# TỔNG QUAN PKI VÀ HỆ THỐNG CHỨNG THỰC

## Tổng quan về hạ tầng PKI

Cơ sở hạ tầng: các bộ phận thiết bị phụ thuộc tạo thành một cơ sở của một hệ thống hay các thiết bị cơ bản cố định của một nhà nước. Phân biệt khái niệm cơ sở hạ tầng trong triết học.

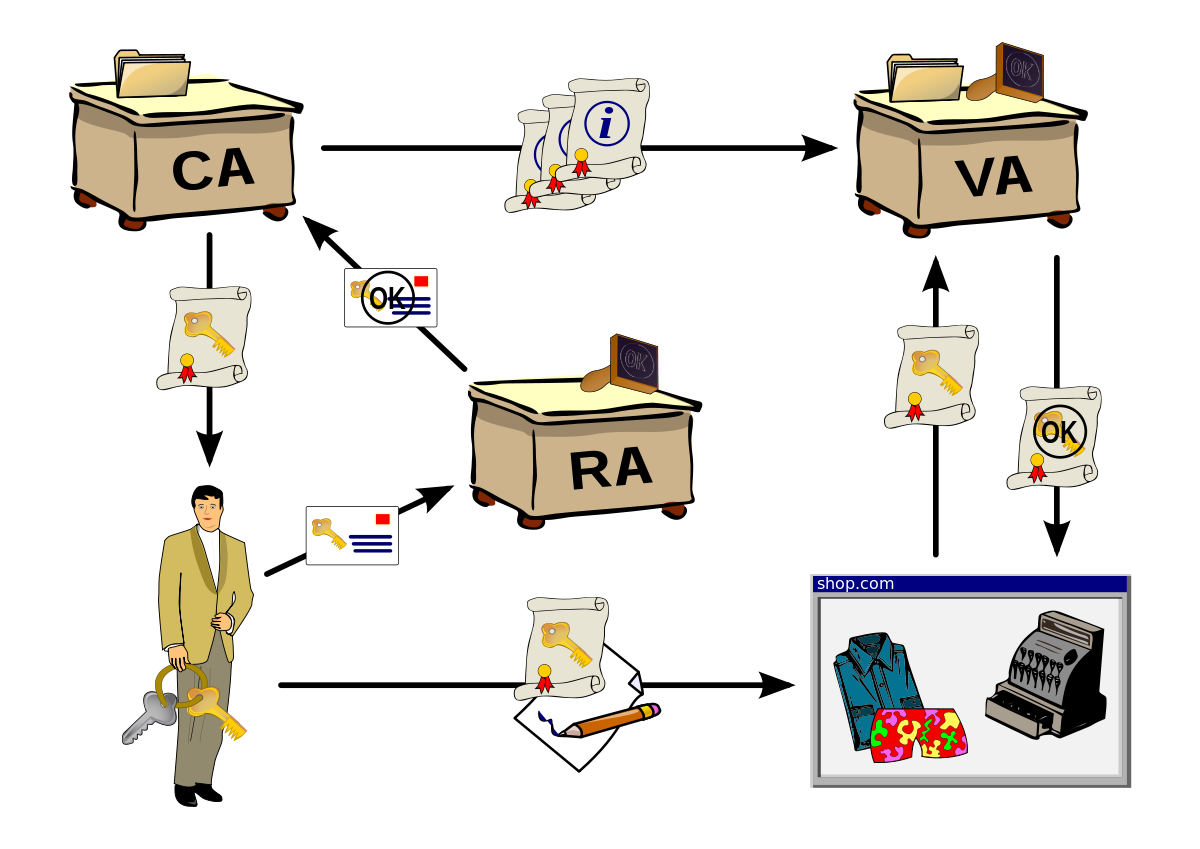
Đặc điểm hạ tầng:

* Lan tỏa rộng khắp (mạng điện, đường...), có thể sử dụng bất cứ khi nào.
* Hỗ trợ các ứng dụng (Trong suốt với người dùng, dễ nhận biết và sử dụng).

Cơ sở hạ tầng khóa công khai (Public Key Infrastructure – PKI) là một hạ tầng an toàn, an ninh mạng, sử dụng các kỹ thuật mật mã khoá công khai nhằm cung cấp các dịch vụ đảm bảo an toàn cho các giao dịch điện tử trên mạng. Mục tiêu chính của hạ tầng mật mã khóa công khai là cung cấp các dịch vụ nhằm đảm bảo an toàn cho các giao dịch điện tử.

Hệ thống chứng thực điện tử (số) là một hệ thống chứng nhận và khẳng định một căp khóa thuộc về một chủ thể xác định. Người dùng sử dụng cặp khóa đã chứng thực để đảm bảo an toàn cho các giao dịch điện tử trong môi trường mạng. Mục tiêu chính của hệ thống chứng thực là tạo ra các thực thể số được tin cậy, đối với những người dùng khác

## Các thành phần của PKI



Hình 1.1. Các thành phần của PKI

Hạ tầng khóa công khai (Public Key Infrastructure – PKI) hoạt động dựa trên mô hình client – server. Hạ tầng (Server) cung cấp dịch vụ các dịch vụ như CA, RA, VA. Client sử dụng dịch vụ bao gồm người dùng và thiết bị. Một hạ tầng khóa công khai PKI bao gồm các thành phần: Thẩm quyền chứng thực (Certificate Authority - CA), thẩm quyền đăng ký (Registration Authority - RA), thẩm quyền xác nhận (Validation Authority - VA) và thực thể cuối (Clients).

Thẩm quyền chứng thực (Certificate Authority – CA):

* Chức năng: Chứng thực cặp khóa thuộc hoặc không thuộc một thuê bao và quản lý vòng đời chứng thư số (cặp khóa) sau khi phát hành.
* Nhiệm vụ: Phát hành, gia hạn, tạm dừng/kích hoạt, thu hồi chứng thư số, khôi phục cặp khóa, phát hành CRL.

Thẩm quyền đăng ký (Registration Authority – RA):

* Xác định và xác thực: Đóng vai trò trung gian giữa CA và người dùng. Khi người dùng cần chứng thư số mới, họ gửi yêu cầu tới RA và RA sẽ xác nhận tất cả các thông tin nhận dạng cần thiết trước khi chuyển tiếp yêu cầu đó tới CA để CA thực hiện tạo và ký số lên chứng thư rồi gửi về cho RA hoặc gửi trực tiếp cho người dùng.
* Hỗ trợ người dùng cuối: tạo cặp khóa, quản lý người dùng và bàn giao kết quả.

