## Certificate Authority là gì?

Certificate Authority (tạm dịch: Nhà cung cấp chứng chỉ số – CA) giúp định danh trang web, người dùng, đóng vai trò quan trọng trong internet. Mã hóa giao dịch

## Chứng chỉ số SSL

[Chứng chỉ SSL](https://vietnix.vn/mua-ssl/) (SSL Certificate) là một loại Chứng chỉ số phổ biến, Chúng liên kết chi tiết quyền sở hữu của máy chủ web (và web) với các khóa mật mã (cryto key)

Các khóa này được sử dụng trong giao thức SSL/TLS.

* Kích hoạt phiên bảo mật giữa trình duyệt và máy chủ web SSL.

Để trình duyệt có thể tin cậy SSL và thiết lập SSL/TLS session mà không bị cảnh báo bảo mật, SSL phải chứa domain name của trang web sử dụng nó (được cấp bởi CA và còn hạn).

Trước khi cấp một Chứng chỉ số, CA sẽ tiến hành một số kiểm tra về danh tính của người nộp đơn. Việc kiểm tra liên quan đến loại chứng chỉ đang được áp dụng. Lấy ví dụ, chứng chỉ SSL xác thực domain sẽ xác minh quyền sở hữu domain name được đưa vào Chứng chỉ. Trong khi đó, SSL xác thực mở rộng sẽ bao gồm thông tin bổ sung về công ty. Các thông tin này sẽ được xác thực bởi CA qua nhiều lần kiểm tra.

Bên cạnh SSL, CA còn có thể cấp các loại chứng chỉ kỹ thuật số cho các mục đích khác như:

* Chứng chỉ chữ ký code được dùng bởi các nhà phát triển phần mềm và lập trình viên để ký vào phần mềm mà họ phân phối.
* Chứng chỉ email cho phép các thực thể ký, mã hóa và xác thực email bằng giao thức S/MIME (Secure Multipurpose Internet Mail Extension) để đảm bảo an toàn khi truy cập tập tin đính kèm.
* Chứng chỉ thiết bị được cấp cho các thiết bị IoT để cho phép quản lý và xác thực cập nhật firmware hoặc phần mềm một cách an toàn.
* Chứng chỉ đối tượng có thể được dùng để ký và xác thực bất cứ đối tượng phần mềm nào.
* Chứng chỉ người dùng hoặc khách hàng, được sử dụng bởi các cá nhân cho các mục đích xác thực khác nhau và đôi khi được gọi chung là chữ ký số.

## Root Program là gì?

Root certificate hay tiếng việt là chứng chỉ gốc, thường được gọi là trusted root, là trung tâm của mô hình ủy thác làm nền cho Public Key Infrastructure và bằng cách mở rộng SSL / TLS. Hãy bắt đầu bằng cách thảo luận về các root program và làm việc theo cách của chúng ta ra khỏi đó.

# Sự khác biệt giữa Root Certificates và Intermediate Certificates

/[Resources](https://hocdevops.com/category/resources/) /Sự khác biệt giữa Root Certificates và Intermediate Certificates

* 12 October, 2021
* khaind
* [Resources](https://hocdevops.com/category/resources/)



**Nội dung chính**[[hide](https://hocdevops.com/resources/su-khac-biet-giua-root-certificates-va-intermediate-certificates/)]

* [1 Chứng chỉ SSL của người dùng cuối đó chỉ là một phần của chuỗi chứng chỉ (certificate chain).](https://hocdevops.com/resources/su-khac-biet-giua-root-certificates-va-intermediate-certificates/#Chung_chi_SSL_cua_nguoi_dung_cuoi_do_chi_la_mot_phan_cua_chuoi_chung_chi_certificate_chain)
* [2 Root Program là gì?](https://hocdevops.com/resources/su-khac-biet-giua-root-certificates-va-intermediate-certificates/#Root_Program_la_gi)
* [3  Certificate chain là gì?](https://hocdevops.com/resources/su-khac-biet-giua-root-certificates-va-intermediate-certificates/#nbspCertificate_chain_la_gi)
* [4 Chứng chỉ trung gian (intermediate certificate) là gì?](https://hocdevops.com/resources/su-khac-biet-giua-root-certificates-va-intermediate-certificates/#Chung_chi_trung_gian_intermediate_certificate_la_gi)
* [5 Chữ ký số đóng vai trò gì?](https://hocdevops.com/resources/su-khac-biet-giua-root-certificates-va-intermediate-certificates/#Chu_ky_so_dong_vai_tro_gi)
* [6 Ok, vậy sự khác biệt giữa Root CA và Intermediate CA là gì?](https://hocdevops.com/resources/su-khac-biet-giua-root-certificates-va-intermediate-certificates/#Ok_vay_su_khac_biet_giua_Root_CA_va_Intermediate_CA_la_gi)
* [7 Sự khác biệt giữa một chained root và một single root là gì?](https://hocdevops.com/resources/su-khac-biet-giua-root-certificates-va-intermediate-certificates/#Su_khac_biet_giua_mot_chained_root_va_mot_single_root_la_gi)
* [8 Một từ cuối cùng về Roots and Intermediates](https://hocdevops.com/resources/su-khac-biet-giua-root-certificates-va-intermediate-certificates/#Mot_tu_cuoi_cung_ve_Roots_and_Intermediates)
  + [8.1 Share this:](https://hocdevops.com/resources/su-khac-biet-giua-root-certificates-va-intermediate-certificates/#Share_this)
  + [8.2 Like this:](https://hocdevops.com/resources/su-khac-biet-giua-root-certificates-va-intermediate-certificates/#Like_this)

