<https://www.ejbca.org/>

<https://viblo.asia/p/phan-2-gioi-thieu-ve-ejbca-va-cach-cai-dat-ejbca-tren-windows-GrLZDvEV5k0>

# Giới thiệu

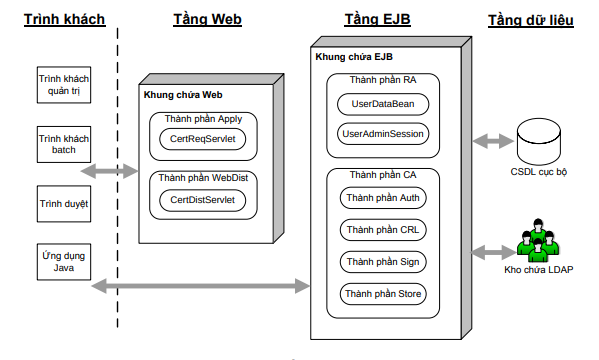
EJBCA là sản phẩm mã nguồn mở của hãng Primekey. Đây là một CA được xây dựng trên công nghệ Java J2EE, nhờ đó hiệu suất hoạt động cũng như khả năng tùy biến của CA là tương đối cao so với các hệ thống mã nguồn mở khác. Bên cạnh đó, EJBCA còn cung cấp tính năng và thành phần (OCSP, RA Service, Publisher,…) giúp cấu thành một hệ thống PKI tương đối đầy đủ và hoàn thiện.

### 1. Đặc điểm kỹ thuật

Được xây dựng dựa trên Java, EJBCA thực sự là một nền tảng độc lập, chạy trên hầu như toàn bộ các phần cứng phổ biến cũng như các hệ điều hành thông dụng như Window, Linux. Để có thể hoạt động, EJBCA cần chạy trên một nền tảng máy chủ ứng dụng (Application Server) cũng như một hệ thống Cơ sở dư liệu nhất định. Về mặt này, EJBCA cũng hỗ trợ hầu hết các nền tảng App Server phổ biến hiện nay như: JBOSS – Oracle Weblogic – IBM Web Sphere… cũng như các hệ cơ sở dữ liệu từ miễn phí đến trả phí: MySQL, Oracle, IBM DB2, MS SQL,…  
Bên cạnh đó, EJBCA còn có một số điểm đặc trưng sau:

* Cung cấp khả năng xây dựng CA theo nhiều mức, không giới hạn số lượng CA;
* Hỗ trợ thuật toán RSA với độ dài khóa lên tới 4096 bits;
* Hỗ trợ các thuật toán DSA với độ dài khóa lên tới 1024 bits;
* Hỗ trợ các hàm băm như MD5, SHA-1, SHA-256;
* Chứng thư được phát hành tuân thủ nghiêm ngặt chuẩn X509.

### 2. Kiến trúc



* **Tầng dữ liệu (Data Tier):** Tầng dữ liệu lưu trữ các chứng nhận, CRL cũng như các thực thể cuối. EJBCA sử dụng một cơ sở dữ liệu mặc định để lưu trữ các thực thể cuối. Các chứng nhận được lưu trữ trong một kho chứa LDAP (Lightweight Directory Access Protocol).
* **Thành phần CA:** Thành phần có chức năng tạo các CA gốc, CA con, chứng nhận, CRL và giao tiếp với kho chứa LDAP để lưu trữ thông tin chứng nhận.
* **Thành phần RA:** Thành phần có chức năng tạo, xóa và hủy bỏ người dùng. Nó giao tiếp với cơ sở dữ liệu cục bộ để chứa thông tin người dùng.
* **Tầng Web:** Đây là giao diện (điển hình là giao diện người – máy bằng đồ họa) để trình khách tương tác với hệ thống EJBCA, đồng thời quy định các cấp độ và phạm vi truy cập thông tin khác nhau cho thực thể cuối.
* **Trình khách:** Trình khách là thực thể cuối hay người sử dụng như trình khách thư điện tử, máy chủ web, trình duyệt web hay cổng VPN. Các thực thể cuối không được phép phát hành chứng nhận đến các thực thể khác, nói cách khác chúng là các nút lá trong PKI.

