Cung cấp thông tin về các nhân viên trong một công ty cùng các tác vụ thêm, sửa xóa.

Phân tích yêu cầu

1. Môi trường:

* Máy chủ windows server 2008
* Web server: internet information services 7.0
* Nền tảng ứng dụng: .NET framework 4.0

1. Các chức năng:

* Xem danh sách nhân viên
* Tìm kiếm nhân viên + Xem thông tin chi tiết của một nhân viên cụ thể
* Sửa đổi thông tin của một nhân viên
* Xóa một nhân viên khỏi danh sách
* Chỉnh sửa quyền hạn của một nhân viên

1. Danh sách quyền hạn

* Ban giám đốc
* Quản lý nhân viên
* Nhân viên

1. Các yêu cầu về bảo mật

* Đảm bảo chính xác quyền hạn với các nhân viên
* Chống các hình thức tấn công giả mạo, chặn giữ thông tin, sửa đổi thông tin
* Chống tấn công thụ động

1. Các hình thức áp dụng

* Xác thực đối với người dùng.
* Bảo mật kênh truyền bằng Secure Socket Layer (SSL) và Mã hóa bản tin bằng chứng chỉ X509.

1. Kịch bản áp dụng bảo mật

* Trường hợp: client muốn sử dụng một dịch vụ nào đó của server
* Các bước:
  + Bước 0: client đăng ký tài khoản và các yêu cầu sử dụng dịch vụ với Server, Server đồng ý và gửi về cho client thông tin tài khoản và chứng chỉ bảo mật. Mật khẩu của client được mã hóa sử dụng bảng băm MD5. Với mỗi một chuỗi mật khẩu có độ dài bất kỳ, bảng băm MD5 sẽ cho ra một chuỗi có độ dài không đổi 128 bit và duy nhất với các chuỗi đầu vào khác nhau. Người quản trị cũng như bên tấn công không thể giải mã được chuỗi mật khẩu đã mã hóa.
  + Bước 1: Khi client muốn sử dụng một dịch vụ của server, client và server sẽ cùng nhau xác thực thông qua chứng chỉ ở phía server và chứng chỉ được cấp phát cho client. Các chứng chỉ này đều có gốc là một chứng chỉ được tin cậy đặt trên máy server. Các bước xác thực bằng chứng chỉ:
    - Client gửi bản tin yêu cầu kết nối cùng bản tin mã hóa bao gồm thông chứng của mình kèm theo nhãn thời gian cho server.
    - Server nhận và giải mã bản tin, sau khi xác nhận chứng chỉ của client cùng nhãn thời gian là hợp lệ, server đồng ý tạo liên kết với client.
  + Bước 2: Client gửi một bản tin được mã hóa mô tả dịch vụ muốn sử dụng, các tham số cùng thông tin bảo mật gồm có:
    - Khóa phiên:
      * Nhãn thời gian.
      * Khóa công khai của client.
    - Tên dịch vụ sử dụng.
    - Các tham số dịch vụ.
    - Định danh (Username – trên truy cập) client đã đăng ký trước đó.
    - Mật khẩu của client.
  + Bước 3: Server nhận và giải mã bản tin, xác thực người dùng hợp lệ và có quyền sử dụng dịch vụ. Server thực hiện dịch vụ dựa trên các danh sách tham số mà người dùng đã gửi tính toán và gửi trả kết quả cho client dưới dạng bản tin đã được mã hóa. Kết quả bao gồm
    - Khóa phiên
      * Nhãn thời gian.
      * Khóa công khai của server.
    - Nhãn thời gian trong bản tin mà client đã gửi trước đó.
    - Tên dịch vụ sử dụng.
    - Các tham số dịch vụ.
    - Kết quả thực hiện dịch vụ.
  + Bước 4: Client nhận bản tin hồi đáp, xác thực người gửi là server cùng dựa vào các thông tin như nhãn thời gian của bản tin yêu cầu, tên dịch vụ, các tham số để đảm bảo rằng kết quả trả về là chính xác. Client gửi lại cho server một bản tin acknowledgement xác nhận lại kết quả là chính xác và tin cậy. Kết thúc quá trình thực hiện một dịch vụ.

