BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC CẦN THƠ**

**KHOA CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG**

**BỘ MÔN MẠNG MÁY TÍNH & TRUYỀN THÔNG**

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

**LUẬN VĂN TỐT NGHIỆP ĐẠI HỌC**

**NGÀNH TRUYỀN THÔNG & MẠNG MÁY TÍNH**

Đề tài

**TÌM HIỂU HỆ THỐNG MÃ HÓA KHÓA CÔNG KHAI VÀ ỨNG DỤNG TRONG**

**HỆ THỐNG QUẢN LÝ ĐIỂM**

**CỦA TRƯỜNG ĐHCT**

**Người hướng dẫn Sinh viên thực hiện**

**TS. Trần Công Án Diệp Thùy Dương**

**MSSV: B1208711**

**Khóa: K38**

Cần Thơ, tháng 11 năm 2016.

## LỜI CẢM ƠN

Em xin gửi lời cảm ơn chân thành nhất tới thầy hướng dẫn, TS. Trần Công Án, người thầy đã cho em những định hướng và những ý kiến rất quý báu để em hoàn thành được luận văn tốt nghiệp này.

Em xin tỏ lòng biết ơn sâu sắc tới quý thầy cô, bạn bè, đặc biệt là Bộ môn Truyền thông và Mạng máy tính, khoa Công nghệ Thông tin, trường Đại Học Cần Thơ đã dìu dắt, giúp đỡ em tiến bộ trong suốt quá trình học tập tại Trường.

Xin cảm ơn Gia đình, những người luôn động viên và giúp đỡ em trong mọi hoàn cảnh khó khăn.

Trân trọng cảm ơn!

Cần Thơ, ngày 24 tháng 11 năm 2016

Diệp Thùy Dương

## MỤC LỤC

[LỜI CẢM ƠN 1](#_Toc468418265)

[MỤC LỤC 2](#_Toc468418266)

[DANH MỤC BẢNG BIỂU 7](#_Toc468418267)

[TÓM TẮT LUẬN VĂN 8](#_Toc468418268)

[PHẦN GIỚI THIỆU 10](#_Toc468418269)

[Lý do chọn đề tài 10](#_Toc468418270)

[Mục tiêu, đối tượng và phạm vi nghiên cứu 10](#_Toc468418271)

[Nội dung và phương pháp nghiên cứu 11](#_Toc468418272)

[PHẦN NỘI DUNG 12](#_Toc468418273)

[CHƯƠNG 1. TỔNG QUAN 12](#_Toc468418274)

[1.1 Tổng quan về mật mã 12](#_Toc468418275)

[1.2 Cơ chế mã hóa 12](#_Toc468418276)

[1.2.1 Mật mã khóa bí mật 12](#_Toc468418277)

[1.2.2 Mật mã khóa công khai 14](#_Toc468418278)

[1.2.3 Đánh giá 15](#_Toc468418279)

[1.3 Các giải thuật cơ bản trong mã hóa bất đối xứng 15](#_Toc468418280)

[1.3.1 Giải thuật băm (hasing) 15](#_Toc468418281)

[1.3.2 Thuật toán khóa công khai 18](#_Toc468418282)

[1.4 Tổ chức chứng nhận khóa công khai 20](#_Toc468418283)

[CHƯƠNG 2. CHỮ KÝ SỐ 21](#_Toc468418284)

[2.1 Giới thiệu về chữ ký số 21](#_Toc468418285)

[2.2 Phân loại chữ ký số theo đặc trưng kiểm tra chữ ký 22](#_Toc468418286)

[2.3 Các sơ đồ chữ ký số có chức năng bổ sung 22](#_Toc468418287)

[2.3.1 Sơ đồ đa chữ ký 23](#_Toc468418288)

[2.3.2 Sơ đồ chữ ký nhóm 23](#_Toc468418289)

[2.3.3 Sơ đồ chữ ký ngưỡng 23](#_Toc468418290)

[2.3.4 Sơ đồ chữ ký không chối bỏ 24](#_Toc468418291)

[2.3.5 Sơ đồ chữ ký mù 24](#_Toc468418292)

[2.3.6 Sơ đồ chữ ký ủy quyền 24](#_Toc468418293)

[2.3.7 Sơ đồ chữ ký trực tiếp 24](#_Toc468418294)

[2.3.8 Sơ đồ chữ ký sai – dừng 24](#_Toc468418295)

[2.3.9 Sơ đồ chữ ký một lần 25](#_Toc468418296)

[2.3.10 Sơ đồ chữ ký trực tuyến/ ngoại tuyến 25](#_Toc468418297)

[2.4 Ứng dụng 25](#_Toc468418298)

[CHƯƠNG 3. CHỨNG CHỈ SỐ 27](#_Toc468418299)

[3.1 Giới thiệu về chứng chỉ số 27](#_Toc468418300)

[3.2 Các loại chứng chỉ số 28](#_Toc468418301)

[3.2.1 Chứng chỉ khóa công khai 28](#_Toc468418302)

[3.2.2 Chứng chỉ thuộc tính 28](#_Toc468418303)

[3.2.3 Chứng chỉ khác 29](#_Toc468418304)

[3.3 Chứng chỉ khóa công khai 29](#_Toc468418305)

[3.3.1 Chứng chỉ X.509 29](#_Toc468418306)

[3.3.2 Chứng chỉ PGP 33](#_Toc468418307)

[3.4 Chu kỳ sống của chứng nhận số 35](#_Toc468418308)

[3.5 Phát hành chứng chỉ 35](#_Toc468418309)

[3.6 Xác minh chứng chỉ 36](#_Toc468418310)

[3.7 Thu hồi chứng chỉ 36](#_Toc468418311)

[3.8 Công bố và gửi thông báo thu hồi chứng chỉ 37](#_Toc468418312)

[3.8.1 Certificate Revocation Lists (CRLs) 37](#_Toc468418313)

[3.8.2 Authority Revocation Lists (ARLs) 38](#_Toc468418314)

[3.8.3 Cơ chế truy vấn On-line (On-line Query Mechanisms) 39](#_Toc468418315)

[CHƯƠNG 4. HẠ TẦNG KHÓA CÔNG KHAI (PKI) 40](#_Toc468418316)

[4.1 Tổng quan về hạ tầng khóa công khai 40](#_Toc468418317)

[4.1.1 Khái niệm về PKI 40](#_Toc468418318)

[4.1.2 Các thành phần và chức năng của PKI 40](#_Toc468418319)

[4.1.3 Mục tiêu 42](#_Toc468418320)

[4.1.4 Thực thể cuối EE 43](#_Toc468418321)

[4.1.5 Cơ quan chứng thực CA 43](#_Toc468418322)

[4.1.6 Cơ quan đăng ký RA 44](#_Toc468418323)

[4.1.7 Hệ thống lưu trữ dữ liệu chứng chỉ 44](#_Toc468418324)

[4.2 Các mô hình tin cậy PKI 45](#_Toc468418325)

[4.2.1 Mô hình phân cấp các CA 45](#_Toc468418326)

[4.2.2 Mô hình tin cậy kiến trúc phân tán 46](#_Toc468418327)

[4.2.3 Mô hình Web 46](#_Toc468418328)

[4.2.4 Mô hình tin cậy tâm điểm người dùng 47](#_Toc468418329)

[4.3 Kiến trúc PKI 48](#_Toc468418330)

[4.3.1 Kiến trúc CA đơn 49](#_Toc468418331)

[4.3.2 Kiến trúc phân cấp 50](#_Toc468418332)

[4.3.3 Kiến trúc mắt lưới 51](#_Toc468418333)

[4.3.4 Kiến trúc PKI doanh nghiệp chứng thực chéo (kiến trúc lai) 53](#_Toc468418334)

[4.3.5 Kiến trúc CA cầu nối 54](#_Toc468418335)

[4.3.6 Kiến trúc danh sách tin cậy mở rộng 54](#_Toc468418336)

[4.4 Ứng dụng của PKI 55](#_Toc468418337)

[CHƯƠNG 5. ỨNG DỤNG MÃ HÓA KHÓA CÔNG KHAI VÀO HỆ THỐNG QUẢN LÝ ĐIỂM CỦA CTU 56](#_Toc468418338)

[5.1 Giới thiệu hệ thống quản lý điểm của CTU 56](#_Toc468418339)

[5.2 Yêu cầu hệ thống 56](#_Toc468418340)

[5.3 Thiết kế hệ thống 58](#_Toc468418341)

[5.3.1 Xác định chức năng 58](#_Toc468418342)

[5.3.2 Thiết kế cơ sở dữ liệu 60](#_Toc468418343)

[5.4 Kết quả 65](#_Toc468418344)

[PHẦN KẾT LUẬN 71](#_Toc468418345)

[Kết quả đạt được 71](#_Toc468418346)

[Hướng phát triển của đề tài 71](#_Toc468418347)

[TÀI LIỆU THAM KHẢO 72](#_Toc468418348)

DANH MỤC HÌNH ẢNH

[Hình 1.1 Mật mã khóa bí mật 13](#_Toc468418386)

[Hình 1.2 Mật mã khóa công khai 15](#_Toc468418387)

[Hình 1.3 Giải thuật băm MD5 16](#_Toc468418388)

[Hình 1.4 Giải thuật băm SHA-1 17](#_Toc468418389)

[Hình 1.5 Giải thuật băm HMAC 18](#_Toc468418390)

[Hình 1.6 Giải thuật RSA 19](#_Toc468418391)

[Hình 2.1 Sơ đồ mình họa chữ ký số 22](#_Toc468418392)

[Hình 2.2 Các sơ đồ chữ ký số có chức năng bổ sung 23](#_Toc468418393)

[Hình 3.1 Khuôn dạng chứng chỉ số 28](#_Toc468418394)

[Hình 3.2 Mô hình của chứng chỉ số theo X.509 version 3 30](#_Toc468418395)

[Hình 3.3 Chu kỳ sống của chứng nhận 35](#_Toc468418396)

[Hình 3.4 Tiến trình phát hành một chứng chỉ số 36](#_Toc468418397)

[Hình 3.5 Khuôn dạng danh sách chứng chỉ bị thu hồi 38](#_Toc468418398)

[Hình 4.1 Cấu trúc của một PKI 41](#_Toc468418399)

[Hình 4.2 Mô hình tin cậy phân cấp 46](#_Toc468418400)

[Hình 4.3 Mô hình tin cậy phân tán 46](#_Toc468418401)

[Hình 4.4 Mô hình Web 47](#_Toc468418402)

[Hình 4.5 Mô hình tin cậy tâm điểm người dùng 48](#_Toc468418403)

[Hình 4.6 Kiến trúc PKI với một CA đơn 49](#_Toc468418404)

[Hình 4.7 Kiến trúc danh sách tin cậy cơ bản 50](#_Toc468418405)

[Hình 4.8 Kiến trúc PKI phân cấp 51](#_Toc468418406)

[Hình 4.9 Kiến trúc PKI mắt lưới 52](#_Toc468418407)

[Hình 4.10 Kiến trúc PKI doanh nghiệp chứng thực chéo 53](#_Toc468418408)

[Hình 4.11 Kiến trúc PKI CA cầu nối 54](#_Toc468418409)

[Hình 5.1 Mô hình phân cấp chức năng của hệ thống quản lý điểm 57](#_Toc468418410)

[Hình 5.2 Sơ đồ usecase (giảng viên) 58](#_Toc468418411)

[Hình 5.3 Sơ đồ usecase (người quản lý) 59](#_Toc468418412)

[Hình 5.4 Mô hình khái niệm 61](#_Toc468418413)

[Hình 5.5 Mô hình thực thể kết hợp 62](#_Toc468418414)

[Hình 5.6 Giao diện đăng nhập 65](#_Toc468418415)

[Hình 5.7 Giao diện trang chủ 66](#_Toc468418416)

[Hình 5.8 Giao diện nhập và chỉnh sửa điểm 66](#_Toc468418417)

[Hình 5.9 Giao diện sau khi đã khóa điểm 67](#_Toc468418418)

[Hình 5.10 Giao diện tạo khóa 67](#_Toc468418419)

[Hình 5.11 Giao diện khóa điểm 68](#_Toc468418420)

[Hình 5.12 Giao diện trang chủ của admin 69](#_Toc468418421)

[Hình 5.13 Giao diện xem điểm 70](#_Toc468418422)

## DANH MỤC BẢNG BIỂU

[***Bảng 4.1*** Tóm tắt các kiến trúc của PKI 55](#_Toc468418423)

[***Bảng 5.1*** Bảng giangvien (giảng viên và admin) 63](#_Toc468418424)

[***Bảng 5.2*** Bảng hocphan (học phần) 63](#_Toc468418425)

[***Bảng 5.3*** Bảng lophocphan (lớp học phần) 63](#_Toc468418426)

[***Bảng 5.4*** Bảng quyenhocphan (quyền học phần) 64](#_Toc468418427)

[***Bảng 5.5*** Bảng lop (lớp) 64](#_Toc468418428)

[***Bảng 5.6*** Bảng sinhvien (sinh viên) 64](#_Toc468418429)

## TÓM TẮT LUẬN VĂN

Luận văn này nhằm tìm hiểu hệ thống mã hóa khóa công khai và ứng dụng trong đảm bảo tính toàn vẹn dữ liệu của hệ thống quản lý điểm của Trường ĐCHT (CTU). Hạ tầng khóa công khai là một bộ khung cơ bản để xây dựng mô hình an ninh, bảo mật trong thương mại điện tử. Đặc biệt là vai trò của chứng thực số trong hạ tầng khóa công khai và trong các giao dịch trực tuyến. Người sử dụng, ngoài hình thức bảo mật thông thường như mật khẩu, cũng phải dùng một chứng thực số cá nhân để xác nhận các hoạt động giao dịch của mình với dịch vụ ngân hàng, thương mại điện tử, giao dịch chứng khoán... Chứng thực số sẽ giúp nhà quản lý đảm bảo rằng khách hàng không thể chối cãi các giao dịch của mình, khi họ đã dùng chứng thực số. Từ đó đặt ra các vấn đề quản lý (cấp phát, xác thực) thu hồi và cấp phát lại chứng thực số. Nhằm minh họa cho ứng dụng của hệ thống khóa công khai, chúng tôi sẽ xây dựng một hệ thống mô phỏng hệ thống quản lý điểm của Trường Đại học Cần Thơ và ứng dụng hệ thống mã hóa khóa công khai để đảm bảo tính toàn vẹn của dữ liệu. Dựa trên các tính chất của hệ thống mã hóa này, chúng tôi đề xuất một mô hình cho phép phát hiện các thay đổi điểm số sau khi cán bộ giảng dạy đã khóa điểm nhằm tăng tính bảo mật cho hệ thống.

**ABSTRACT**

This thesis is to study the public key encryption system and apply this encryption system to ensure the integrity of data in the learning managament system of Cantho University. Public key infrastructure is a basic framework to build a model of security and privacy in electronic commerce. Especially the role of digital certificates for public key infrastructure and online transactions. The users, in addition to conventional forms of security such as a password, and to use a personal digital certificates to authenticate their transactions with banking, e-commerce, stock exchanges,... certification will help managers ensure that customers can not be denied their transactions when they use digital certificates. To demonstration the application of the public key infrastructure, we built a simulated learning management system of Cantho University and apply the public key infrastructure to ensure the integrity of the data. Based on the properties of this encryption system, we propose a model that allow to detect any modifications on the data (student grades) after the lectures finish their grading to increase the security of the system.

# PHẦN GIỚI THIỆU

## Lý do chọn đề tài

Ngày nay, với sự phát triển của hạ tầng truyền thông công nghệ thông tin, việc giao tiếp qua mạng Internet đang trở thành một nhu cầu cần thiết. Hầu hết mọi hoạt động như giao tiếp, giải trí, kinh doanh,… đều chuyển từ cách thức truyền thống sang môi trường điện tử. Môi trường làm việc này mang đến nhiều cơ hội nhưng cũng nảy sinh rất nhiều vấn đề về an toàn thông tin nghiêm trọng. Hầu hết các thông tin kinh quan trọng đều được lưu trữ và trao đổi dưới hình thức điện tử như mã số tài khoản, thông tin mật, … Nhưng với các thủ đoạn tinh vi, nguy cơ những thông tin này bị đánh cắp qua mạng thật sự là vấn đề đáng quan tâm.

Giao thức TCP/IP được sử dụng chủ yếu trong truyền thông tin trên mạng Internet. Giao thức này cho phép thông tin được gửi từ máy tính này đến máy tính khác thông qua một loạt các máy trung gian hoặc các mạng riêng biệt nên đã tạo cơ hội cho những kẻ trộm có thể thực hiện các hành vi phi pháp như nghe trộm, giả mạo, mạo danh,… Biện pháp bảo mật hiện nay như dùng mật khẩu đều không đảm bảo vì có thể bị nghe trộm hoặc bị dò ra nhanh chóng do người sử dụng thường chọn mật khẩu ngắn, dễ nhớ, dùng chung và ít khi thay đổi mật khẩu. Mặt khác, do các thông tin điện tử này không được xác thực trong quá trình trao đổi nên khi bị sao chép hay sửa đổi sẽ không thể phát hiện được.

Chữ ký số ra đời đã giải quyết được vấn đề đó. Chữ ký số dựa trên kỹ thuật mã hóa bất đối xứng, trong đó mỗi người có một cặp khóa, một khóa bí mật và một khóa công khai. Khóa công khai được công bố rộng rãi còn khóa bí mật được giữ kín và không thể tìm được khóa bí mật nếu chỉ biết khóa công khai. Để trao đổi thông tin bí mật, người gửi sử dụng khóa công khai của người nhận để mã hóa thông điệp cần gửi, sau đó người nhận sẽ sử dụng khóa bí mật tương ứng của mình giải mã thông điệp nhận được. Để đảm bảo tính toàn vẹn, chống bị giả mạo hoặc thay đổi nội dung trong quá trình gửi, người gửi sử dụng khóa bí mật của mình để “ký” vào thông điệp cần gửi, sau đó người nhận sẽ sử dụng khóa công khai của người gửi để xác nhận chữ ký trên thông điệp nhận được.

Nhận thấy tính thiết thực của vấn đề này và được sự gợi ý của giáo viên hướng dẫn, em đã chọn đề tài “Tìm hiểu hệ thống mã hóa khóa công khai và ứng dụng trong hệ thống quản lý điểm của Trường ĐCHT” làm đề tài cho luận văn của mình.

## Mục tiêu, đối tượng và phạm vi nghiên cứu

Mục tiêu luận văn: tìm hiểu hệ thống khóa công khai và ứng dụng của nó.

Đối tượng nghiên cứu chính của luận văn: hệ thống mã hóa khóa công khai và các hệ thống thông tin ứng dụng hệ thống mã hóa khóa công khai.

Phạm vi nghiên cứu: ứng dụng hệ thống mã hóa khóa công khai để đảm bảo tính toàn vẹn dữ liệu của hệ thống quản lý điểm tại Trường Đại học Cần Thơ.

## Nội dung và phương pháp nghiên cứu

Tìm hiểu hạ tầng khóa công khai PKI và các ứng dụng của hệ thống mã hóa khóa công khai. Từ đó, đề xuất một mô hình để ứng dụng vào việc đảm bảo tính toàn vẹn của dữ liệu trong hệ thống quản lý điểm của sinh viên.

# PHẦN NỘI DUNG

# TỔNG QUAN

## Tổng quan về mật mã

Mật mã (cryptography) dùng đảm bảo an toàn và bảo mật thông tin. Nó là sự kết hợp của hai quá trình mã hóa thông tin (encryption) và giải mã thông tin (decryption).

Mật mã gắn liền với quá trình mã hóa. Nó dùng để đảm bảo tính bí mật của các thông tin quan trọng thường được điều khiển bởi “khóa” – là một chuỗi các bit số dùng để làm tham số cho thuật toán mã hóa. Điều này có nghĩa nó sẽ biến đổi dữ liệu gốc từ dạng thông thường có thể nhận thức thành dạng không thể nhận thức, tức là làm cho thông tin trở thành dạng không thể đọc được và sau đó khôi phục lại để sử dụng trong một số mục đích cụ thể.

