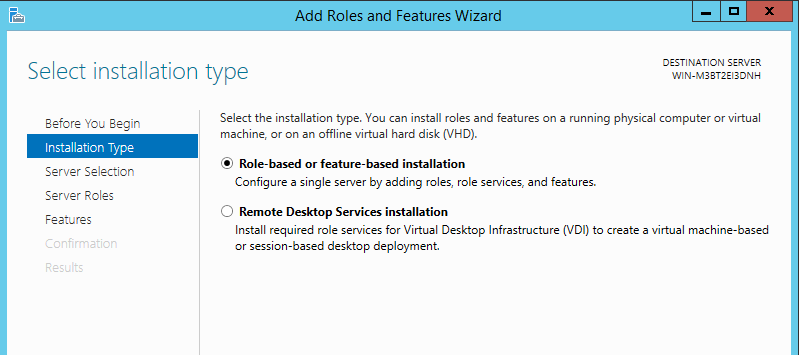
* Bước 1: Truy cập theo đường dẫn để cài đặt dịch vụ DNS: **Server Manager → Manage → Add Roles and Features**



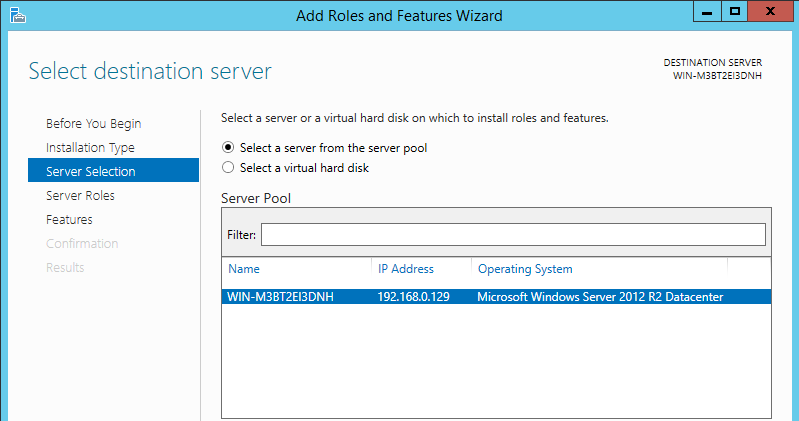
* Bước 2: Chọn Next để bắt đầu quá trình cài đặt



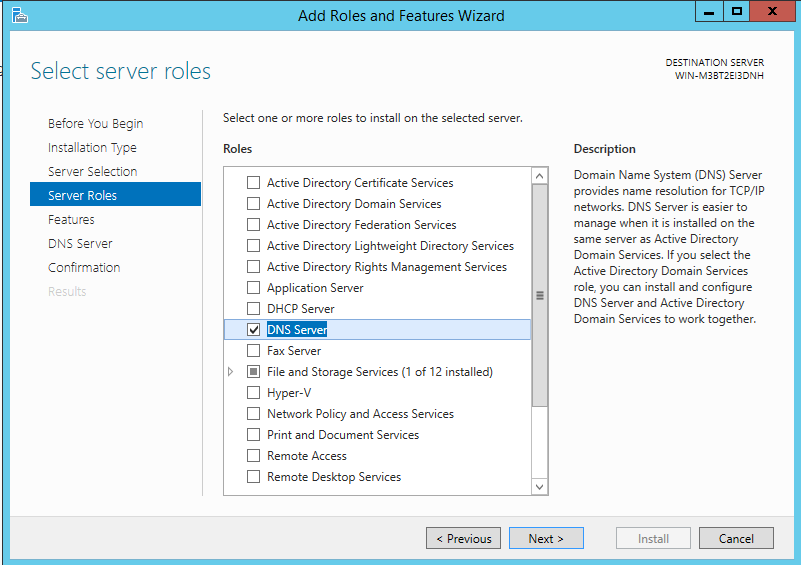
* Bước 3: Trong lựa chọn **Select installation type** → chọn **Role-based or feature-based installation** để cài đặt các dịch vụ và tính năng cho máy chủ.



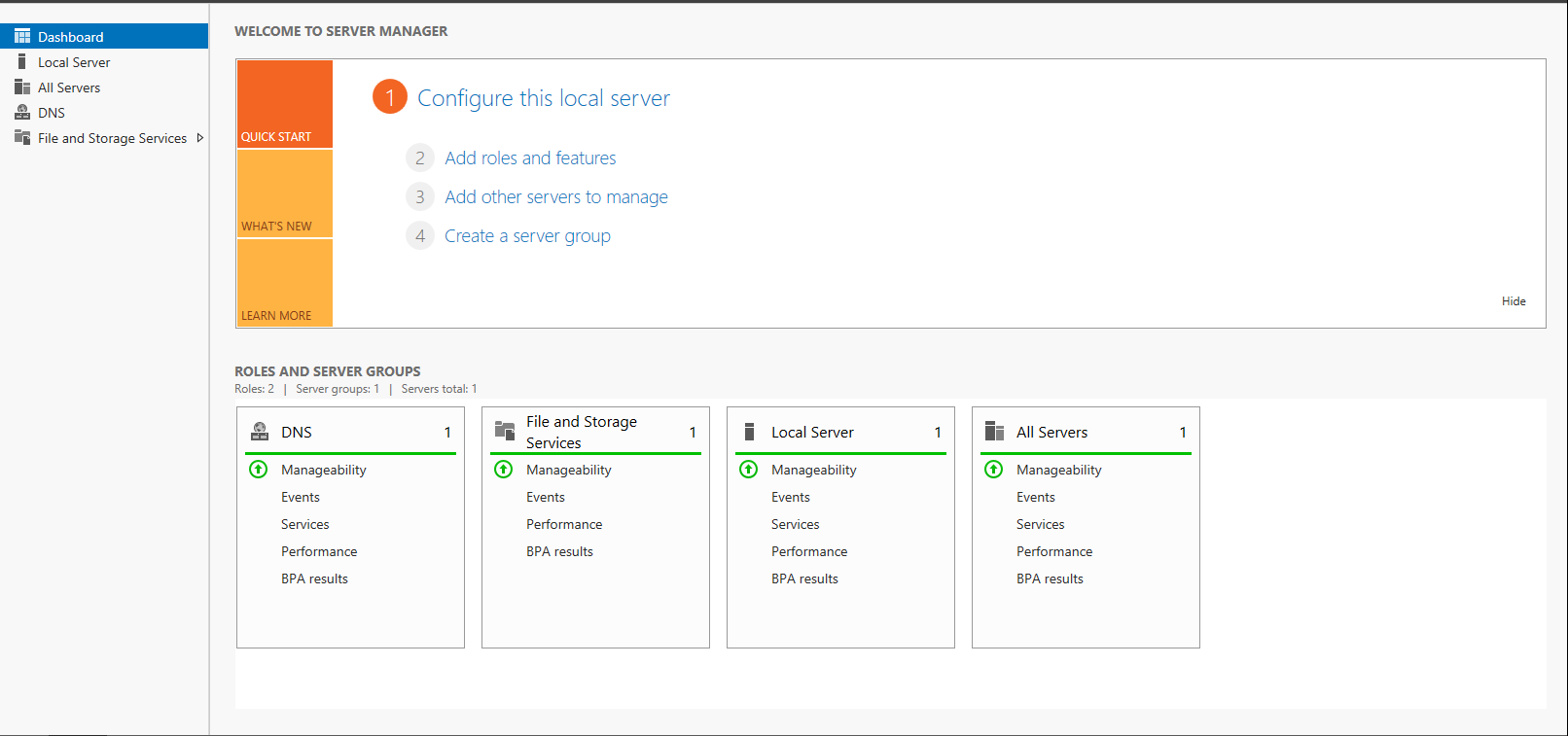
* Bước 4: Trong tùy chọn **Select destination server** → Chọn **Select a server from the server pool**.



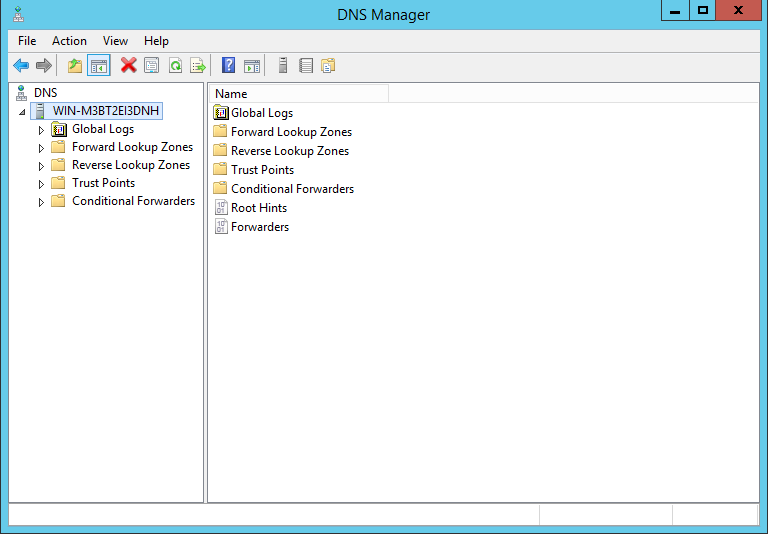
* Bước 5: Trong tùy chọn **Select server roles** → chọn dịch vụ **DNS server** để cài đặt dịch vụ DNS.



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



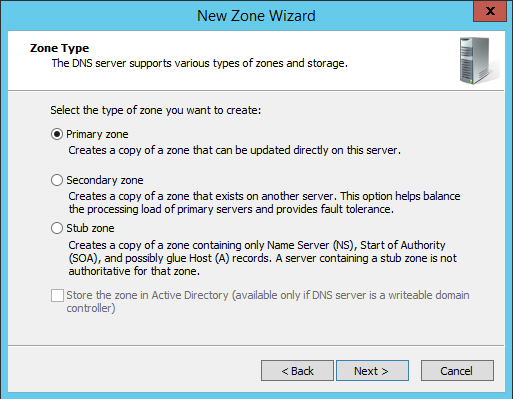
* Bước 6: Mở dịch vụ DNS và tiến hành cấu hình dịch vụ DNS để phân giải tên miền



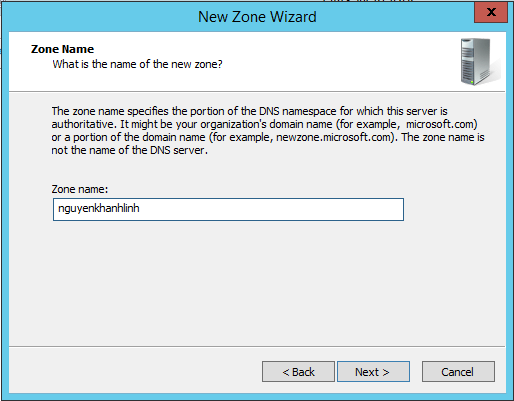
* Bước 7: Để cấu hình phân giải xuôi, chuột phải vào mục **Forward Lookup Zones** → chọn **New Zone.** Trong mục Zone Type → chọn Primary zone



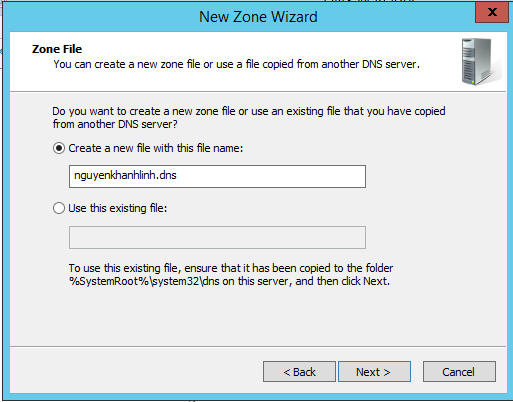
* Bước 8: Trong mục **Zone Type** → chọn **Primary zone**



