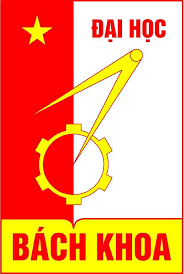
BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**---------------**

****

**Báo cáo cuối kỳ**

**MÔN NHẬP MÔN AN TOÀN THÔNG TIN**

**Đề tài: “*Hạ tầng khóa công khai PKI*”**

**GVHD:** PGS.Nguyễn Linh Giang

**Sinh viên thực hiện:**

1. Nguyễn Huy Đạt 20173006

2.Trần Văn Thắng 20173365

3. Mai Ngọc Tùng Sơn 20173350

MỤC LỤC

[Bài tập tiểu luận 1](#_Toc42359775)

[1. Các phân hệ và chức năng của hạ tầng khóa công khai 1](#_Toc42359776)

[1.1. Các thành phần của hạ tầng khóa công khai 1](#_Toc42359777)

[1.2. Vai trò và chức năng 4](#_Toc42359778)

[2. Sản phẩm mã nguồn mở 5](#_Toc42359779)

[2.1. EJBCA 5](#_Toc42359780)

[2.1.1. Đặc điểm kĩ thuật 5](#_Toc42359781)

[2.1.2. Kiến trúc 5](#_Toc42359782)

[2.1.3. Chức năng 7](#_Toc42359783)

[3. Chứng thư số 7](#_Toc42359784)

[3.1. Chứng nhận X.509 7](#_Toc42359785)

[3.2. Chu kỳ sống của chứng thư số 11](#_Toc42359786)

[3.3. Các chức năng chính 11](#_Toc42359787)

# **Các phân hệ và chức năng của hạ tầng khóa công khai**

### **Vai trò và chức năng**

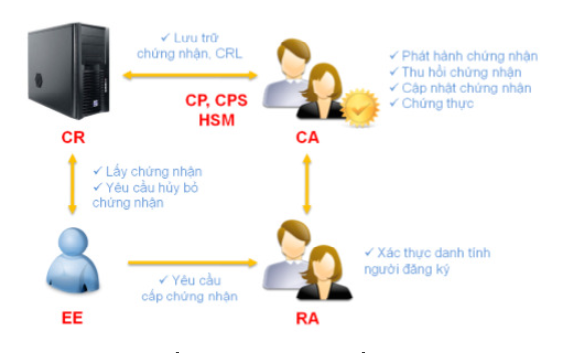
PKI cho phép những người tham gia xác thực lẫn nhau. Mục tiêu chính của PKI là cung cấp khóa công khai và xác định mối liên hệ giữa khóa và định danh người dùng. Nhờ vậy người dùng có thể sử dụng trong một số ứng dụng như:

* Mã hóa, giải mã văn bản;
* Xác thực người dùng ứng dụng;
* Mã hóa email hoặc xác thực người gửi email;
* Tạo chữ ký số trên văn bản điện tử.

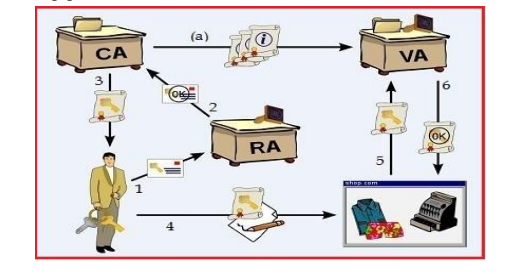
   Một PKI phải đảm bảo được các tính chất sau trong một hệ thống trao đổi thông tin:

* ***Tính bí mật (Confidentiality):*** PKI phải đảm bảo tính bí mật của dữ liệu.
* ***Tính toàn vẹn (Integrity):*** PKI phải đảm bảo dữ liệu không thể bị mất mát hoặc chỉnh sửa và các giao tác không thể bị thay đổi.
* ***Tính xác thực (Authentication):*** PKI phải đảm bảo danh tính của thực thể được xác minh.
* ***Tính không thể chối từ (Non-Repudiation):*** PKI phải đảm bảo dữ liệu không thể bị không thừa nhận hoặc giao tác bị từ chối.

### **Các thành phần của hạ tầng khóa công khai**

   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.