## Cơ chế mã hóa

Người ta dùng kỹ thuật mã hoá cho các giao dịch thương mại điện tử để đảm bảo an toàn bảo mật thông tin. Mã hoá là quá trình trộn văn bản với khoá mã tạo thành văn bản không thể đọc, được truyền trên mạng. Khi nhận được bản mã, phải dùng khoá mã để giải thành bản rõ. Mã hoá và giải mã gồm năm thành phần cơ bản:

- P (Plaintext): Văn bản rõ – các thông tin rõ nghĩa ban đầu.

- C (Ciphertext): Văn bản đã mã.

- K (Key): Khoá.

- E (Encryption algorithm): Thuật toán mã hoá.

- D: Thuật toán giải mã.

Có hai cơ chế mã hóa cơ bản: mật mã khóa bí mật (mã hóa đối xứng) và mật mã khóa công khai (mã hóa bất đối xứng).

### Mật mã khóa bí mật

Mật mã khóa bí mật (Secret Key Cryptography - SKC) là phương pháp mã hóa. Trong đó, các khóa dùng cho việc sinh mã và giải mã hoàn toàn giống nhau và bí mật đối với tất cả những người không liên quan nhằm giữ gìn sự bí mật trong kênh truyền thông tin; nói cách khác, hai bên gửi và nhận tin chia sẻ chung một khóa bí mật duy nhất. Vai trò của hai phía tham gia là giống nhau và có thể đổi vai trò, gửi và nhận tin cho nhau, nên hệ thống này còn được gọi là “mật mã hóa đối xứng (Symmetric Cryptography)”. Có thể chia ra làm hai loại:

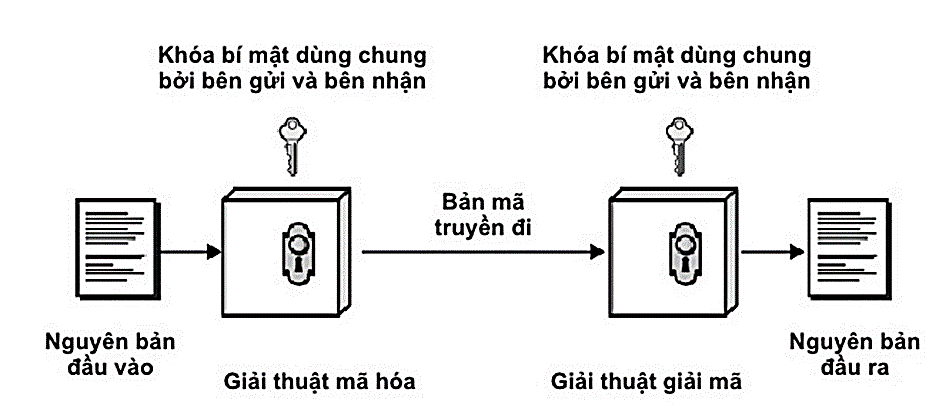
Mật mã luồng (stream ciphers): mã hóa từng bit của thông điệp.

Mật mã khối (block ciphers): gộp một số bit lại và mật mã hóa chúng như một đơn vị.

Hạn chế:

* Hệ thống mật mã khóa bí mật có những nhược điểm lớn trên phương diện xác lập và phân phối khóa. Trong hệ thống này, các khóa ở hai bên tham gia phải được giữ bí mật và phân phối trước cho các đối tác liên lạc với nhau thông qua kênh truyền an toàn. Vấn đề đặt ra là làm thế nào để hai bên không quen biết, chưa được phân phối khóa lại có thể tin cậy và liên lạc mật với nhau nếu không có một kênh bí mật từ trước.
* Một khía cạnh yếu điểm khác là phương diện quản lý và lưu trữ. Nó hầu như không đáp ứng được các yêu cầu đặt ra trong môi trường Internet đang phát triển như hiện nay, do có rất nhiều người thuộc nhiều tổ chức khác nhau và ở các quốc gia khác nhau cùng tham gia vào việc truyền nhận thông tin. Với hệ thống khóa bí mật này thì số lượng khóa mà mỗi công ty hay mỗi cá nhân cần được cung cấp là vô cùng lớn (cụ thể là (n(n-1))/2 khóa); việc phân phối, lưu trữ cũng như quản lý gặp rất nhiều khó khăn dẫn đến việc kiểm soát an toàn thông tin các khóa riêng biệt này không thật sự được bảo mật tuyệt đối.

Đây là thách thức lớn đối với hệ thống mật mã khóa bí mật.



* + - * 1. Mật mã khóa bí mật

(Nguồn: https://m2teknikinformatika2010.wordpress.com/2013/04/28/cryptography-and-network-security-principles-and-practices/)

### Mật mã khóa công khai

Mật mã khóa công khai (Public Key Cryptography – PKC) là một dạng mã hóa cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa bí mật. Điều này được thực hiện bằng cách sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai (public key) và khóa bí mật (private key).

Nếu dùng khóa công khai để mã hóa thì sẽ dùng khóa bí mật sẽ dùng để giải mã và ngược lại. Điều quan trọng đối với hệ thống là không thể tìm ra khóa bí mật nếu chỉ biết khóa công khai, do vậy không cần giữ bí mật khóa công khai mà chỉ cần chắc chắn là bên gửi thông tin đã sử dụng đúng khóa công khai của bên nhận. Khóa công khai cần được xác thực theo một phương thức nào đó, thông thường là qua các chứng chỉ số do một cơ quan chứng thực cấp.

Mật mã khóa công khai được ứng dụng nhiều trong môi trường mạng, đặc biệt là trong các giao dịch điện tử vì nó đưa ra giải pháp nhằm giải quyết được những hạn chế của mật mã khóa bí mật.

An toàn của các thuật toán này đều dựa trên các ước lượng về khối lượng tính toán để giải các bài toán gắn với chúng. Tuy nhiên, phương pháp này cho phép trao đổi khóa một cách dễ dàng và tiện lợi.

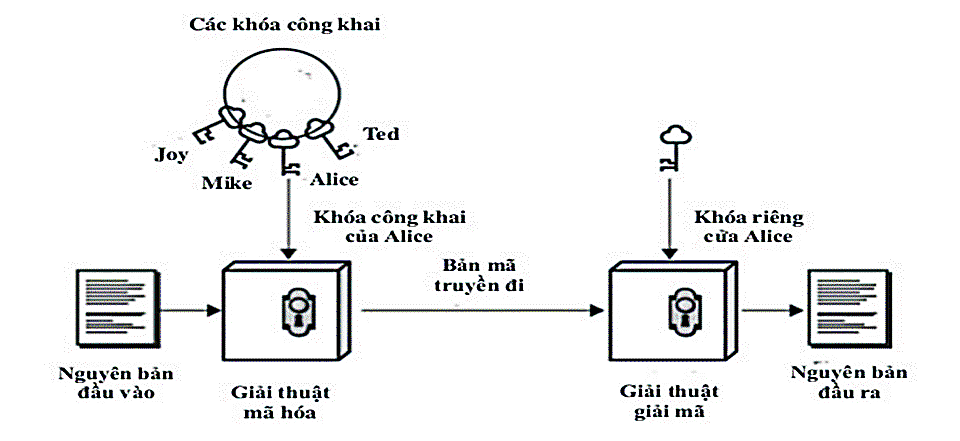
Hạn chế:

- Tốc độ mã hóa khá chậm nên chỉ được sử dụng cho mẫu dữ liệu nhỏ.

- Chưa có thuật toán mã hóa khóa bất đối xứng nào được chứng minh là an toàn trước các tấn công dựa trên bản chất toán học của thuật toán. Nó vẫn tồn tại khả năng bị tấn công và tìm ra khóa bí mật, mặc dù độ an toàn tương đối được đảm bảo.

- Một số dạng tấn công đã đơn giản hóa việc tìm khóa giải mã dựa trên việc đo đạc chính xác thời gian mà một hệ thống phần cứng thực hiện mã hóa.

- Một điểm yếu tiềm tàng trong việc sử dụng khóa bất đối xứng là khả năng bị tấn công dạng kẻ tấn công đứng giữa. Kẻ tấn công lợi dụng việc phân phối khóa công khai để thay đổi khóa công khai. Sau khi đã giả mạo được khóa công khai, kẻ tấn công đứng ở giữa 2 bên để nhận các gói tin, giải mã rồi lại mã hóa với khóa đúng và gửi đến nơi nhận để tránh bị phát hiện. Dạng tấn công kiểu này có thể phòng ngừa bằng các phương pháp trao đổi khóa an toàn nhằm đảm bảo nhận thực người gửi và toàn vẹn thông tin.



* + - * 1. Mật mã khóa công khai

(Nguồn: http://www.slideshare.net/ayyakathir/cryptography-and-network-security-52030389)

### Đánh giá

Mật mã khóa bí mật thường không được sử dụng độc lập trong thiết kế của các hệ thống hiện đại. Cả hai loại mật mã sẽ được phối hợp để tận dụng tối đa các ưu điểm của nhau.

Ví dụ: SSL (Secure Sockets Layer), PGP (Pretty Good Privacy) và GPG (GNU Privacy Guard)...

## Các giải thuật cơ bản trong mã hóa bất đối xứng

Mật mã sử dụng các giải thuật cơ bản: giải thuật băm, mã hóa đối xứng và mã hóa bất đối xứng.

Mã hóa là một hình thức của mật mã nhằm tạo ra sự bảo mật cho dữ liệu khi lưu trữ hay truyền đi trên mạng. Mã hóa sử dụng những giải thuật để biến đổi dữ liệu gốc (plaintext) sang dạng dữ liệu không thể hiểu được (ciphertext). Nó dùng khóa (key) để mã hóa và giải mã. Khóa càng dài thì độ bảo mật càng cao.

### Giải thuật băm (hasing)

Thuật toán băm biến đổi dữ liệu đầu vào thành dữ liệu đầu ra tương đối nhỏ về kích thước mà không sử dụng một khóa nào cả. Nó sinh ra giá trị băm tương ứng với mỗi khối dữ liệu. Giá trị băm đóng vai trò như một khóa, tuy nhiên vẫn xảy ra trường hợp đụng độ và người ta đang cố gắng cải thiện giải thuật để giảm thiểu sự đụng độ đó.

Băm dùng để tạo ra “dấu vân tay” (MAC – message authentication code hay message digest) của dữ liệu. Giá trị này được gửi kèm với dữ liệu để nơi nhận để kiểm tra tính toàn vẹn của dữ liệu.

Băm (hasing) công dụng không phải là mã hóa (encryption).

Các giải thuật băm:

- Message-Digest Algorithm 5 (MD5).

- Secure Hash Algorithm 1 (SHA-1).

#### Giải thuật băm MD5

Được phát minh bởi Ronald Rivest của RSA Security. Và được mô tả trong RFC-1321.

MD5 thường dùng để checksum của những phần mềm cho phép download từ Internet nhằm đảm bảo nó không phải là phần mềm giả tạo.

Đầu ra của MD5 luôn là một digest có giá trị 128 bits (được chia làm bốn từ 32 bits, với ký hiệu là A, B, C, D) hay 32 ký tự trong Hex (hệ thập lục phân). Mẩu tin đầu vào được chia thành từng đoạn 512 bit, mẩu tin sau đó được “độn” sao cho chiều dài của nó chia chẵn cho 512. Chúng được khởi tạo với những hằng số cố định. Giải thuật chính sau đó sẽ xử lý các khối tin 512 bits, mỗi khối xác định một trạng thái.



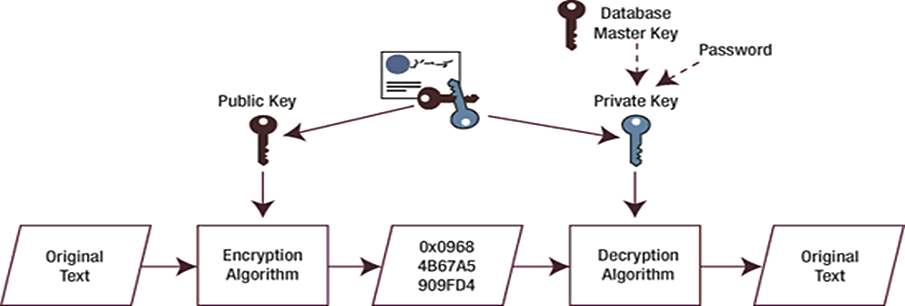
* + - * 1. Giải thuật băm MD5

#### Giải thuật băm SHA-1

Được tạo ra bởi chính phủ Mỹ (NIST và NSA). Mô tả trong RFC-3174. Giải thuật băm SHA-1 ra đời nhằm khắc phục điểm yếu trong MD5.

SHA-1 thông thường được sử dụng trong việc cài đặt IPSec, S/MINE.

Đầu ra của SHA-1 luôn là một digest có giá trị 160 bits (bảo mật hơn MD5). Ngay cả một thay đổi nhỏ trong đoạn dữ liệu gốc sẽ có khả năng rất lớn tạo nên một giá trị băm hoàn toàn khác.



* + - * 1. Giải thuật băm SHA-1

(Nguồn: https://en.wikipedia.org/wiki/Public-key\_cryptography)

#### Giải thuật băm HMAC

Các giải thuật có yếu điểm khi gặp dạng tấn công “kẻ đứng giữa”. Nó giả mạo dữ liệu và cả digest gửi kèm. Nên HMACs đưa vào thêm một khóa bí mật trước khi dùng giải thuật băm: Data + Key => Digest

Cơ chế dùng thêm khóa bí mật gọi là “Message Authentication Codes”.

Khóa bí mật chỉ được biết giữa hai người gửi và người nhận.

Dùng HMAC với hai giải thuật băm chính:

- HMAC + MD5 = HMAC-MD5 sử dụng khóa 128 bits.

- HMAC + SHA-1 = HMAC-SHA-1 sử dụng khóa 160 bits.

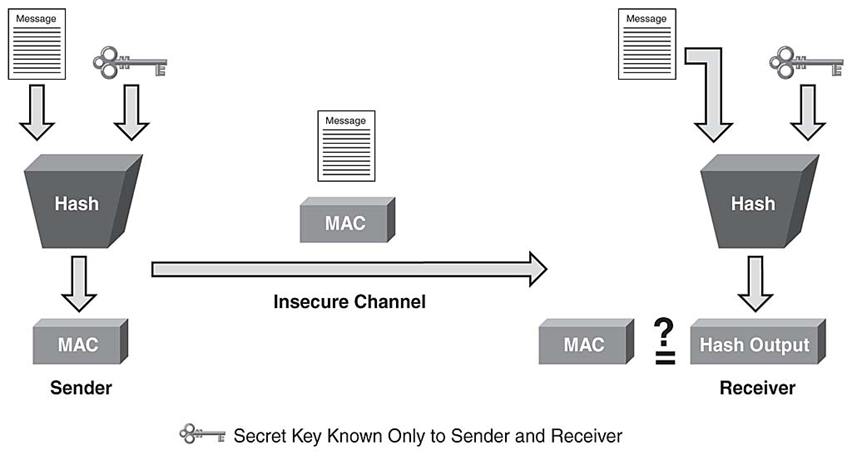
Sức mạnh mã hóa của HMAC phụ thuộc vào:

- Sức mạnh mật mã của hàm băm.

- Kích thước đầu ra băm của nó.

- Kích thước và chất lượng của khoá.

HMAC-MD5 và HMAC-SHA-1 thường được sử dụng trong các giao thức IPSec và TLS.



* + - * 1. Giải thuật băm HMAC

(Nguồn: http://www.networkworld.com/article/2268575/lan-wan/chapter-2--ssl-vpn-technology.html)

### Thuật toán khóa công khai

Các thuật toán thường được dùng là RSA, DSA, DH với độ dài khóa là 512, 1024 và 2048. Khóa có độ dài 1024 trong thuật toán này có mức độ phức tạp tương đương với chuẩn 3DES của thuật toán mã hóa bí mật.

Hạn chế:

- Giải thuật thực thi chậm.

- Yêu cầu tài nguyên của bộ vi xử lý lớn hơn thuật toán mã hóa bí mật (như DES).

- Không hiệu quả đối với dữ liệu có dung lượng lớn.

Một số giải thuật mã hóa bất đối xứng:

- RSA (Rivest Shamir Adleman).

- DSA (Digital Signature Algorithm).

- DH (Diffie – Hellman).

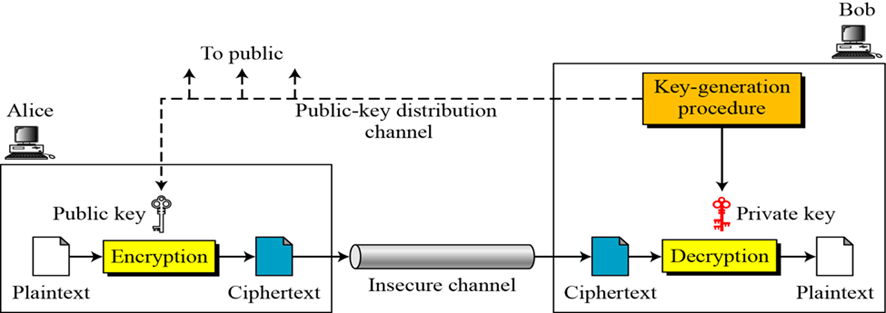
- ECC (Error Correcting Code).

- EI Gamal.

#### Giải thuật mã hóa RSA

RSA được Ron Rivest, Adi Shamir và Len Adleman phát minh vào năm 1977 tại MIT (Học viện Công nghệ Massachusetts). Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công khai. RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.

Mã hóa dữ liệu: dùng khóa chung (public key) để mã hóa, khóa riêng (private key) để giải mã. Khóa có độ dài từ 1024 – 2048 bits. Giải thuật rất phức tạp sử dụng nhiều công thức toán học và gần như không có phương pháp nào tìm ngược lại khóa riêng từ dữ liệu được mã hóa và khóa chung.



* + - * 1. Giải thuật RSA

(Nguồn: http://slideplayer.com/slide/6035944/)

Tạo chữ ký số: khóa riêng để giải mã, khóa chung để mã hóa.

Được sử dụng trong IPSec, tốc độ thực thi chậm hơn DES và các giải thuật mã hóa đối xứng khác.

#### Giải thuật mã hóa DSA

DSA là chuẩn của chính phủ Mỹ trong việc tạo ra chữ ký điện tử, được đề nghị bởi NIST vào năm 1994.

Tốc độ tương đương như RSA khi tạo ra chữ ký số nhưng lại chậm hơn 10 đến 40 lần khi kiểm tra chữ ký số.

Sử dụng SHA-1 cho giải thuật băm, có độ dài khóa từ 512 -1024 bits. Hiện nay, được khuyến cáo nên dùng khóa có độ dài là 2048 bits.

#### Giải thuật mã hóa DH

DH là một phương pháp trao đổi khóa được phát minh sớm nhất trong mật mã học được công bố bởi Whitfield Diffie và Martin Hellman năm 1976.

Nó dùng để tạo ra “khóa bí mật chia sẻ” (sử dụng cho mã hóa đối xứng) giữa hai host trên đường truyền không an toàn. Nó cung cấp cơ chế bảo mật nhưng không cung cấp dịch vụ chứng thực.

DH có điểm yếu với dạng tấn công kẻ đứng giữa.

## Tổ chức chứng nhận khóa công khai

Một chứng nhận điện tử có thể được xem như là một “hộ chiếu” hay “chứng minh thư”. Nó được một tổ chức tin cậy (như VeriSign, Entrust, CyberTrust,...) tạo ra. Tổ chức này được gọi là tổ chức chứng nhận khóa công khai Certificate Authority (CA). Một khi public key đã được CA chứng nhận thì có thể dùng khóa đó để trao đổi dữ liệu trên mạng với mức độ bảo mật cao.

Cấu trúc của một chứng nhận điện tử gồm các thành phần chính như sau:

- Issuer: tên của CA tạo ra chứng nhận.

- Period of validity: ngày hết hạn của chứng nhận.

- Subject: bao gồm những thông tin về thực thể được chứng nhận.

- Public key: khóa công khai được chứng nhận.

- Signature: do private key của CA tạo ra và đảm bảo giá trị của chứng nhận.