* Bước 9: Trong mục **Zone Name** điền tên cho Zone→ Next



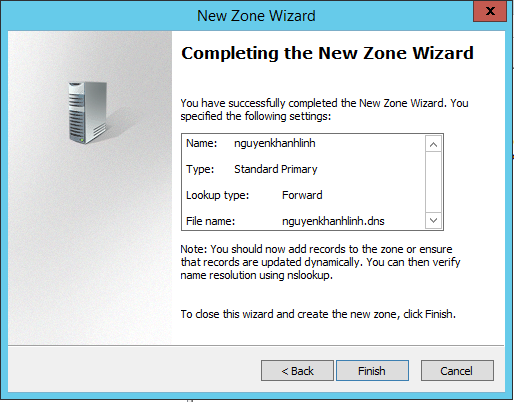
* Bước 10: Trong mục **Zone File** để mặc định → Next



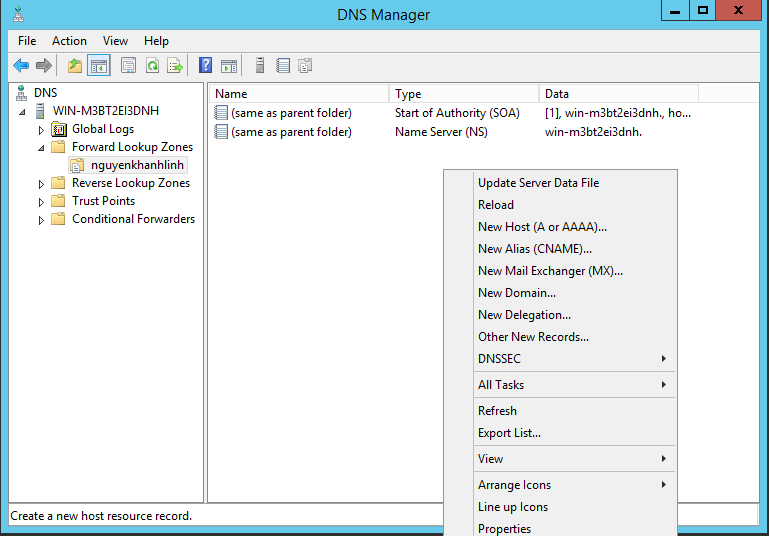
* Bước 11: Trong mục **Dynamic Update** → chọn **Allow both nonsecure and secure dynamic update**



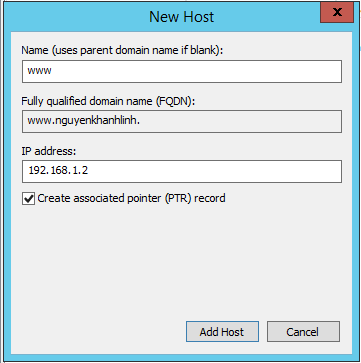
* Bước 11: Chọn Finish để hoàn thành quá trình cài đặt



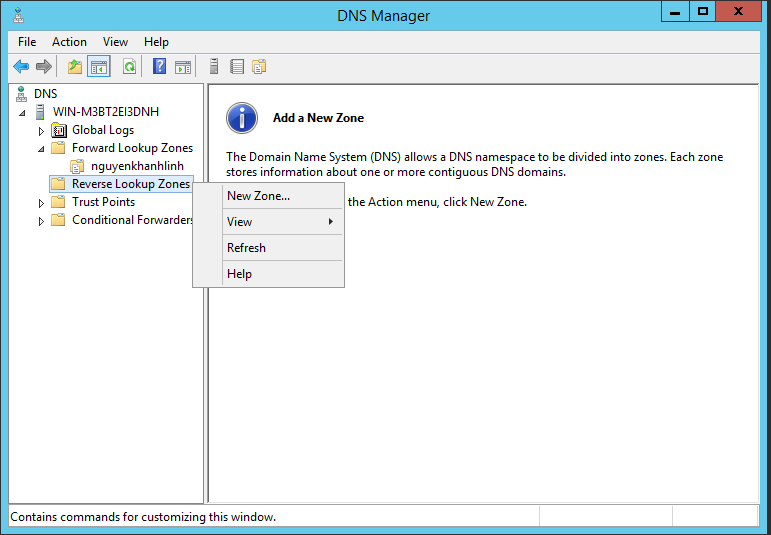
* Bước 12: Để tạo bản ghi Host A (www), chuột phải vào mục nguyenkhanhlinh chọn New Host



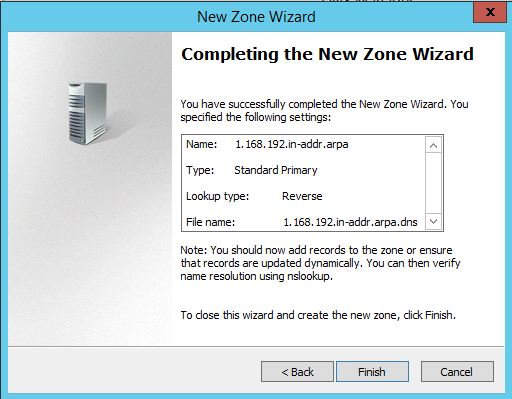
* Bước 13: Thêm các tham số như hình bên dưới



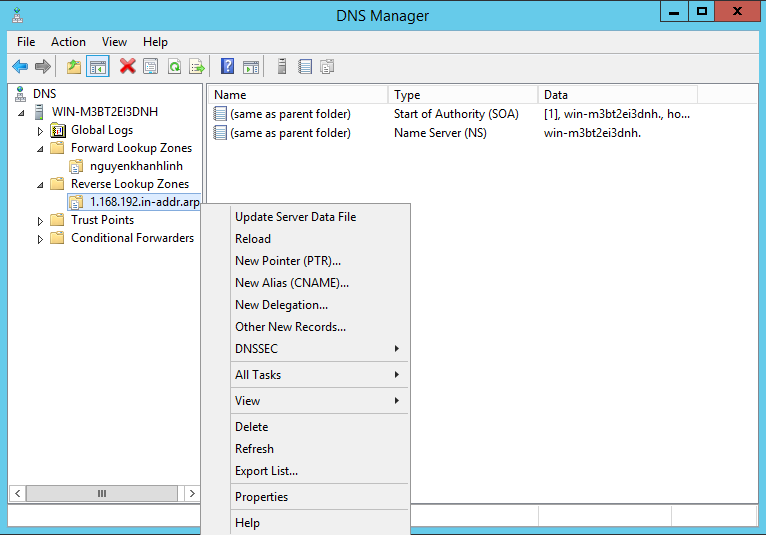
* Bước 14: Để cấu hình phân giải ngược, chuột phải vào mục Reverse Lookup Zone chọn New Zone
* Trong mục **Zone Type** → chọn **Primary Zone**
* Trong mục **Reverse Lookup Zone Name** → chọn **Ipv4 Lookup zone** → Next
* Trong mục **Network ID** nhập dải địa chỉ IP máy chủ sử dụng: **192.168.1** → Next
* Trong mục **Zone file** để mặc định → Next
* Trong mục **Dynamic Update chọn Allow both nonsecure and secure dynamic update** → Next → Finish



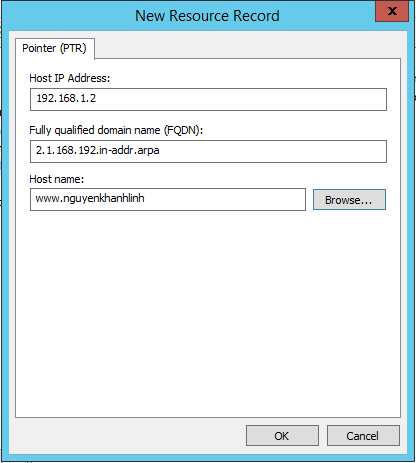
* Bước 15: Chọn Finish để hoàn thành quá trình cài đặt



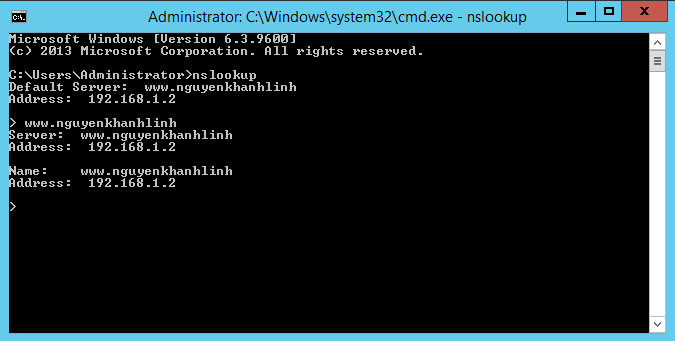
* Bước 16: Để tạo bản ghi phân giải ngược PTR, chuột phải vào dải IP đã khai báo chọn New Pointer



* Bước 17: Thêm các tham số như hình bên dưới

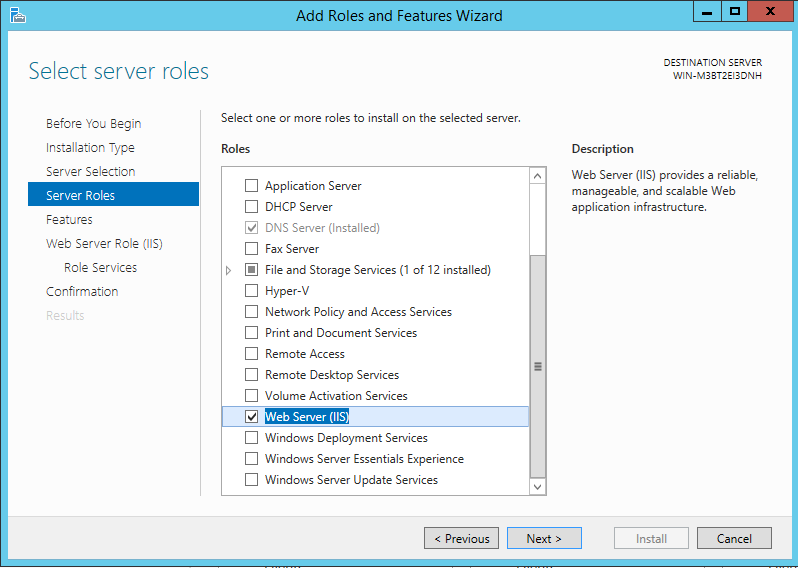


* Bước 18: Bật cửa sổ dòng lệnh CMD, sử dụng lệnh nslookup để kiểm tra phân giải tên miền.