PKI gồm các thành phần chính sau:

* ***Thực thể cuối (End Entity – EE):***
  + Đối tượng sử dụng chứng nhận (chứng thư số): có thể là một tổ chức, một người cụ thể hay một dịch vụ trên máy chủ, …
* ***Tổ chức chứng nhận(Certificate Authority – CA):***
  + Có nhiệm vụ phát hành, quản lý và hủy bỏ các chứng thư số
  + Là thực thể quan trọng trong một PKI mà được thực thể cuối tín nhiệm
  + Gồm tập hợp các con người và các hệ thống máy tính có độ an toàn cao
* ***Chứng nhận khoá công khai (Public Key Certificate):***
  + Một chứng nhận khóa công khai thể hiện hay chứng nhận sự ràng buộc của danh tính và khóa công khai của thực thể cuối
  + Chứng nhận khóa công khai chứa đủ thông tin cho những thực thể khác có thể xác nhận hoặc kiể m tra danh tính của chủ nhận chứng nhận đó
  + Định dạng được sử dụng rộng rãi nhất của chứng nhận số dựa trên chuẩn IETF X.509.
* ***Tổ chức đăng kí chứng nhận (Registration Authority – RA):*** Mục đích chính của RA là để giảm tải công việc của CA
  + Xác thực cá nhân, chủ thể đăng ký chứng thư số.
  + 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 thư số được yêu cầu.
  + Kiểm tra xem chủ thể có thực sự sở hữu khóa riêng đang được đăng ký hay không (chứng minh sở hữu).
  + Tạo cặp khóa bí mật, công khai. (nếu chủ thể yêu cầu)
  + Phân phối bí mật được chia sẻ đến thực thể cuối (ví dụ khóa công khai của CA).
  + Thay mặt chủ thể thực thể cuối khởi tạo quá trình đăng ký với CA.
  + Lưu trữ khóa riêng.
  + Khởi sinh quá trình khôi phục khóa
  + Phân phối thẻ bài vật lý (thẻ thông minh)
* ***Kho lưu trữ chứng nhận (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 Revocatio Lists).  
      
    
* (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
* sCA (a))

# **Sản phẩm mã nguồn mở**

## **EJBCA**

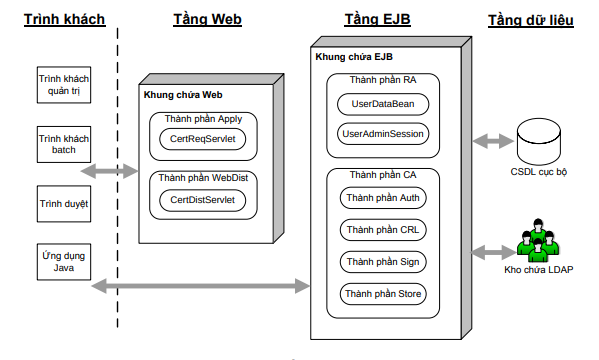
EJBCA là sản phẩm mã nguồn mở của hãng Primekey. Đây là một CA được xây dựng trên công nghệ Java J2EE, nhờ đó hiệu suất hoạt động cũng như khả năng tùy biến của CA là tương đối cao so với các hệ thống mã nguồn mở khác. Bên cạnh đó, EJBCA còn cung cấp tính năng và thành phần (OCSP, RA Service, Publisher,…)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

### **Đặc điểm kĩ 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 X50

### **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.

### **Chức năng**

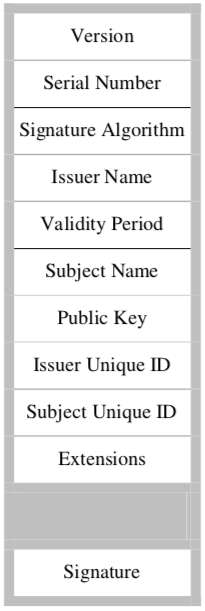
* EJBCA là một tổ chức chứng nhận rất phổ biến hiện đang được sử dụng
* Tùy chọn chọn giữa các thuật toán SHA1 hay SHA256 với RSA và với các kích thước khóa khác nhau như 1024, 2048 và 4096.
* Cung cấp một số tính năng nổi bật về lựa chọn ngôn ngữ trong quá trình cấu hình hệ thống.
* Ngoài ra cũng có 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).

# **Chứng thư số**

Để khóa công khai của mình được chứng nhận, người dùng phải tạo ra một cặp khóa bất đối xứng và gửi cặp khóa này cho tổ chức CA. Người dùng phải gửi kèm các thông tin về bản thân như tên hoặc địa chỉ. Khi tổ chức CA đã kiểm tra tính xác thực các thông tin của người dùng , CA sẽ phát hành một giấy chứng nhận khóa công khai cho người dùng . Giấy chứng nhận là một tập tin nhị phân có thể dễ dàng chuyển đổi qua mạng máy tính.  
   Tổ chức CA áp dụng chữ ký điện tử của mình cho giấy chứng nhận khóa công khai mà CA đó phát hành. Một tổ chức CA chứng nhận khóa công khai bằng cách ký nhận chúng. Nếu phía người dùng bên kia tin tưởng vào tổ chức CA thì họ có thể tin vào chữ ký của CA đó  
   Một số loại giấy chứng nhận khóa công khai có thể được phát hành như chứng nhận X.509, chứng nhận chất lượng và chứng nhận thuộc tính.  
   Ở đây mình chỉ giới thiệu về chứng nhận X.509 bởi vì nó được sử dụng nhiều

### **Chứng nhận X.509**

Chứng nhận X.509 là chứng nhận khóa công khai phổ biến nhất. Hiệp hội Viễn thông quốc tế (International Telecommunications Union – ITU) đã chỉ định chuẩn X.509 vào năm 1988. Đây là định dạng phiên bản 1 của chuẩn X.509. Vào năm 1993, phiên bản 2 của chuẩn X.509 được phát hành với 2 trường tên nhận dạng duy nhất được bổ sung. Phiên bản 3 của chuẩn X.509 được bổ sung thêm trường mở rộng đã phát hành vào năm 1997.