# CHỮ KÝ SỐ

## Giới thiệu về chữ ký số

Với sự phát triển của công nghệ thông tin như ngày nay, thương mại điện tử trở thành một phương thức kinh doanh nhanh chóng và hiệu quả. Phương thức này đã làm thay đổi cán cân của các lĩnh vực hoạt động kinh tế. Thông tin trở thành tài nguyên, hàng hóa thì việc xác định chủ sở hữu là một nhu cầu tất yếu. Chữ ký số ra đời, cung cấp giải pháp hàng đầu cho nhu cầu tất yếu này. Nó có khả năng xác thực người ký, đảm bảo tính toàn vẹn dữ liệu, thông điệp và không chối bỏ trong giao dịch.

Chữ ký số (Digital Signature) là tập con của chữ ký điện tử (electronic signature) và là một chuỗi số gắn kết một thông điệp với một hoặc nhiều thực thể nguồn nào đó. Nó dựa trên kỹ thuật mã hóa với khóa công khai. Trong đó, mỗi người sẽ được cung cấp một cặp khóa (khóa công khai và khóa bí mật).

Chữ ký số điện tử bao gồm 3 thành phần: thuật toán tạo ra khóa, hàm tạo chữ ký và hàm kiểm tra chữ ký.

Nó là thông tin đính kèm theo dữ liệu (văn bản, hình ảnh, video,...) nhằm mục đích xác định chủ thể của dữ liệu đó. Đặc biệt, khi một thông điệp thay đổi thì chữ ký số cũng thay đổi, do vậy nó đảm bảo được tính toàn vẹn của thông điệp được ký.

Cách tạo chữ ký điện tử:

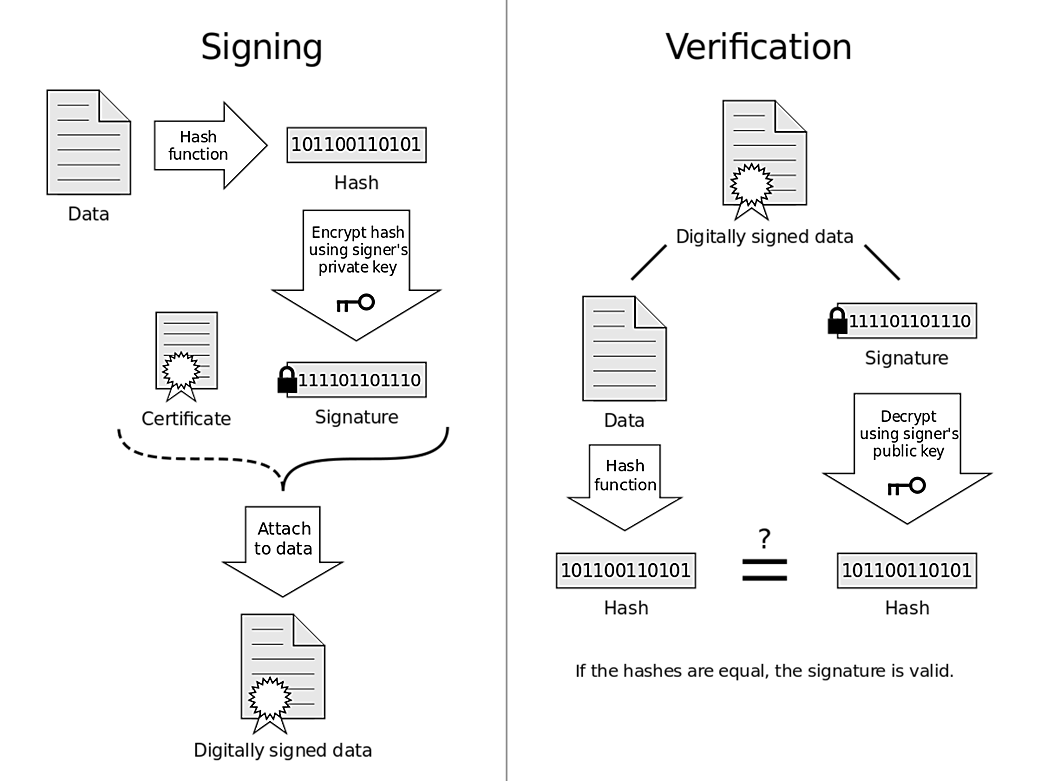
- Vân tay.

- Sơ đồ võng mạc.

- Sơ đồ tĩnh mạch trong bàn tay.

- ADN.

- Các yếu tố sinh học khác.



* + - * 1. Sơ đồ mình họa chữ ký số

(Nguồn: https://kientrucphanmemviet.wordpress.com/2015/10/16/ung-dung-chu-ky-so-trong-cac-du-an-chinh-phu-dien-tu/)

## Phân loại chữ ký số theo đặc trưng kiểm tra chữ ký

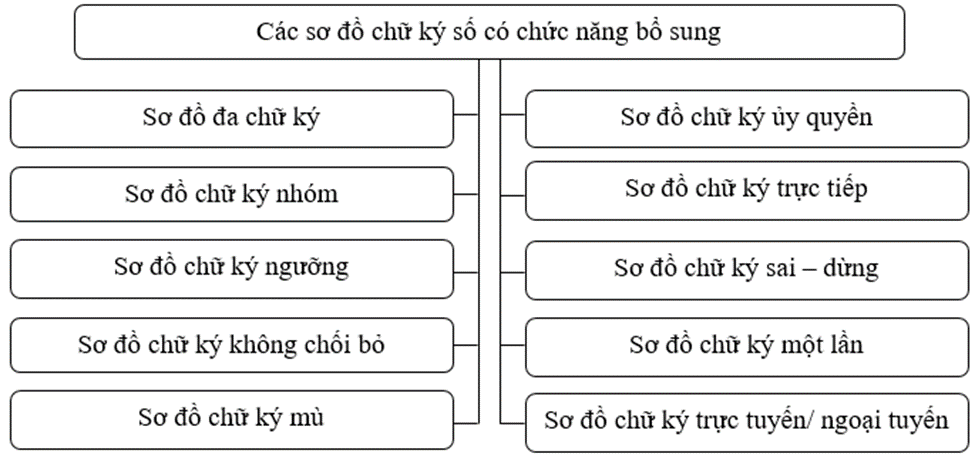
Dựa theo thuật toán xác minh chữ ký số. Có thể chia làm hai loại:

- Chữ ký số kèm thông điệp (digital signature schemes with appendix): cần có thông điệp (gốc) cho quá trình kiểm tra. Nó là loại chữ ký, trong đó, người gửi cần gửi “chữ ký”, phải kèm theo cả thông điệp được “ký” bởi “chữ ký” này. Nhưng người nhận sẽ không có được thông điệp gốc này.

- Chữ ký số khôi phục thông điệp (digital signature schemes with message recovery): không cần thông điệp (gốc) cho quá trình kiểm tra mà thông điệp (gốc) sẽ được khôi phục lại từ bản thân chữ ký. Có nghĩa là, người gửi chỉ cần gửi “chữ ký”, người nhận có thể khôi phục lại thông điệp đã được “ký” bởi “chữ ký” này.

## Các sơ đồ chữ ký số có chức năng bổ sung

Sơ đồ chữ ký số có chức năng bổ sung là sơ đồ chữ ký số ngoài chức năng xác thực còn có thêm các chức năng khác.



* + - * 1. Các sơ đồ chữ ký số có chức năng bổ sung

### Sơ đồ đa chữ ký

Có nhiều ứng dụng thương mại trong đó cần nhiều người ký vào một văn bản. Do vậy, cần một sơ đồ có nhiều khóa để ký, sơ đồ đa chữ ký (Multi-signature scheme) ra đời để giải quyết vấn đề này. Nó được áp dụng nhiều trong hợp đồng cần được ký bởi nhiều đối tác.

### Sơ đồ chữ ký nhóm

Chữ ký nhóm (Group signature scheme) cho phép mỗi thành viên trong nhóm được cho quyền đại diện cho nhóm để ký vào thông điệp theo cách:

- Chỉ một thành viên của nhóm được ký vào thông điệp.

- Người nhận chữ ký có thể xác minh được đó là chữ ký nhóm hợp lê.

- Người nhận chữ ký không thể nhận dạng được thành viên nào trong nhóm là người ký .

### Sơ đồ chữ ký ngưỡng

Hầu hết người ký vào một sơ đồ chữ ký số là một người đơn độc. Tuy nhiên, vẫn có một số trường hợp mà một nhóm cùng quyết định và thông điệp là đại diện cho một tổ chức.

Trong sơ đồ chữ ký ngưỡng, một nhóm con hoặc cổ đông của cổ đông của một nhóm được chỉ định có thể tạo ra một chứ ký nhóm hợp lệ và người xác minh có thể kiểm tra tính hợp lệ của chữ ký mà không cần nhận dạng những người ký.

Tuy vậy, các sơ đồ chữ ký ngưỡng có một khuyết điểm: nếu một nhóm người cùng cấu kết, họ có thể giả mạo chữ ký mà không có bất kỳ trách nhiệm nào đối với chữ ký và không thể truy lại những người ký.

### Sơ đồ chữ ký không chối bỏ

Sơ đồ chữ ký không chối bỏ (Undeniable signature scheme) do Chaum và Van Antwerpen đề xuất là sơ đồ chữ ký không tự xác minh. Các chữ ký chỉ có thể xác minh dưới sự đồng ý của người ký. Đồng thời, một người ký cũng không thể từ chối xác thực một thông điệp thật thông qua một thủ tục thêm vào gọi là thủ tục chối.

Sơ đồ chữ ký không chối được gồm ba phần: thuật toán ký, giao thức xác minh và giao thức từ chối.

Trong sơ đồ này, xác xuất người ký chối bỏ thành công là rất nhỏ. Việc xác minh được thực hiện theo thủ tục yêu cầu – đáp ứng; trong đó, người xác minh gửi một yêu cầu đến người ký và xem xét trả lời để xác minh chữ ký.

### Sơ đồ chữ ký mù

Các sơ đồ chữ ký mù (Blind signaute scheme) được đề xuất bởi Chaum, trong đó nội dung của thông điệp cần được ký được "che" đi trước khi ký nhưng lại vẫn được xác thực như là một chữ ký số thông thường.

Sơ đồ chữ ký mù có nhiều ứng dụng như: gắn dấu thời gian, kiểm soát truy nhập nặc danh và tiền điện tử,..

### Sơ đồ chữ ký ủy quyền

Sơ đồ chữ ký ủy quyền (Proxy signaute scheme) được thiết kế có khả năng ủy quyền ký một cách hiệu quả và minh bạch.

Các sơ đồ chữ ký thông thường dựa trên một khóa riêng mà chỉ có chủ nhân của nó mới biết. Nếu khóa riêng này được ủy quyền cho người khác một cách trực tiếp thì nó không còn được đại diện cho người đó và chữ ký số không còn giá trị. Do đó, chúng ta cần ủy quyền khả năng ký mà không tiết lộ khóa riêng, sao cho người nhận có thể xác minh chữ ký của người ký gốc với sự trợ giúp của chữ ký ủy quyền.

### Sơ đồ chữ ký trực tiếp

Sơ đồ chữ ký trực tiếp (Directed signature scheme) là sơ đồ chữ ký mà người nhận chữ ký có toàn quyền kiểm soát tiến trình xác minh. Không ai có thể kiểm tra sự đúng đắn của chữ ký mà không có sự cộng tác của người nhận chữ ký.

### Sơ đồ chữ ký sai – dừng

Sơ đồ chữ ký sai – dừng (Fail-stop signature scheme) được đề xuất bởi Van Heyst và Pedeson để bảo vệ chống khả năng một kẻ tấn công có thể giả mạo chữ ký của một người nào đó. Nó là biến thể của sơ đồ chữ ký một lần, trong đó chỉ có một thông điệp đơn lẻ được ký.

Nếu kẻ tấn công có thể giả mạo được chữ ký thì người ký thật sự có thể chứng minh đã có sự giả mạo bằng cách đưa ra lời giải cho bài toán khó là cơ sở cho sơ đồ chữ ký đó. Sơ đồ này, giúp người ký phát hiện ra các lổ hổng của sơ đồ nếu có kẻ tấn công thành công.

### Sơ đồ chữ ký một lần

Sơ đồ chữ ký một lần (One-time signature scheme) cho phép sử dụng khóa cho trước để ký một thông điệp riêng lẻ, vì vậy nó tương đối nhanh. Tuy nhiên, sơ đồ này khó kiểm soát khi sử dụng để xác thực nhiều thông điệp, vì đối với mỗi thông điệp mới thì cần điều chỉnh cả khi ký và khi xác minh chữ ký.

### Sơ đồ chữ ký trực tuyến/ ngoại tuyến

Sơ đồ chữ ký trực tuyến/ ngoại tuyến (On-line/off-line signature scheme) được tao ra trên cơ sở kết hợp sơ đồ chữ ký thông thường với một sơ đồ chữ ký một lần sao cho phần lớn các gánh nặng tính toán của thuật toán ký được thực hiện trước khi người ký biết được thông điệp sẽ được ký.

Sơ đồ chữ ký trực tuyến/ ngoại tuyến được xem xét tương tự như kỹ thuật phong bì điện tử.

## Ứng dụng

Giải pháp dùng chữ ký số là tối ưu vì nó có hiệu lực pháp luật. Các chữ ký số được sử dụng để cung cấp các dịch vụ mật mã cơ bản: tính toàn vẹn dữ liệu, xác thực nguồn dữ liệu và không chối bỏ.

Chữ ký số được phát hành bởi bên thứ ba là cơ quan chứng thực có thẩm quyền cấp phát, thu hồi, quản lý chứng chỉ số cho các thực thể thực hiện các giao dịch an toàn (Certificate Authority hoặc CA) nên đảm bảo tính khách quan. Như vậy, quá trình tạo chữ ký số, xác nhận các yêu cầu pháp lý, bao gồm xác thực người ký, xác thực tin nhắn.

Chính vì những ưu điểm của chữ ký số nên nó được ứng dụng trong nhiều lĩnh vực khác nhau: đảm bảo an ninh truyền thông, ngân hàng trực tuyến, thương mại điện tử, đảm bảo an ninh cho thư điện tử, chính phủ điện tử, xác thực toàn vẹn dữ liệu,…

Hệ thống thư điện tử: tiết kiệm được chi phí giao dịch bằng văn bản giấy thông thường (giấy, mực in, chuyển phát,…). Ngoài ra việc ứng dụng chữ ký số trong giao dịch điện tử giữa các cơ quan doanh nghiệp và người dân làm tăng tính hiệu quả, phương pháp làm việc chính xác làm cơ sở để thúc đẩy quá trình ứng dụng công nghệ thông tin, các dịch vụ hành chính công và tiến tới xây dựng hoàn thiện Chính quyền điện tử.

Thương mại điện tử: bán hàng trực tuyến và giao dịch dùng thẻ, điển vào các văn bản thuế và các văn bản pháp quy khác,…

Hệ thống chuyển tiền điện tử: chữ ký được sử dụng cho thông điệp chuyển tiền trước khi nó được gửi đi rằng thông điệp nhận là chính xác và không thể bị chối bỏ.

# CHỨNG CHỈ SỐ

## Giới thiệu về chứng chỉ số

Chứng chỉ số là một cấu trúc dữ liệu, liên kết một tên với một khóa công khai bằng một chữ ký. Do vậy, bản thân nó đã mang tính xác thực. Nó cũng là thành phần làm nền tảng cho hoạt động của PKI.

Chứng chỉ số là một tài liệu điện tử được sử dụng để nhận dạng và đại diện cho một cá nhân, một tổ chức, máy tính, thiết bị mạng hoặc dịch vụ nào đó và gắn chỉ danh của đối tượng đó. Nó được phát hành bởi một Certification Authority (CA) và được liên kết với một cặp khóa công khai và khóa bí mật.

Khuôn dạng chứng chỉ số được sử dụng rộng rãi nhất theo tiêu chuẩn ITU-T X.509.

Một chứng chỉ là một tập tin được ký số, có kích thước từ 2KB đến 4KB và thường bao gồm các thông tin cơ bản sau:

- Thông tin về người dùng, máy tính, thiết bị mạng,..

- Thông tin về CA phát hành chứng chỉ.

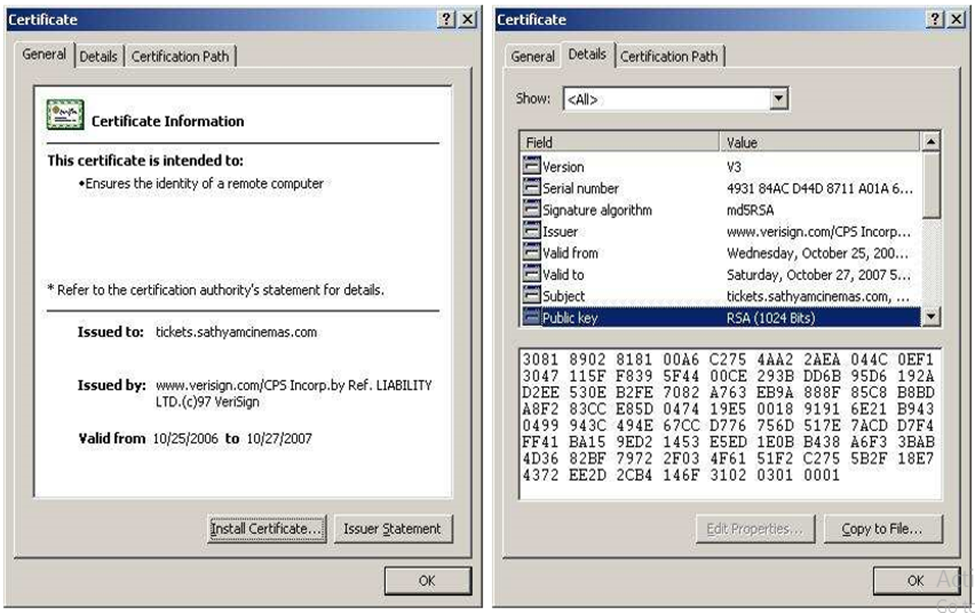
- Khóa công khai tương ứng với khóa bí mật được liên kết với chứng chỉ.

- Tên của các thuật toán để mã hóa và thuật toán tạo chữ ký số cho chứng chỉ.

- Một danh sách các phần mở rộng (extension) cho loại chứng chỉ X.509 version 3.

- Thông tin giúp xác định trạng thái thu hồi (revocation) và tính hiệu lực của chứng chỉ (như ngày phát hành và ngày hết hạn).

CA phải bảo đảm nhận dạng của đối tượng yêu cầu là xác thực trước khi cấp chứng chỉ. Việc xác minh nhận dạng có thể được thực hiện dựa trên các giấy phép an ninh (security credential) của đối tượng hoặc thực hiện thông qua cuộc gặp mặt và trao đổi trực tiếp với người yêu cầu. Sau khi nhận dạng được kiểm chứng là hợp lệ, CA sẽ cấp chứng chỉ được ký số bởi khóa bí mật của nó cho họ. Chữ ký số này cho biết nguồn gốc của chứng chỉ (do CA nào cấp), đảm bảo khóa công khai là thuộc về chủ thể của chứng chỉ và giúp phát hiện những thay đổi, giả mạo nếu có trong nội dung của chứng chỉ.



* + - * 1. Khuôn dạng chứng chỉ số

(Nguồn: https://manthang.wordpress.com/)

## Các loại chứng chỉ số

### Chứng chỉ khóa công khai

Chứng chỉ khóa công khai (public key certificate) liên kết khóa công khai với một chủ thể gồm:

- Khóa công khai: có thể được coi là lý do tồn tại của chứng chỉ khóa công khai.

- Thông tin về tên: được dùng để nhận biết chủ sở hữu.

- Một hoặc nhiều chữ ký số: để chứng thực các thông tin trong chứng chỉ (khóa công khai và thông tin về tên).

Có hai khuôn dạng cho chứng chỉ khóa công khai:

- Chứng chỉ theo chuẩn X.509.

- Chứng chỉ PGP (Pretty Good Privacy) dùng cho PGP hoặc OpenPGP.

### Chứng chỉ thuộc tính

Chứng chỉ thuộc tính (attribute certificate) vể cấu trúc tương tự như chứng chỉ khóa công khai. Nhưng thay bằng việc liên kết chủ thể với khóa công khai thì chứng chỉ thuộc tính liên kết chủ thể với các thuộc tính.