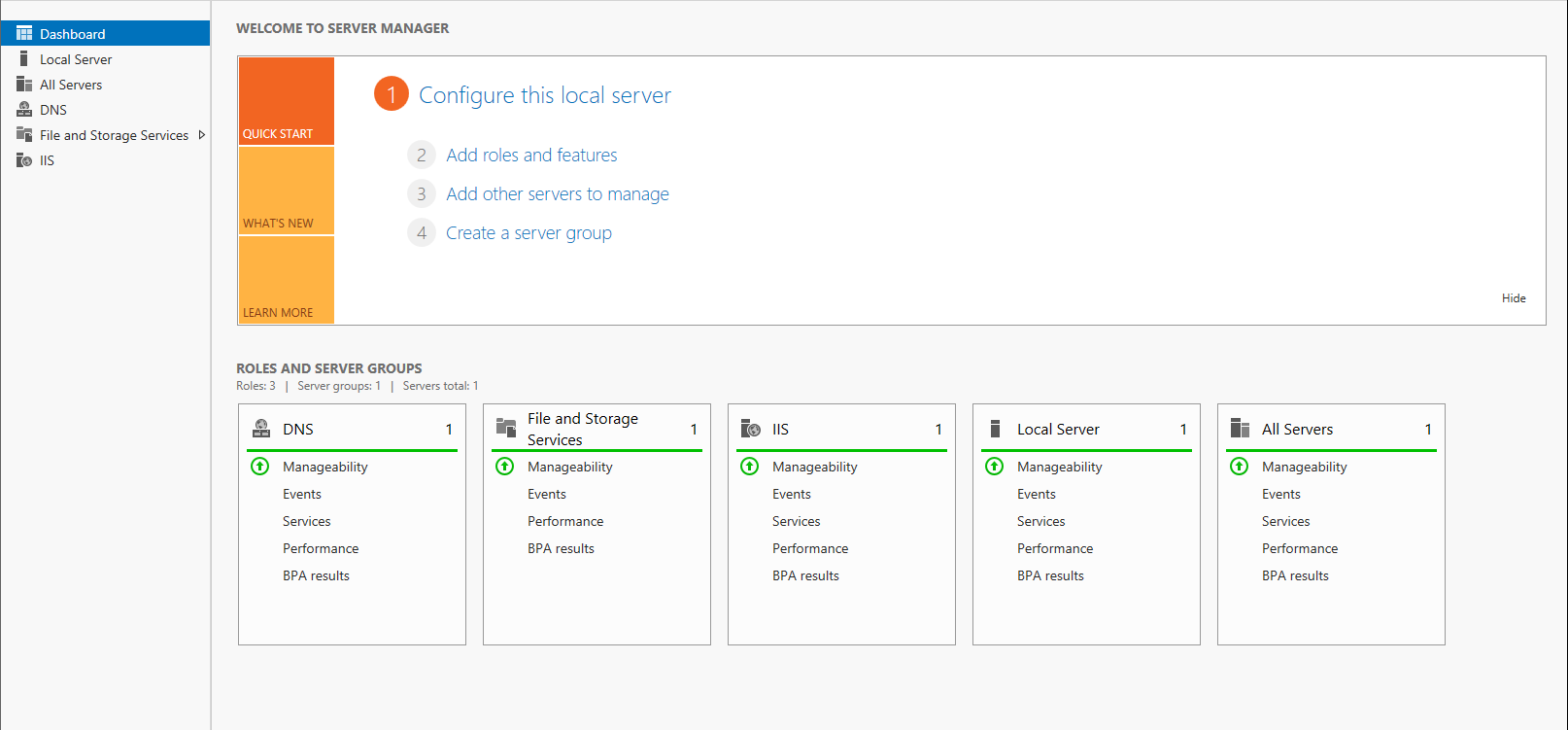


### 3.2.3. Cài đặt dịch vụ web IIS trên máy chủ Windows Server 2012

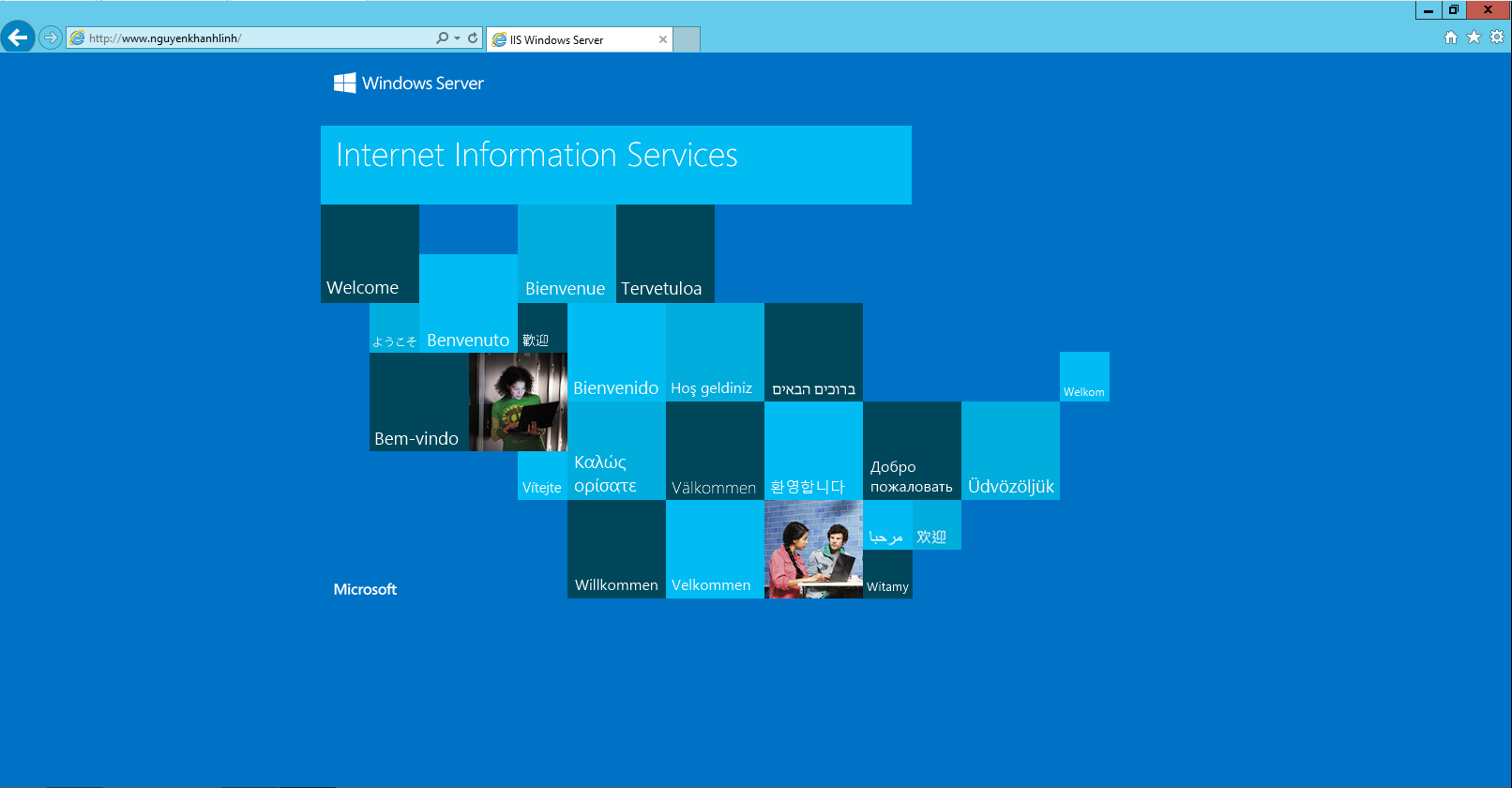
* Bước 1: Để cài đặt dịch vụ IIS, thực hiện cấu hình tương tự dịch vụ DNS. Trong tùy chọn **Select server roles** → chọn dịch vụ **Web server (IIS)**.



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

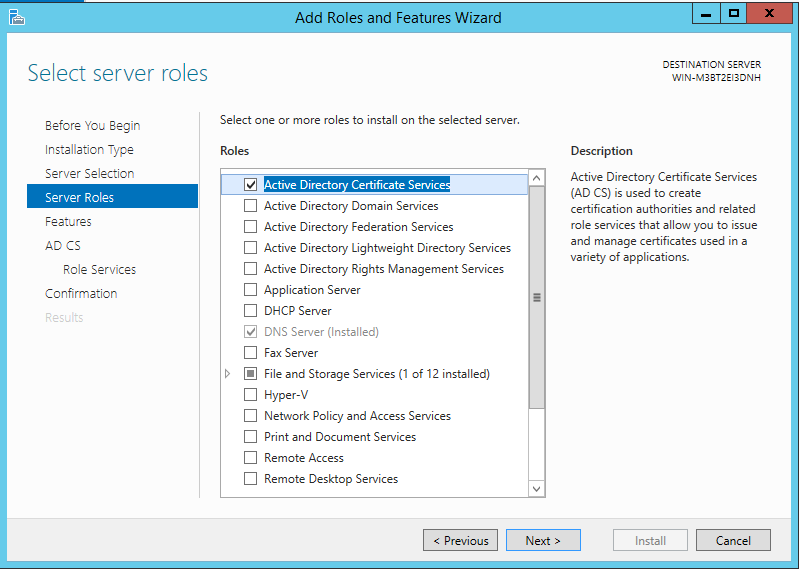


* Bước 2: Mở trình duyệt web IE và gõ tên miền [www.nguyenkhanhlinh](http://www.nguyenkhanhlinh) để kiểm tra hoạt động của Web Server