Thẩm quyền xác nhận (Validation Authority – VA):

* Khẳng định tính hợp lệ và tin cậy của chứng thư số (cặp khóa). Kho công cộng chứa chứng thư số và CRL (LDAP), OCSP.
* Dịch vụ dấu thời gian (TimeStamp).

Thực thể cuối (Clients):

* Người dùng, thiết bị, sử dụng chứng thư số - relying party.
* Chủ thể sử hữu chứng thư số (thuê bao) – subscriber.

## Vai trò và chức năng của PKI

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

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

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

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

## Chứng thư số

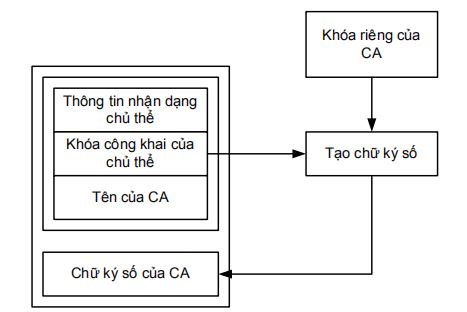
### Khái niệm chứng thư số

Chứng thư số là một phương tiện thông qua nó tổ chức chứng thực chứng nhận một cặp khóa thuộc về một chủ thể. Bản chất của chứng thư số là cấu trúc dữ liệu gắn các thông tin xác định chủ thể với một khóa công khai và được ký bởi cơ quan phát hành (Tổ chức chứng thực).

Đặc điểm của chứng thư số:

* Chứng thư số được CA ký số, nên chúng tự bảo vệ đối với tính toàn vẹn và chỉ chứa những thông tin công khai nên có thể được phát tán một cách tự do.
* Chứng thư số chứa (gắn kết) tên thuê bao và khóa công khai, nó giải quyết được hai vấn đề của mật mã khóa công khai khi áp dụng vào thực tiễn (xác thực cặp khóa, chống chối bỏ).

Hệ thống chứng thư khoá công khai làm việc như sau: CA phát hành chứng thư cho những người nắm giữ cặp khoá công khai và khoá riêng. Mỗi chứng thư gồm có một khoá công khai và thông tin nhận dạng duy nhất của chủ thể của chứng thư. Chủ thể của chứng thư có thể là một người, thiết bị, hoặc một thực thể khác có nắm giữ khoá riêng tương ứng, xem hình sau:



Hình 1.2. Chứng thư số khóa công khai đơn giản

Khi chủ thể của chứng thư là một người hoặc một kiểu thực thể hợp pháp nào đó, thì chủ thể thường được gọi là một thuê bao của CA. Các chứng thư được CA ký bằng khoá riêng của CA.

Một khi các chứng thư này được thiết lập, nhiệm vụ của người sử dụng rất đơn giản. Giả thiết rằng, một người sử dụng đã có khoá công khai của CA một cách an toàn (ví dụ, thông qua phân phối khoá công khai thủ công) và anh ta tin cậy CA phát hành các chứng thư hợp lệ, Nếu người dùng cần khoá công khai của một trong các thuê bao của CA này, anh ta có thể thu được khoá công khai của thuê bao đó bằng cách lấy từ bản sao chứng thư của thuê bao. Chứng thư của thuê bao có thể được kiểm tra bằng cách kiểm tra chữ ký của CA có trên chứng thư. Người sử dụng các chứng thư theo các này được gọi là thành viên đáng tin cậy.

Kiểu hệ thống này tương đối đơn giản và kinh tế khi thiết lập trên diện rộng và theo hình thức tự động, bởi vì một trong các đặc tính quan trong của các chứng thư là: Các chứng thư có thể được phát hành mà không cần phải bảo vệ thông qua các dịch vụ an toàn truyền thông truyền thống để đảm báo bí mật, xác thực và tính toàn vẹn. Không cần phải giữ bí mật khoá công khai, như vậy các chứng thư không phải là bí mật. Hơn nữa, ở đây không đòi hỏi các yêu cầu về tính xác thực và toàn vẹn, do các chứng thư tự bảo vệ (chữ ký số của CA có trong chứng thư đảm bảo tính xác thực và toàn vẹn). Nếu một đối tượng truy nhập trái phép định làm giả một chứng thư được phát hành cho một người sử dụng khoá công khai, anh ta sẽ bị người này phát hiện vì có thể kiểm tra được chữ ký số của CA. Chính vì vậy, các chứng thư khoá công khai được phát hành theo các cách không an toàn, ví dụ như thông qua các máy chủ, các hệ thống thư mục và/hoặc các giao thức truyền thông không an toàn. Lợi ích cơ bản của một hệ thống chứng thư khoá công khai là một người sử dụng có thể có được một số lượng lớn các khoá công khai của các thành viên khác một cách tin cậy, xuất phát từ thông tin khoá công khai của một thành viên, đó chính là khoá công khai của CA. Lưu ý rằng, một chứng thư hợp lệ là khi người sử dụng khoá công khai tin tưởng rằng CA phát hành các chứng thư hợp lệ.

### Phân loại chứng thư số

Căn cứ vào đối tượng của chứng thư số có thể phân loại chứng thư số thực thể cuối và chứng thư số CA. Chứng thư số thực thể cuối là loại chứng thư số do một CA phát hành cho thực thể cuối. Chứng thư thực thể cuối này không dùng để phát hành chứng thư khác. Chứng thư số CA là chứng thư số do một CA phát hành cho một CA được phân biệt bởi trường Basic constraint. Chứng thư số CA này có thể dùng để phát hành chứng thư khác. Chứng thư số CA có thể là:

* Chứng thư số tự phát hành: là một loại chứng thư số đặc biệt trong đó chủ thể phát hành (issuer) và chủ thể sở hữu (subject) là một (giống nhau). Loại chứng thư số này được tạo ra cho những mục đích đặc biệt như kiểm tra hợp lệ cặp khóa mới khi khóa của CA hết hạn.
* Chứng thư số tự ký - chứng thư số của RootCA: là một loại chứng thư số tự phát hành. Trong đó khóa riêng ký chứng thư số tương ứng với khóa công khai trong chứng thư số.
* Chứng thư số chéo: là một loại chứng thư số mà chủ thể phát hành và chủ thể sở hữu là các CA khác nhau. Chứng thư số chéo dùng để xây dựng mối quan hệ tin cậy giữa các CA.

