Hướng dẫn sử dụng và triển khai Trang Web 123Certificate.com (Chức năng Certificate Authority)

I. Giới thiệu chung:

Trong thời đại bùng nổ các dịch vụ trên internet như hiện nay, các tổ chức tài chính , ngân hàng ngày càng cung cấp đa dạng các sản phẩm, dịch vụ trực tuyến của mình tới đông đảo khách hảng qua mạng internet. Tuy vậy, bên cạnh những lợi ích mà các dịch vụ trực tuyến đem lại, các tổ chức tài chính , chính phủ, doanh nghiệp và các cá nhân đòi hỏi không những phải bảo vệ toàn vẹn thông tin lưu chuyển trên Internet mà còn phải cho họ cảm giác tin cậy giống như khi giao dịch trên giấy tờ.

Trước khi giao phó các giao dịch nhạy cảm của mình cho internet, người sử dụng đòi hỏi mức an toàn đặc biệt. Họ muốn rằng giao dịch điện tử phải đáng tin cậy và phải được bảo vệ chống xem trộm. Họ muốn được bảo đảm rằng không ai có thể phủ nhận hành vi liên quan của mình trong giao dịch khi có sự cố sảy ra.

Dựa trên cách sử dụng của chìa khóa công cộng và chữ ký điện tử , một chìa khóa công cộng là bộ khung các chính sách, dịch vụ và phần mềm mã hóa, đáp ứng nhu cầu bảo mật của người sử dụng khi gởi đi những thông tin quan trọng qua internet và các mạng khác.

Chìa khóa công cộng bảo đảm độ tin cậy đối với các thông tin hoặc thông điệp quan trọng bằng cách sử dụng các thuật toán, hay còn gọi là chìa khóa, để mã hóa dữ liệu và một chìa khóa để giải mã chúng. Trong dịch vụ chìa khóa mật mã công cộng, người sử dụng nhận được phần mềm mã hóa đặc biệt và một cặp chìa khóa. Trong đó có một chìa khóa là khóa công cộng(public key) để có thể sử dụng dịch vụ, chia khóa còn lại là chìa khóa cá nhân(private key) mà người dùng phải giữ bí mật.

Hai chìa khóa này có mối liên hệ mật thiết với nhau, sao cho một thông điệp được mã hóa bởi một chìa khóa công cộng thì chỉ giải mã được bởi chìa khóa cá nhân tương ứng.

Tổ chức chứng nhận khóa công CA là một thành phần chính của PKI. Nó là một tổ chức thứ ba đáng tin cậy chịu trách nhiệm phát hành giấy chứng nhận kỹ thuật số và quản lý chúng trong thời hạn có hiệu lực. Chứng nhận kỹ thuật số là những tập tin điện tử chứa các chìa khóa mật mã công cộng và các thông tin nhận dạng đặc biệt về người sử dụng. Các chứng nhận này có "dán tem" xác nhận và không thể làm giả được. Cũng giống như việc phát hành hộ chiếu, tổ chức cấp giấy chứng nhận xác nhận rằng cá nhân được cấp giấy chứng nhận kỹ thuật số là người đáp ứng đủ điều kiện.

Chữ ký điện tử là một xác minh điện tử ngang bằng với một chữ ký truyền thống trên giấy. tức là có giá trị duy nhất, có thể kiểm chứng được và chỉ người ký mới có thể tạo ra nó. Thông điệp hay tài liệu dù đã được mã hóa hay chưa, hễ có chữ ký điện tử thì cũng đảm bảo được răng thông tin đó không bị xâm phạm trong quá trình lưu chuyển.

Các chính phủ, doanh nghiệp, cá nhân hội nhập vào cuộc cách mạng số hóa đều sẽ dùng chứng nhận kỹ thuật số. Khi phát hành một số lượng lớn giấy chứng nhận như vậy thì cần thì cần phải đề ra biện pháp quản lý việc sử dụng. Quản lý giấy chứng nhận là công việc lâu dài của tổ chức cấp giấy chứng nhận PKI. Trên khắp thế giới, các công ty lớn và nhỏ đều đầu tư cho cơ sở hạ tầng chìa khóa công cộng như là một giải pháp hữu hiệu cho sáng tạo tập trung, phân phối, quản lý, chứng nhận cải tiến và đổi mới.