1. Các bước triển khai

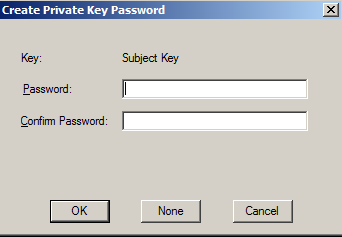
* Xây dựng và triển khai ứng dụng cung cấp web services với các chức năng tương ứng, ứng dụng có tên SecurceContact, chạy trên IIS 7.0
  + Xem toàn bộ danh sách nhân viên.
  + Tìm kiếm nhân viên theo ID và xem chi tiết của một nhân viên cụ thể.
  + Sửa đổi thông tin của nhân viên.
  + Xóa nhân viên khỏi danh sách.
  + Chính sửa quyền hạn của nhân viên.

Bên cạnh các chức năng, ứng dụng phải đảm bảo các quy trình bảo mật đã nêu ở trên.

* Cấu hình ứng dụng sử dụng SSL
  + Tạo chứng chỉ bảo mật theo X509 gốc RootCA
  + Vào Command Prompt. Gõ dòng lệnh

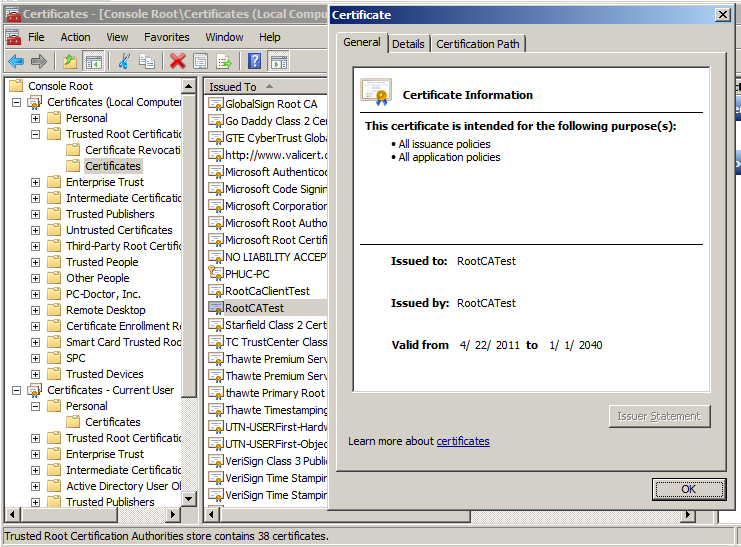
makecert ‐n "CN=RootCATest" ‐r ‐sv RootCATest.pvk RootCATest.cer.

* + Gõ mật khẩu, đây có thể coi là khóa chung chia sẻ giữa client và server.



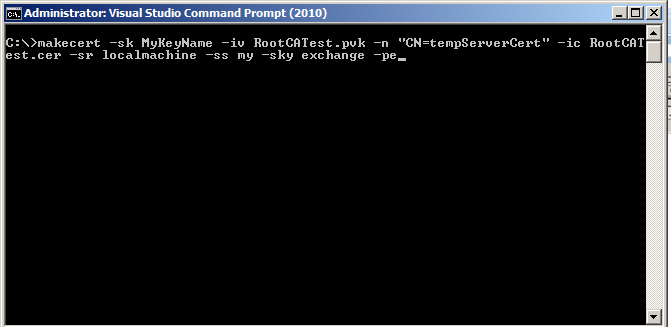
Sau khi thực hiện, ta có 2 file "RootCATest.pvk" và "RootCATest.cer".

* + Tạo  Certificate Revocation List từ các file đã làm ở bước trên bằng cách gõ dòng lệnh trong Command Prompt
    - * + makecert ‐crl ‐n "CN=RootCATest" ‐r ‐sv RootCATest.pvk RootCATest.crl
  + Tiến hành cài đặt lên server
    - * + Mở Microsoft Management Console bằng cách vào Run, gõ mmc.
        + Cài đặt chứng chỉ vào Local Machine 🡪 Trusted Root Certification Authorities 🡪Certificates

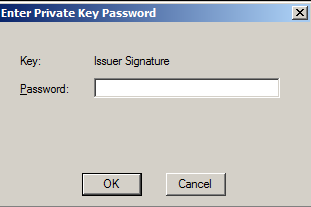


* + Tạo chứng chỉ phía server
    - Dựa trên những file chứng chỉ đã có, tạo chứng chỉ dựa trên RootCATest, gõ đoạn lệnh sau trong Command Prompt makecert ‐sk MyKeyName ‐iv RootCATest.pvk ‐n "CN=tempServerCert" ‐ic