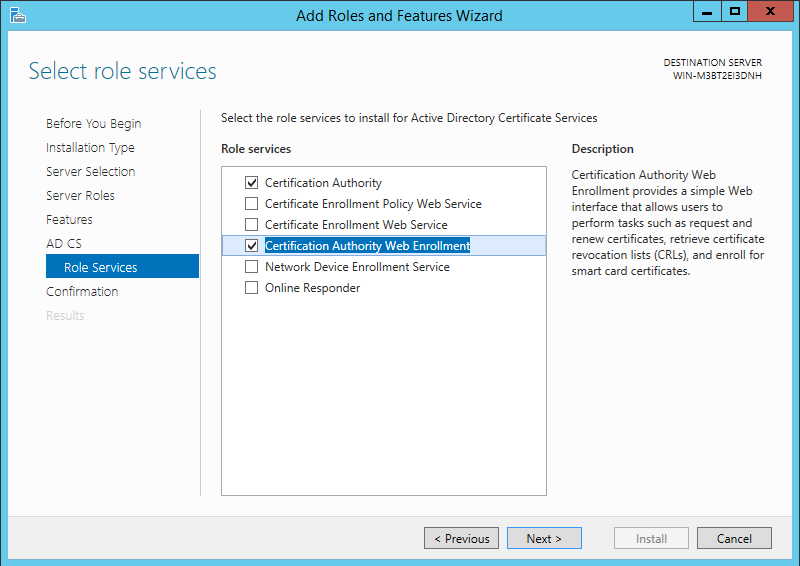


### 3.2.4. Cài đặt dịch vụ Certification Authority (CA)

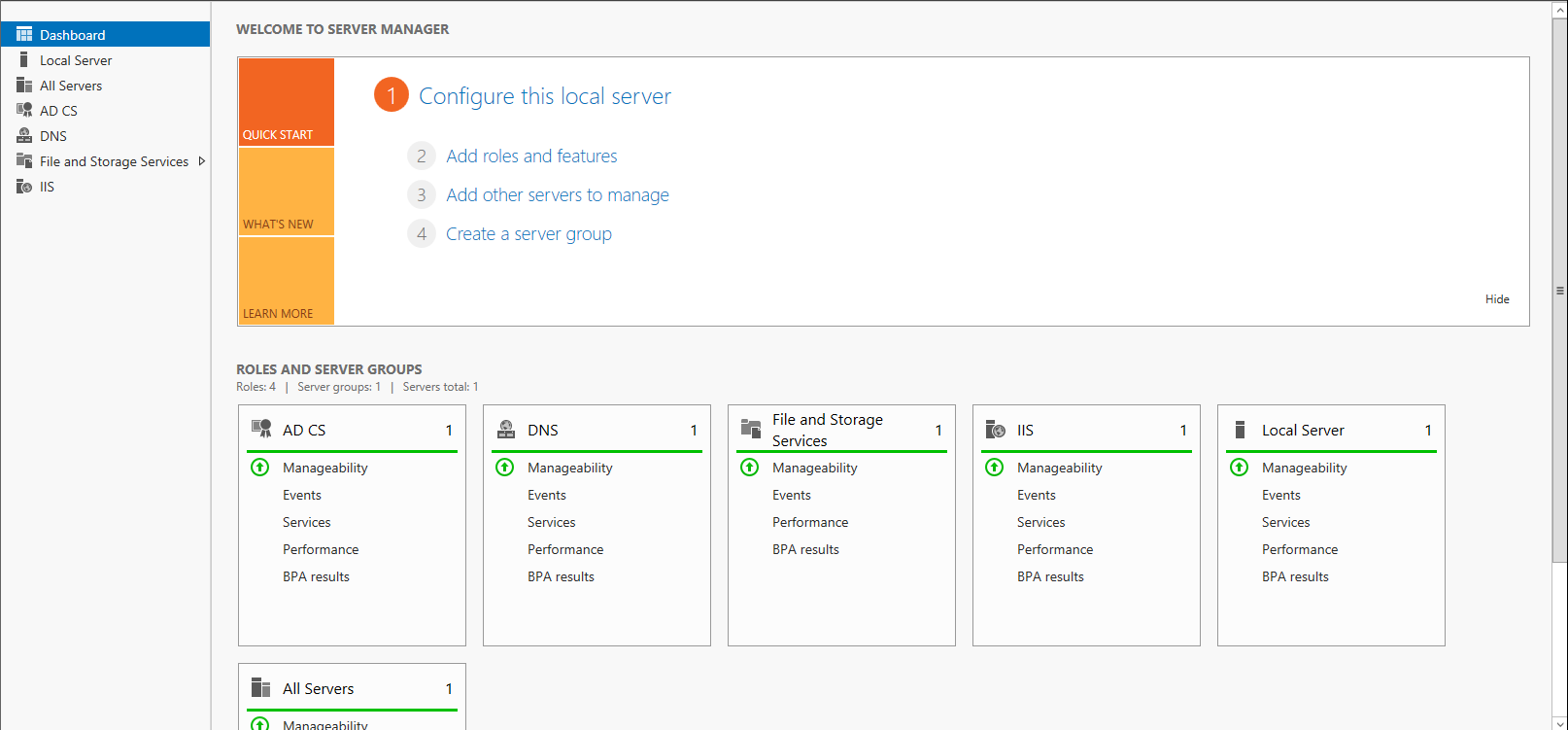
* Bước 1: Để cài đặt dịch vụ Certification Authority (CA), thực hiện cấu hình tương tự dịch vụ DNS. Trong tùy chọn **Select server roles** → chọn dịch vụ **Active Directory Certificate Service**.



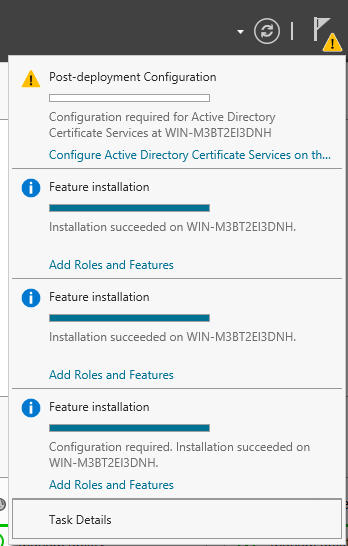
* Bước 2: Trong mục **Select role services** lựa chọn 2 dịch vụ: **Certification Authority** và **Certification Authority Web Enrollment**.



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



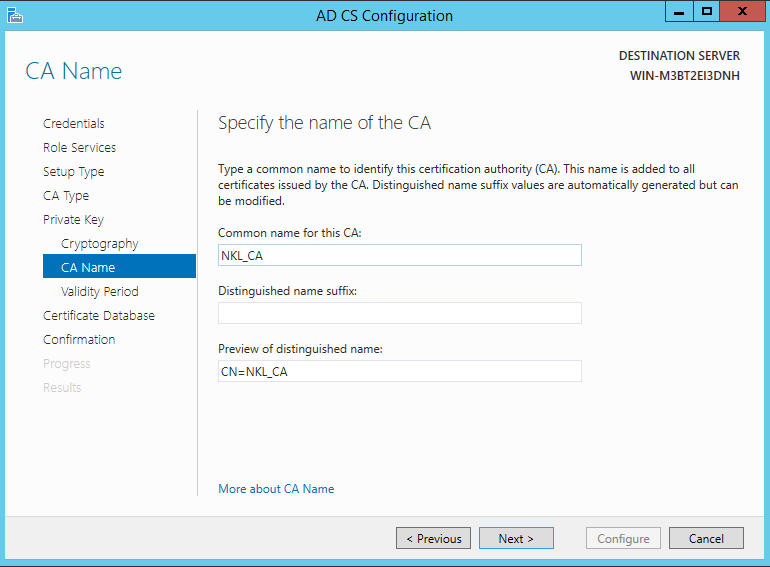
* Bước 3: Sau khi cài đặt dịch vụ CA thành công, chọn vào biểu tượng hình lá cờ trong giao diện Server Manager → **Configure Active Directory Certificate Services**.



* Bước 4: Trong giao diện Role Services tích chọn 2 tùy chọn **Certification Authority** và **Certification Authority Web Enrollment**.



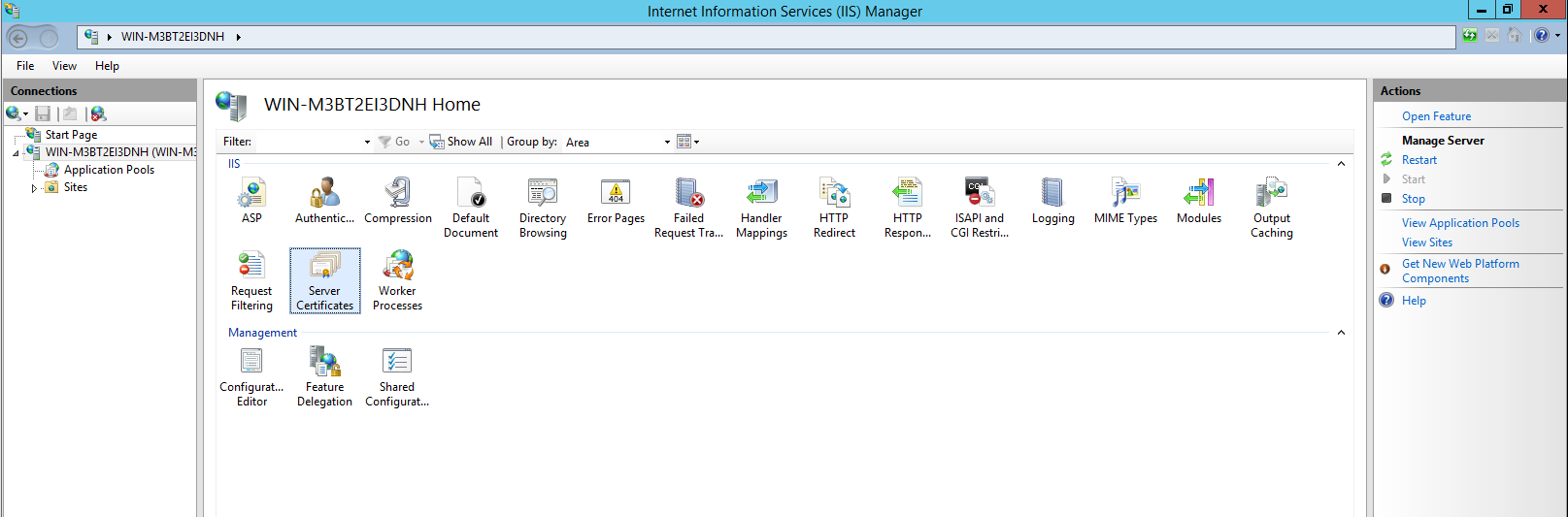
* Trong giao diện **Setup Type chọn Standalone CA** → Next.
* Trong giao diện **CA Type chọn Root CA** → Next.
* Trong giao diện **Private Key chọn Create a new private key** → Next.
* Trong giao diện **Cryptography for CA** chọn mặc định → Next.
* Trong giao diện **CA Name** đặt tên cho CA → Next.



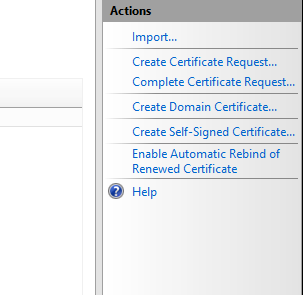
* Trong giao diện **Validity Period** để mặc định là 5 năm → Next.
* Trong giao diện **CA database** để mặc định

### 3.2.5. Cấu hình SSL cho dịch vụ Web

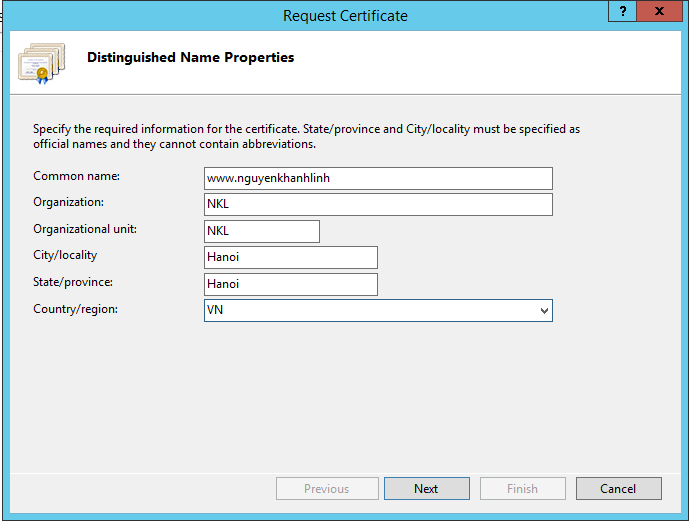
* Bước 1: Mở dịch vụ IIS lên, chọn tên của máy chủ web, chọn dịch vụ Server Certificates → Open feature



* Bước 2: Trong giao diện của Server Certificates, ở cột Action chọn Create Certificate Request



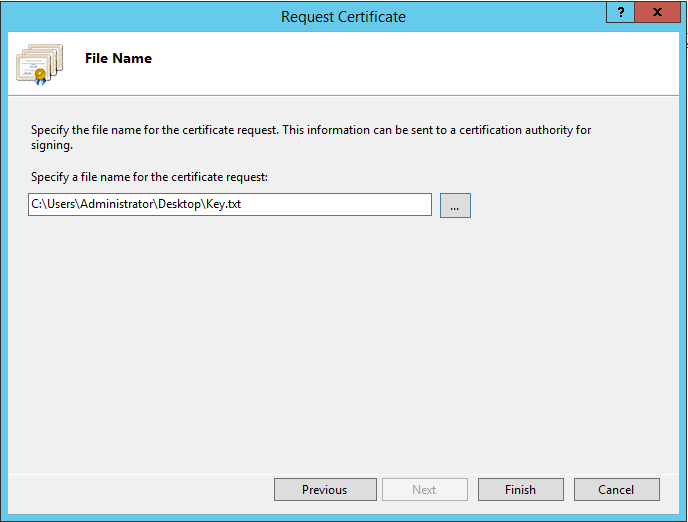
* Bước 3: Thêm các thông tin như hình bên dưới



