Tìm hiểu về phần mềm EJBCA

1. Giới thiệu

EJBCA là sản phẩm mã nguồn mở của hàng 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.

2. 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 phần cứng phổ biến cũng như các hệ điều hành thông dụng hiện nay 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 dữ 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 miễn phí đến trả phí: MySQL, Oracle, IBM DB2, ….

Bên cạnh đó EJBCAcòn có một số điểm đặc trưng như 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 bit
* Hỗ trợ các thuật toán DSA với độ dài khóa lên tới 1024 bit
* Hỗ trợ các hàm băm như MD5, SHA-1, SHA256
* Chứng thư được phát hành tuân thủ nghiêm ngặt X509

2. Kiến trúc

Diagram

Description automatically generated

* 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 nhất 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 ra 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 chứa thông tin người dùng.
* Tầng Web: Đây là giao diện (điển hình là giao diện người – máy bằng đồ họa) để trình khác 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 chugns là nút lá trong PKI.

3. Chức năng

* EJBCA là một tổ chức chứng nhận rất phổ biến hiện đang được sử dụng
* Tùy chọn giữa các thuật toán SHA1 hay SHA256 với RSA và với các kích thước khóa khác nhau như 1024, 2048, 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 chứng nhận có thể là tự ký (self-signed), CA bên ngoài (external CA) hay CA quản trị (admin CA).