Căn cứ vào mục đích sử dụng, chứng thư số còn có thể được phân thành chứng thư số khóa công khai (Public Key Certificate), chứng thư số đủ điều kiện, và chứng thư số thuộc tính, CVC.

Chứng thư số thuộc tính (Attribute Certificate) là chứng thư số chứa các thông tin như: thành viên nhóm, vai trò-role, mức an toàn ... và các thông tin về sự cho phép kết hợp với thông tin về chủ sở hữu chứng thư. Chứng thư số thuộc tính không chứa khóa công khai và dùng để cấp phép thực hiện hành vi đối với mỗi chủ thể (Authorization).

Chứng thư số đủ điều kiện (Qualified Certificate) là một loại chứng thư số được dùng để xác định một người với mức an toàn nhất định. Chứng thư số đủ điều kiện thường gồm các thông tin xác định chủ thể như, họ tên, ngày sinh, ,.. thông tin sinh trắc (ảnh, vân tay..).

Card Verifiable Certificates (CVC) được thiết kế để có thể xử lý bởi các thiết bị có khả năng tính toán hạn chế như thẻ thông minh. Sử dụng cấu trúc (TLV) với các trường cố định. (mỗi trường trong chứng chỉ có độ dài cố định hoặc tối đa và mỗi trường theo thứ tự được xác định rõ).

Một số chuẩn chứng thư số phổ biến:

* Chứng thư số X.509
* Chứng thư số SPKI (Simple Public Key Infrastructure)
* Chứng thư số PGP (Pretty Good Privacy)
* Chứng thư số SET (Secure Electronic Transaction)
* PKCS #6.

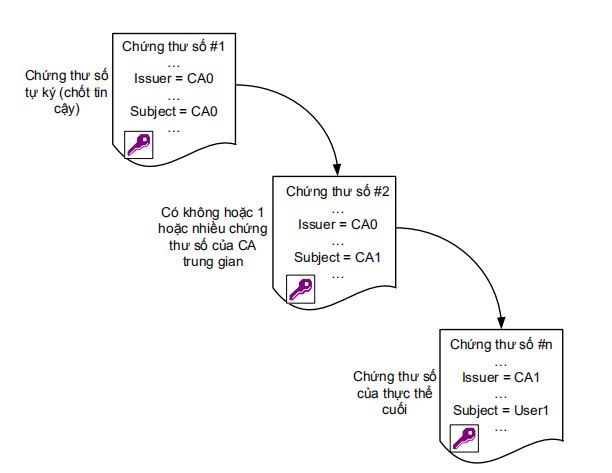
### Đường dẫn chứng thực

Như chúng ta thấy PKI mang lại sự tin cậy của thế giới thực vào thế giới công nghệ thông tin bằng thực hiện giao dịch và liên lạc điện tử tin cậy. Một ví dụ điển hình giúp hiểu rõ việc thiết lập sự tin cậy trong môi trường công nghệ thông tin sử dụng PKI là giả sử A muốn nhận một tài liệu đã được B ký số lên đó.

Để xác thực tính hợp lệ của chữ ký trên tài liệu có phải là của B hay không, A cần sử dụng khóa công khai của B, ở đây nảy sinh câu hỏi về sự tin cậy. Làm sao A có thể chắc chắn khóa công khai đó là khóa công khai thực tế B đang sử dụng mà không phải là của người khác giả mạo B. Câu trả lời cho vấn đề này chính là chứng thư số, như ta đã biết, chứng thư số là một tài liệu gắn kết thông tin của người sở hữu chứng thư số với khóa công khai. Chứng thư này được ký số bởi một bên thứ ba, được gọi là bên thứ 3 tin cậy (TTP) hay còn gọi là thẩm quyền chứng thư số (CA). Do đó, để xác thực chứng thư số của B, đầu tiên A cần có được khóa công khai của CA. Ở đây lại một lần nữa mức độ tin cậy lại được đặt câu hỏi, làm sao A có thể tin cậy vào khóa công khai của CA. A có thể có các khóa công khai của CA bên ngoài. Bằng cách này A tin cậy vào khóa công khai của CA khi A đã chắc chắn vào việc xác minh được khóa công khai. Bằng việc sử dụng khóa công khai tin cậy, A có thể xác thực được chứng thư số của B và từ đó tin tưởng chữ ký số của B. Thêm vào đó, để chứng thực các người dùng, CA có thể chứng thực các CA khác, bằng việc phân phối khóa theo cách thức tin cậy như nhau. Tương tự, các CA này có thể chứng thực CA khác nữa. Bằng cách này, các thực thể có thể tin tưởng lẫn nhau, giúp thiết lập một chuỗi tin cậy từ CA tin cậy này tới CA tin cậy của thực thể khác, chuỗi này được gọi là đường dẫn chứng thực. Số lượng các CA trong đường dẫn chứng thực và sự sắp xếp các CA này xác định các kiến trúc PKI khác nhau.

Đường dẫn chứng thực là một chuỗi các chứng thư được cấp phát. Trong đó, thực thể cấp phát chứng thư đầu tiên là một điểm chốt tin cậy. Chủ thể của chứng thư cuối cùng là thực thể cuối cùng nhận được chứng thư. Trong một đường dẫn chứng thực, có thể có nhiều điểm tin cậy (phụ thuộc vào số lượng các CAs trên đường dẫn đó) Trước khi sử dụng một chứng thư số, ta cần phải thiết lập đường dẫn chứng thực giữa các điểm chốt tin cậy và các chứng thư. Mục đích là tập hợp, liên kết các chứng thư cần thiết lại với nhau (từ chứng thư của những người cấp phát tới chứng thư gốc) để tạo thành một đường dẫn được tin tưởng Chứng thư thực thể cuối (End entity certificate) được cấp phát trực tiếp từ điểm tin tưởng của nó.

Một ví dụ cho đường dẫn chứng thực như sau: giả sử chứng thư của B được ký bởi CA2, chứng thư của CA2 lại được ký bởi CA1. Chứng thư của CA1 được ký bởi CA gốc. A (với khoá công khai của gốc là kR) có thể kiểm tra chứng thư của CA1, và do đó trích bản sao tin cậy của khoá công khai của CA1 là k1. Sau đó, khóa này có thể được sử dụng để kiểm tra chứng thư của CA2, một cách tương tự dẫn tới bản sao tin cậy khoá công khai của CA2 là k2. Khoá k2 có thể được sử dụng để kiểm tra chứng thư của B, dẫn tới bản sao khoá công khai của B là kB. Bây giờ A có thể sử dụng khoá mong muốn kB.