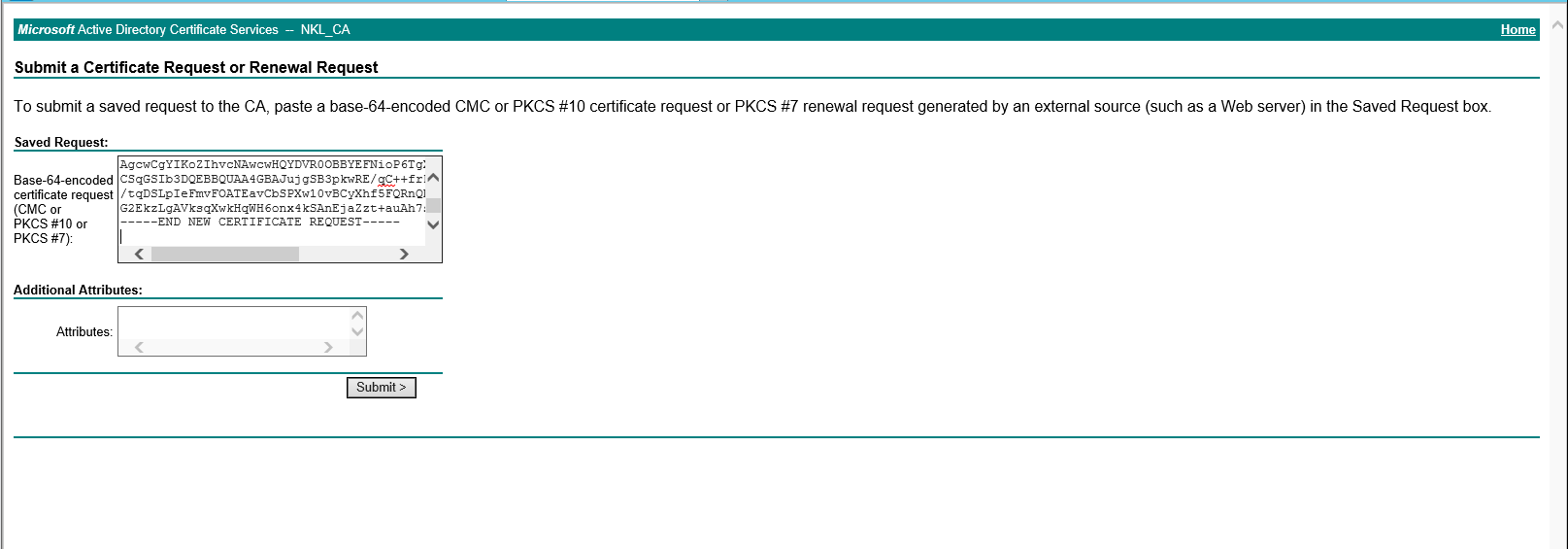
* Trong giao diện tiếp theo tùy chọn của độ dài khóa mã, mặc định là 1024 bit.



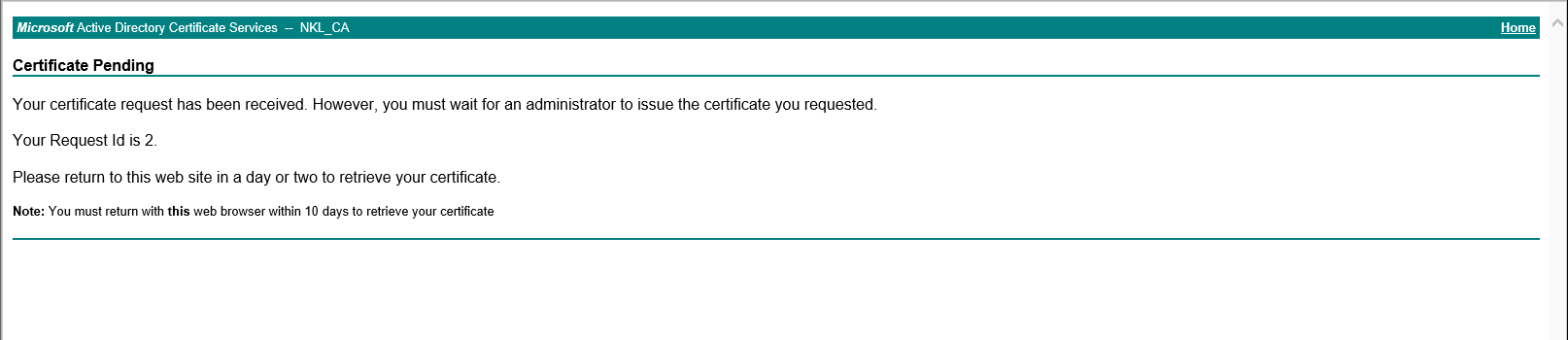
* Trong giao diện tiếp theo File Name, trỏ đến nơi lưu trữ file và đặt tên cho file. File này lưu trữ thông tin về khóa.



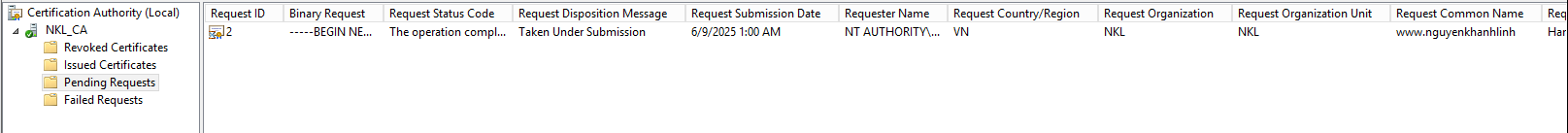
* Bước 4: Gắn thông tin về khóa với chứng thư số
* Mở trình duyệt Web IE lên và truy cập theo tên miền vào đường đường dẫn của CA **http://www.nguyenkhanhlinh/certsrv**
* Chọn tùy chọn Request a Certificate → Advanced certificate request → Submit a certificate request by using...
* Mở file Key.txt vừa tạo ở trên, copy nội dung của file và dán vào ô Saved Request



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

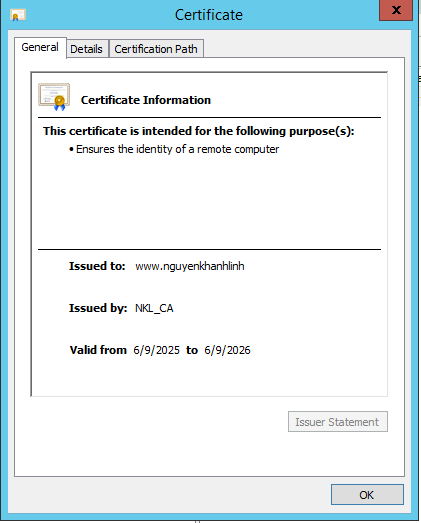


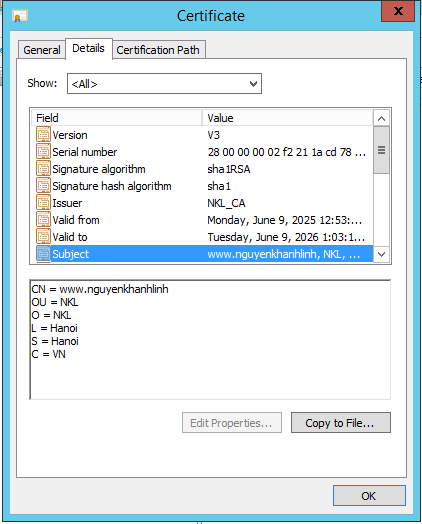
* Bước 5: Thực hiện cấp chứng thư số cho IIS
* Mở dịch vụ CA lên, truy cập vào mục Pending Requests, thấy có 1 chứng thư đang chờ đợi duyệt của CA.



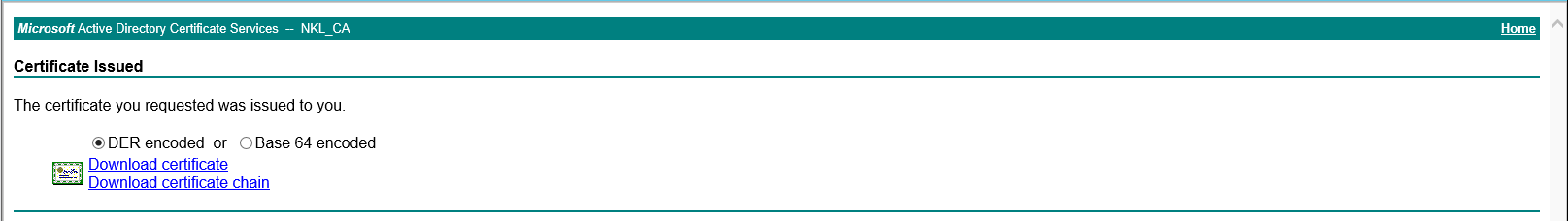
* Chuột phải vào chứng thư số có ID là 2 và chọn All Tasks → Issue

=> 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.

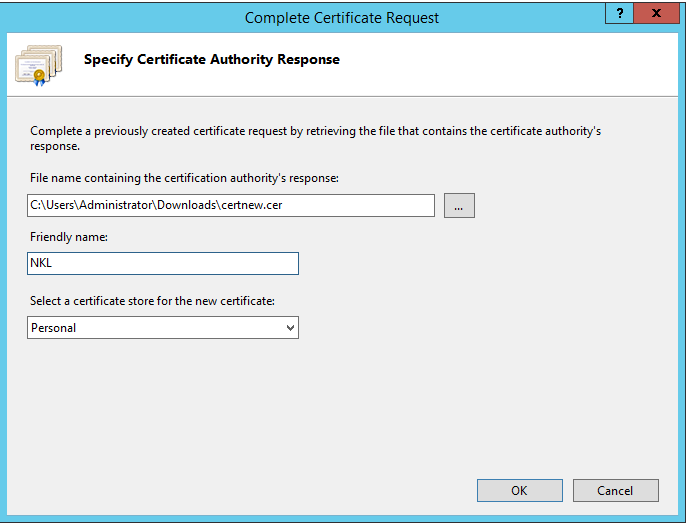




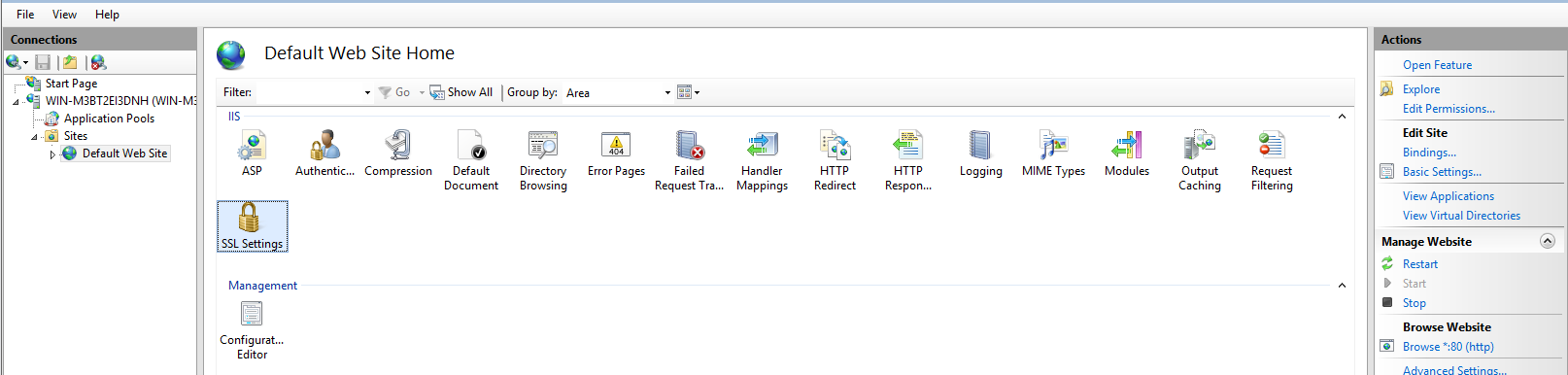
* Mở trình duyệt Web IE lên và truy cập đường đường dẫn của CA **http://www.nguyenkhanhlinh/certsrv,** chọn View the status of a pending certificate request → **Saved-Request Certificate** để lưu chứng thư → **Download certificate** để tải chứng thư xuống



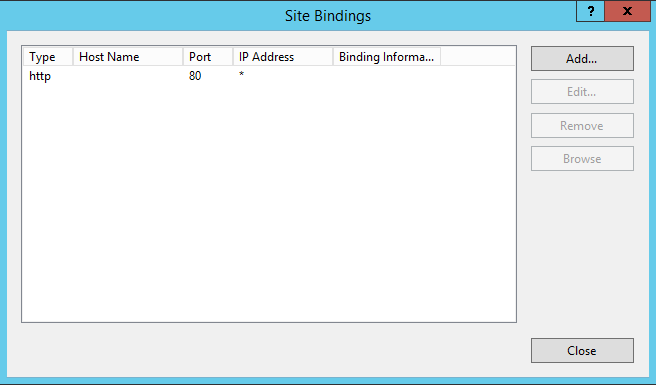
* Mở dịch vụ IIS → chọn máy chủ IIS → chọn **Server Certificates** → trong mục Action chọn **Open feature** → **Complete Certificate Request.** Sau đó trỏ đến nơi lưu trữ chứng thư đã tải trước đó.