### Chứng chỉ khác

Chứng chỉ cho quyền (authorization certificate) là một loại chứng chỉ khóa công khai nhưng gắn kết khóa công khai với các quyền truy cập vào một tài nguyên.

Các loại chứng chỉ khác về cơ bản hoạt động theo nguyên tắc của các chứng chỉ trên. Nhưng đã được sửa đổi, thiết kế lại cho phù hợp với đặc thù của các ứng dụng trong các lĩnh vực.

## Chứng chỉ khóa công khai

### Chứng chỉ X.509

X.509 là một đề nghị của ITU (International Telecommunication Union) định nghĩa một framework về chứng thực (certificate). X.509 dựa trên X.500, mà bản thân X.500 còn chưa được định nghĩa hoàn hảo.

X.509 hỗ trợ cả hai mã bí mật (mã đơn) và mã công khai. X.509 định nghĩa các nội dung về một chứng thực, bao gồm số phiên bản, số serial, ID chữ ký, tên công bố, thời điểm có hiệu lực, định nghĩa chủ đề, phần mở rộng và chữ ký trên các trường trên.

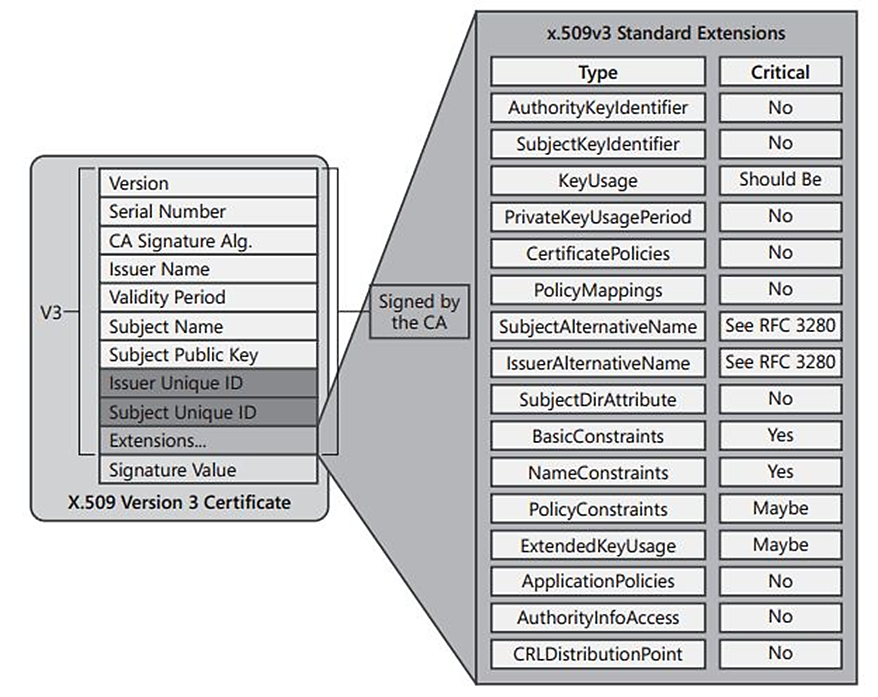
Về cơ bản, một người có trách nhiệm chứng nhận sẽ đặt khóa công khai của một người nào đó có nhu cầu chứng thực vào thủ tục chứng thực và sau đó xác thực lại bằng khóa riêng. Điều này bắt buộc khóa và thủ tục chứng thực phải luôn đi kèm với nhau. Bất cứ ai cần dùng khóa công cộng của một đối tượng nào đó đều có thể mở thủ tục chứng thực bằng khóa công cộng của các đối tượng này do người có trách nhiệm chứng thực cung cấp (các khóa công cộng này được ký hoặc khóa bằng khóa riêng của người có trách nhiệm chứng thực). Vì vậy, người sử dụng phải tin rằng người có trách nhiệm chứng thực sẽ bảo đảm việc hợp lệ hóa người chủ của khóa công khai và thực sự khóa công khai ở đây chính là khóa công khai của người có trách nhiệm chứng thực.

Có 3 phiên bản của chứng chỉ số được dùng trong một hệ tầng PKI là:

- Chứng chỉ X.509 version 1: được công bố năm 1988, được triển khai rộng rãi và là tiêu chuẩn chung nhất.

- Chứng chỉ X.509 version 2: phiên bản sửa đổi năm 1993 đưa ra hai trường Subject unique identifier và Issuer unique identifier để xử lý khả năng sử dụng lại tên chủ thể (subject name) và tên tổ chức phát hành (issuer name) theo thời gian. Tuy nhiên, nhiều khuyến nghị không nên sử dụng lại các tên và các chứng chỉ dùng các dạng duy nhất (unique idetifier). Do vậy, phiên bản 2 không được sử dụng rộng rãi.

- Chứng chỉ X.509 version 3: được ra đời vào năm 1996 và bổ sung thêm các phần mở rộng (extension) để khắc phục các vấn đề liên quan đến việc so khớp Issuer Unique ID và Subject Unique ID cũng như là các vấn đề về xác thực chứng chỉ. Một chứng chỉ X.509 version 3 có thể chứa một hoặc nhiều extension.



* + - * 1. Mô hình của chứng chỉ số theo X.509 version 3

(Nguồn: https://manthang.wordpress.com/)

- Chứng chỉ X.509 version 4: ở dạng dự thảo được công bố vào năm 2000, phiên bản này có một số bổ sung về liên quan đến thu hồi chứng chỉ và những tính năng mới trong chứng chỉ thuộc tính, cũng như xác định việc sử dụng chứng chỉ thuộc tính để kiểm soát truy cập và trao quyền.

Nó được sử dụng trong các ứng dụng và giao thức hỗ trợ PKI như SSL, IPSec, S/MINE,SET, PEM (Privacy Enhanced Mail),...

Các trường chứng chỉ như sau:

- Version (Phiên bản): Ứng với mỗi phiên bản khác nhau thì thông tin cụ thể trong chứng chỉ cũng khác nhau.

- Certificate Serial Number (Số hiệu của chứng chỉ): Do CA gán để phân biệt chứng chỉ này với chứng chỉ khác. Nó cùng với Issuer name sẽ xác định một chứng chỉ duy nhất.

- Signature Algorithm Identifier (Nhận dạng thuật toán ký): Chỉ ra thuật toán và hàm băm mà CA sử dụng để ký chứng chỉ. Có thể là thuật toán RSA hay DSA,...

- Issuer name (Tên tổ chức phát hành chứng chỉ): Tên theo chuẩn X.500 của thực thể ký và phát hành chứng chỉ.

- Validity Period (Thời gian hợp lệ): Chỉ ra khoảng thời gian mà chứng chỉ có hiệu lực (xác định thời gian chứng chỉ bắt đầu có hiệu lực và thời điểm hết hạn). Được mô tả bằng ngày, giờ bắt đầu và ngày, giờ kết thúc.

- Subject name (Tên của chủ thể): Xác định tên của thực thể có trong khóa công khai ghi trên chứng chỉ. Tên của chủ thể phải duy nhất đối với mỗi thực thể CA xác nhận gọi là tên phân biệt gồm có:

* Tên thường dùng (DN – Common Name).
* Đơn vị (OU – Organizational Unit).
* Tổ chức (O – Organization).
* Nước (C – Country).

- Subject Public Key Information (Thông tin về khóa công khai của chủ thể - SPKI): Chứa khóa công khai và những tham số liên quan, xác định tên thuật toán sử dụng khóa công khai này.

- Issuer Unique Identifier (Nhận dạng duy nhất của tổ chức phát hành chứng chỉ): Trường này không bắt buộc, nó cho phép sử dụng lại tên người cấp và hiếm được sử dụng trong triển khai thực tế. Đây là trường tùy chọn theo phiên bản 2.

- Subject Unique Identifier (Nhận dạng duy nhất của chủ thể): Trường này không bắt buộc. Nó dùng để nhận dạng duy nhất một chủ thể trong trường hợp sử dụng lại tên. Đây là trường tùy chọn theo phiên bản 2.

- Extensions (Các trường mở rộng): Cho phép thêm các trường mới vào chứng chỉ. Đây là trường tùy chọn theo phiên bản 3. Gồm ba phần:

* Extension Identifier: là một mã nhận dạng đối tượng (Object Identifier – OID) cho biết kiểu định dạng và các định nghĩa của extension.
* Criticality Flag: là một dấu hiệu cho biết thông tin trong extension có quan trọng (critical) hay không. Nếu một ứng dụng không thể nhận diện được trạng thái critical của extension hoặc extension không hề chứa giá trị nào thì chứng chỉ đó không thể được chấp nhận hoặc được sử dụng. Nếu mục criticality flag này không được thiết lập thì một có thể sử dụng chứng chỉ ngay cả khi ứng dụng đó không nhận diện được extension.
* Extension Value: là giá trị được gán cho extension. Nó phụ thuộc vào từng extension cụ thể.

Đây là các trường trong extension:

AuthorityKeyIdentifier: nhận dạng khóa công khai được sử dụng để xác minh chữ ký chứng chỉ (không thiết yếu).

SubjectKeyIdentifier: nhận dạng khóa công khai của chứng chỉ (không thiết yếu)..

KeyUsage: nhận dạng mục đích sử dụng khóa công khai của chứng chỉ (thiết yếu hoặc không thiết yếu).

PrivateKeyUsagePeriod: chỉ thị khoảng thời gian sử dụng khóa riêng tương ứng với khóa công khai của chứng chỉ (không thiết yếu).

CertificatePolicies: nhận dạng các chính sách chứng chỉ của CA áp dụng cho chứng chỉ này (thiết yếu hoặc không thiết yếu).

PolicyMappings: chỉ dành cho chứng chỉ CA, dùng để ánh xạ chính sách chứng chỉ của một vùng (domain) này tới chính sách chứng chỉ của vùng khác (không thiết yếu).

SubjectAltName: nhận dạng các tên thay thế của chủ thể chứng chỉ (thiết yếu hoặc không thiết yếu).

IssuerAltName: nhận dạng các tên thay thế của tổ chức phát hành chứng chỉ (không thiết yếu).

*BasicConstraints*: gồm hai trường (thiết yếu hoặc không thiết yếu)

*PathLengthConstraint*: chỉ định số lớn nhất các chứng chỉ có thể theo sau chứng chỉ này trong đường dẫn chứng thực.

*NameConstraints*: chỉ thị không gian tên (name space) chứa tất cả các tên chủ thể của chứng chỉ kế tiếp trong một đường dẫn chứng thực (thiết yếu hoặc không thiết yếu).

*PolicyConstraints*: xác định các ràng buộc như yêu cầu nhận dạng chính sách chứng chỉ một cách tường minh hoặc ngăn cấm ánh xạ chính sách cho phần còn lại của đường dẫn chứng thực (thiết yếu hoặc không thiết yếu).

*InhibitAnyPolicy*: xác định một chứng chỉ nào đó không được coi là phù hợp rõ ràng với các chính sách chứng chỉ khác (thiết yếu hoặc không thiết yếu).

*CRLDistributionPoints*: xác định điểm phân phát CLR mà người dùng chứng chỉ cần tham chiếu để kiểm tra chứng chỉ đã bị thu hồi hay chưa (thiết yếu hoặc không thiết yếu).

*Signatue* (chữ ký): chỉ định chữ ký số cho nội dung của chứng chỉ.

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 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 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.

### Chứng chỉ PGP

Chứng chỉ PGP linh hoạt hơn chứng chỉ X.509 version 3 và phù hợp hơn cho việc thiết lập các mối quan hệ tin cậy giữa các cá nhân.

Mật mã hóa PGP (Pretty Good Privacy - Riêng tư tốt đẹp) là một phần mềm máy tính dùng để mật mã hóa dữ liệu và xác thực. Phiên bản PGP đầu tiên do Phil Zimmermann được công bố vào năm 1991. Kể từ đó, phần mềm này đã có nhiều cải tiến và hiện nay tập đoàn PGP cung cấp nhiều phần mềm dựa trên nền tảng này. Với mục tiêu ban đầu là phục vụ cho mã hóa thư điện tử, PGP hiện nay đã trở thành một giải pháp mã hóa cho các công ty lớn, chính phủ cũng như các cá nhân. Các phần mềm dựa trên PGP được dùng để mã hóa và bảo vệ thông tin lưu trữ trên laptop, máy tính để bàn, máy chủ và trong quá trình trao đổi thông qua email hoặc chuyển file. Giao thức hoạt động của hệ thống này có ảnh hưởng lớn và trở thành một trong hai tiêu chuẩn mã hóa (tiêu chuẩn còn lại là S/MIME).

Khi một khóa mới được thêm vào danh sách khóa, thuê bao sẽ quyết định mức độ tin cậy cho khóa này. Các mức độ tin cậy được xác định là:

- Tin cậy hoàn toàn (Complete trust).

- Tin cậy ít (Marginal trust).

- Không được tin cậy (Not trusted).

Một khóa thêm vào được coi là hợp lệ nếu nó được xác minh bởi một khóa tin cậy hoàn toàn hoặc hai khóa tin cậy ít.

Cấu trúc dữ liệu của chứng chỉ PGP gồm các trường sau:

- Version number (số phiên bản): sử dụng để nhận biết phiên bản nào của PGP đã được dùng để tạo cặp khóa công khai trong chứng chỉ.

- Public key (khóa công khai): sử dụng để chứa khóa công khai và nhận dạng một thuật toán tương ứng.

- Certificate owner information (thông tin chủ sở hữu chứng chỉ): sử dụng để chứa thông tin nhận dạng về chủ sở hữu chứng chỉ và người giữ khóa riêng tương ứng. Có thể có nhiều dạng người dùng và chữ ký.

- Self-signature (chữ ký tự ký): sử dụng để chứa chữ ký của người chủ sỡ hữu chứng chỉ, sử dụng khóa riêng tương ứng với khóa công khai của chứng chỉ.

- Validity period (thời gian hợp lệ): sử dụng để quyết định thời gian bắt đầu và hết hạn của chứng chỉ.

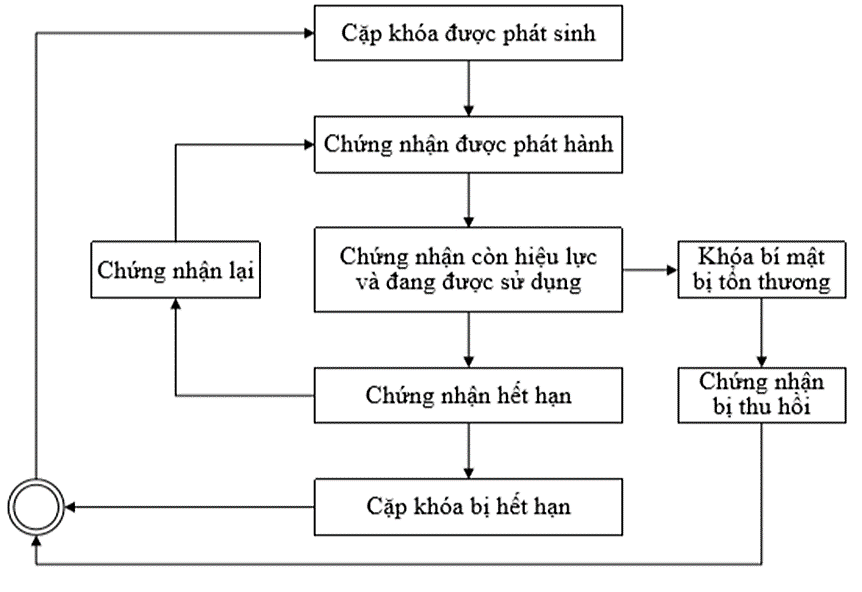
- Preferred encryption algorithm (thuật toán mã hóa được chọn): sử dụng để nhận biết thuật toán đã được chọn cho chủ sỡ hữu chứng chỉ. Ví dụ: IDEA, CAST, 3DES,…

## Chu kỳ sống của chứng nhận số

Trước khi phát hành chứng nhận, cặp khóa bí mật/công khai sẽ được phát sinh. Trong khi chứng nhận có hiệu lực và được sử dụng, chứng nhận có thể hết hạn hoặc khóa bí mật của người sử dụng bị tổn thương (bị mất hoặc lộ khóa).

Trong trường hợp chứng nhận hết hạn, cặp khóa cũng sẽ không còn hiệu lực hoặc người sử dụng có thể yêu cầu gia hạn chứng nhận cho họ.

Trong trường hợp khóa bí mật bị tổn thương, chứng nhận sẽ được thu hồi.

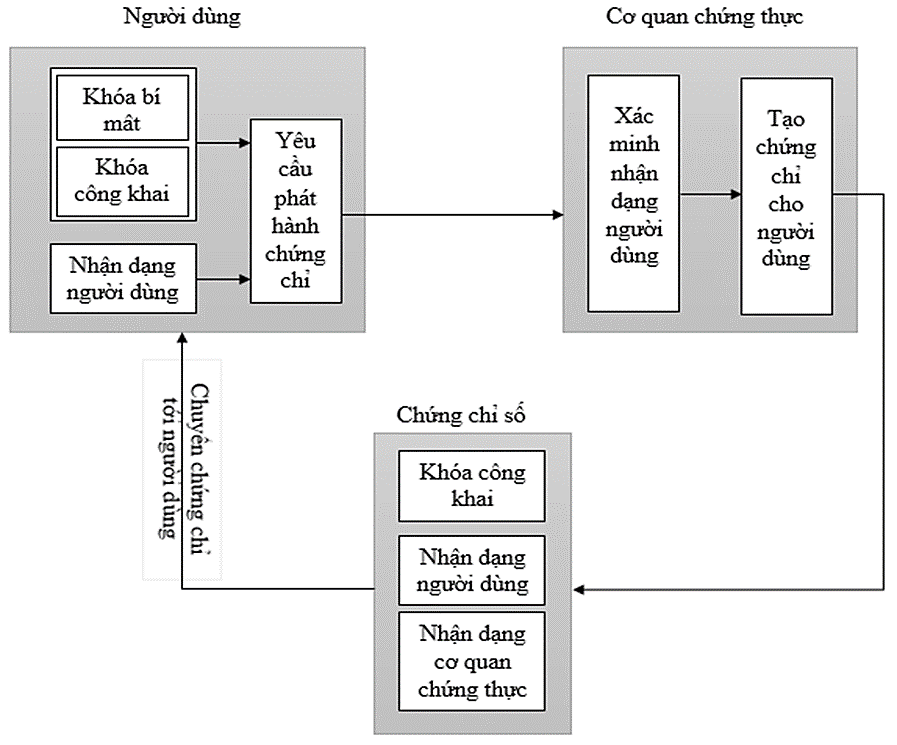


* + - * 1. Chu kỳ sống của chứng nhận

(Nguồn: https://kientrucphanmemviet.wordpress.com/2015/10/16/ung-dung-chu-ky-so-trong-cac-du-an-chinh-phu-dien-tu/)

## Phát hành chứng chỉ

Việc phát hành chứng chỉ tùy thuộc vào cơ sở hạ tầng kỹ thuật của CA và chính sách chứng chỉ do CA thiết lập. Nó được phát hành tương tự như cấp giấy phép lái xe, chứng minh nhân dân,…



* + - * 1. Tiến trình phát hành một chứng chỉ số

## Xác minh chứng chỉ

Xác minh chứng chỉ là một quy trình để chắc chắn rằng một chứng chỉ hợp lệ tại một thời điểm xác định. Nó có thể bao gồm cả việc xây dựng và quản lý đường dẫn chứng thực để đảm bảo mọi chứng chỉ trong đường dẫn đó là hợp lệ.

Khi gửi thông điệp, bên gửi ký và gửi kèm chứng chỉ số để xác thực bên gửi đã gửi thông điệp. Khi bên nhận nhận thông điệp, bên nhận sẽ xác minh chứng chỉ số của người ký không có giả mạo hay lỗi xảy ra. Các chứng chỉ cần xác minh được ghép thành chuỗi chứng chỉ và nó chứa kèm theo cơ quan chứng thực chứng chỉ cao nhất, có thể tin cậy được. Bên nhận sẽ đi theo chuỗi chứng chỉ để đi tới CA gốc nên người ký được xác minh (do CA gốc được tin cậy).