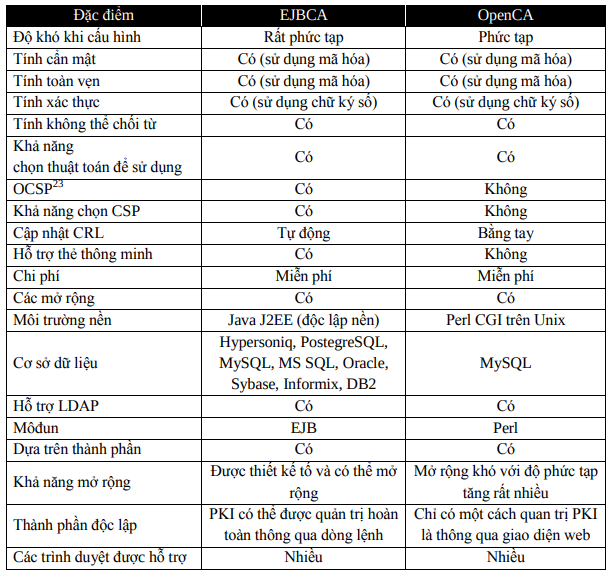
### 3. Chức năng

* EJBCA là một tổ chức chứng nhận rất phổ biến hiện đang được sử dụng
* Tùy chọn chọn giữa các thuật toán SHA1 hay SHA256 với RSA và với các kích thước khóa khác nhau như 1024, 2048 và 4096.
* Cung cấp một số tính năng nổi bật về lựa chọn ngôn ngữ trong quá trình cấu hình hệ thống.
* Ngoài ra cũng có thể chọn loại publisher mình muốn như LDAP, thư mục động (AD – Active Directory) hay một kết nối publisher tự làm.
* Sự phát hành của chứng nhận luôn luôn thuộc chuẩn X509
* Việc ký chứng nhận có thể là tự ký (self-signed), CA bên ngoài (external CA) hay CA quản trị (admin CA).

### 4. So sánh với các gói phần mềm khác

Ngoài EJBCA còn có các sản phẩm khác có thể triển khai hệ thống PKI hoàn chỉnh như OpenCA và Windows 2003 Server CA. Do Windows 2003 Server CA không phải là sản phẩm mã nguồn mở, không thể tự do phát triển cũng như kiểm soát được quá trình phát triển và độ an toàn nên không được quan tâm tìm hiểu. EJBCA và OpenCA đều là các dự án PKI mã nguồn mở mạnh và hiện cũng có nhiều phát triển đang được thực hiện trên cả hai phần mềm này.

* ***Bảng so sánh một số đặc điểm giữa EJBCA và OpenCA***

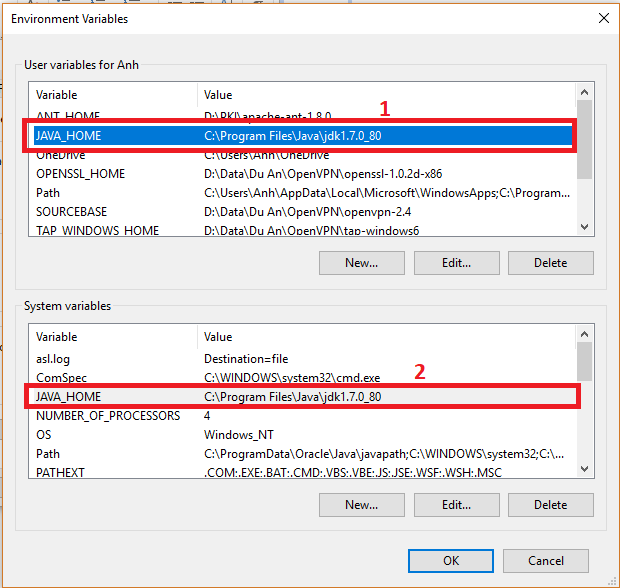
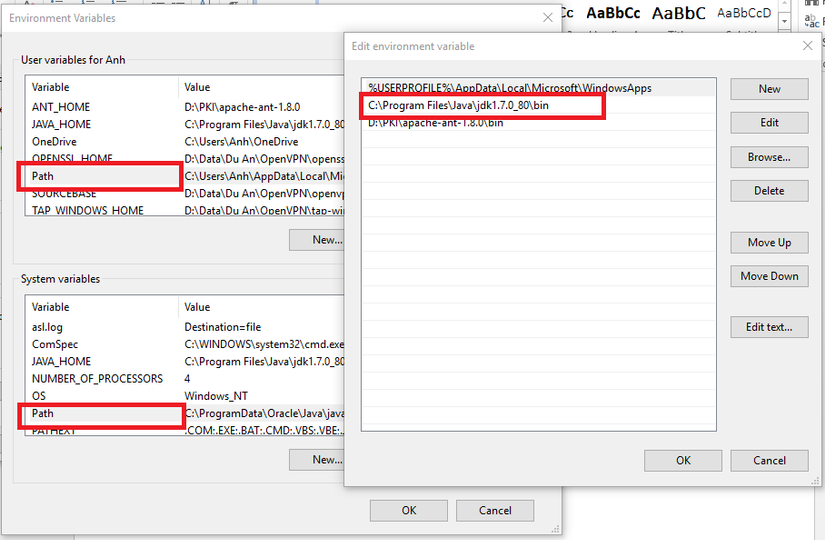