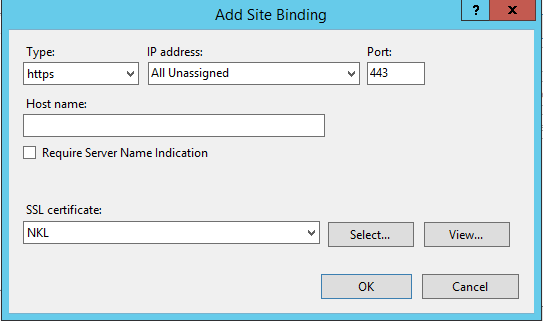
* Bước 6: Cấu hình để máy chủ IIS chạy dịch vụ SSL
* Từ giao diện quản trị của IIS truy cập tới Sites → Default Web Site, trong các chức năng ở cột giữa Default Web Site Home tìm đến chức năng SSL setting. Trong mục **Action** chọn Bindings...



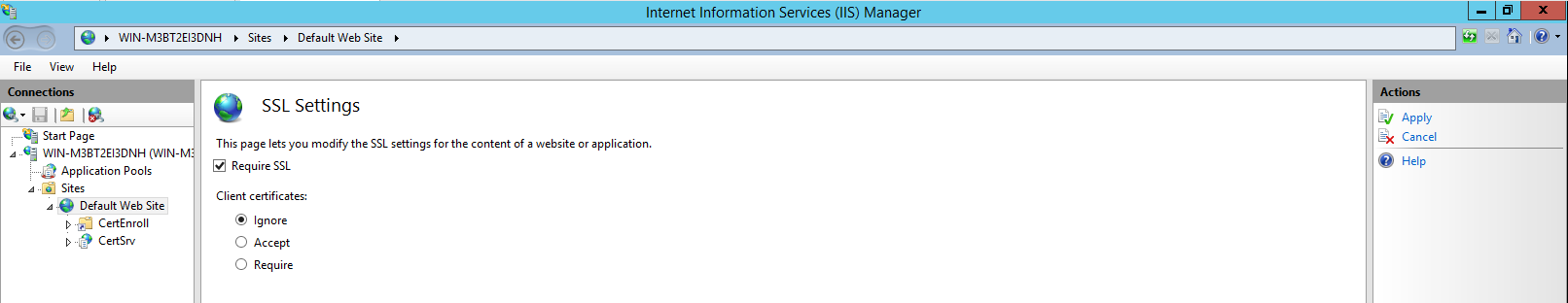
* Chọn Add để thêm một binding mới.



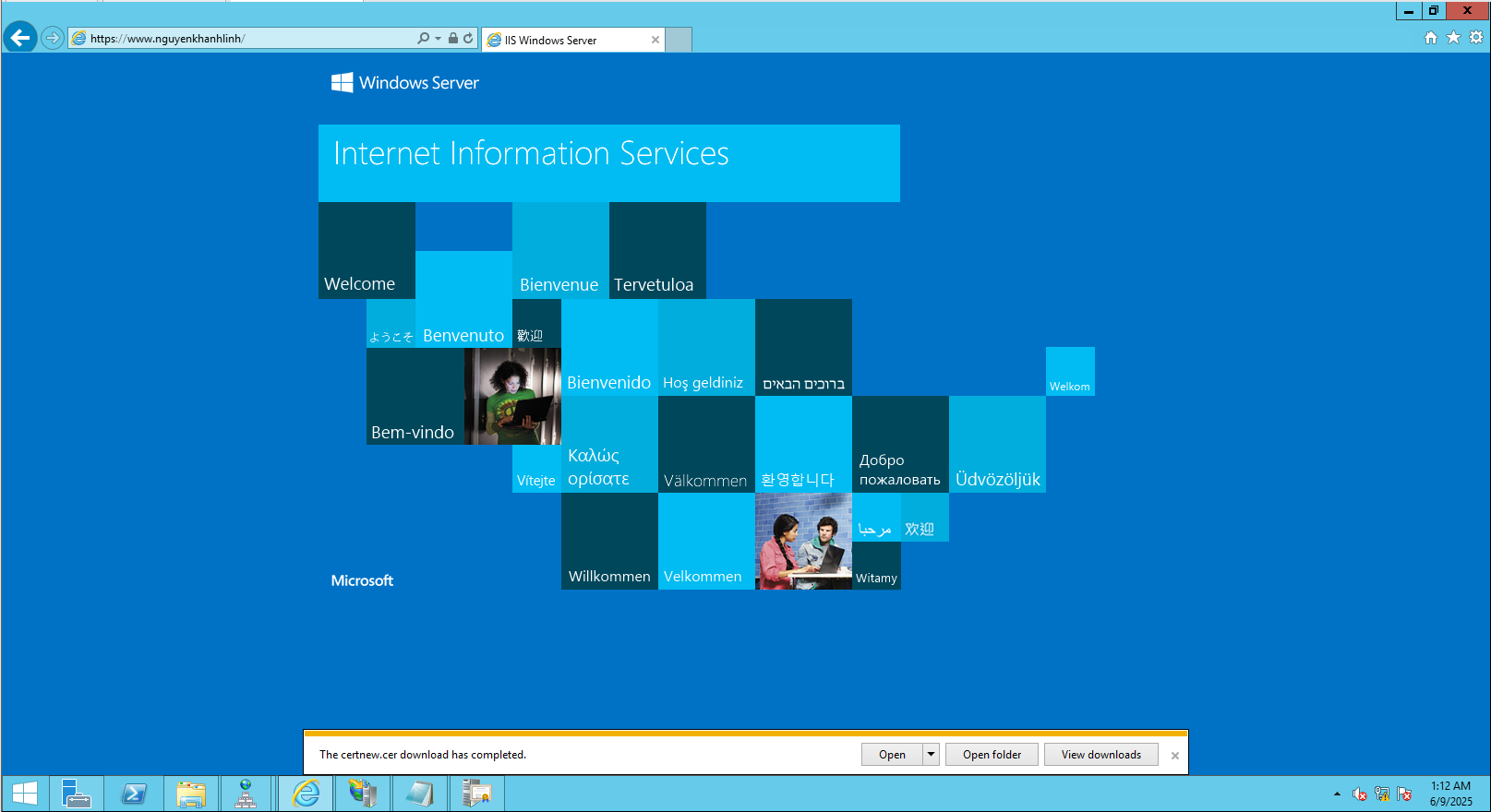
* Trong mục Type chọn https : Port 443. Trong mục SSL Certificate → Select → chọn chứng thư đã cài đặt.



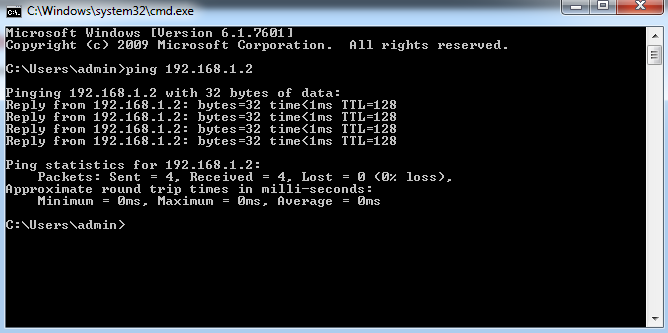
* Trở lại giao diện Default Web Site Home chọn SSL Settings, mục Action chọn Open feature. Chọn vào yêu cầu SSL, mục Action chọn Apply

****

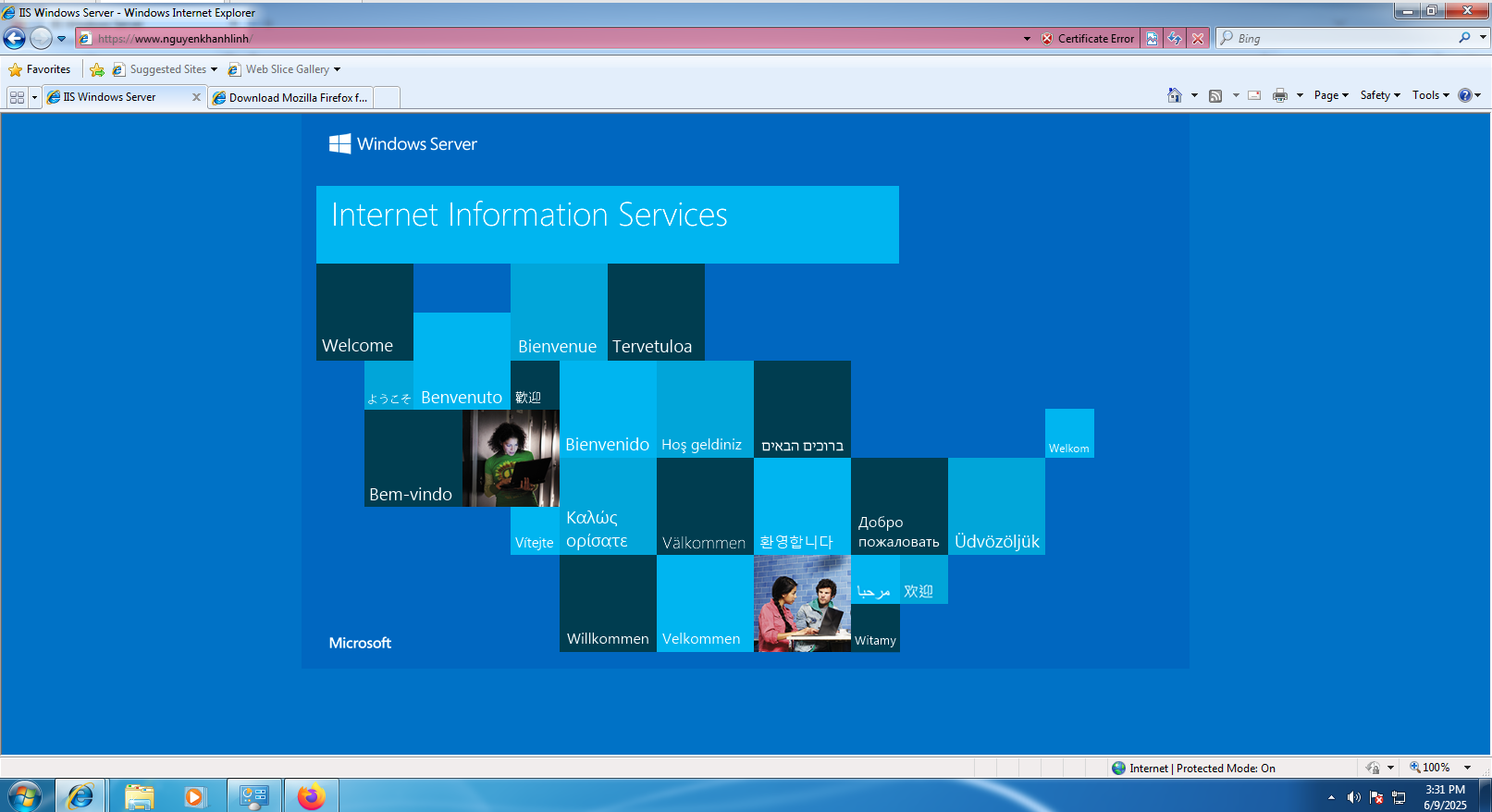
* Bước 7: Bật trình duyệt web IE và gõ tên miền với https => Kết quả truy cập thành công