CA(Certificate Authority) : là từ dùng để nói về một tổ chức được tin nhiệm để cấp giấy chứng nhận khóa công (certificate) cho những cá nhân và tổ chức khác.

Việc kiểm tra giấy chứng nhận khóa công gồm các bước sau đây:

1. Xem certificate này được ai ký, tổ chức ký certificate đó cáo đáng tin cậy hay không?
2. Xem certificate này còn hạn sử dụng không?
3. Xem certificate này có bị vô hiệu hóa chưa?
4. ….

II. Điều kiện tiên quyết để triển khai trang web 123Certificate.com:

Đê thực hiện lab này bạn phải cài đặt và cài đặt đầy đủ những phần mềm sau:

- JDK 1.6
- Tomcat 6.0
- Eclipse
- Axis2-1.5.1

III. Hướng dẫn cài đặt triển khai.

Đầu tiên bạn phải cài đặt Apache2, JDK 1.6 Tomcat 6.0, eclipse, axis2-1.5.1 hướng dẫn cài đặt những tài liệu này các bạn tham khảo ở document HuongDanTrienKhaiTrang webCA.doc.

Download Tomcat 6.0.20 từ địa chỉ http://tomcat.apache.org.

1. **Đây là trang chủ của 123certificate.com.**

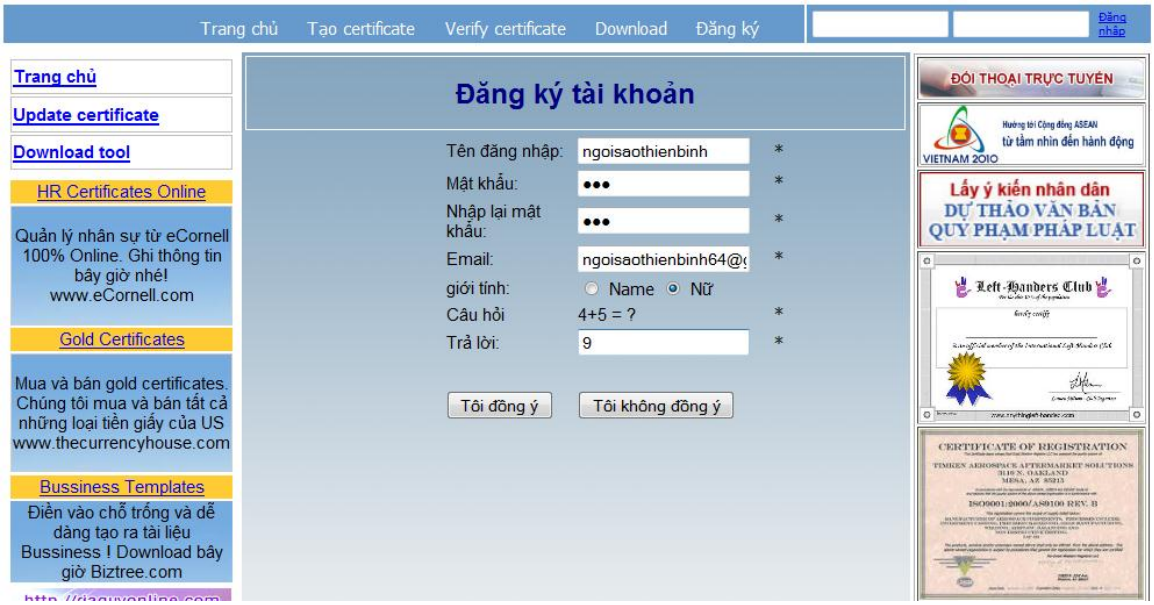
2. **Download tool tạo cặp key và chữ ký điện tử.**

Bạn đăng nhập vào địa chỉ:

Trình duyệt sẽ hiển thị màn hình sau đây:

Click vào download để download tool về.
http://localhost:8080/WebCA_12_10_2010/Redirect?page=form_DownloadTool.jsp

3. **Để đăng ký một tài khoản trên certificate.com bạn đăng nhập vào địa chỉ:** http://localhost:8080/WebCA_12_10_2010/Redirect?page=form_register.jsp, điền tên cũng như thông tin cá nhân để khởi tạo.
   Lưu ý: bạn phải điền vào đầy đủ các trường trong form đăng ký. Và username phải chưa tồn tại trong cơ sở dữ liệu.