* ***Lý do chọn gói phần mềm mã nguồn mở EJBCA***
  + EJBCA đảm bỏ tất cả các tiêu chí trong bảng trên
  + Là một CA và là một hệ thống quản lý PKI hoàn chỉnh, là một giải pháp PKI rất mạnh, độc lập môi trường, hiệu suất cao, có thể mở rộng và dựa trên thành phần.
  + Linh hoạt trong việc cung cấp các cách thức hoạt động tùy chọn như một CA độc lập hoặc được tích hợp hoàn toàn trong ứng dụng thương mại bất kỳ
  + Việc cập nhật CRL trong EJBCA hoàn toàn tự động.
  + Tuy việc cấu hình hệ thống EJBCA phức tạp hơn OpenCA rất nhiều nhưng hệ thống EJBCA khi đã đi vào hoạt động lại mang đến rất nhiều tiện lợi và đơn giản cho người sử dụng trong việc phát sinh và quản lý chứng nhận.

# Cài đặt EJBCA trên Windows

Ở đây mình dùng ejbca6, jboss7, java7, ant1.8 và mysql

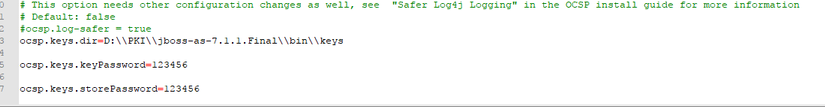
### 1. Cài đặt JAVA

* Downlod bộ cài jdk7 trên trang (<https://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase7-521261.html>)  
  Các bạn chọn windows x86 (x64) đều được. (chú ý không sử dụng java8 vì jboss7 chỉ chạy được trên jdk7)
* Cài đặt java (file .exe)
* Cấu hình biến môi trường JAVA\_HOME
* Vào tab: Control Panel\System and Security\System
* Chọn Advanced system settings > Advanced  
    
    
  Tạo 2 biến JAVA\_HOME và value trỏ đến folder jdk (như hình vẽ)
* Edit dòng path: thêm folder bin của jdk  
  

### 2. Cài đặt Ant

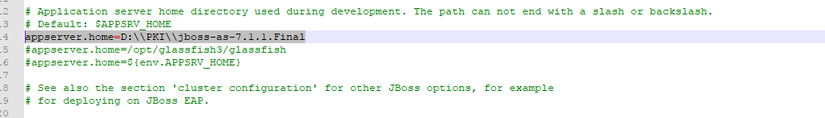
* Download ant 1.8.2 trên trang <https://archive.apache.org/dist/ant/binaries/> (bản zip)
* Giải nén
* Cấu hình ANT\_HOME (tương tự như cấu hình JAVA\_HOME ở trên)

### 3. Cài đặt Database

* Các bạn có thể lên trang <https://dev.mysql.com/downloads/workbench/5.2.html> này để tải về.  
  Nếu bạn nào chưa biết cách cài có thể lên trang <https://www.youtube.com/watch?v=ySWpNLwpJx4> này xem để cài. (Mình thấy video này hướng dẫn rất dễ hiểu)
* Sau đó tạo 1 database để lưu dữ liệu.
  + Giả sử tạo 1 csdl có user/pass là: root/123456
  + Tạo database tên là ejbca
* Cấu hình CSDL ở file: \ejbcace6311\conf\database.properties
* Cấu hình OCSP ở file: : \ejbcace6311\conf\ocsp.properties 