****

* Bước 8: Thực hiện Ping để kiểm tra kết nối giữa 2 máy Windows Server 2012 và Windows 7

****

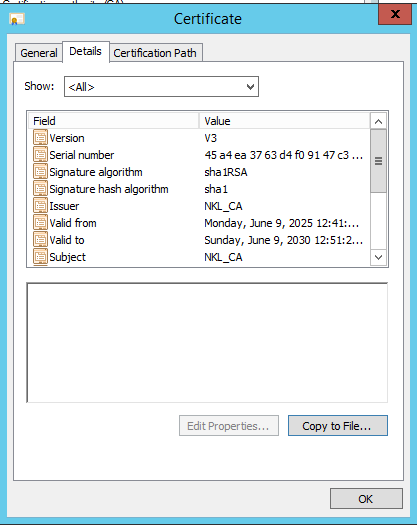
* Bước 9: Trên máy Windows 7, bật trình duyệt web IE và gõ tên miền với https => Kết quả truy cập thành công tuy nhiên xuất hiện lỗi Certificate Error

****

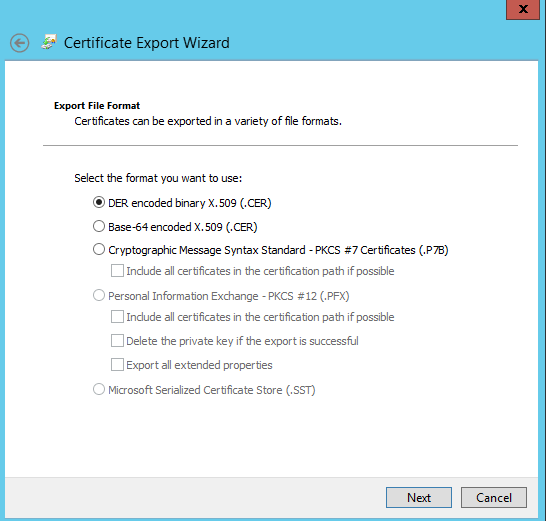
* Bước 10: Để khắc phục lỗi này, chuột phải vào **NKL\_CA** → Chọn **Properties** → Chọn **View Certificate** để xem các thông tin về chứng chỉ này.

****

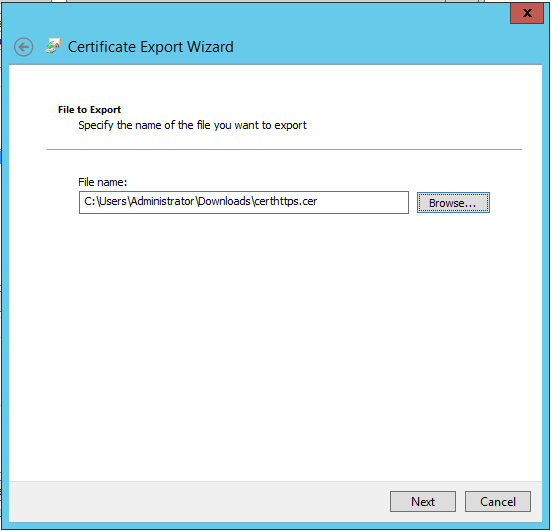
* Bước 11: Trong tab Details, Chọn Copy to file để thực hiện Export chứng chỉ



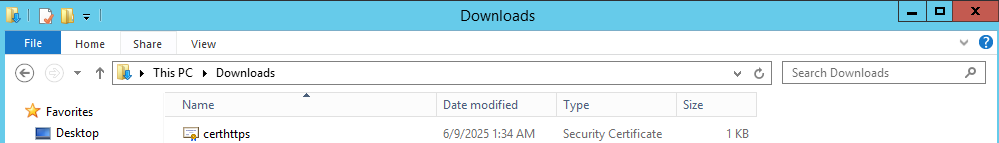
* Bước 12: Trong **Export File Format**, chọn **DER encoded binary X.509 (.CER).**

****

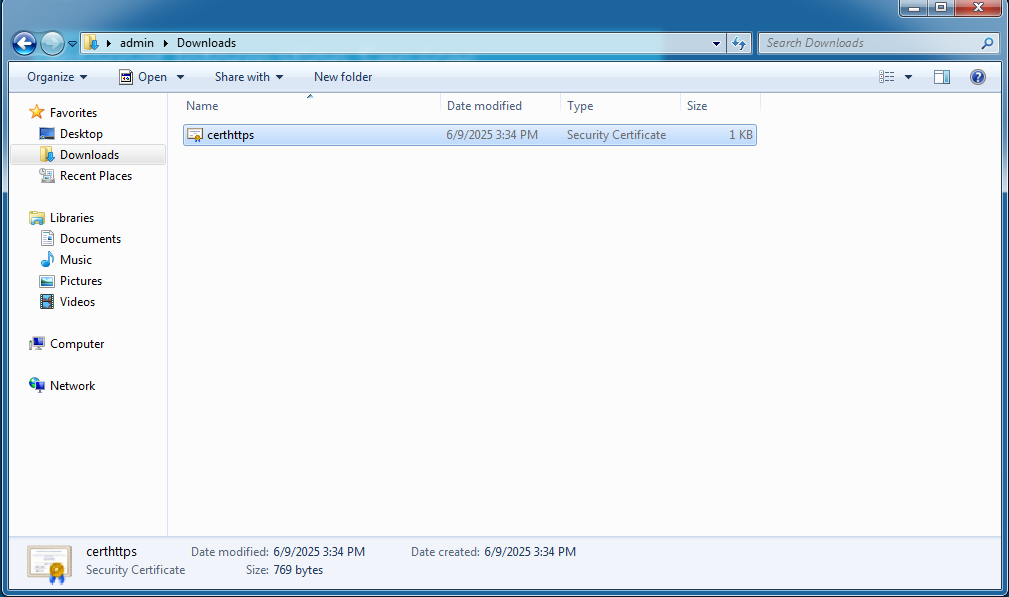
* Bước 13: Thêm file dùng để lưu trữ chứng chỉ vào mục File Name và chọn Next.

****

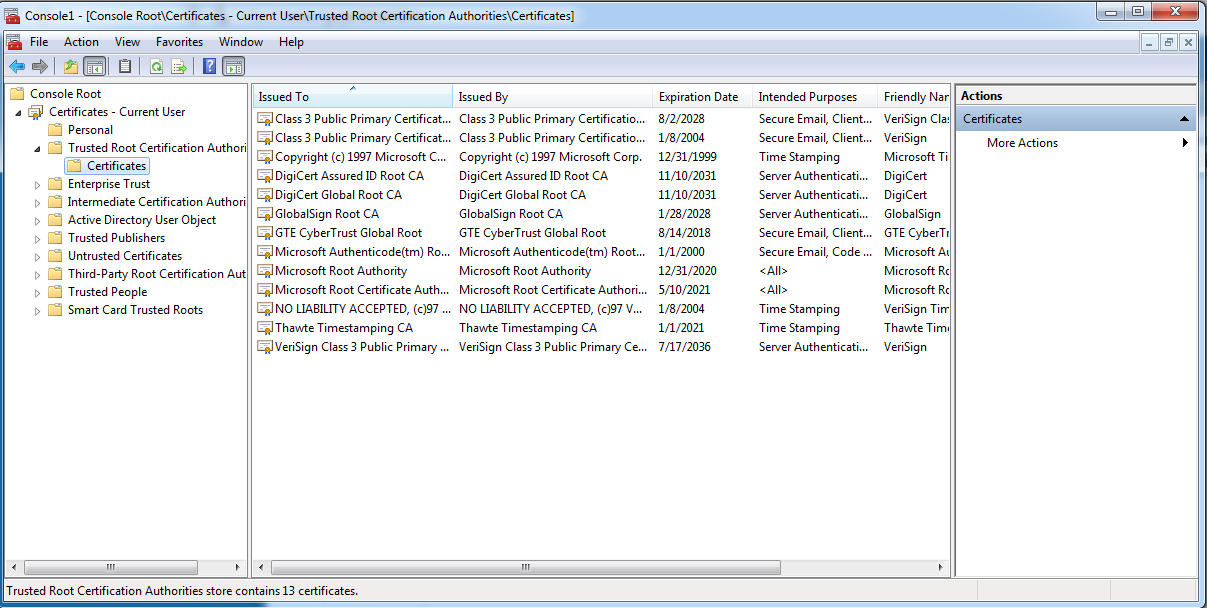
=> Trích xuất thành công chứng chỉ **Certificatehttps**

****

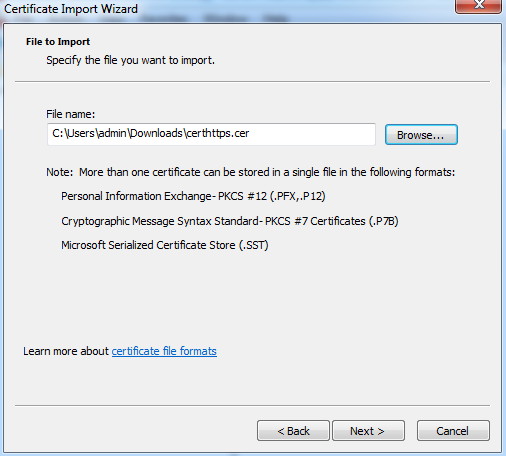
* Bước 14: Sao chép chứng chỉ **Certificatehttps** từ máy Window Server 2012 sang máy Windows 7

****

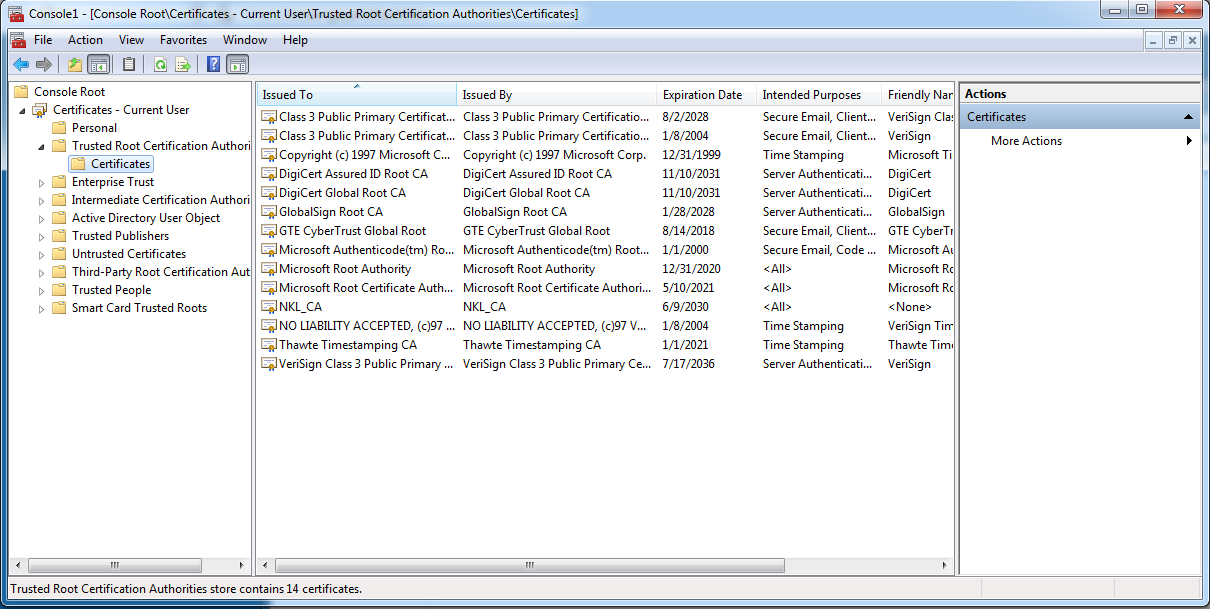
* Bước 15: Trên máy Windows 7, bật cửa sổ dòng lệnh CMD, sử dụng lệnh mmc để mở giao diện quản lý tập trung (console). Chọn **Console Root** → Chọn **Certificates - Current User** → Chọn **Trusted Root Certification Authorities** → Chọn **Certificates**