## Thu hồi chứng chỉ

Thu hồi chứng chỉ là chứng chỉ do CA phát hành trước đó không còn hiệu lực nữa. Có rất nhiều lý do để thu hổi chứng chỉ. Do đó, cần có một cơ chế cho phép người sử dụng chứng chỉ kiểm tra được trạng thái thu hồi chứng chỉ. X.509 cho phép kiểm tra chứng chỉ trong các trường hợp sau:

- Chứng chỉ không bị thu hồi.

- Chứng chỉ bị thu hồi.

- Chứng chỉ do một tổ chức có thẩm quyền mà CA ủy thác có trách nhiệm thu hồi chứng chỉ.

Về mặt lý thuyết, có bốn cách tiếp cận việc thu hồi:

- Các chứng chỉ tự động quá hạn sau một khoảng thời gian xác định và đòi hỏi phải định kỳ cấp lại.

- Liệt kê danh sách chứng chỉ không bị thu hồi trong hệ thống và chỉ chấp nhận những chứng chỉ trong danh sách này.

- Định kỳ phát hành các danh sách chứng chỉ bị thu hồi và không còn sử dụng được nữa.

- Tạo cơ chế kiểm tra chứng chỉ có bị thu hồi hay chưa.

Vị trí của thông tin thu hồi có thể khác nhau tùy theo CA khác nhau. Bản thân chứng chỉ có thể chứa con trỏ đến nơi thông tin thu hồi được xác định vị trí. Người sử dụng chứng chỉ có thể biết được thư mục, kho lưu trữ hay cơ chế để lấy được thông tin thu hồi dựa trên những thông tin thiết lập trong quá trình khởi sinh. Để duy trì tính nhất quán và khả năng kiểm tra, CA yêu cầu:

- Duy trì bản ghi kiểm tra chứng chỉ thu hồi.

- Cung cấp thông tin trạng thái thu hồi.

- Công bố CRLs khi CRL là danh sách trống.

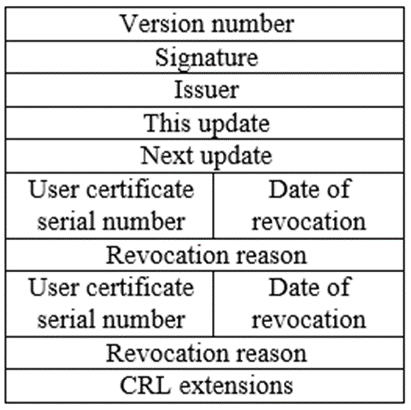
## Công bố và gửi thông báo thu hồi chứng chỉ

Thông thường chứng chỉ sẽ hợp lệ trong khoảng thời gian có hiệu lực. Nhưng trong một số trường hợp, chứng chỉ lại không hợp lệ trước thời gian hết hạn. Danh sách thu hồi chứng chỉ là cách tiếp cận thu hồi chứng chỉ đơn giản nhất. Nó là một cấu trúc dữ liệu dùng để nhận dạng các chứng chỉ bị thu hồi và một trong những phương pháp thông báo đến người sử dụng trạng thái của chứng chỉ là công bố CRLs định kỳ hoặc khi cần thiết. Ngoài ra, có một số phương pháp khác như phương pháp trực tuyến Online Certificate Status Protocol.

### Certificate Revocation Lists (CRLs)

CRLs là một cấu trúc dữ liệu được ký như chứng chỉ người sử dụng. Nó chứa danh sách chứng chỉ bị thu hồi và những thông tin cần thiết khác.

CRL thông thường do một CA cấp. Tuy nhiên, nó cũng có thể được sử dụng để cung cấp thông tin cho nhiều CA nếu nó được định nghĩa như một CRL gián tiếp. Những thông tin này được chứa trong trường mở rộng CRL Scope.



* + - * 1. Khuôn dạng danh sách chứng chỉ bị thu hồi

Trong đó:

- Version number: phiên bản của CRL.

- Signature: nhận dạng hàm băm và thuật toán ký được sử dụng để ký danh sách thu hồi.

- Issuer: tên của thực thể cấp và ký.

- This update: ngày và thời gian CRL được công bố.

- Next update: ngày và thời gian của lần cập nhật kế tiếp được cấp.

- Certificate serial number: số hiệu của chứng chỉ bị thu hồi.

- Revocation date: ngày thu hồi chứng chỉ.

- Revocation reason: nguyên nhân thu hồi chứng chỉ.

- CRL extensions: các trường mở rộng trong CRL.

Những chứng chỉ đã bị CA thu hồi được ghi vào danh sách theo thứ tự của List of revoked certificates. Mỗi đầu vào nhận biết chứng chỉ thông qua số serial và ngày thu hồi, trong đó có ghi rõ thời gian mà CA thu hồi.

### Authority Revocation Lists (ARLs)

ARL là một CRL đặc biệt chứa thông tin thu hồi về chứng chỉ CA. ARLs không chứa chứng chỉ của người sử dụng cuối. Những thay đổi thông thường trong ARL thường hiếm khi xảy ra. Vì chứng chỉ của CA chỉ bị thu hồi khi khóa riêng bị xâm hại.

ARLs được sử dụng chủ yếu trong quá trình thẩm tra đường dẫn chứng chỉ nếu môi trường tin cậy này bao gồm CA có chứng chỉ xác thực chéo.

### Cơ chế truy vấn On-line (On-line Query Mechanisms)

CRLs và ARLs giúp người sử dụng cuối nhận biết được tình trạng thu hồi chứng chỉ. Có một vấn đề phát sinh nếu CA thu hồi chứng chỉ ngay sau khi vừa công bố CRL. Không có người sử dụng nào nhận biết được về việc thu hồi này đến khi một CRL mới được thông báo.

Sử dụng dịch vụ online có một số ưu điểm sau:

- Trả lời thường xuyên.

- Thời gian trả lời nhanh.

- Giảm thiểu việc sử dụng băng thông mạng sẵn có.

- Tổng phí xử lý client thấp.

Tuy nhiên, dịch vụ online cũng có hạn chế trong trường hợp cần kiểm tra trạng thái thu hồi và vấn đề bảo mật cũng được đặt ra đối với loại dịch vụ này.

# HẠ TẦNG KHÓA CÔNG KHAI (PKI)

## Tổng quan về hạ tầng khóa công khai

### Khái niệm về PKI

Trong ngành mật mã học, PKI (Public key infrastructure)là hạ tầng khóa công khai. Nó là một cơ chế để cho một bên thứ 3 (thường là nhà cung cấp chứng thực số) cung cấp và xác thực định danh các bên tham gia vào quá trình trao đổi thông tin.

Từng bên tham gia sẽ cung cấp cặp khóa công khai và khóa bí mật:

* *Mã hóa*: mã hóa bằng khóa công khai, giải mã bằng khóa bí mật.
* *Chữ ký điện tử*: mã hóa bằng khóa bí mật, giải mã bằng khóa công khai.

Vai trò của PKI là quản lý khóa công khai trong phạm vi rộng:

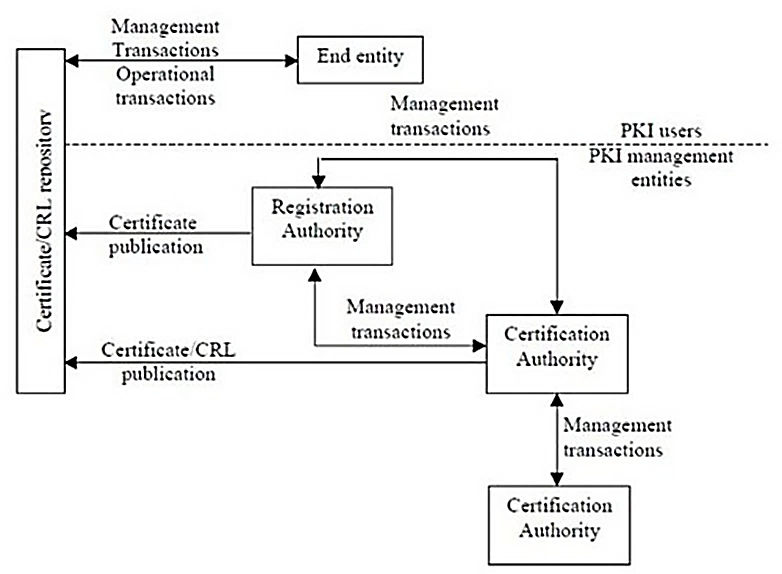
* Đăng ký và phát hành.
* Lưu trữ và phân phối.
* Thu hồi và xác minh trạng thái.
* Sao lưu dự phòng và khôi phục.

### Các thành phần và chức năng của PKI

#### Các thành phần của PKI

Một hệ thống PKI gồm bốn thành phần:

* Thực thể cuối EE (End Entity): là người dùng (chủ sở hữu chứng chỉ, đối tượng sử dụng các chứng chỉ).
* Cơ quan chứng thực CA (Certificate Authority): là cơ quan tin cậy để xác thực các nhận dạng của thực thể liên quan trong các giao dịch điện tử. CA có chức năng phát hành, lưu trữ và thu hồi các chứng chỉ.
* Cơ quan đăng ký RA (Registration Authority): là một hệ thống tùy chọn mà CA ủy quyền một số chức năng quản lý nhất định.
* Hệ thống dữ liệu chứng chỉ CR (Certificate Repository): một hệ thống hoặc một tập hợp các hệ thống phân tán có chức năng lưu trữ và cho phép các thực thể cuối tiếp cận các chứng chỉ và danh sách chứng chỉ bị thu hồi.



* + - * 1. Cấu trúc của một PKI

(Nguồn: http://www.vnpro.org/forum/forum/c%C3%B4ng-ngh%E1%BB%87-m%E1%BA%A1ng/lan-technologies-data-center)

#### Chức năng của PKI

PKI có các chức năng chính là:

Đăng ký thuê bao: thu thập thông tin, xác minh, nhận dạng người dùng.

Phát hành chứng chỉ: tạo chứng chỉ theo yêu cầu của người dùng.

Tạo các danh sách chứng chỉ thu hồi.

Lưu trữ và tìm kiếm các chứng chỉ và danh sách các chứng chỉ thu hồi.

Gia hạn chứng chỉ số.

Quản lý chu kỳ sống của khóa: cập nhật, lưu, khôi phục khóa của người dùng.

Các chức năng khác như: tạo cặp khóa cho người dùng, xác minh chứng chỉ, gắn dấu thời gian,…

Đặc biệt, nó cho phép các giao dịch điện tử được diễn ra đảm bảo bốn tính chất:

Tính bảo mật (Confidentiality) nghĩa là bảo đảm tính bí mật của dữ liệu. Tính bí mật này được cung cấp bởi các cơ chế mã hóa mật mã học, bằng cách sử dụng cả mã hóa khoá công khai lẫn mã hóa khóa bí mật. Do mã hóa khóa công khai không hiệu quả bằng mã hóa bí mật trong việc mã hóa dữ liệu lớn, nó thường được sử dụng để mã hóa những đối tượng dữ liệu tương đối nhỏ như các khóa bí mật được sử dụng trong các hệ thống mã hóa bất đối xứng.

Tính toàn vẹn (Integrity) nghĩa là đảm bảo dữ liệu không thể bị mất mát hoặc chỉnh sửa và các giao tác không thể bị thay đổi. Tính toàn vẹn có thể được cung cấp bên trong PKI bằng cách sử dụng cả mã hóa công khai và mã hóa bí mật. Mã hóa khóa công khai đặc biệt được sử dụng chung với một thuật toán băm như SHA-1 hay MD5 để cung cấp tính toàn vẹn. Một PKI được thiết kế tốt sẽ sử dụng các giao thức đòi hỏi sử dụng các thuật toán đó để cung cấp cơ chế toàn vẹn hiệu quả.

Tính xác thực (Authentication) nghĩa là danh tính của thực thể được xác minh. Tính xác thực trong môi trường thương mại điện tử được thực hiện rất tốt bằng các hệ thống mã hóa khóa công khai, dựa trên mối quan hệ toán học giữa khóa công khai và khóa bí mật. Thông điệp được ký bởi một thực thể có thể được kiểm tra bởi bất kỳ thực thể nào quan tâm. Các thực thể này có thể an tâm rằng chỉ có chủ của khóa bí mật mới có thể tạo ra thông điệp này, bởi vì chỉ có người đó mới có khóa bí mật.

Tính không thể chối từ (Non-Repudiation) nghĩa là đảm bảo dữ liệu không thể bị không thừa nhận hoặc giao tác bị từ chối. Đây là một dịch vụ bảo mật then chốt của bất kỳ ứng dụng thương mại nào trong đó việc trao đổi giá trị hay các quy định pháp luật được thỏa hiệp. Tính không thể chối từ được cung cấp thông qua mã hóa khóa công khai bằng chữ ký số. Khi dữ liệu được ký theo cách mật mã học sử dụng khóa bí mật của cặp khóa, bất kỳ ai có thể truy cập khóa công khai của cặp khóa này đều có thể xác định rằng chỉ có chủ của cặp khóa mới có thể ký vào dữ liệu.

### Mục tiêu

Mục tiêu chính của PKI là cung cấp và xác thực mối liên hệ giữa khóa và danh tính người dùng. Nhờ vậy người dùng có thể sử dụng trong một số ứng dụng như:

Mã hoá email hoặc xác thực người gửi email (OpenPGP hay S/MIME).

Ký và xác thực văn bản.

Xác thực người dùng ứng dụng (đăng nhập bằng thẻ thông minh – smartcard, nhận thực người dùng trong SSL, bầu cử).

Ngoài ra, việc sử dụng PKI và mã hóa công khai trong thương mại điện tử giúp các tổ chức giảm chi phí xử lý giao tác, giảm rủi ro và giảm độ phức tạp của các hệ thống bảo mật với các phương pháp đối xứng.

### Thực thể cuối EE

Thực thể cuối trong PKI có thể là con người, thiết bị, thậm chí có thể là một chương trình phần mềm nhưng thường là người sử dụng hệ thống. Thực thể cuối sẽ thực hiện những chức năng mật mã (mã hóa, giải mã và ký số).

### Cơ quan chứng thực CA

CA là một thực thể phát hành chứng chỉ và là thành phần trung tâm của PKI. Trong hạ tầng cơ sở khóa công khai, chứng chỉ có vai trò gắn kết định danh với khóa. Sự gắn kết này được thể hiện ở dạng cấu trúc dữ liệu được ký số.

Tổ chức chứng thực – CA cũng được gọi là bên thứ ba được tin tưởng vì người sử dụng cuối tin tưởng vào chữ ký số của CA trên chứng chỉ trong khi thực hiện những hoạt động mã hóa công khai cần thiết.

Thông thường, CA thực hiện chức năng xác thực bằng cách cấp chứng chỉ cho các CA khác và cho thực thể cuối trong hệ thống. Nếu CA nằm ở đỉnh của mô hình phân cấp PKI và chỉ cấp chứng chỉ cho những CA ở cấp thấp hơn thì chứng chỉ này được gọi là chứng chỉ gốc (root certificate).

Một CA có thể phát hành các loại chứng chỉ sau:

Chứng chỉ CA (CA certificate): chứng chỉ CA chứng nhận một khóa công khai thộc về một CA, trong trường hợp CA phát hành cho chính mình thì đây là chứng chỉ tự ký (self-sihned).

Chứng chỉ Server (Server certificate): dùng để nhận dạng một máy chủ hoặc máy tính. Nó chứa tên máy chủ và dùng các thiết lập kết nối an toàn cho các giao dịch trực tuyến giữa máy chủ và máy khách.

Chứng chỉ cá nhân (Personal certificate): dùng để nhận dạng một người. Nó bao gồm tên đầy đủ và đặc điểm riêng biệt của một cá nhân. Được ứng dụng vào các lĩnh vực như thư điện tử, kiểm soát truy cập,…

Chứng chỉ nhà phân phối phần mềm (Software publisher certificate): được cấp cho các nhà phân phối phần mềm để bảo vệ tính xác thực và toàn vẹn dữ liệu của các phần mềm phân phối qua Internet.

Chứng chỉ chéo (Cross certificate): sử dụng trong chứng thực chéo.

Một số loại CA khác nhau như: CA nội bộ (Internal CA), CA làm thuê (Outsourced Employee CA), CA khách hàng thuê (Outsourced Customer CA), CA bên tin cậy thứ ba (Trusted Third-Party CA), CA Chính phủ, CA tư nhân, CA của các tổ chức quốc tế,…

### Cơ quan đăng ký RA

Cơ quan đăng ký là một thành phần tùy chọn của PKI. Mặc dù CA có thể thực hiện chức năng đăng ký cần thiết, nhưng nó vẫn cần có thực thể độc lập thực hiện chức năng này.

Mục đích của RA là để giảm tải công việc của CA. RA đặc biệt hiệu quả khi được sử dụng để mở rộng phạm vi sử dụng hoạt động của CA qua các vùng địa lý khác nhau. Chức năng thực hiện của một RA cụ thể sẽ khác nhau theo nhu cầu triển khai PKI nhưng chủ yếu bao gồm các chức năng sau:

* Xác nhận cá nhân chủ thể đăng ký chứng chỉ.
* Kiểm tra tính hợp lệ của thông tin do chủ thể cung cấp.
* Xác nhận quyền của chủ thể đối với thuộc tính chứng chỉ được yêu cầu.
* Kiểm tra xem chủ thể có thực sự sở hữu khóa riêng đang được ký hay không (proof of possession – POP).
* Tạo cặp khóa bí mật và khóa công khai.
* Phân phối bí mật được chia sẻ đến thực thể cuối.
* Thay mặt 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 chứa khóa riêng.

RA xử lý việc trao đổi giữa chủ thể thực thể cuối với quá trình đăng ký, phân phối và quản lý vòng đời chứng chỉ/khóa.

Tuy nhiên, trong bất kỳ trường hợp nào thì RA cũng chỉ đưa ra những khai báo tin cậy ban đầu về chủ thể và chỉ CA mới có thể cấp chứng chỉ hay đưa ra thông tin trạng thái thu hồi chứng chỉ như CRL.

### Hệ thống lưu trữ dữ liệu chứng chỉ

Hệ thống lưu trữ dữ liệu chứng chỉ CR là một cơ sở dữ liệu quản lý và lưu trữ toàn bộ các chứng chỉ đã cấp và các danh sách chứng chỉ thu hồi CRL, cho phép truy cập trực tuyến để xác thực tính hợp lệ của một chứng chỉ. Có hai phương pháp phân phối chứng chỉ:

#### Phân phối cá nhân

Phân phối cá nhân là cách phân phối cơ bản nhất. Trong phương pháp này, mỗi cá nhân sẽ trực tiếp đưa chứng chỉ của họ cho người dùng khác. Cách này thực hiện tốt trong một nhóm ít người dùng, nhưng khi số lượng người dùng tăng lên thì có thể xảy ra vấn đề về quản lý.

#### Phân phối công khai

Một phương pháp khác phổ biến hơn để phân phối chứng chỉ và thông tin thu hồi chứng chỉ là công bố các chứng chỉ rộng rãi, các chứng chỉ này có thể sử dụng một cách công khai và được đặt ở vị trí có thể truy cập dễ dàng. Những vị trí này được gọi là cơ sở dữ liệu.

Ví dụ:

X.500 Directory System Agents (DSAs).

Lightweight Directory Access Protocol (LDAP) Server.

Online Cerfiticate Status Protocol (OCSP) Responders.

Domain name System (DNS) và Web servers.

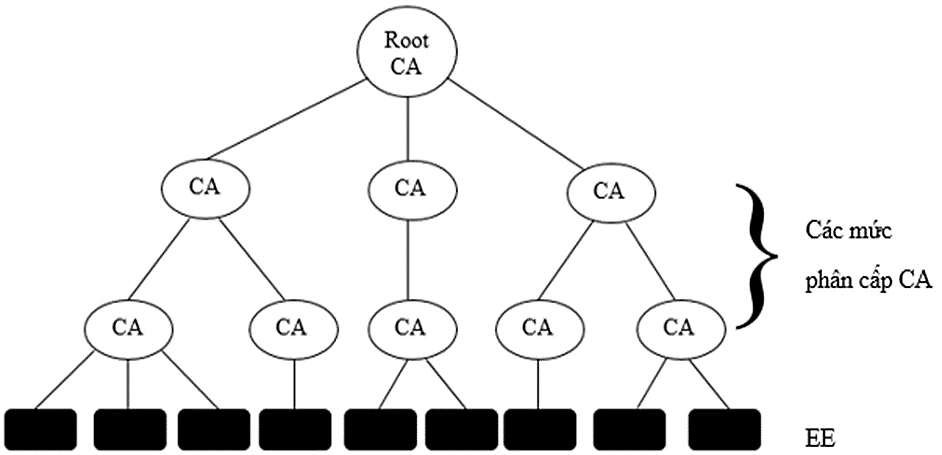
File Transfer Protocol (FPT) Servers và Corporate Databases.