Hình 1.3. Mô hình đường dẫn chứng thực

Cần lưu ý rằng CA của một tổ chức có thể ở bên trong hoặc bên ngoài của tổ chức. Giải pháp sử dụng CA ở bên ngoài hay thiết lập CA bên trong tổ chức phụ thuộc vào mô hình kinh doanh của tổ chức đó. Ví dụ, một cơ quan yêu cầu bắt buộc các nhân viên phải đưa ra được bằng chứng định danh cho các nhân viên khác khi thực hiện giao dịch và trao đổi thì tổ chức đó cần thiết lập một CA ở bên trong tổ chức để phát hành và xác thực định danh của nhân viên từ khuôn dạng của chứng thư số. Khuôn dạng chứng thư số được sử dụng rộng rãi nhất là khuôn dạng chứng thư số X.509 (liên hiệp viễn thông quốc).

## Chữ ký số

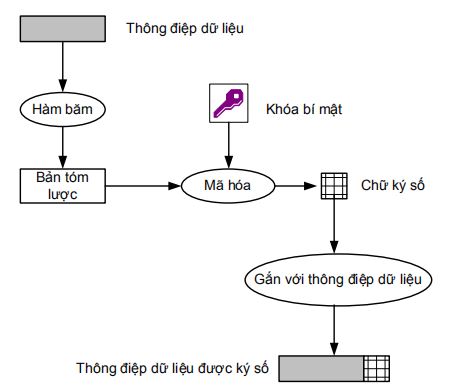
### Khái niệm chữ ký số

Chữ ký số là một kết quả quan trọng của mật mã khóa công khai, về định nghĩa chữ ký số là một tập con của chữ ký điện tử. Chữ ký điện tử được tạo lập dưới dạng từ, chữ, số, ký hiệu, âm thanh hoặc các hình thức khác bằng phương tiện điện tử, gắn liền hoặc kết hợp một cách lô gíc với thông điệp dữ liệu, có khả năng xác nhận người ký thông điệp dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu được ký.

Còn "chữ ký số" là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã khóa công khai theo đó người có được thông điệp dữ liệu ban đầu và khoá công khai của người ký có thể xác định được chính xác: Việc biến đổi nêu trên được tạo ra bằng đúng khoá bí mật tương ứng với khoá công khai trong cùng một cặp khóa và sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.

### Quy trình tạo và kiểm tra chữ ký số

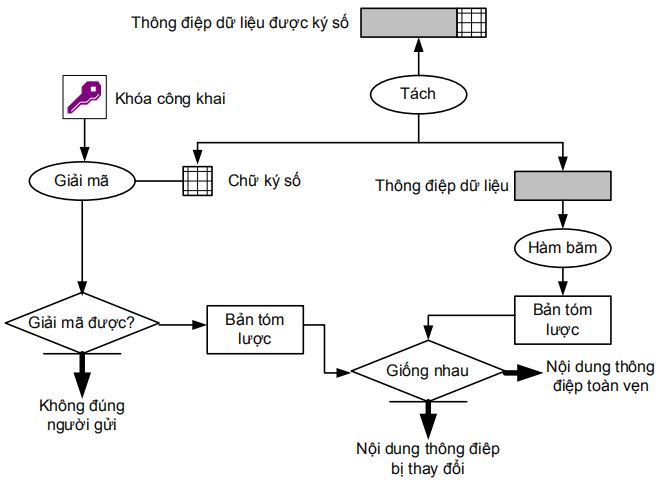
Tạo chữ ký số:



Hình 1.4. Quá trình tạo chữ ký số

* Bước 1: Sử dụng hàm băm tạo ra mã băm (là một chuỗi có độ dài cố định hay còn gọi là giá trị băm) của thông điệp gốc.
* Bước 2: Sử dụng thuật toán mã hoá khoá công khai, mã hoá mã băm bằng khoá bí mật của người ký. Giá trị đã được mã hoá này là chữ ký số của người ký đối thông điệp gốc.
* Bước 3: Thông điệp gốc được đính kèm chữ ký số và gửi đến người nhận.

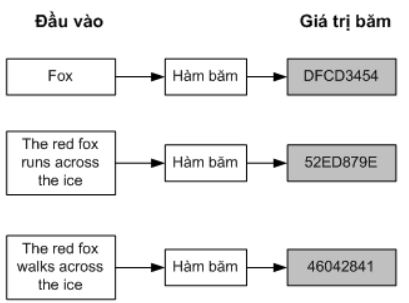
Kiểm tra chữ ký số:



Hình 1.5. Quá trình kiểm tra chữ ký số

* Bước 1: Khi nhận được văn bản gửi kèm chữ ký số, người nhận tách văn bản gốc và chữ ký số và tiến hành kiểm tra.
* Bước 2: Dùng khoá công khai của người gửi để giải mã chữ ký số (giá trị băm đã bị mã hoá bằng khoá bí mật trước đó).
* Bước 3: Dùng cùng một hàm băm tạo ra mã băm của thông điệp nhận được, nếu giá trị này giống với giá trị đã được giải mã từ chữ ký số ở bước 2 thì thông điệp do người ký khởi tạo và nội dung của thông điệp không bị thay đổi kể từ lúc ký.

### Hàm băm an toàn

****

Hình 1.6. Hàm băm an toàn

Hàm băm mật mã học là hàm băm và có tính chất là hàm 1 chiều. Từ khối dữ liệu hay giá trị băm đầu vào chỉ có thể đưa ra 1 giá trị băm duy nhất. Như chúng ta đã biết đối với tính chất của hàm 1 chiều. Một người nào đó dù bắt được giá trị băm họ cũng không thể suy ngược lại giá trị, đoạn tin nhắn băm khởi điểm. Hàm băm thường được dùng trong bảng băm nhằm giảm chi phí tính toán khi tìm một khối dữ liệu trong một tập hợp. Giá trị băm đóng vai trò gần như một khóa để phân biệt các khối dữ liệu. Giá trị đầu vào(tin nhắn, dữ liệu...) bị thay đổi tương ứng giá trị băm cũng bị thay đổi. Do vậy nếu 1 kẻ tấn công phá hoại, chỉnh sửa dữ liệu thì server có thể biết ngay lập tức.