****

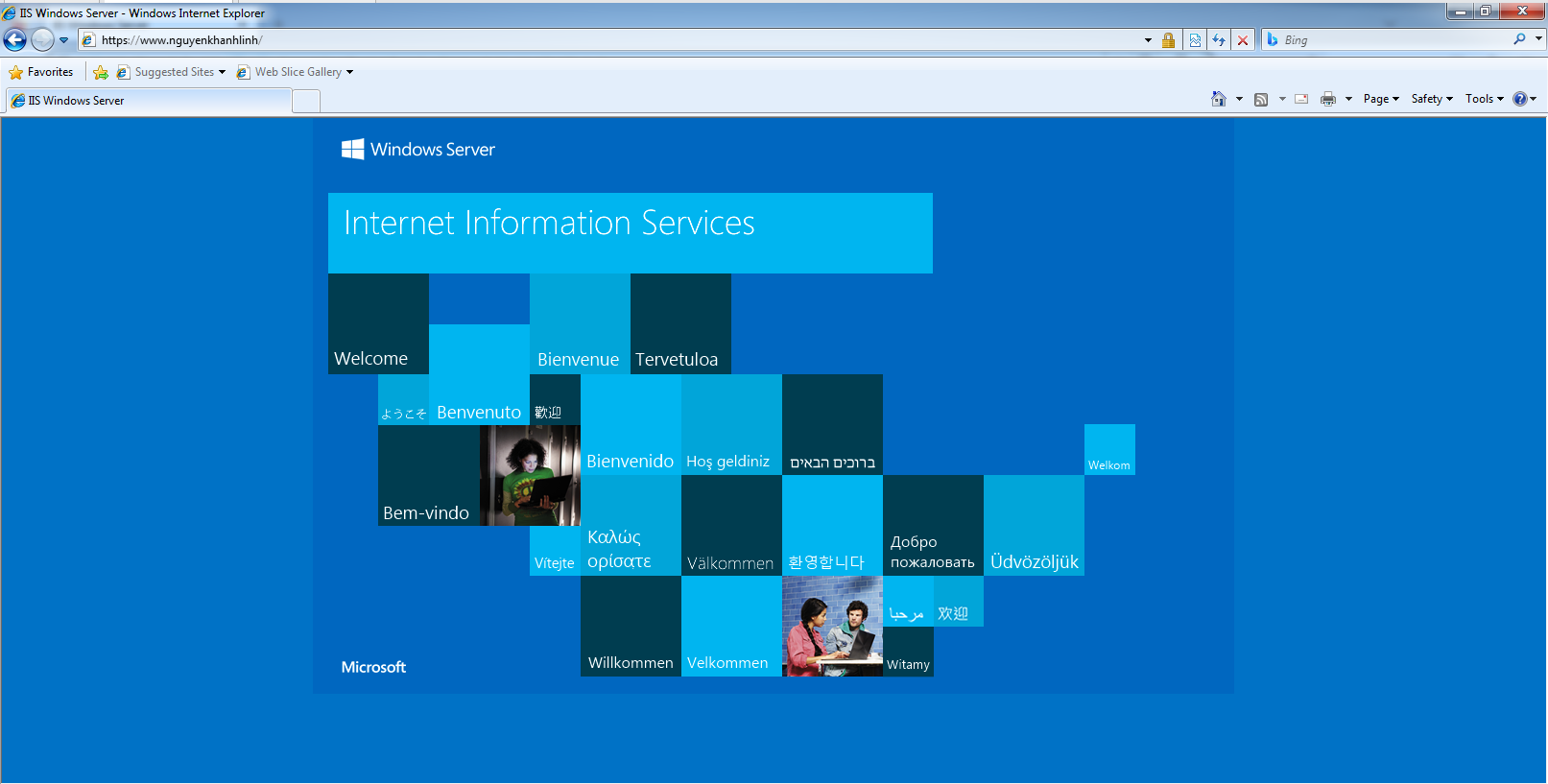
* Bước 16: Thực hiện thêm mới Certificate bằng cách chọn All Tasks → Import → Thêm đường dẫn của Certificatehttps vào File name → Finish

****

=> Chứng chỉ đã được thêm vào thành công

****

* Bước 17: Bật lại trình duyệt web IE và gõ tên miền với **https://www.nguyenkhanhlinh/** => Lỗi Certificate Error đã biến mất

****

## 3.3. Kết luận chương 3

Dựa trên mục tiêu đặt ra, chương 3 đã tiến hành triển khai thực nghiệm hệ thống dịch vụ mạng bao gồm: DNS, IIS và Certification Authority (CA) một cách đầy đủ và có hệ thống. Trước hết, dịch vụ DNS đã được cài đặt và cấu hình thành công nhằm phân giải tên miền, hỗ trợ việc truy cập website qua tên miền thay vì địa chỉ IP. Tiếp theo, dịch vụ web IIS được thiết lập để cung cấp nội dung web, đảm bảo khả năng truy cập và hiển thị trang web thông qua tên miền nội bộ. Bên cạnh đó, dịch vụ CA được triển khai để cấp phát chứng thư số, phục vụ cho việc cấu hình giao thức bảo mật SSL. Việc yêu cầu và cấp phát chứng thư số đã được thực hiện trọn vẹn, cho phép mã hóa dữ liệu truyền tải giữa máy khách và máy chủ web, nâng cao tính bảo mật và đảm bảo toàn vẹn thông tin. Cuối cùng, quá trình kiểm thử cho thấy kết nối giữa các máy trong hệ thống diễn ra thành công, chứng chỉ SSL được công nhận hợp lệ sau khi cài đặt CA tin cậy trên máy trạm.

# KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

## 1. Kết quả đạt được

### 1.1. Về mặt lý thuyết

* Tìm hiểu được tổng quan về cơ sở hạ tầng khóa công khai PKI, mục đích cũng như chức năng của cơ sở hạ tầng khóa công khai PKI trong việc xác thực và đảm bảo tính toàn vẹn của dữ liệu
* Đã biết thành phần cơ bản của CA
* Tìm hiểu về tổng quan về Windows CA, vai trò của Windows CA trong việc đảm bảo vệ dịch vụ Web
* Biết về dịch vụ Active Directory Certificate Services trên Windows Server
* Phân tích các ưu và nhược điểm của dịch vụ Active Directory Certificate Services trong việc bảo mật hệ thống, bảo vệ dữ liệu và quá trình xác thực Website thông qua CA

### 1.2. Về mặt thực nghiệm

* Thực hiện triển khai được hệ thống dịch vụ mạng bao gồm: DNS, IIS, CA
* Với DNS giúp phân giải tên miền, truy cập Website thông qua domain thay vì địa chỉ IP
* IIS thiết lập nội dung Web đảm bảo truy cập và hiển thị nội dung khi truy cập tên miền
* CA trung tâm phát hành chứng thư số phục vụ cho cấu hình giao thức bảo mật SSL giúp tăng bảo mật thông qua mã hoá và đảm bảo tính toàn vẹn dữ liệu trong quá trình truyền dẫn
* Phân tích các kết quả thực nghiệm và đưa ra được so sánh trước và sau khi CA tin cậy được cài đặt trên máy trạm (SSL certificate được công nhận)

## 2. Hạn chế

Bài báo cáo của nhóm vẫn còn một số thiếu sót. Trước hết, báo cáo hiện tại mới chỉ triển khai phần tích thực nghiệm cài đặt CA trên máy trạm thông qua việc export chứng thư từ máy chủ sau đó import vào máy trạm và chỉ dừng lại ở việc cấp phát chứng thư số cơ bản phục vụ giao thức SSL. Phần triển khai cũng chỉ dừng lại ở việc cấu hình và triển khai ở mức hiểu biết, v.v. Do hạn chế về thời gian và kiến thức còn hạn chế, nhóm rất mong nhận được sự góp ý và nhận xét từ quý thầy cô và bạn bè để tiếp tục nghiên cứu, hoàn thiện báo cáo và nâng cao kiến thức trong tương lai.

Ngoài ra, nhóm cũng nhận thấy rằng việc chỉ dựa vào các triển khai theo lab cơ bản như vậy không thể bao quát hết các tình huống thực tế có thể gặp phải. Việc tập trung vào một số loại tài liệu cụ thể cũng giới hạn phạm vi nghiên cứu của nhóm.

## 3. Hướng phát triển trong tương lai

Trong tương lai, nhóm mong rằng có thể được phát triển theo hướng nâng cao vai trò của Certification Authority (CA) trong việc quản lý và đảm bảo an toàn cho hệ thống mạng nội bộ. Thay vì chỉ dừng lại ở việc cấp phát chứng thư số cơ bản phục vụ giao thức SSL, hệ thống CA có thể được mở rộng để xây dựng một hạ tầng khóa công khai (PKI) hoàn chỉnh, bao gồm việc triển khai các chính sách chứng thực (Certificate Policies), thiết lập cơ chế thu hồi chứng thư (CRL – Certificate Revocation List) và tích hợp giao thức OCSP (Online Certificate Status Protocol) nhằm đảm bảo khả năng kiểm tra trạng thái chứng thư theo thời gian thực.

Bên cạnh đó, có thể nghiên cứu việc phân tầng CA (gồm root CA và subordinate CA) để nâng cao tính an toàn và khả năng kiểm soát trong môi trường mạng lớn, đồng thời đảm bảo việc cấp phát chứng thư tuân theo chuẩn mực và quy định cụ thể theo từng cấp tổ chức. Hướng phát triển khác cũng có thể bao gồm việc tích hợp CA vào các hệ thống xác thực người dùng như RADIUS hoặc Active Directory Certificate Services (AD CS), từ đó nâng cao khả năng kiểm soát truy cập và chứng thực thiết bị trong môi trường doanh nghiệp.

Cuối cùng, để đáp ứng yêu cầu triển khai thực tế trong các môi trường đa dạng như điện toán đám mây hoặc mạng phân tán, việc tự động hóa toàn bộ quy trình cấp phát, gia hạn và thu hồi chứng thư thông qua các công cụ như Certbot, HashiCorp Vault hoặc Microsoft Intune cũng là một hướng đi tiềm năng, giúp hệ thống linh hoạt và bảo mật hơn trước các mối đe dọa ngày càng phức tạp. Nhóm mong nhận được sự hướng dẫn và góp ý từ các chuyên gia để có thể cải thiện và phát triển nghiên cứu một cách toàn diện và hiệu quả hơn. Với sự hỗ trợ này, nhóm tin rằng sẽ có thể đạt được những kết quả tốt hơn trong những dự án tiếp theo.

# TÀI LIỆU THAM KHẢO

[1] Lê Quang Tùng, Nguyễn Thị Hồng Hà, Giáo trình Chứng thực điện tử, Học viện kỹ thuật mật mã, 2013.

[2] TS. Lương Thế Dũng, KS. Cao Minh Tuấn, Giáo trình Quản trị an toàn hệ thống, Học viện kỹ thuật mật mã, 2013.

[3] Suranjan Choudhury, Kartik Bhatnagar, Wasim Haque, &NIIT, Public Key Infrastructure: Implementation and Design, ISBN978-0-7645-4879-6, M&T Books, 2002.

[4] Matthew Burr, Practical Guide to PKI with Windows Server.

## 