## Các mô hình tin cậy PKI

### Mô hình phân cấp các CA

Mô hình phân cấp các CA (Strict Hierarchy of CAs) còn được gọi là mô hình tin cậy phân cấp (Hierarchical Trust Model). Trong mô hình này, PKI có một CA là CA gốc (RCA) đứng ở vị trí cao nhất. Các CA bên dưới RCA được gọi là CA trung gian (intermediate CA) hay CA cấp dưới (subordiate CA) và không bắt buộc trong phân cấp. Mỗi CA trung gian có thể nhận các CA ngay bên dưới nó.

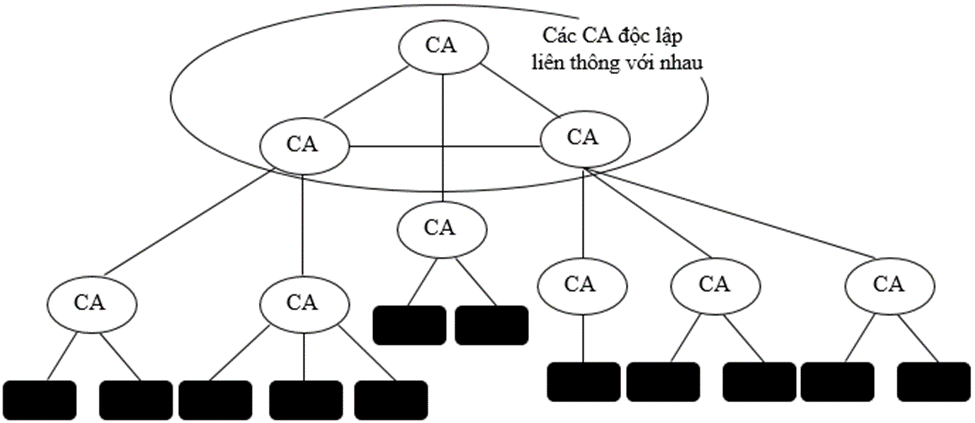
Với mô hình này, có thể đơn giản việc thêm một CA mới do mỗi CA có một cấp trên nên việc xử lý đường dẫn chứng thực dễ dàng. Mỗi CA cấp dưới kế thừa chính sách và quy chế của CA cấp trên dẫn đến việc liên thông và quản trị không phức tạp.



* + - * 1. Mô hình tin cậy phân cấp

### Mô hình tin cậy kiến trúc phân tán

Mô hình tin cậy kiến trúc phân tán (Distributed Trust Architecture) còn được gọi là mô hình tin cậy phân tán (Distributed Trust Model). Thay bằng việc tin cậy một CA gốc duy nhất, một mô hình trải rộng sự tin cậy tới nhiều CA gốc. Mô hình này còn được gọi là mô hình ngang hàng (peer-to-peer model) do mỗi CA gốc hoạt động độc lập và tương đương nhau.



* + - * 1. Mô hình tin cậy phân tán

### Mô hình Web

Mô hình Web (Web Model) được lấy ra từ tên của nó (www), xuất phát từ thực tế một số trình duyệt Web đã cài đặt một bộ các khóa công khai mà người dùng trình duyệt tin tưởng như là các gốc để xác thực các chứng chỉ.

Danh sách tin cậy phần lớn được sử dụng để xác thực web server mà những server này được CA xác nhận trong danh sách trình duyệt Client. Quá trình này được thực hiện một cách tự động với các giao thức SSL. Nó đơn giản trong việc thực thi và đối với người dùng. Dẫn đến khả năng để triển khai nhanh. Và nó đặc biệt thích hợp cho yêu cầu PKI của những ứng dụng dựa trên Web.

Khả năng xử lý đường dẫn chứng thực của các trình duyệt Web hiện nay tương đối bị giới hạn. Nó có khả năng hạn chế trong việc lấy một chứng chỉ từ một thư mục LDAP theo yêu cầu của người dùng và không có khả năng tìm một đường dẫn chứng thực gồm nhiều bước một cách tự động.

Ưu điểm:

Dễ triển khai vì danh sách đã có trong trình duyệt.

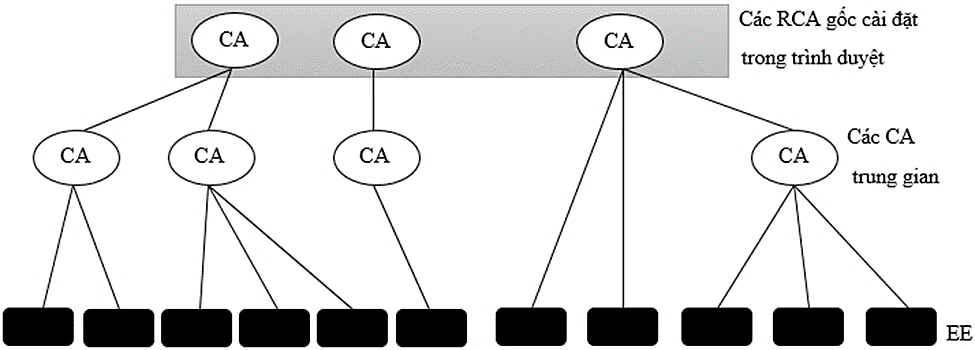
Không cần thay đổi khi làm việc với trình duyệt Web (Internet Explorer) và tiện ích e-mail (Microsoft Outlook).

Nhược điểm:

Về mật công nghệ có thể thêm hay sửa đổi một root CA mới nhưng hầu hết người dùng trình duyệt lại không quen thuộc với công nghệ PKI và phụ thuộc vào những CA trong trình duyệt này.

Hiện nay chưa có cách để phân biệt mức độ xác thực giữa các chứng chỉ.

Không thể thông báo đến tất cả các trình duyệt của người sử dụng nếu khóa công khai của một CA bị xâm hại.



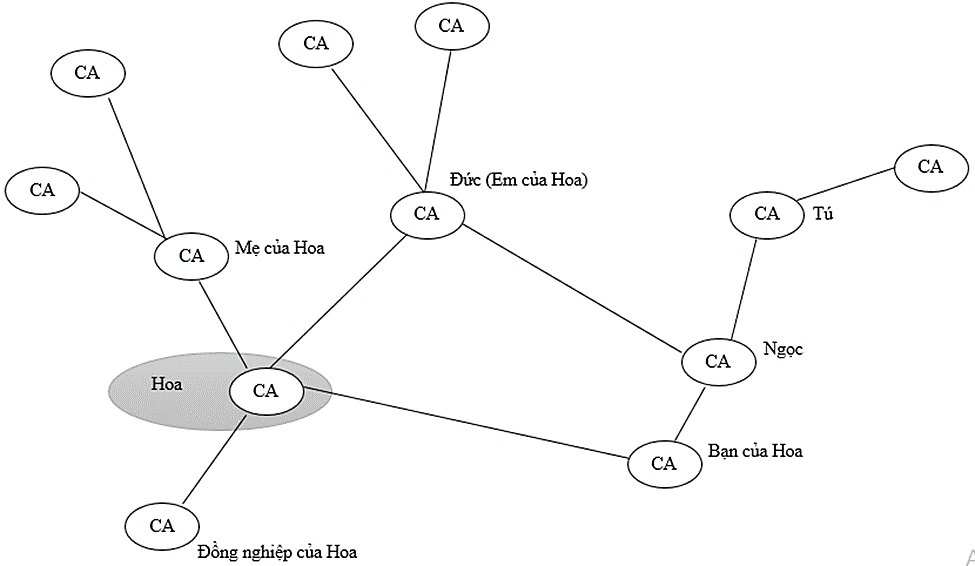
* + - * 1. Mô hình Web

### Mô hình tin cậy tâm điểm người dùng

Mô hình tin cậy tâm điểm người dùng (User Centric Trust) còn được gọi là “Web of Trust”. Trong mô hình này, mỗi người sử dụng trực tiếp và hoàn toàn có trách nhiệm trong việc quyết định tin tưởng hay từ chối chứng chỉ. Mỗi người sử dụng giữ một khóa vòng và khóa này đóng vai trò như một CA của họ.

Khóa vòng chứa khóa công khai được tin cậy của những người sử dụng khác trong cộng đồng. Đây là mô hình tin cậy tích lũy, trong đó một chứng chỉ có thể được tin cậy trực tiếp hoặc tin cậy qua một xâu chuỗi chứng chỉ tới một chứng chỉ gốc được tin cậy trực tiếp.

Các khóa tin cậy ban đầu thường là của các đối tượng mà người dùng biết theo cá nhân như bạn bè, gia đình, đồng nghiệp. Nó đã được triển khai trong chương trình phần mềm an toàn Pretty Good Privacy (PGP). Tuy nhiên, mô hình này không phù hợp với những cộng đồng đòi hỏi kiểm soát tin cậy người dùng theo kiểu tập trung như các cơ quan nhà nước và người sử dụng, do nó dựa vào sự tin cậy của cá nhân hơn là sự tin cậy của công chúng. Hiện nay, chưa có kiến trúc PKI dựa trên chứng chỉ X.509 nào áp dụng mô hình tin cậy này.



* + - * 1. Mô hình tin cậy tâm điểm người dùng

## Kiến trúc PKI

Tùy vào các yêu cầu, quy mô và khả năng của từng tổ chức mà có thể chọn triển khai một trong những mô hình PKI phổ biến sau:

Kiến trúc CA đơn (Simple PKI Architecture).

Kiến trúc phân cấp (Hierarchial PKI)

Kiến trúc mắt lưới (Mesh PKI)

Kiến trúc PKI doanh nghiệp chứng thực chéo

Kiến trúc CA cầu nối

Kiến trúc danh sách tin cậy mở rộng

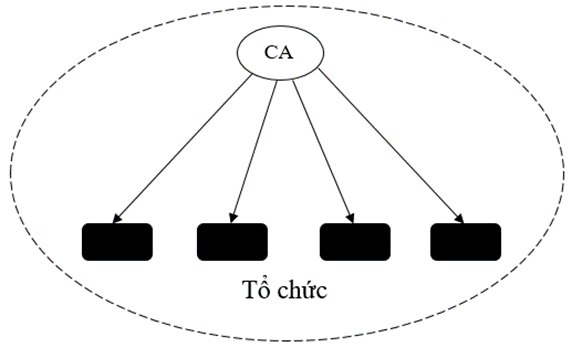
### Kiến trúc CA đơn

#### Kiến trúc một CA đơn (Single CA)

Đây là kiến trúc cơ bản nhất, phù hợp với các tổ chức nhỏ. Trong đó, chỉ có một CA cung cấp dịch vụ cho toàn hệ thống và tất cả người dùng đặt sự tin cậy vào CA này. Mọi thực thể muốn tham gia vào PKI và xin cấp chứng chỉ đều phải thông qua CA duy nhất này.

Kiến trúc dễ phát triển và triển khai nhưng có một số hạn chế riêng:

* Khả năng co giãn – khi quy mô tổ chức được mở rộng, chỉ có một CA thì khó quản lý chứng chỉ và đáp ứng tốt dịch vụ.
* Là điểm chịu lỗi duy nhất – nếu nó ngưng hoạt động thì cả hệ thống sẽ bị tê liệt.
* Xảy ra nguy hiểm nếu khóa tin cậy bị xâm hại và tất cả các chứng chỉ số này phải được cấp lại nếu CA này phục hồi.

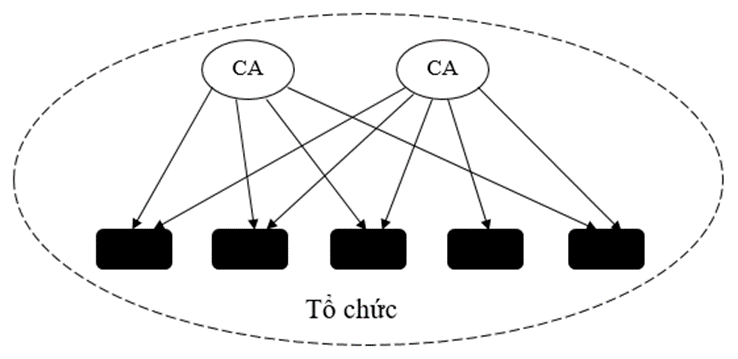


* + - * 1. Kiến trúc PKI với một CA đơn

#### Kiến trúc danh sách tin cậy cơ bản (Basic Trust CA)

Khi số lượng người dùng trong tổ chức tăng lên, việc quản lý và xác minh trở nên phức tạp và đòi hỏi nhiều thời gian hơn đối với một CA riêng lẻ. Giải pháp để giải quyết vấn đề này là đưa nhiều CA vào trong cấu trúc.

Với nhiều CA người dùng có thể yêu cầu chứng chỉ từ nhiều CA. Nhưng các CA này không có quan hệ tin cậy với nhau. Nên trong kiến trúc này, người dùng cần nắm giữ một danh sách các CA tin cậy.



* + - * 1. Kiến trúc danh sách tin cậy cơ bản

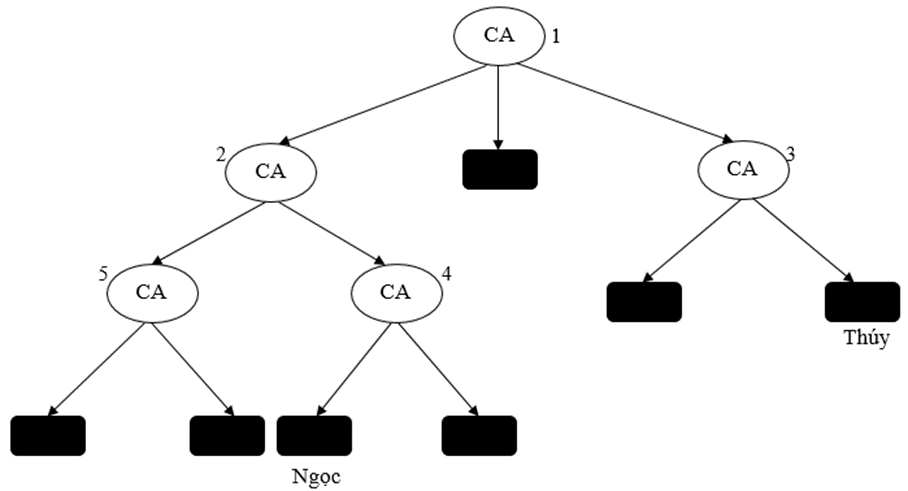
### Kiến trúc phân cấp

Đây là kiến trúc PKI phổ biến nhất. Nó còn được gọi là kiến trúc phân cấp đơn gốc (single root hierarchy) hay phân cấp thứ bậc (subordinated hierarchy). Kiến trúc này tương ứng với mô hình phân cấp (CA gốc và các CA cấp dưới).

CA gốc chứng thực các CA cấp ngay dưới nó và tiếp tục các CA cấp dưới này lại chứng thực CA cấp dưới của mình. Mỗi CA đóng một vai trò cụ thể tùy theo vị trí của CA trong kiến trúc phân cấp. Những vai trò thông thường là CA gốc, CA chính sách (policy CA), CA phát hành (issuing CA).

Các CA chính sách thường nằm ở tầng hai của cấu trúc phân cấp. Nó mô tả chính sách và thủ tục mà một tổ chức cần thực hiện để đảm bảo an toàn cho kiến trúc PKI, tiến trình xác nhận tính hợp lệ, tiến trình quản lý chứng chỉ. Nó chỉ phát hành chứng chỉ cho các CA khác, các CA nhận chứng chỉ này phải duy trì và thực thi các chính sách do CA chính sách đặt ra.

Các CA phát hành thường nằm ở tầng thấp nhất của cấu trúc phân cấp. Nó cấp chứng chỉ cho các thực thể cuối EE như máy tính, người sử dụng, thiết bị mạng, dịch vụ hoặc các CA phát hành khác. Nó thực thi các chính sách và thủ tục do CA chính sách đặt ra (luôn trực tuyến). Và bất kỳ một chứng chỉ nào cũng có thể được xác minh thông qua việc xác minh đường dẫn chứng thực chỉ ngược về CA gốc. Ví dụ: Thúy xác minh chứng chỉ của Ngọc được phát hành bởi CA 4, sau đó xác minh chứng chỉ của CA 4 được phát hành bởi CA 2 và chứng chỉ của CA 2 được phát hành bởi CA 1 là CA gốc có khóa công khai mà Thúy biết.



* + - * 1. Kiến trúc PKI phân cấp

Ưu điểm:

Dễ vận hành giữa các tổ chức khác nhau nên rất phù hợp khi áp dụng vào các tổ chức như các cơ quan Chính phủ, quân đội, các doanh nghiệp.

Mô hình gọn gàng, ngăn nắp, cho phép kiểm soát chặt chẽ các chứng chỉ phát hành.

Nhược điểm:

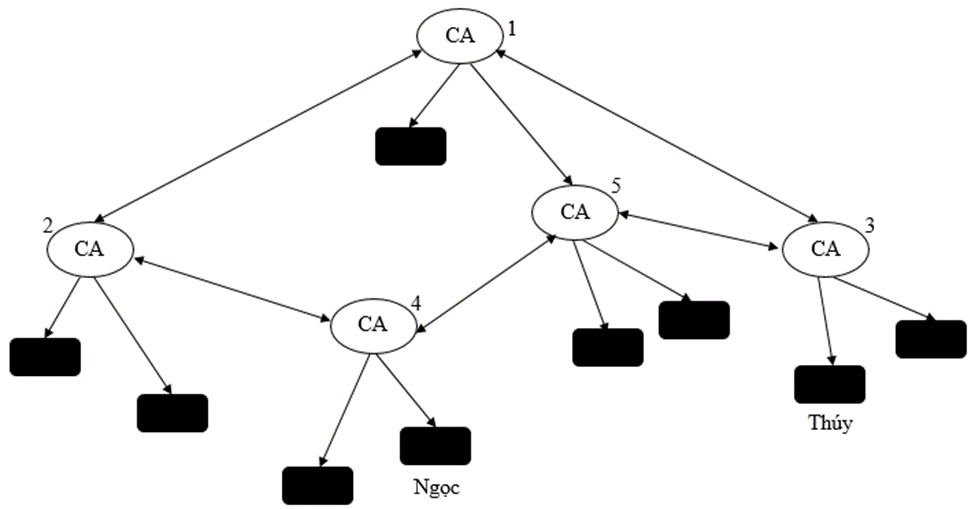
Không thể áp dụng trên toàn thế giới chỉ với một CA gốc.

Có thể không thích hợp cho những mối quan hệ ngang hàng giữa Chính phủ và doanh nghiệp và các quan hệ tin cậy thương mại, kinh doanh cũng không cần thiết phải phân cấp.

Dễ đổ vỡ nếu có khủng hoảng về sự tin cậy ở mức trên của tháp sẽ ảnh hưởng nặng đến tháp ơ mức dưới.

### Kiến trúc mắt lưới

Kiến trúc mắt lưới còn được gọi là peer-to-peer hay networked model. Các CA chứng thực chéo lẫn nhau để tạo thành một mạng mắt lưới các quan hệ tin cậy hai chiều giữa các CA và không có một CA cụ thể nào được tất cả các thực thể tin cậy mà mỗi CA trong một PKI mắt lưới đều là điểm tin cậy của PKI. Một thực thể cuối có thể chọn bất kỳ CA nào trong kiến trúc PKI để tin cậy.