Sau đó click vào Tôi đồng ý để đăng nhập. Nếu đăng nhập thành công màn hình sẽ hiển thị thông báo thành công. Click để trở về trang chủ.

4. **Tạo certificate:**
   Chức năng này chỉ được thực hiện khi bạn đã login thành công vào hệ thống.

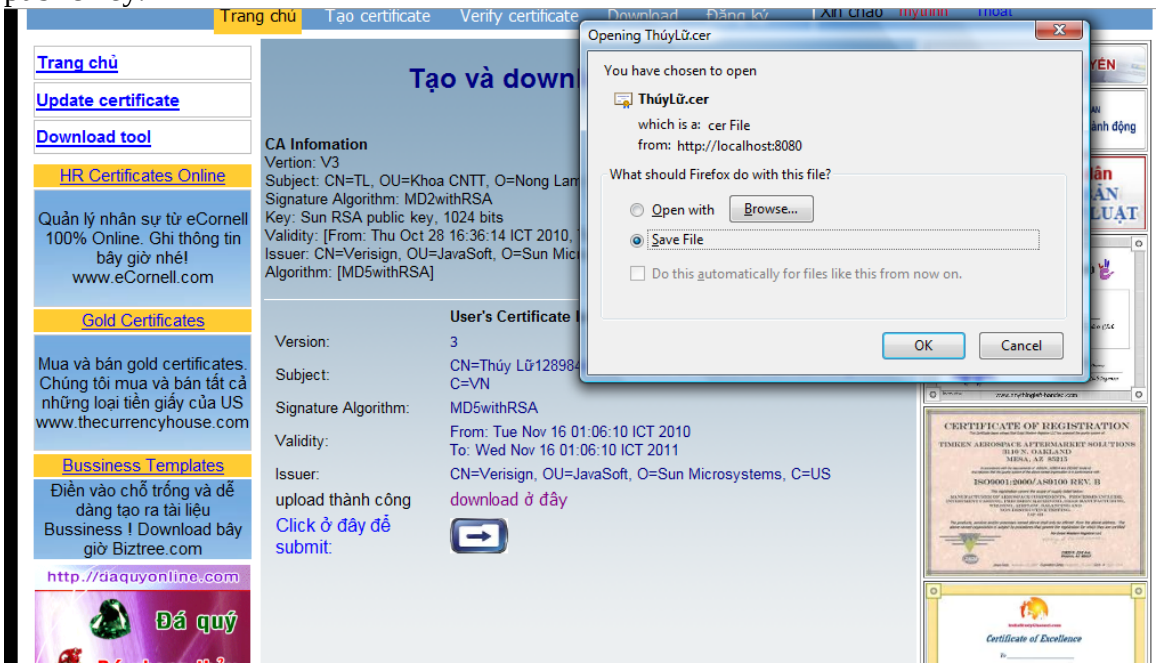
Bạn đăng nhập vào địa chỉ:
http://localhost:8080/WebCA_12_10_2010/Redirect?page=form_create_cert.jsp.

Điền đầy đủ thông tin tên , đơn vị tổ chức, thành phố, hoặc tỉnh, nước sau đó click vào button submit.

- Các trường nhập không đúng định dạng. Hệ thống sẽ yêu cầu bạn nhập lại .
- Các trường nhập đúng định dạng. Hệ thống sẽ hiển thị thông tin certificate của bạn sắp được tạo. Yêu cầu bạn upload public key để tạo certificate.