## Các tiêu chuẩn mã hóa khóa công khai – PKCS

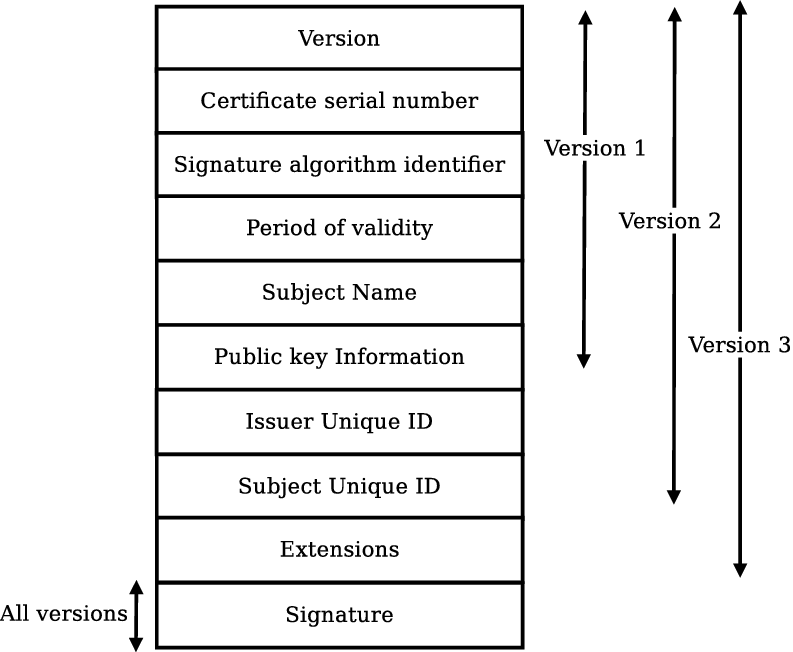
PKCS (Public Key Cryptography Standards) là bộ các tiêu chuẩn mật mã hoá khoá công khai được phát triển bởi công ty RSA Security (tiền thân là phòng thí nghiệm RSA) từ những năm 1990. Công ty xây dựng các tiêu chuẩn PKCS nhằm đẩy mạnh việc sử dụng các kỹ thuật mật mã mã họ nắm bản quyền, như là giải thuật RSA, giải thuật chữ ký Schnorr và một số khác. Mặc dù PKCS không phải là các tiêu chuẩn công nghiệp (vì vẫn được kiểm soát bởi RSA Security), một số PKCS đã được công bố thành các tiêu chuẩn Internet - RFC (Request for Comments) bởi tổ chức IETF (Internet Engineer-ing Task Force).

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiêu chuẩn** | **Phiên bản** | **Tên** | **Ghi chú** |
| PKCS#1 | 2.2 | RSA Cryptography Standard - Tiêu chuẩn mật mã RSA | Phiên bản 2.1 – RFC 3447  Phiên bản 2.2 – RFC 8017  Định nghĩa các thuộc tính toán học, định dạng của khoá bí mật và khoá công khai giải thuật RSA; các thuật toán mật mã hoá cơ bản và các lược đồ dùng cho mã hoá/giải mã, ký/kiểm tra chữ ký. |
| PKCS#2 | - | - | Hủy bỏ từ năm 2010, đã được hợp nhất vào PKCS#1. |
| PKCS#3 | 1.4 | Diffie – Hellman Key Agreement Standard – Tiêu chuẩn thoả thuận Diffie – Hellman | Giao thức mã hoá cho phép hai bên (người, thực thể giao tiếp) thiết lập một khóa [bí mật chung](https://vi.wikipedia.org/w/index.php?title=B%C3%AD_m%E1%BA%ADt_chung&action=edit&redlink=1) để mã hóa dữ liệu sử dụng trên [kênh truyền thông](https://vi.wikipedia.org/w/index.php?title=K%C3%AAnh_(truy%E1%BB%81n_th%C3%B4ng)&action=edit&redlink=1) không an toàn mà không cần có sự thỏa thuận trước về khóa bí mật giữa hai bên. Khóa bí mật tạo ra sẽ được sử dụng để mã hóa dữ liệu với phương pháp mã hóa [khóa đối xứng](https://vi.wikipedia.org/wiki/Kh%C3%B3a_%C4%91%E1%BB%91i_x%E1%BB%A9ng). |
| PKCS#4 | - | - | Hủy bỏ từ năm 2010, đã được hợp nhất vào PKCS#1. |
| PKCS#5 | 2.1 | Password-based Encryption Standard – Tiêu chuẩn mã hoá dựa trên mật khẩu | RFC 8018  Đưa ra khuyến nghị cho việc thực hiện mã hoá dựa trên mật khẩu, bao gồm các hàm sinh khoá, lược đồ mã hoá và lược đồ xác thực bản tin. |
| PKCS#6 | 1.5 | Extended-Certificate Syntax Standard – Tiêu chuẩn cú pháp chứng chỉ mở rộng | Định nghĩa các trường mở rộng cho chuẩn chứng chỉ X.509 phiên bản 1. |
| PKCS#7 | 1.5 | Cryptographic Message Syntax Standard – Tiêu chuẩn cú pháp thông điệp mật mã | RFC 2315  Tiêu chuẩn về cú pháp dữ liệu trong mã hoá thông điệp và ký. |
| PKCS#8 | 1.2 | Private-Key Information Syntax Standard – Tiêu chuẩn cú pháp thông tin khoá bí mật | RFC 5958  Tiêu chuẩn về cú pháp cho thông tin khoá bí mật và các thuộc tính của nó. |
| PKCS#9 | 2.0 | Selected Attribute Types – Tiêu chuẩn các loại thuộc tính lựa chọn. | RFC 2985  Định nghĩa các loại thuộc tính lựa chọn sử dụng cho các trường mở rộng của chứng chỉ trong PKCS#6; thông điệp được ký số trong PKCS#7; thông tin khoá bí mật trong PKCS#8; và yêu cầu xác thực trong PKCS#10. |
| PKCS#10 | 1.7 | Certification Request Standard – Tiêu chuẩn yêu cầu chứng thực | RFC 2986  Định dạng yêu cầu gửi tới tổ chức chứng thực, yêu cầu xác thực khoá công khai (hay cấp chứng chỉ). |
| PKCS#11 | 2.4 | Cryptographic Token Interface – Giao tiếp thẻ mật mã | Còn gọi là “Cryptoki”  Là một API định nghĩa tiêu chuẩn giao tiếp với các thẻ mật mã (HSM, USB token, smartcard,…). |
| PKCS#12 | 1.1 | Personal Information Exchange Syntax Standard – Tiêu chuẩn cú pháp trao đổi thông tin cá nhân | RFC 7292  Định nghĩa một chuẩn file phổ biến dùng cho lưu trữ khoá bí mật cùng với chứng chỉ số và khoá công khai tương ứng, được bảo vệ bằng mật khẩu dựa trên khoá đối xứng.  Định dạng file .pfx, .p12 |
| PKCS#13 | - | Elliptic Curve Cryptography Standard | Huỷ bỏ |
| PKCS#14 | - | Pseudo-random Number Generation | Huỷ bỏ |
| PKCS#15 | 1.1 | Cryptographic Token Information Format Standard – Tiêu chuẩn định dạng thông tin thẻ mật mã | Định nghĩa các định dạng thông tin trong thẻ mật mã bao gồm 4 lớp: Keys, Certificates, Authentication Objects và Data Objects. |