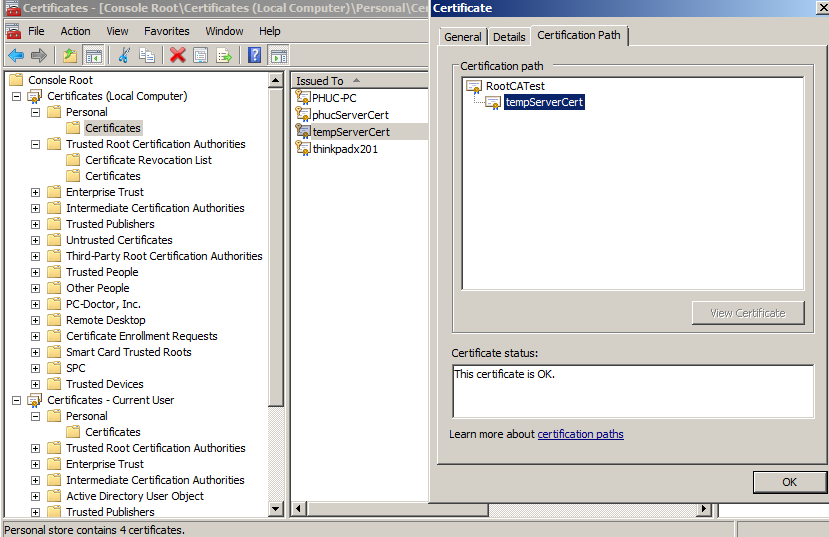
RootCATest.cer ‐sr localmachine ‐ss my ‐sky exchange ‐pe



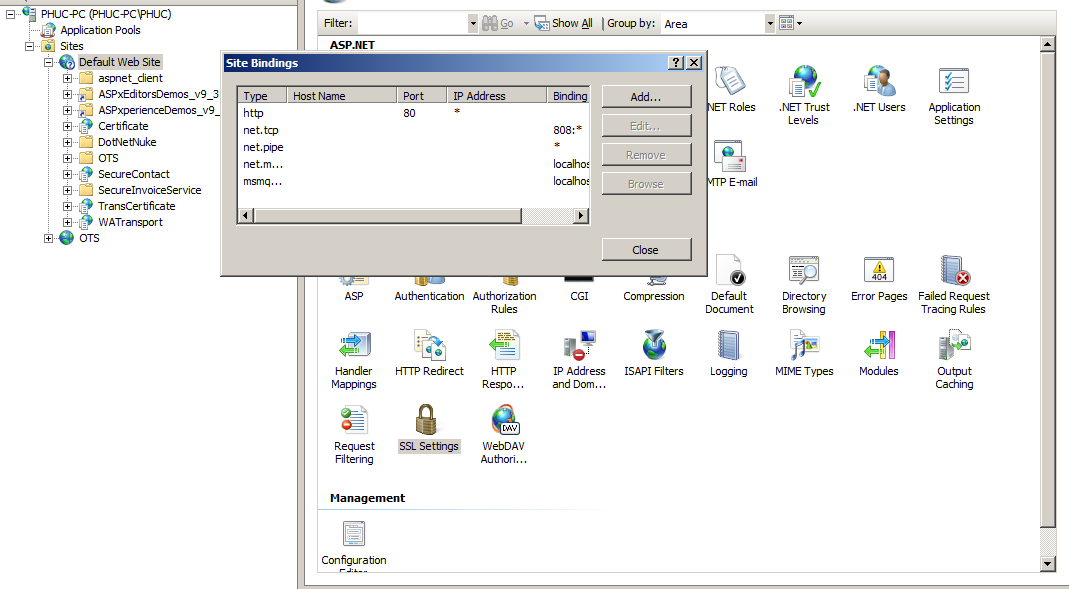
* + - Điền mật khẩu, mật khẩu này phải giống với mật khẩu của RootCATest



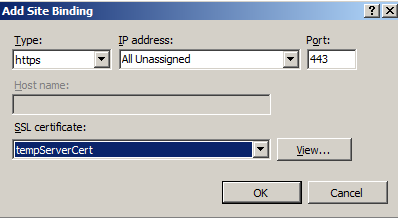
* + - Sau khi tạo chứng chỉ thành công, chứng chỉ sẽ được cài đặt vào các chứng chỉ của LocalMachine 🡪 Personal 🡪 Certificates



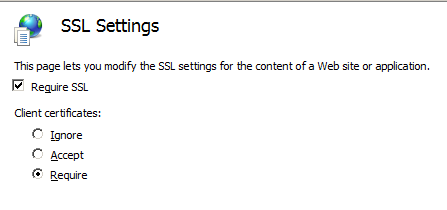
* + - Cấu hình ứng dụng sử dụng SSL
      * Sau khi đã cài đặt chứng chỉ cho server, iis cũng sử dụng chứng chỉ đó để thực hiện bảo mật. Cấu hình chứng chỉ cho website, chọn mục Bindings trong website.