## Chứng chỉ SSL của người dùng cuối đó chỉ là một phần của chuỗi chứng chỉ (certificate chain).

Chúng ta hãy nói về intermediate và root CA certificate trong vài phút. SSL (hay chính xác hơn, TLS) là một công nghệ mà hầu hết người dùng cuối biết rất ít hoặc không biết gì về nó. Ngay cả những người cài đặt được nó thường không biết nhiều ngoài việc thực tế là họ cần chứng chỉ SSL và họ phải cài đặt nó trên máy chủ của họ để phục vụ trang web của họ thông qua HTTPS.

Đó là lý do tại sao khi bạn bắt đầu đề cập đến Intermediate certificates (chứng chỉ trung gian) và CAs, Root certificates và CAs hầu hết mọi người bắt đầu khó hiểu, điều này làm cho nó trở thành một chủ đề bạn muốn tránh xa. Nó có vẻ như rất nhiều lúc đầu, nhưng hy vọng vào cuối bài viết này nó sẽ có vẻ khá đơn giản.

## Root Program là gì?

Root certificate hay tiếng việt là chứng chỉ gốc, thường được gọi là trusted root, là trung tâm của mô hình ủy thác làm nền cho Public Key Infrastructure và bằng cách mở rộng SSL / TLS. Hãy bắt đầu bằng cách thảo luận về các root program và làm việc theo cách của chúng ta ra khỏi đó.

Mỗi thiết bị bao gồm một cái gì đó được gọi là root store.Root store là một bộ sưu tập các chứng chỉ gốc (root certificate) được tải xuống trước (và các public key của chúng) lưu trữ trên chính thiết bị. Nói chung, thiết bị sẽ sử dụng bất kỳ root store nào có nguồn gốc từ hệ điều hành của nó, nếu không nó có thể sử dụng root store của bên thứ ba thông qua một ứng dụng như trình duyệt web. Có một số root program:

* Microsoft
* Apple
* Google
* Mozilla

Người dùng Apple, cả macOS và iOS, đều dựa vào Apple root store, tương tự như vậy cho người dùng Microsoft và root store của nó. Android sử dụng google. Và bộ sản phẩm Mozilla sử dụng root store độc quyền của riêng mình.

Các root program chạy theo các hướng dẫn cực kỳ nghiêm ngặt. Ngoài các quy định và hạn chế được đưa ra bởi các yêu cầu cơ bản của CA/B, một số root program – ví dụ, Mozilla – thêm các yêu cầu nghiêm ngặt hơn lên hàng đầu.

Lý do cho điều này rất đơn giản: trust.

Chứng chỉ gốc (root certificate) là vô giá, bởi vì bất kỳ chứng chỉ nào được sign bằng private key của nó sẽ được các trình duyệt tự động trust. Bạn thực sự cần phải chắc chắn rằng bạn có thể tin tưởng Cơ quan chứng chỉ cấp từ nó.

Theo nghĩa này, có thể hữu ích khi xem trust trong hai bối cảnh cụ thể:

* Social Trust
* Technical Trust

Cái sau hoàn toàn phụ thuộc vào cái trước. Các yêu cầu nghiêm ngặt mà các CAs phải tuân thủ, kiểm toán, giám sát công khai – tất cả đều nhằm đảm bảo rằng các CA duy trì đủ **Social Trust** để xứng đáng với **Technical Trust** đi kèm với việc có một root đáng tin cậy.