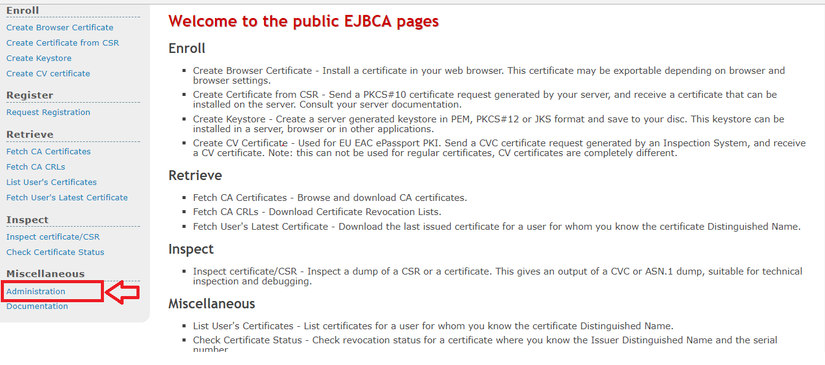
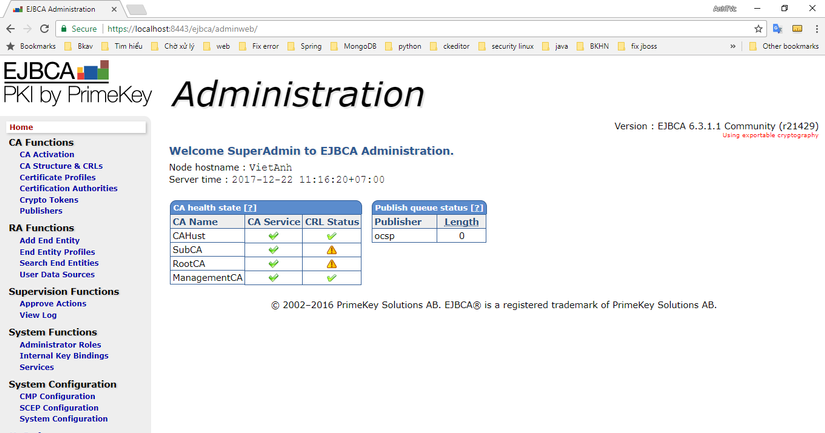
### 4. Cài đặt ejbca, jboss

Ở đây mình cài ejbca và jboss trên ổ D của mình. Các bạn cũng có thể cài ở bất kỳ ổ nào các bạn muốn

* Download ejbca (<https://sourceforge.net/projects/ejbca/files/ejbca6/ejbca_6_3_1_1/ejbca_ce_6_3_1_1.zip/download>) và jboss (<http://jbossas.jboss.org/downloads>)
* Ở đây mình sẽ giải nén 2 file này và để đường dẫn D:\PKI\
* Cấu hình biến môi trường JBOSS\_HOME và EJBCA\_HOME tương tự JAVA\_HOME ở trên
* Source ejbca là opensource để build lên hệ thống PKI, quá trình build sử dụng **ant**
* Jboss là web server mà ejbca sử dụng
* CA (CA Management) đã được install và được lưu trong CSDL tạo ở phần cài đặt database. Chỉ cần **deploy** là sử dụng được.
* Cấu hình JBOSS\_HOME trong ejbca config ở file: D:\PKI\ejbcace6311\ ejbca.properties 
* Quá trình deploy như sau:
  + Mở cmd chạy jboss trước:
    - $cd D:\PKI\jboss-as-7.1.1.Final\bin
    - $standalone.bat
  + deploy ejbca (vào cmd khác)
    - $cd D:\PKI\ejbca\_ce\_6\_3\_1\_1
    - $ant clean
    - $ant deploy

***Note***: Chú ý biến môi trường java, ant. Sau khi deploy source ejbca file war sẽ ở folder: ejbcace6311\dist\ejbca.war.  
Sau khi deploy ejbca, ejbca sẽ tự động kết nối tới jboss-cli để add data source. Tuy nhiên quá trình add này hay bị lỗi do đang sử dụng jboss bản free. Có thể copy trực tiếp file ejbca.war tới folder jboss-as-7.1.1.Final\standalone\deployments và chạy lại jboss  
Bản chất quá trình add data source của ejbca thực chất là việc cấu hình lại trong file trong file: jboss-as-7.1.1.Final\standalone\configuration\standalone.xml. Chúng ta có thể mở file này ra và edit trực tiếp các thông số cần thiết như: keystore, mysql.

### 4. Đăng nhập hệ thống

* Bật trình duyệt (browser) gõ <http://localhost:8080/ejbca> để vào CA.
* Để vào được trang quản trị (administration), cần import chứng nhận từ file superadmin.p12 trong folder: \ejbcace6311\p12
* Click chuột phải vào file >> Install PFX >> nhập mật khẩu (bạn tự tạo) >> next next
* Sau đó chạy jboss và vào link: <http://localhost:8080/ejbca/>
* Click  
    
  Web quản trị như sau:  
  

### Tổng kết

Trên đây là tổng quan về EJBCA và cách cài đặt nó trên windows. Tiếp theo mình sẽ viết bài về thử nghiệm 1 số pha làm việc trên hệ thống ejbca này.

### Nguồn tham khảo

<http://data.uet.vnu.edu.vn:8080/xmlui/bitstream/handle/123456789/896/HTTT_LeThiThuHuyen_ToanVanLuanVan.pdf?sequence=1>  
<http://dulieu.tailieuhoctap.vn/books/luan-van-de-tai/luan-van-de-tai-cao-hoc/file_goc_779802.pdf>