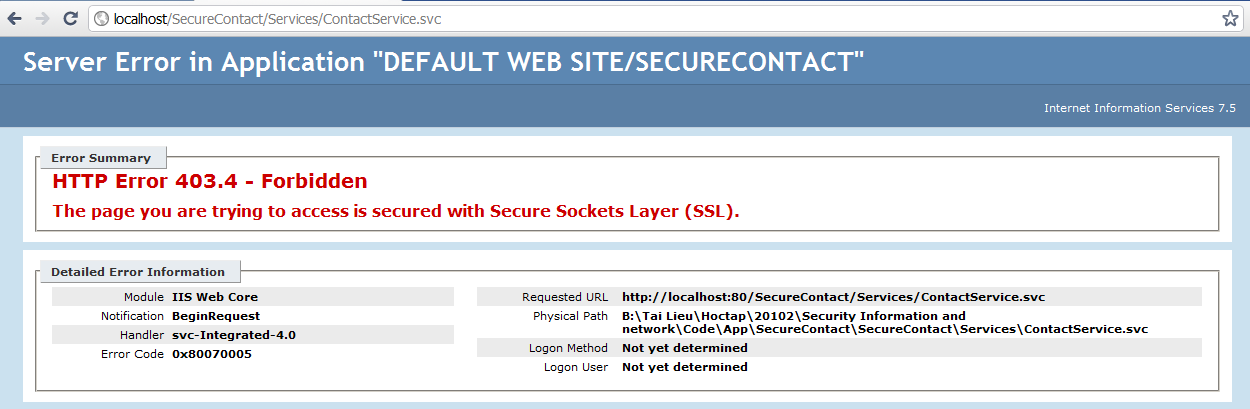
* + - * Chọn Add, cấu hình https và chọn chứng chỉ vừa cài đặt.



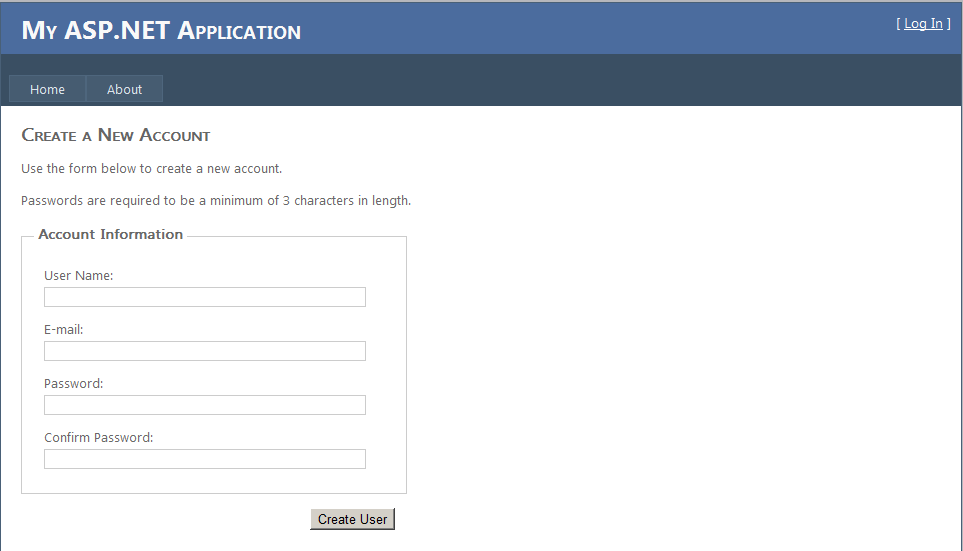
* + - * Cấu hình yêu cầu website buộc phải truy cập qua SSL, vào mục SSL Setting, chọn Require SSL



Sau khi cấu hình xong, người dùng không thể truy cập địa chỉ của trang thông qua phương thức bình thường, trang báo lỗi như sau



* Xây dựng ứng dụng phía client.
  + Để ứng dụng có thể sử dụng dịch vụ của server cung cấp, trước tiên người dùng phải đăng ký với ứng dụng.



* + Ứng dụng sẽ cấp cho client một chứng chỉ dựa trên chứng chỉ RootCATest. VD: tempClientCert. Phía client phải cài đặt chứng chỉ thông qua Microsoft Management Console vào: CurrentUser (tài khoản người dùng hiện tại trên Windows) 🡪 Personal 🡪 Certificates.