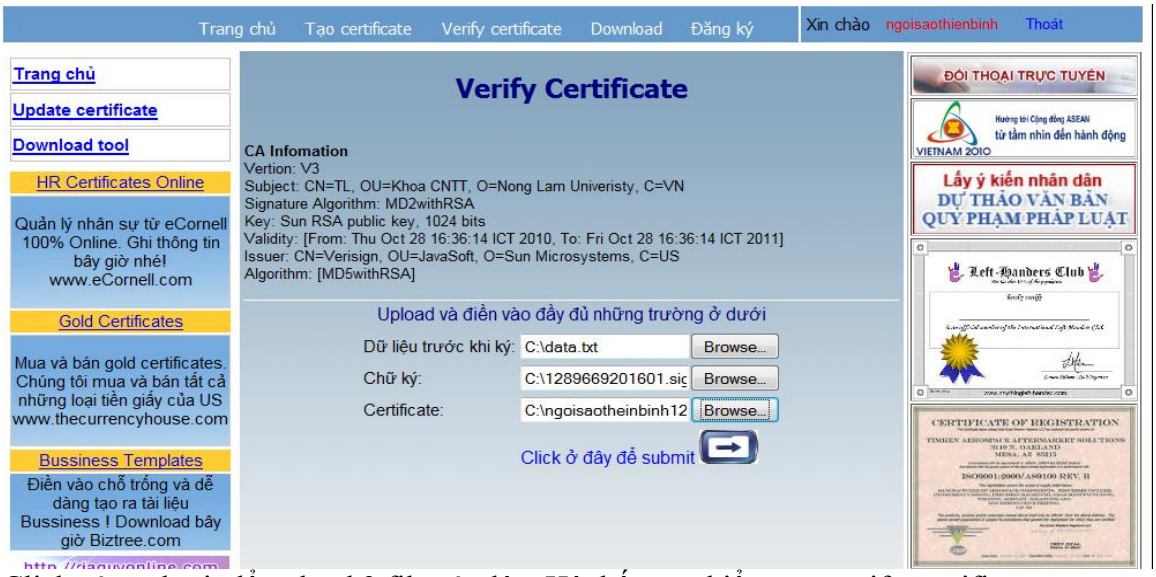
- Bạn đồng ý click button submit . Hệ thống sẽ thực hiện quá trinh upload public key và tạo certificate.

- Nếu file public key bạn truyền vào đúng hệ thống thông báo thành công. Hiển thị thông tin certificate và yêu cầu bạn download certificate.
- Nếu file certificate bạn truyền vào không đúng hệ thống yêu cầu bạn upload lại public key.



5. Verify Certificate:

- Bạn phải đăng nhập vào hệ thống trước khi thực hiện chức năng này.
- Đăng nhập vào địa chỉ: http://localhost:8080/WebCA_12_10_2010/Redirect?page=form_verify_cert.jsp
- Nhập thông tin đầy đủ vào form:
  - Form dữ liệu trước khi ký: Chỉ đường dẫn đến file dữ liệu gốc bạn cần ký.
  - Form chữ ký: chỉ đường dẫn đến file đã được ký.
  - Form certificate: chỉ đường dẫn đến file certificate của bạn.



- Click vào submit để upload 3 file này lên. Hệ thống sẽ kiểm tra, verify certificate.
  - Các thông tin này bị sai lệch hệ thống thông báo xác thực không thành công. Ngược lại thành công browser sẽ xuất hiện màn hình sau:

6. Download certificate:

- Bạn phải đăng nhập trước khi thực hiện chức năng này.
- Đăng nhập vào địa chỉ: http://localhost:8080/WebCA_12_10_2010/Redirect?page=form_download_cert.jsp.
- Tài khoản đăng nhập vào đã từng tạo certificate nào sẽ được download chính những certificate đó về.
    - VD: ở đây ngoisaothienbinh đã tạo được hai certificate.

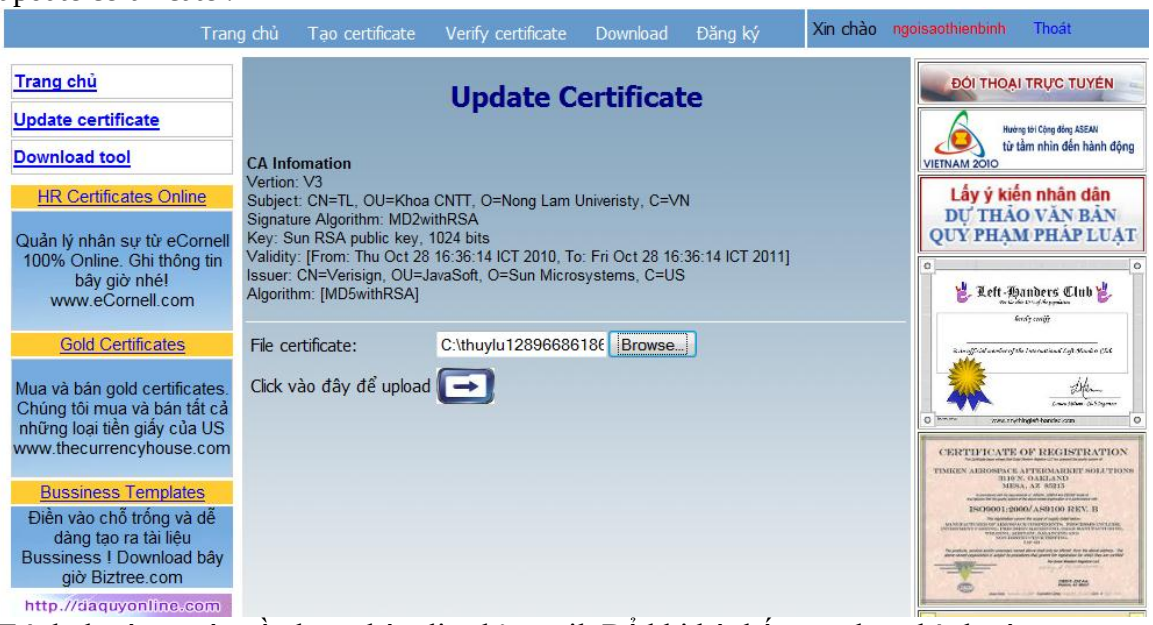
- Chọn certificate cần download. Click vào chi tiết: browser hiển thị trang có đầy đủ thông tin của certificate bạn cần download về.