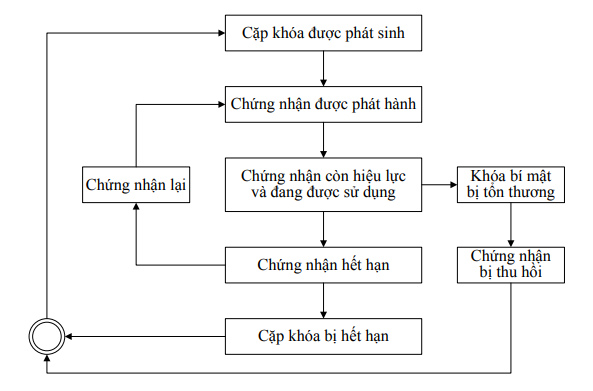
   Một chứng nhận khóa công khai kết buộc một khóa công khai với sự nhận diện của một người (hoặc một thiết bị). Khóa công khai và tên thực thể sở hữu khóa này là hai mục quan trọng trong một chứng nhận.

Phiên bản 3 của chứng nhận X.509

* **Version**: Chỉ định phiên bản của chứng nhận X.509.
* **Serial Number**: Số loạt phát hành được gán bởi CA. Mỗi CA nên gán một mã số loạt duy nhất cho mỗi giấy chứng nhận mà nó phát hành.
* **Signature Algorithm:** Thuật toán chữ ký chỉ rõ thuật toán mã hóa được CA sử dụng để ký giấy chứng nhận. Trong chứng nhận X.509 thường là sự kết hợp giữa thuật toán băm (chẳng hạn như MD5 hoặc SHA-1) và thuật toán khóa công khai (chẳng hạn như RSA).
* **Issuer Name:** Tên tổ chức CA phát hành giấy chứng nhận, đây là một tên phân biệt theo chuẩn X.500 (xem Phụ lục A). Hai CA không được sử dụng cùng một tên phát hành.
* **Validity Period**: Trường này bao gồm 2 giá trị chỉ định khoảng thời gian mà giấy chứng nhận có hiệu lực.  
  Hai phần của trường này là not-before và not-after.
  + **Not-before** chỉ định thời gian mà chứng nhận này bắt đầu có hiệu lực,
  + **Not-after** chỉ định thời gian mà chứng nhận hết hiệu lực.  
    Các giá trị thời gian này được đo theo chuẩn thời gian Quốc tế, chính xác đến từng giây.
* **Subject Name:** là một X.500 DN, xác định đối tượng sở hữu giấy chứng nhận mà cũng là sở hữu của khóa công khai. Một CA không thể phát hành 2 giấy chứng nhận có cùng một Subject Name.
* **Public key:** Xác định thuật toán của khóa công khai (như RSA) và chứa khóa công khai được định dạng tùy vào kiểu của nó.
* **Issuer Unique ID và Subject Unique ID**: Hai trường này được giới thiệu trong X.509 phiên bản 2, được dùng để xác định hai tổ chức CA hoặc hai chủ thể khi chúng có cùng DN. RFC 2459 đề nghị không nên sử dụng 2 trường này.
* **Extensions**: Chứa các thông tin bổ sung cần thiết mà người thao tác CA muốn đặt vào chứng nhận. Trường này được giới thiệu trong X.509 phiên bản 3.
* **Signature**: Đây là chữ ký điện tử được tổ chức CA áp dụng. Tổ chức CA sử dụng khóa bí mật có kiểu quy định trong trường thuật toán chữ ký. Chữ ký bao gồm tất cả các phần khác trong giấy chứng nhận. Do đó, tổ chức CA chứng nhận cho tất cả các thông tin khác trong giấy chứng nhận chứ không chỉ cho tên chủ thể và khóa công khai.  
  Những phần mở rộng của tên tập tin phổ biến cho chứng nhận X.509 bao gồm:
  + **.cer**: chứng nhận được mã hóa theo luật mã hóa tiêu chuẩn (Canonical Encoding Rules – CER).
  + **.der**: chứng nhận được mã hóa theo luật mã hóa phân biệt (Distinguished Encoding Rules – DER).
  + **.pem** (Privacy-Enhanced Electronic Mail): định dạng mã hóa được sử dụng để lưu trữ các chứng nhận và khóa. Một tập tin được định dạng với chuẩn này có thể chứa các khóa bí mật (RSA và DSA), khóa công khai (RSA và DSA) và các chứng nhận X509. Định dạng này lưu trữ dữ liệu ở định dạng DER được mã hóa cơ sở 64, nằm giữa "-----BEGIN CERTIFICATE-----" và "-----END CERTIFICATE-----", phù hợp cho việc trao đổi ở dạng văn bản giữa các hệ thống.
  + **.p7b, p7c**: PKCS #7 là một định dạng mã hóa cho việc lưu trữ một chứng nhận số và chuỗi chứng nhận của nó dưới dạng các ký tự ASCII. Định dạng này được sử dụng bởi CA để trả về các chứng nhận được phát hành cùng với chuỗi chứng nhận. Định dạng này có có thể được sử dụng như đầu vào cho yêu cầu gia hạn chứng nhận đến một CA.