# SỬ DỤNG CHỨNG THƯ SỐ ĐÃ TẠO ĐỂ KÝ SỐ VÀ KIỂM TRA CHỮ KỸ SỐ TRÊN CÁC TÀI LIỆU PDF

## Chứng thư số X.509

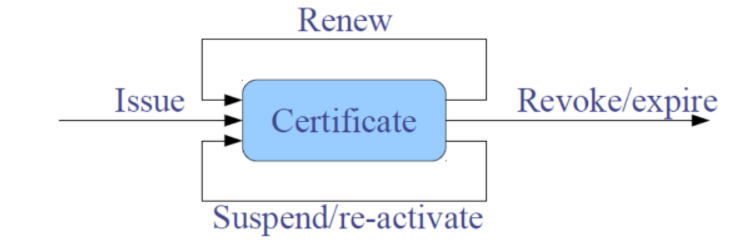
Chứng thư số X.509 là chứng thư số khóa công khai phổ biến nhất. Hiệp hội Viễn thông quốc tế (International Telecommunications Union – ITU) đã chỉ định chuẩn X.509 vào năm 1988. Đây là định dạng phiên bản 1 của chuẩn X.509. Vào năm 1993, phiên bản 2 của chuẩn X.509 được phát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



Hình 2.1. Cấu trúc của chứng thư số X.509

* **Version**: Chỉ định phiên bản của chứng thư số X.509.
* **Serial Number**: Số loạt phát hành được gán bởi CA. Mỗi CA nên gán một mã số loạt duy nhất cho mỗi giấy chứng nhận mà nó phát hành.
* **Signature Algorithm:** Thuật toán chữ ký chỉ rõ thuật toán mã hóa được CA sử dụng để ký giấy chứng thư số. Trong chứng thư số X.509 thường là sự kết hợp giữa thuật toán băm (chẳng hạn như MD5 hoặc SHA-1) và thuật toán khóa công khai (chẳng hạn như RSA).
* **Issuer Name:** Tên tổ chức CA phát hành chứng thư số, đây là một tên phân biệt theo chuẩn X.500 (xem Phụ lục A). Hai CA không được sử dụng cùng một tên phát hành.
* **Validity Period**: Trường này bao gồm 2 giá trị chỉ định khoảng thời gian mà chứng thư số có hiệu lực. Hai phần của trường này là *not-before* và *not-after*.
  + **Not-before** chỉ định thời gian mà chứng thư số này bắt đầu có hiệu lực.
  + **Not-after** chỉ định thời gian mà chứng thư số hết hiệu lực.  
    Các giá trị thời gian này được đo theo chuẩn thời gian Quốc tế, chính xác đến từng giây.
* **Subject Name:** là một X.500 DN, xác định đối tượng sở hữu chứng thư số mà cũng là sở hữu của khóa công khai. Một CA không thể phát hành 2 chứng thư số có cùng một Subject Name.
* **Public key:** Xác định thuật toán của khóa công khai (như RSA) và chứa khóa công khai được định dạng tùy vào kiểu của nó.
* **Issuer Unique ID và Subject Unique ID**: Hai trường này được giới thiệu trong X.509 phiên bản 2, được dùng để xác định hai tổ chức CA hoặc hai chủ thể khi chúng có cùng DN. RFC 2459 đề nghị không nên sử dụng 2 trường này.
* **Extensions**: Chứa các thông tin bổ sung cần thiết mà người thao tác CA muốn đặt chứng thư số. Trường này được giới thiệu trong X.509 phiên bản 3.
* **Signature**: Đây là chữ ký điện tử được tổ chức CA áp dụng. Tổ chức CA sử dụng khóa bí mật có kiểu quy định trong trường thuật toán chữ ký. Chữ ký bao gồm tất cả các phần khác trong chứng thư số. Do đó, tổ chức CA chứng nhận cho tất cả các thông tin khác trong chứng thư số chứ không chỉ cho tên chủ thể và khóa công khai. Những phần mở rộng của tên tập tin phổ biến cho chứng nhận X.509 bao gồm:
  + **.cer**: chứng thư số được mã hóa theo luật mã hóa tiêu chuẩn (Canonical Encoding Rules – CER).
  + **.der**: chứng thư số được mã hóa theo luật mã hóa phân biệt (Distinguished Encoding Rules – DER).
  + **.pem** (Privacy-Enhanced Electronic Mail): định dạng mã hóa được sử dụng để lưu trữ các chứng nhận và khóa. Một tập tin được định dạng với chuẩn này có thể chứa các khóa bí mật (RSA và DSA), khóa công khai (RSA và DSA) và các chứng nhận X509. Định dạng này lưu trữ dữ liệu ở định dạng DER được mã hóa cơ sở 64, nằm giữa "-----BEGIN CERTIFICATE-----" và "-----END CERTIFICATE-----", phù hợp cho việc trao đổi ở dạng văn bản giữa các hệ thống.
  + **.p7b, p7c**: PKCS #7 là một định dạng mã hóa cho việc lưu trữ một chứng nhận số và chuỗi chứng nhận của nó dưới dạng các ký tự ASCII. Định dạng này được sử dụng bởi CA để trả về các chứng thư số được phát hành cùng với chuỗi chứng nhận. Định dạng này có có thể được sử dụng như đầu vào cho yêu cầu gia hạn chứng nhận đến một CA.
  + **.pfx, .p12:** PKCS #12 là một định dạng mã hóa cho việc lưu trữ một chứng thư 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.