- Click vào download để download certificate về.

7. Update certificate:

- Khi certificate của bạn bị hết hạn, bạn có thể update lại certificate.
- Phải đăng nhập trước khi thực hiện chức năng này.

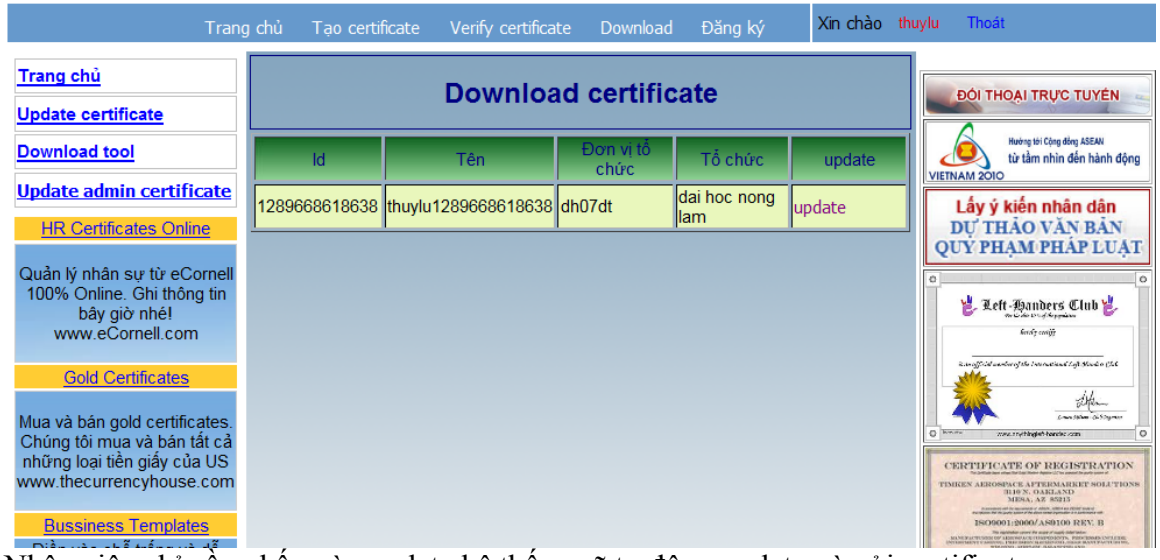
- Đăng nhập theo địa chỉ sau: http://localhost:8080/WebCA_12_10_2010/Redirect?page=form_update_certificate.jsp
- Form file certificate: Bạn chỉ đường dẫn đến file certificate cần update. Click vào update certificate .



- Trình duyệt sẽ yêu cầu bạn nhập địa chỉ email. Để khi hệ thống update thành công hệ thống sẽ gửi certificate qua địa chỉ email.

8. Admin update certificate:

- Đăng nhập với quyền là nhân viên của hệ thống để thực hiện chức năng này.
- Đăng nhập theo địa chỉ: http://localhost:8080/WebCA_12_10_2010/Redirect?page=from_adminUpdateCert.jsp
- Xuất hiển màn hình sau:



- Nhân viên chỉ cần nhấn vào update hệ thống sẽ tự động update và gửi certificate vừa mới được tạo cho nhân viên đó qua địa chỉ email.