**.pfx, .p12:** PKCS #12 là một định dạng mã hóa cho việc lưu trữ một chứng nhận số và kết hợp với khóa bí mật dưới dạng các ký tự ASCII. Định dạng này luôn luôn được trả về bởi CA khi CA phát sinh các khóa và phát hành chứng nhận đồng thời.

### **Chu kì sống của chứng thư số**

 Trước khi phát hành chứng thư, cặp khóa bí mật/ công khai sẽ được phát sinh. Trong khi chứng thư có hiệu lực và được sử dụng, chứng thư có thể hết hạn hoặc khóa bí mật của người sử dụng bị tổn thương (bị mất hoặc lộ khóa). Trong trường hợp chứng thư hết hạn, cặp khóa cũng sẽ không còn hiệu lực hoặc người sử dụng có thể yêu cầu gia hạn chứng thư cho họ. Trong trường hợp khóa bí mật bị tổn thương, chứng thư sẽ được thu hồi để phát hành chứng thư cho cặp khóa khác.

### **3.3. Các chức năng chính**

**a) Khởi tạo**  
   Trước khi yêu cầu một chứng thư, người dùng phải biết về CA mà mình muốn tham gia. Người dùng phải có địa chỉ của tổ chức CA và kho lưu trữ (nếu tồn tại). Người dùng cũng cần phải có giấy chứng nhận của tổ chức CA và cuối cùng cần phải có cách tạo ra cặp khóa bất đối xứng và lựa chọn các thuộc tính cho tên phân biệt (DN).  
      **b) Yêu cầu chứng thư**  
   Hầu hết các CA sử dụng một trong hai phương thức tiêu chuẩn của yêu cầu chứng nhận: PKCS #10 và CRMF

* ***PKCS #10***: Định dạng của thông điệp được gửi đến CA để yêu cầu chứng nhận khóa công khai
* ***CRMF***: Định dạng của thông điệp được gửi đến CA để yêu cầu bất cứ trường nào của chứng nhận X.509  
        **c) Tạo lại chứng thư**  
  Vì nhiều lý do như giấy chứng nhận hết hạn, thêm thông tin mới vào chứng nhận, xác nhận lại khóa công khai hiện có, hoặc xác nhận khóa mới mà người dùng có thể muốn tạo mới lại chứng nhận của mình. Khi tổ chức CA đáp ứng yêu cầu tạo mới lại này, nó sẽ phát hành cho đối tác một chứng thư mới và có thể xuất bản chứng thư mới này vào kho lưu trữ.  
        **d) Hủy bỏ chứng thư**  
  Lý do để hủy một chứng thư là do sự nhận diện được xác nhận bởi CA đã thay đổi.  
  Danh sách hủy bỏ chứng nhận (Certificate Revocation List – CRL) chứa thông tin thời gian nhằm xác định thời điểm tổ chức CA phát hành nó. CA ký CRL với cùng khóa bí mật được dùng để ký các chứng thư. Các CRL thường được chứa trong cùng kho với các chứng thư nhằm dễ dàng cho việc rút trích.  
  Các CA phát hành các CRL theo định kì, thường là hàng giờ hoặc hàng ngày.  
        **e) Lưu trữ và phục hồi khóa**  
  Lưu trữ khóa là một dịch vụ được cung cấp bởi nhiều tổ chức CA. Dùng để tránh trường hợp không giải mã được dữ liệu khi bị mất khóa. Để lưu trữ khóa, người dùng phải gửi khóa bí mật tới nơi lưu trữ. Bởi vì các yêu cầu lưu trữ hay khôi phục khóa đều phải được xác minh nên người sử dụng không thể thao tác trực tiếp đến nơi lưu trữ mà phải thông qua CA phát hành chứng nhận đó.