* + - * 1. Kiến trúc PKI mắt lưới

Ví dụ: Thúy biết khóa công khai của CA 3, trong khi Ngọc biết khóa công khai của CA 4. Có một vài đường dẫn chứng chỉ từ Ngọc về Thúy, nhưng đường ngắn nhất yêu cầu Thúy xác minh chứng chỉ của Ngọc được phát hành bởi CA 4 là xác minh chứng chỉ của CA 4 được phát hành bởi CA 5 và CA 5 được phát hành bởi CA 3 là CA mà Thúy tin cậy và biết khóa công khai.

Ưu điểm:

Tương đối linh hoạt và phù hợp với các nhu cầu giao dịch như hiện nay, tạo điều kiện hình thành các quan hệ tin cậy phi thể thức, các quan hệ song phương.

Cho phép cạnh tranh.

Cho phép những nhóm người sử dụng khác nhau có thể tự do phát triển và thực thi những chính sách và chuẩn khác nhau.

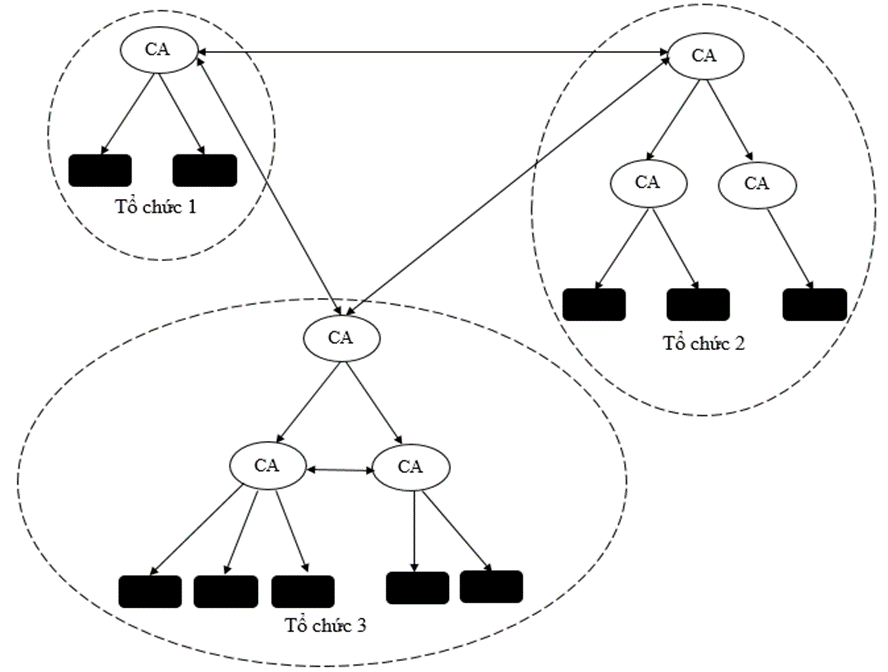
Khắc phục được những nhược điểm của mô hình phân cấp.

Nhược điểm:

Phức tạp và khó quản lý vì việc xác thực chéo.

Một người dùng không thể cung cấp đường dẫn chứng chỉ đảm bảo cho tất cả người dùng khác của PKI có thể sử dụng để xác minh.

### Kiến trúc PKI doanh nghiệp chứng thực chéo (kiến trúc lai)



* + - * 1. Kiến trúc PKI doanh nghiệp chứng thực chéo

Kiến trúc lai có các đặc điểm sau:

Tồn tại nhiều CA gốc.

Tất cả các CA không phải là gốc vẫn được chứng thực trong một phân cấp CA gốc.

Cho phép có các chứng thực chéo chọn lọc giữa các CA không phải là gốc.

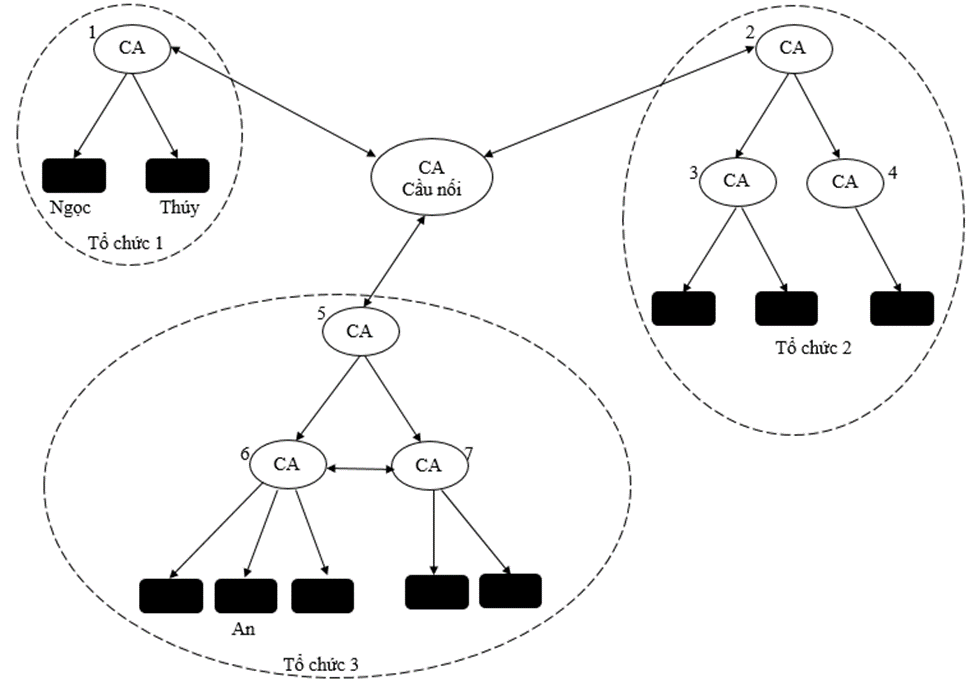
Kiến trúc này cho phép cắt ngắn chiều dài của chuỗi xác minh. Nó phù hợp với các môi trường mà các tổ chức thông tin không có quan hệ phân cấp với nhau, nhưng cũng có thể áp dụng mô hình cấu trúc phân cấp.

Ưu điểm:

Khả năng xây dựng các đường dẫn theo mong muốn là đơn giản hơn.

Khả năng thực hiện các chứng thực chéo trực tiếp rút ngắn đối với các đường dẫn thường sử dụng.

### Kiến trúc CA cầu nối



* + - * 1. Kiến trúc PKI CA cầu nối

Đây là kiến trúc PKI mở, trong đó các CA thiết lập quan hệ tin cậy với nhau thông qua CA cầu nối (bridge CA). CA cầu nối là một cơ quan chứng thực chéo ở trung tâm, quan hệ trực tiếp với tất cả các đối tác và làm nhiệm vụ thiết lập quan hệ tin cậy giữa các đối tác đó. Nhờ vậy, các đối tác mới dễ dàng gia nhập hệ thống mà không cần thiết phải thực hiện một loạt các quá trình cấp phát chứng chỉ trực tiếp với các CA khác. Nó sẽ thiết lập quan hệ với các CA gốc của PKI kiến trúc phân cấp hoặc chỉ một CA trong kiến trúc mắt lưới. Các CA tham gia vào quan hệ tin cậy với CA cầu nối được gọi là CA chính (principle CA).

### Kiến trúc danh sách tin cậy mở rộng

Trong kiến trúc này, mọi người dùng thuộc PKI đều lưu trữ một danh sách mở rộng của tất cả các điểm tin cậy trong cấu trúc của những tổ chức khác (một CA đơn, nhiều hơn một CA đơn, tất cả những CA của các tổ chức khác) làm điểm tin cậy cho chính mình.

Ưu điểm:

Đơn giản, dễ triển khai dẫn đến tăng tốc độ xử lý.

Người dùng đầu cuối kiểm soát toàn bọ danh sách CA tin tưởng.

Nhược điểm:

Khó khăn trong việc quản lý và ngăn ngừa người dùng cá nhân thay đổi danh sách các CA tin cậy.

Không hỗ trợ cho chứng thực chéo dẫn đến hạn chế vai trò CA trong việc quản lý tin cậy và không hỗ trợ về chính sách chứng chỉ.

Tóm tắt các kiến trúc của PKI

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Đặc điểm | Phân cấp | Mắt lưới | Lai | CA cầu nối | Danh sách tin cậy mở rộng |
| Neo tin cậy | CA gốc | CA nội bộ | CA gốc hoặc CA nội bộ | CA nội bộ | CA tin cậy trong danh sách tin cậy |
| Tương tác liên vùng | Kém khi vượt quá gốc chung | Tốt | Tốt | Rất tốt | Tốt |
| Xây dựng đường dẫn chứng thực | Đơn giản (chỉ cần đi từ gốc xuống) | Khó khăn (do có thể có nhiều đường đi đến một nguồn) | Trung bình (có thể có nhiều đường đi nhưng đường đơn giản) | Đơn giản (do tất cả các đường không phải là đường đi cục bộ thì đều qua CA cầu nối) | Đơn giản (danh sách chứng chỉ tin cậy đã được sắp đặt theo trật tự từ trước) |
| Sự phụ thuộc vào hệ thống chứng chỉ | Thấp | Cao | Trung bình | Trung bình | Trung bình |
| Cách phát triển của kiến trúc | Từ trên xuống dưới | Nối với các CA | Từ trên xuống dưới hoặc nối với các CA | Nối với CA cầu nối | Phát hành và cập nhật lại danh sách tin cậy |

## Ứng dụng của PKI

* Open PGP: mã hóa email và chứng thực người gửi email.
* Mã hóa và xác thực văn bản.
* Chứng thực người dùng ứng dụng: đăng nhập bằng smartcard, trong SSL.
* Trong các giao thức truyền thông an toàn.

# ỨNG DỤNG MÃ HÓA KHÓA CÔNG KHAI VÀO HỆ THỐNG QUẢN LÝ ĐIỂM CỦA CTU

## Giới thiệu hệ thống quản lý điểm của CTU

Hệ thống quản lý điểm sinh viên là một trong những hệ thống được quan tâm nhất trong hệ thống giáo dục hiện nay. Việc tin học hóa sẽ làm cho các công việc trở nên dễ dàng, chính xác, có tính chuyên nghiệp và tính bảo mật cao đối với các người sử dụng khác nhau. Hơn nữa, chiến lược tin học hóa ngành giáo dục, hiện đại hóa phương pháp quản lý sinh viên thật sự rất cần thiết, mà các trường phải đề ra trong định hướng phát triển của trường mình. Và hiện nay, CTU đã tin học hóa việc quản lý và xây dựng hệ thống quản lý điểm với các chức năng chính như sau: xem thông tin cá nhân, quản lý điểm, quản lý tài sản, quản lý ô tô, xem thời khóa biểu và khối lượng giảng dạy… nhưng ở đây chúng ta chỉ đề cập đến vấn đề quản lý điểm của sinh viên.

Hệ thống sẽ lấy danh sách sinh viên đã đăng ký lớp học phần mở trong một học kỳ để import vào hệ thống quản lý điểm của cán bộ phụ trách giảng dạy học phần đó. Sau khi kết thúc một học kỳ, cán bộ giảng dạy sẽ phải nhập và khóa điểm để gửi thông tin điểm của sinh viên về hệ thống cấp cao hơn.

Dữ liệu điểm số của sinh viên là rất quan trọng, tuy nhiên thì hiện nay chưa có một giải pháp để đảm bảo tính toàn vẹn của dữ liệu trên hệ thống này. Sau khi khóa điểm thì cán bộ giảng dạy không có quyền sửa điểm nhưng còn rất nhiều cấp quản lý có thể truy cập vào, thậm chí còn có cả những quản trị hệ thống, những người bảo trì, nâng cấp,...

Để giúp cho việc xác minh trở nên đơn giản và bảo mật hơn, em đã xây dựng hệ thống với mục tiêu: hệ thống sẽ vận hành đơn giản, tương tự hệ thống đã có sẵn.

## Yêu cầu hệ thống

Hệ thống phải đảm bảo lưu trữ tất cả chi tiết về thông tin sinh viên (họ tên, mã số sinh viên, điểm, lớp, giới tính,…) một cách chính xác và tin cậy, giao diện thân thiện, dễ sử dụng, xử lý dữ liệu nhanh chóng. Đảm bảo độ bảo mật cho hệ thống. Với những mục tiêu đặt ra của đề tài, phương pháp - công cụ để xây dựng và phát triển hệ thống được trình bày dưới đây. Nó giúp chứng minh tính toàn vẹn của dữ liệu và tính không chối bỏ.

Xây dựng mô hình phân cấp chức năng cho ta cái nhìn tổng quát về các chức năng của hệ thống, nó giúp xác định phạm vi nghiên cứu. Qua khảo sát thực trạng và tìm hiểu yêu cầu thực tế, em đã thiết kế hệ thống với sơ đồ phân cấp chức năng bên dưới. Nó sẽ đáp ứng những chức năng cơ bản thuộc hai phân hệ người dùng khác nhau như sau:

* Người quản lý :
* Xem thông tin bảng điểm.
* Xem khóa công khai của từng giảng viên.
* Giảng viên :
* Nhập và chỉnh sửa điểm của sinh viên.
* Tạo cặp khóa (bí mật và công khai) cho giảng viên.
* Khóa quyền nhập điểm của giảng viên.

Quản lý điểm

Giảng viên

Người quản lý

Đăng nhập

Nhập thông tin điểm cho từng môn

Sửa thông tin điểm

Đăng nhập

Xem khóa

Tạo khóa

Khóa quyền nhập điểm

Xem thông tin điểm từng môn

* + - * 1. Mô hình phân cấp chức năng của hệ thống quản lý điểm

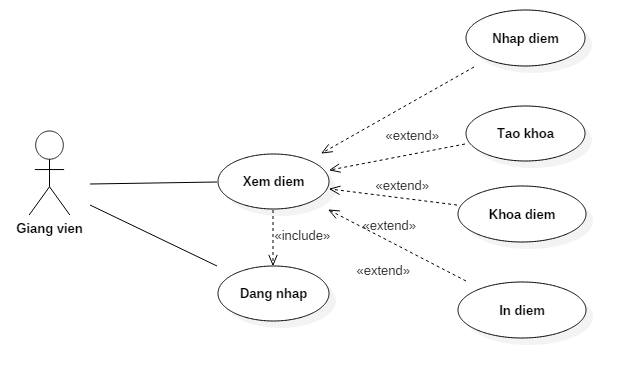
## Thiết kế hệ thống

### Xác định chức năng

#### Giảng viên

Giảng viên khi đăng nhập vào hệ thống sẽ được thiết lập các quyền:

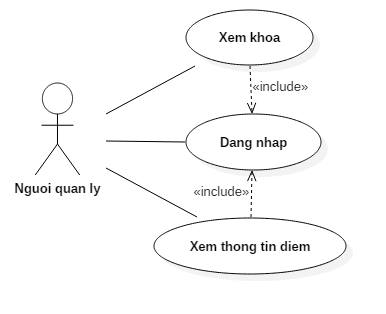
* Nhập thông tin điểm cho từng môn học, nếu quá trình nhập điểm xảy ra sai sót, giảng viên có thể chỉnh sửa điểm với điều kiện giảng viên đó chưa xác nhận khóa điểm. Ngược lại, nếu giảng viên đã xác nhận khóa điểm thì mặc nhiên hệ thống sẽ khóa quyền nhập cũng như chỉnh sửa điểm của giảng viên.
* Sau khi chắc chắn tất cả thông tin điểm đã đúng hoàn toàn thì giảng viên sẽ khóa điểm bằng cách nhập khóa mà giảng viên đăng ký với hệ thống chứng chỉ. Nếu nhập đúng, hệ thống sẽ dùng khóa bí mật để mã hóa thông tin và gửi về trang admin của người quản lý.
* Nếu giảng viên chưa có khóa bí mật và khóa công khai, hệ thống sẽ tự động cấp phát khóa cho giảng viên để kết thúc được quá trình khóa điểm.
* Giảng viên cũng có thể in thông tin học phần nếu cần phục vụ cho công tác giảng dạy.



* + - * 1. Sơ đồ usecase (giảng viên)

#### Người quản lý

Người quản lý khi đăng nhập vào hệ thống sẽ có các quyền :

* Xem khóa công khai của từng giảng viên để biết được giảng viên nào đã có cặp khóa công khai/ bí mật.
* Xem thông tin điểm từng môn của giảng viên thông qua việc áp dụng cơ chế hoạt động của giải thuật RSA, họ sẽ dùng khóa công khai để giải mã bảng điểm nhằm kiểm tra tính toàn vẹn dữ liệu khi giảng viên đã xác nhận ký vào bảng điểm.
* Nếu giảng viên dạy học phần đó chưa khóa điểm thì người quản lý sẽ không xem được file điểm vì hệ thống chưa kết nối với cơ sở dữ liệu để export ra file điểm.
* Nếu giảng viên đó đã khóa quyền nhập điểm thì người quản lý có thể xem thông tin điểm của từng môn học, có thể in bảng điểm ra nếu muốn.
  + - * 1. Sơ đồ usecase (người quản lý)

### Thiết kế cơ sở dữ liệu

#### Mô hình khái niệm

**Mô hình thực thể đơn**:

Quyền học phần

Quyền học phần

Lớp học phần

Tên học phần

Nhóm học

Điểm số

Lớp

Tên lớp

Học phần

Tên học phần

Sinh viên

mssv

Họ tên

Giới tính

Giảng viên

mscb

Họ tên

Giới tính

Email

Chữ ký

File điểm

Nội dung file

#### Mối quan hệ giữa các thực thể:

Học phần

Tên học phần

Lớp học phần

Tên học phần

Nhóm học

Điểm số

Giảng viên

mscb

Họ tên

Giới tính

Email

Chữ ký

Sinh viên

mssv

Họ tên

Giới tính

Lớp học phần

Tên học phần

Nhóm học

Điểm số

Lớp học phần

Tên học phần

Nhóm học

Điểm số

Quyền học phần

Quyền học phần

File điểm

Nội dung file

Lớp học phần

Tên học phần

Nhóm học

Điểm số

Sinh viên

mssv

Họ tên

Giới tính

Lớp

Tên lớp

#### Mối quan hệ tổng quát giữa các thực thể:

* + - * 1. Mô hình khái niệm

#### Mô hình thực thể kết hợp (EER Diagram)

* + - * 1. Mô hình thực thể kết hợp

Mối liên kết giữa các thực thể :

* Liên kết giữa thực thể học phần (hocphan) và thực thể lớp học phần (lophocphan) là kiểu liên kết nhiều – một thông qua thuộc tính hp\_id. Vì một học phần có thể có nhiều lớp học phần, nhưng một lớp học phần chỉ có thể thuộc một học phần nào đó.
* Liên kết giữa thực thể quyền học phần (quyenhocphan) và thực thể lớp học phần (lophocphan) là kiểu liên kết một – một thông qua thuộc tính hp\_id và gv\_id. Vì một giảng viên chỉ có một quyền trên một lớp học phần và một lớp học phần nào đó chỉ thuộc về một giảng viên giảng dạy.
* Liên kết giữa thực thể giảng dạy (giangday) và thực thể lớp học phần (lophocphan) là kiểu liên kết một – nhiều thông qua thuộc tính gv\_id. Vì một giảng viên có thể dạy nhiều lớp học, nhưng một lớp học phần chỉ có thể thuộc một giảng viên nào đó.
* Liên kết giữa thực thể file điểm (filediem) và thực thể lớp học phần (lophocphan) là kiểu liên kết một – một thông qua thuộc tính hp\_id và gv\_id. Vì một giảng viên chỉ có một file điểm trên một lớp học phần và một lớp học phần nào đó chỉ có một file điểm thuộc về một giảng viên giảng dạy.
* Liên kết giữa thực thể sinh viên (sinhvien) và thực thể lớp học phần (lophocphan) là kiểu liên kết một – nhiều thông qua thuộc tính sv\_id. Vì một sinh viên chỉ thuộc một lớp học phần, nhưng một lớp học phần có thể có nhiều sinh viên.

Liên kết giữa thực thể sinh viên (sinhvien) và thực thể lớp (lop) là kiểu liên kết một – nhiều thông qua thuộc tính lop\_id. Vì một sinh viên chỉ thuộc một lớp chuyên ngành nào đó, nhưng một lớp chuyên ngành có thể có nhiều sinh viên học.