## Quản lý vòng đời chứng thư số



Hình 2.2. Vòng đời chứng thư số

* Tạo mới (Issue): là tiến trình người dùng gửi yêu cầu đăng ký và phát hành chứng thư số.
* Gia hạn (Renewal): thay đổi thời hạn của chứng thư khi chứng thư đã hết hạn (Cập nhật chứng thư).
* Tạm dừng/kích hoạt (Suspend/re-activate): là tiến trình treo hoạt động (tạm dừng, mất hiệu lực) của một chứng thư trong một khoảng thời gian nhất định.
* Thu hồi (Revocation): là tiến trình làm mất hiệu lực chứng thư trước khi chứng thư số hết hạn tự nhiên.

## Quản lý chứng thư số

### Đăng ký phát hành chứng thư số:

Đăng ký (registration), phát hành (issue) chứng thư số còn được gọi là kết nạp (enrollment) gồm 2 bước: bước đăng ký và bước tạo chứng thư số.

* Đăng ký là quá trình thiết lập và kiểm tra định danh của người dùng hoặc chương trình. Mức độ kiểm tra định danh của thực thể cuối phụ thuộc vào Chính sách phát hành chứng thư số (CP) và quy chế chứng thực (CPS). Đăng ký chứng thư số là bước đầu tiên của người dùng khi tham gia vào hệ thống gồm những việc sau: Người dùng gửi yêu cầu đăng ký và tổ chức chứng thực xác thực thông tin đăng ký của người dùng.
* Phát hành (tạo) chứng thư số chỉ được thực hiện tại CA. Nếu khoá công khai không do CA sinh ra thì khoá công khai đó phải được chuyển an toàn tới CA để đặt vào trong chứng thư số.

### Phân phối chứng thư số

Phân phối chứng thư số: Khi cặp khóa và chứng thư số đã được tạo ra thì phải được phân phối thích hợp tới thuê bao. Phân phối khoá và chứng thư số phụ thuộc vào nhiều yếu tố: vị trí sinh khóa, mục đích sử dụng của chứng thư số, và các ràng buộc về chức năng hay về chính sách. Chứng thư số được phân phối kèm với khóa riêng và qua kho chứng thư số. Khóa riêng được chuyển tới thuê bao bằng con đường an toàn.

### Phổ biến chứng thư số

Phân phối cá nhân (riêng) là hình thức chuyển các thông tin PKI giữa hai thực thể qua các phương tiện: trực tiếp, email, giao thức ... Phân phối cá nhân có một số nhược điểm như việc không thích hợp với miền PKI có số lượng thực thể lớn và không đảm bảo phân phối thông tin tới tất cả các thực thể.

Phân phối công cộng là hình thức chuyển các thông tin PKI tới một vị trí dễ truy nhập, nhiều người biết và luôn sẵn sàng. Vị trí này được gọi là kho chứa công cộng (public repository). Kho chứa công cộng về bản chất là một CSDL tập trung dễ dàng, thuận tiện truy nhập chứa chứng thư số và CRL. Thông tin trong kho chứa có thể được truy nhập thông qua giao thức LDAP, HTTP, FTP... Vị trí của kho chứa chứng thư số được xác định thông qua các trường mở rộng trong chứng thư số và CRL: AIA, SIA, CRL Distribution Points.

### Gia hạn chứng thư số

Gia hạn chứng thư số: là việc cấp thời hạn mới cho chứng thư số khi hết hạn sử dụng tự nhiên. Khi môt chứng thư số hết hạn, một trong các sự kiện sau có thể xảy ra:

* Không làm gì: chủ thể sở hữu sẽ không thuộc về miền PKI đó nữa.
* Gia hạn chứng thư số: vẫn khoá công khai cũ được đặt vào trong chứng thư số mới với thời hạn hợp lệ mới.
* Cập nhật chứng thư số: cặp khoá mới được sinh ra và chứng thư số mới được phát hành.

Quy trình gia hạn chứng thư số đầu tiên người dùng cuối gửi yêu cầu gia hạn sau đó tổ chức chứng thực tiến hành hoạt động gia hạn và gửi chứng thư số tới người dùng.

### Tạm dừng chứng thư số

Tạm dừng (treo - suspend) chứng thư số là việc tạm thời làm cho chứng thư số không còn hợp lệ nữa, làm cho chứng thư số tạm thời mất hiệu lực trước khi nó hết hạn một cách tự nhiên. Tạm dừng chứng thư số có thể hiểu là tạm thời thu hồi chứng thư số trong ngắn hạn. Nguyên nhân tạm dừng chứng thư số như việc nghi ngờ lộ khoá bí mật, thay đổi trạng thái của người dùng... Yêu cầu tạm dừng chứng thư số từ người dùng có thể qua mạng (trực tuyến), hoặc phương tiện khác (điện thoại, gặp trực tiếp). Công bố thông tin tạm dừng chứng thư số được thực hiện ngay sau khi tạm dừng thông qua 2 phương tiện là CRL và OCSP.

### Thu hồi chứng thư số

Thu hồi chứng thư số là khẳng định rằng một chứng thư số (và khoá riêng tương ứng) không còn hợp lệ nữa. Thu hồi chứng thư số là làm hết hiệu lực của chứng thư số trước khi nó hết hạn một cách tự nhiên. Nguyên nhân thu hồi chứng thư số như nghi ngờ lộ khoá bí mật, thay đổi trạng thái công việc... Yêu cầu thu hồi chứng thư số từ người dùng có thể qua mạng (trực tuyến), hoặc phương tiện khác (điện thoại, gặp trực tiếp). Công bố thông tin thu hồi chứng thư số được thực hiện ngay sau khi thu hồi thông qua 2 phương tiện là CRL và OCSP.

### Sử dụng chứng thư số

Mục đích sử dụng chứng thư số là thực hiện các hành động mật mã (xác thực, ký số, mã hóa thông tin)... Trước khi sử dụng chứng thư số cần phải được kiểm tra tính hợp lệ. Các bước kiểm tra tính hợp lệ của chứng thư số:

* Toàn vẹn: xây dựng đường dẫn chứng thực.
* Xác định: thời gian, trạng thái hợp lệ.
* Tin cậy: chứng thư đính kèm, OS cert store, CA cert store.