#### Xây dựng cơ sở dữ liệu

Bảng giangvien (giảng viên và admin)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tính chất** | **Tên trường** | **Kiểu dữ liệu** | **Kích thước** | **Chú thích** |
| Primary key | gv\_id | Int | 10 | AUTO\_INCREMENT |
| Unique | gv\_mscb | Varchar | 15 |  |
|  | gv\_matkhau | Varchar | 100 | MD5 |
|  | gv\_ten | Varchar | 255 |  |
|  | gv\_email | Varchar | 100 |  |
|  | gv\_passchuky | Varchar | 100 | MD5 |

Bảng hocphan (học phần)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tính chất** | **Tên trường** | **Kiểu dữ liệu** | **Kích thước** | **Chú thích** |
| Primary key | hp\_id | Int | 10 | AUTO\_INCREMENT |
|  | hp\_ma | Varchar | 100 |  |
|  | hp\_ten | Varchar | 255 |  |

Bảng lophocphan (lớp học phần)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tính chất** | **Tên trường** | **Kiểu dữ liệu** | **Kích thước** | **Chú thích** |
| Primary key | lhp\_id | Int | 10 | AUTO\_INCREMENT |
| Foreign key | hp\_id | Int | 10 |  |
| Foreign key | gv\_id | Int | 10 |  |
|  | lhp\_nhom | Varchar | 5 |  |
| Foreign key | sv\_id | Int | 10 |  |
|  | lhp\_diem | Float |  |  |

Bảng quyenhocphan (quyền học phần)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tính chất** | **Tên trường** | **Kiểu dữ liệu** | **Kích thước** | **Chú thích** |
| Primary key | qhp\_id | Int | 10 | AUTO\_INCREMENT |
| Foreign key | gv\_id | Int | 10 |  |
| Foreign key | hp\_id | Int | 10 |  |
|  | qhp\_quyen | Int | 11 |  |

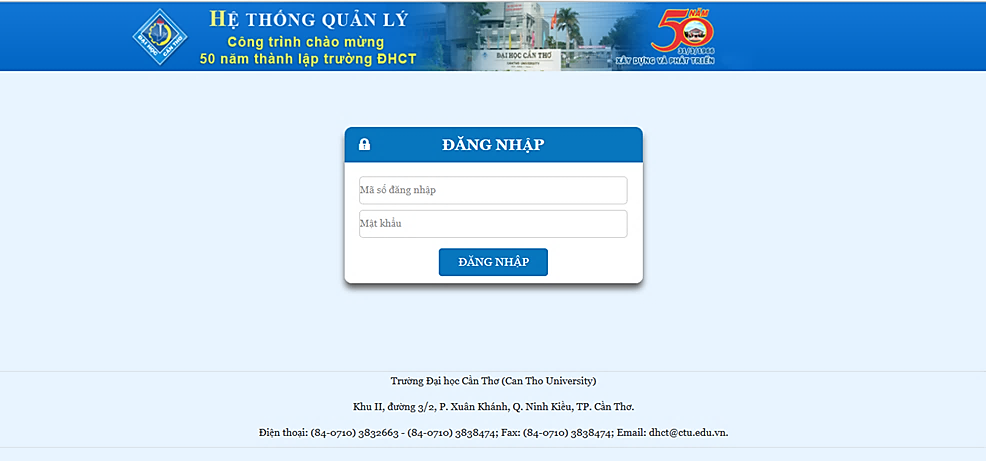
Bảng lop (lớp)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tính chất** | **Tên trường** | **Kiểu dữ liệu** | **Kích thước** | **Chú thích** |
| Primary key | lop\_id | Int | 10 | AUTO\_INCREMENT |
|  | lop\_ten | Varchar | 255 |  |

Bảng sinhvien (sinh viên)

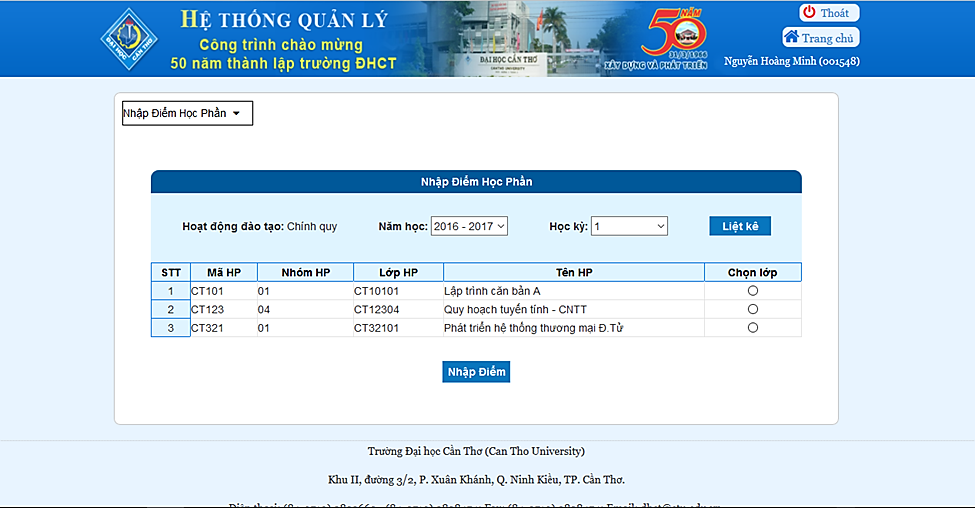
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tính chất** | **Tên trường** | **Kiểu dữ liệu** | **Kích thước** | **Chú thích** |
| Primary key | sv\_id | Int | 10 | AUTO\_INCREMENT |
| Foreign key | sv\_mssv | Varchar | 15 |  |
|  | sv\_holot | Varchar | 255 |  |
|  | sv\_ten | Varchar | 50 |  |
|  | sv\_nu | Varchar | 2 |  |
| Foreign key | lop\_id | Int | 10 |  |

## Kết quả



* + - * 1. Giao diện đăng nhập

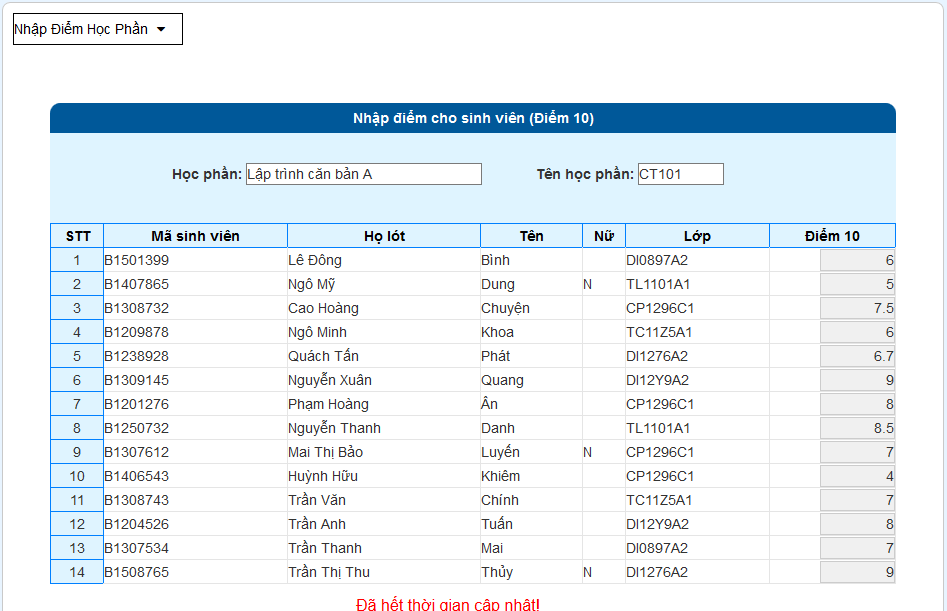
Giao diện đăng nhập giúp hệ thống nhận biết và phân quyền cho từng người dùng trong hệ thống. Để đăng nhập vào hệ thống, chúng ta sử dụng username và password được cung cấp riêng cho từng cán bộ. Khi đăng nhập sai, hệ thống sẽ có thông báo mời người dùng đăng nhập lại.

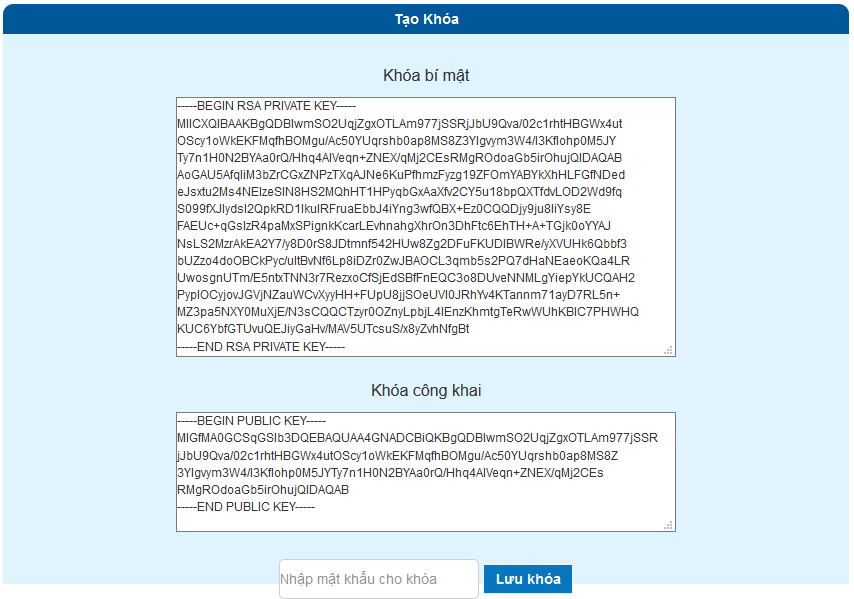
* + - * 1. Giao diện trang chủ

Sau khi đăng nhập theo quyền của cán bộ giảng dạy thành công. Tại đây, nó sẽ hiển thị thông tin các lớp học phần mà giảng viên giảng dạy trong một học kỳ.

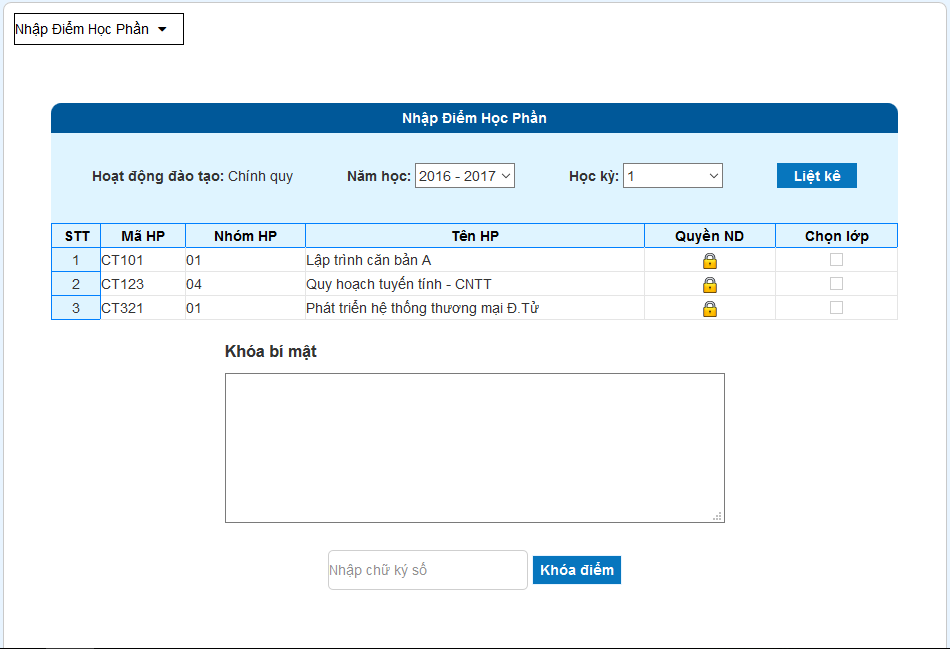
* + - * 1. Giao diện nhập và chỉnh sửa điểm

Giao diện nhập và chỉnh sửa điểm chỉ cho phép giảng viên làm việc với thông tin về điểm, những thông tin còn lại phụ thuộc vào sinh viên đăng ký lớp học phần và giảng viên giảng dạy.

* + - * 1. Giao diện sau khi đã khóa điểm

Giao diện sau khi khóa điểm sẽ không cho giảng viên được quyền chỉnh sửa điểm sau khi đã xác nhận khóa điểm ở giao diện khóa điểm.

* + - * 1. Giao diện tạo khóa

Giao diện tạo khóa hỗ trợ những cán bộ giảng dạy chưa có khóa bí mật và khóa công khai khi đăng nhập vào hệ thống sẽ được cung cấp khóa tự động và sau khi cung cấp, hệ thống sẽ tự import khóa công khai vào cơ sở dữ liệu. Ô nhập mật khẩu cho khóa dùng để yêu cầu giảng viên xác minh việc tạo khóa. Nếu không có mật khẩu ở khâu này, chúng ta không hoàn thành việc tạo khóa.

* + - * 1. Giao diện khóa điểm

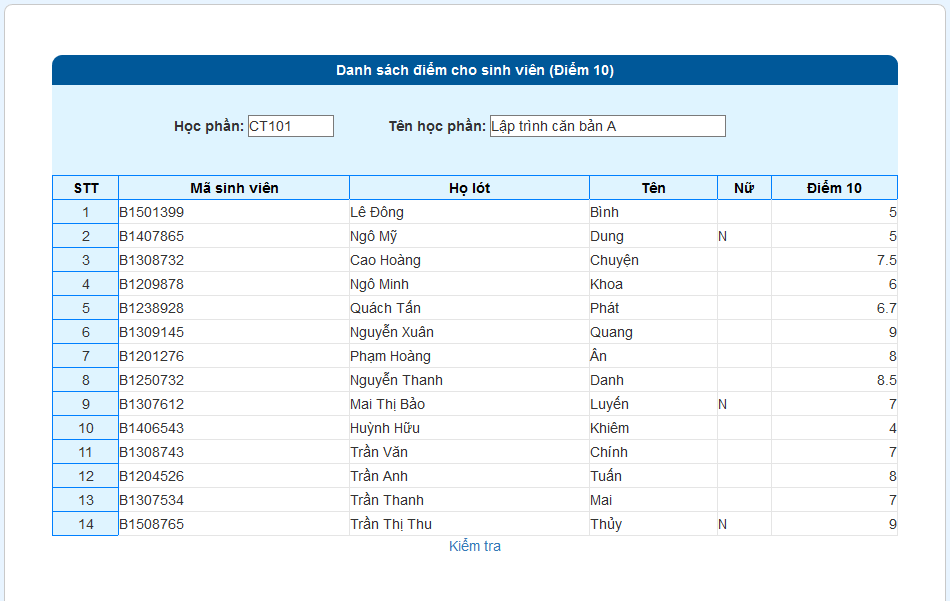
Giao diện khóa điểm sẽ khóa quyền nhập và chỉnh điểm khi giảng viên click vào lớp học phần muốn khóa và nhập đúng mật khẩu dùng để mã hóa khóa bí mật.

Hệ thống sẽ dùng mật khẩu được cung cấp để giải mã khóa bí mật đã được lưu trong cơ sở dữ liệu và dùng khóa này để tạo chữ ký cho bảng điểm. Nếu giảng viên nhập sai hoặc chọn khóa điểm mà chưa nhập mật khẩu, hệ thống sẽ có thông báo yêu cầu nhập lại.

* + - * 1. Giao diện trang chủ của admin

Giao diện xem điểm sẽ cho phép người quản lý xem điểm của từng lớp học phần thuộc từng giảng viên cụ thể nếu giảng viên đó đã khóa quyền nhập điểm; hệ thống sẽ hiển thị đường link để người quản lý có thể dễ dàng xem thông tin điểm mà giảng viên đã khóa.

Nếu giảng viên chưa khóa điểm thì hệ thống sẽ hiển thị dòng chữ ‘‘Chưa khóa’’

* + - * 1. Giao diện xem điểm

Giao diện xem điểm từng lớp học phần sẽ được hiển thị sau khi người quản lý click chuột vào ‘‘Xem điểm’’. Hệ thống sẽ hiển thị thông tin cơ bản của một lớp học phần trong danh sách lớp học phần.

Nếu quản lý nhấn vào kiểm tra, hệ thống sẽ dùng bảng điểm đang hiển thị đem so sánh với bảng điểm được khóa quyền xem điểm của giảng viên khi đã giải mã dữ liệu thành công, nếu nó trùng khớp thì dữ liệu sẽ không bị thay đổi, đồng thời nó sẽ xuất hiện bảng thông báo ‘’Dữ liệu toàn vẹn !’’.

Nếu nó không khớp với dữ liệu đã được giải mã, thì dữ liệu đã bị thay đổi sau quá trình khóa quyền nhập điểm của giảng viên.

# PHẦN KẾT LUẬN

## Kết quả đạt được

Đề tài “Tìm hiểu hệ thống mã hóa khóa công khai và ứng dụng trong hệ thống quản lý điểm của trường ĐHCT” cơ bản hoàn thành được các mục tiêu đã đề ra, cụ thể là:

Nghiên cứu hệ thống mã hóa khóa công khai và cơ sở hạ tầng khóa công khai PKI bao gồm: các thành phần, giải thuật, mô hình và cơ chế hoạt động của hệ thống mã hóa khóa công khai và các PKI.

Xây dựng mô hình quản lý điểm của sinh viên tại trường Đại học Cần Thơ, phân tích và áp dụng hệ thống mã hóa khóa công khai vào mô hình để chứng minh tính toàn vẹn dữ liệu và tính không thể chối bỏ.

Do hạn chế về thời gian và khả năng chuyên môn nên mô hình quản lý điểm của sinh viên hiện tại còn một số thiếu sót (tính chuyên nghiệp chưa cao, chức năng còn ít), cần được cải thiện để hoàn chỉnh hơn trong thời gian tới. Vì vậy, em hy vọng nhận được nhiều sự cổ vũ cũng như các ý kiến đóng góp của các thầy cô và các bạn.

## Hướng phát triển của đề tài

Áp dụng mô hình này vào hệ thống thực tế. Ngoài ra, tiếp tục nghiên cứu hạ tầng khóa công khai EJBCA và nối kết phần mềm này vào hệ thống quản lý điểm nhằm cho phép xin chứng thư từ hạ tầng khóa công khai này.

# TÀI LIỆU THAM KHẢO

1. Đỗ Xuân Bình,  *Chữ ký số, chứng chỉ số và cơ sở hạ tầng khóa công khai* NXB Bưu Điện - Hà Nội, 2007
2. Đặng Bình Phương, *“Nghiên cứu kiến trúc và xây dựng hệ thống chứng thực tập trung”*, Luận văn thạc sĩ, trường Đại học Khoa học Tự nhiên – Đại học Quốc gia TP.HCM, 2008
3. Hoàng Thị Thúy, *“ Nghiên cứu giải pháp xây dựng hệ thống cấp chứng chỉ số dựa trên hạ tầng khóa công khai”,* Luận văn thạc sĩ, trường Đại học Công nghệ thông tin và Truyền thông - Đại học Thái Nguyên, 2013
4. Nguyễn Ngộc Điệp, *“Tìm hiểu và triển khai hệ thống chứng thực khóa công khai sử dụng gói phần mềm mã nguồn mở EJBCA ứng dụng trong các giao dịch thương mại điện tử”,* Luận văn thạc sĩ, Học viện Công nghệ Bưu chính Viễn thông – Hà Nội, 2012
5. Nguyễn Huy Thắng, *“Nghiên cứu về chữ ký số và ứng dụng trong hóa đơn điện tử tại VNPT Hà Nội”*, Luận văn thạc sĩ, Học viện Công nghệ Bưu chính Viễn thông – Hà Nội, 2013
6. Lê Anh Tuấn, *“Nghiên cứu về hạ tầng khóa công khai PKI, ứng dụng vào bảo mật thông tin trong phần mềm quản lý bệnh viện”*, Luận văn thạc sĩ, Học viện Công nghệ Bưu chính Viễn thông – Hà Nội, 2013
7. Trần Quang Thuận, *“Nghiên cứu và xây dựng hạ tầng khóa công khai”*, Luận văn đại học, trường Đại học Công nghệ - Đại học Quốc gia Hà Nội, 2010
8. Enterprise Java Beans Certificate Authority at: https://www.ejbca.org/