## Danh sách thu hồi chứng thư số

CRL (Certificate Revocation List) là danh sách các chứng thư số bị thu hồi và không còn được tin dùng nữa. Mỗi một mục (entry) trong CRL tương ứng với một chứng thư và thường gồm 3 thông tin sau: Serial number của chứng thư số; Thời điểm bị thu hồi; và Lý do thu hồi. Một CRL được tạo và phát hành định kỳ sau 1 khoảng thời gian nào đó do người quản trị CA chỉ định, ví dụ: 1 giờ, 1 ngày, 1 tuần, v.v. Một CRL cũng có thể được cập nhật và phát hành ngay sau khi một chứng thư số bị thu hồi. Các CA sẽ đẩy CRL do nó cấp phát và quản lý tới kho chứa là LDAP server hoặc Web server.

Để ngăn chặn nguy cơ CRL có thể bị làm giả dẫn đến việc một chứng thư số bị cố ý đưa vào hoặc bị loại bỏ khỏi CRL, các CRL đều có một chữ ký số được ký bởi CA đã phát hành. Để xác thực chữ ký, người dùng cần đến chứng thư số của CA. Thông thường chứng thư số của các CA phổ biến đều được nạp sẵn bên trong các ứng dụng có hỗ trợ PKI như các trình duyệt web, đọc email hay hệ điều hành.

Khi ứng dụng PKI nhận được một chứng thư số, thì bản thân chứng thư không chứa nội dung của CRL mà nó có một extension là CRL Distribution Points (CDP), cho biết địa chỉ URL của CRL (là file có đuôi .crl) mà nó cần tải về. Sau đó ứng dụng PKI phải phân tích file .crl này để xác định xem chứng thư số đã bị thu hồi hay chưa, nói cách khác nếu serial number không có trong CRL thì chứng thư số đó được tin dùng.

## Giao thức kiểm tra trạng thái chứng thư số trực tuyến – OCSP

OCSP (Online Certificate Status Protocol) là một giao thức được sử dụng để nhận về trạng thái thu hồi của một chứng thư có chuẩn định dạng là X.509. Hoạt động theo mô hình client/server. Các thông điệp OCSP (request, response) được mã hóa theo chuẩn ASN.1 và được truyền qua giao thức HTTP. Server cũng thường được gọi là OCSP responder.

Về cơ bản, OCSP hoạt động như sau: đầu tiên người dùng gửi một yêu cầu chứa serial number của chứng thư cần kiểm tra tới server. Sau đó máy chủ response trả về người dùng cho biết 1 trong 3 trạng thái có thể của chứng thư số là: “good” không bị thu hồi; “revoked” bị thu hồi; hoặc “unknown” server không biết tới serial number có trong yêu cầu. Response cũng được ký số bởi server. Nếu server không thể xử lý yêu cầu, người dùng sẽ nhận được response không được ký, chứa thông báo lỗi.

OCSP có các ưu điểm như sau:

* Tiết kiệm băng thông do các request và response có kích thước nhỏ hơn nhiều (thường chỉ 4KB) so với file .crl.
* Tiết kiệm thời gian vì chỉ phải kiểm tra trạng thái của 1 certificate thay vì phải phân tích file .crl.
* Nếu thông tin thu hồi có sẵn trong cache tại client và server thì tiết kiệm được được cả thời gian lẫn băng thông.
* Hệ thống kiểm tra trạng thái chứng thư số với OCSP có thể dễ dàng được mở rộng, với độ sẵn sàng cao khi cần xử lý một lượng lớn các yêu cầu.
* OCSP responder đảm bảo luôn sử dụng các phiên bản CRL mới nhất làm cơ sở cho việc kiểm tra tính hiệu lực của chứng thư cũng như là khả năng phản hồi gần như lập tức (real-time) khi nó nhận được yêu cầu từ người dùng.
* Một OCSP server có thể phục vụ công tác kiểm tra trạng thái chứng thư số cho nhiều CA. Điều này giúp người dùng tránh phải lưu nhiều CRL.

## Thư viện OpenSSL

### Giới thiệu về OpenSSL

OpenSSL là một thư viện nguồn mở được sử dụng để mã hóa dữ liệu và triển khai các giao thức mạng. Được phát hành lần đầu tiên vào năm 1998, nó có sẵn trong các hệ thống Linux, Windows, macOS và BSD. OpenSSL cho phép người dùng thực hiện các tác vụ liên quan đến SSL khác nhau, bao gồm CSR (Yêu cầu ký chứng chỉ), tạo khóa riêng và cài đặt chứng chỉ SSL.

OpenSSL gồm các phần mềm nguồn mở cho phép triển khai các giao thức mạng và mã hóa dữ liệu khác nhau như SSL và TLS. Thư viên gốc của phần mềm này được viết bằng ngôn ngữ lập trình C. Trong đó có sẵn những phần mềm cho phép người dùng sử dụng thư viện OpenSSL với nhiều ngôn ngữ khác nhau cùng với các chức năng mật mã tổng quát để có thể mã hóa và giải mã dữ liệu. OpenSSL cũng được sử dụng từ dòng lệnh để có thể yêu cầu, tạo và quản lý các chứng thực số.

### Các phiên bản phát hành chính

Các thư viện của OpensSL được viết bằng ngôn ngữ lập trình C, nó hoạt động trên tất cả các nền tảng lớn, bao gồm tất cả các hệ điều hành Unix và tất cả các phiên bản của Microsoft Windows

|  |  |
| --- | --- |
| Phiên bản | Ngày phát hành |
| 0.9.1c | 23/12/1998 |
| 0.9.2b | 22/03/1999 |
| 0.9.3 | 25/05/1999 |
| 0.9.4 | 09/08/1999 |
| 0.9.5 | 28/02/2000 |
| 0.9.6 | 24/09/2000 |
| 0.9.7 | 31/12/2002 |
| 0.9.8 | 05/07/2005 |
| 1.0.0 | 29/03/2010 |
| 1.0.1 | 14/03/2012 |
| 1.0.2 | 22/01/2015 |
| 1.1.0 | 25/08/2016 |
| 1.1.1 | 11/09/2018 |
| 3.0.0 | N/A |

### Các chức năng của OpenSSL

Chương trình OpenSSL là một công cụ dòng lệnh để sử dụng các chức năng mật mã của các thư viện Crypto của OpenSSL:

* Sử dụng để băm dữ liệu.
* Mã hóa dữ liệu.
* Tạo mật khẩu đã được mã hóa.
* Ký và xác thực chữ ký.
* Tạo khóa RSA, DSA hay EC.
* Kiểm tra số nguyên tố.
* Kiểm tra hiệu suất phần cứng của hệ thống.