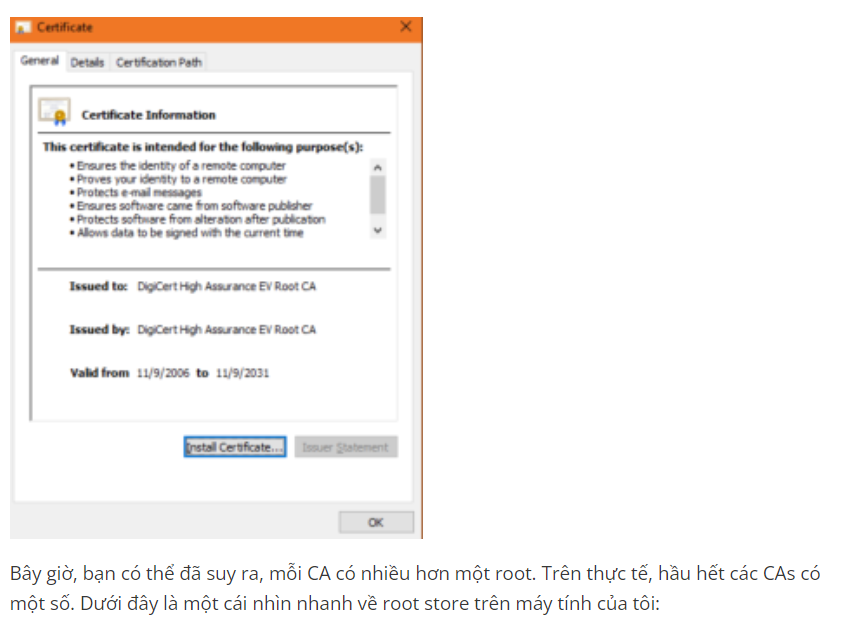
Nói chung, những điều này khá đơn giản, thường là CA đã được phát hành bởi một trung gian có chữ ký chéo (chúng ta sẽ đạt được điều đó trong một giây) và tiến hành sử dụng CA của riêng mình trong một khoảng thời gian trước khi có một trusted root. Hoặc, nói cách khác, bạn không thể chỉ tạo thành một CA và ngay lập tức áp dụng để có trusted root.

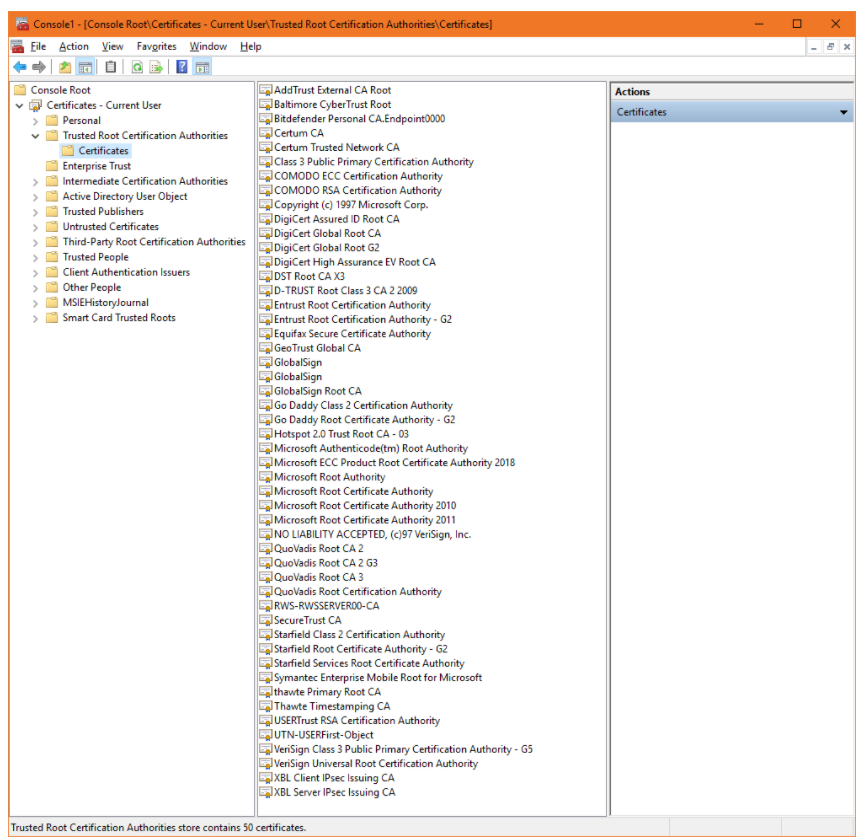
Bất kể, một khi CA đã được chấp nhận đơn đăng ký và chứng minh mình đáng tin cậy, nó sẽ được thêm nguồn gốc vào root store.

Chứng chỉ root đáng tin cậy là gì?

Như chúng ta vừa đề cập, chứng chỉ gốc là một loại chứng chỉ kỹ thuật số X.509 đặc biệt có thể được sử dụng để cấp các chứng chỉ khác.

Đối với người mới bắt đầu, trong khi chứng chỉ SSL của người dùng cuối (và nói chung là bất kỳ loại chứng chỉ PKI đáng tin cậy nào) có tuổi thọ hai năm hoặc ít hơn – chứng chỉ gốc sống lâu hơn nhiều. Dưới đây là một trong những nguồn gốc EV của DigiCert, hãy xem thời hạn hiệu lực của nó:





Nói chung các root khác nhau sẽ có các thuộc tính khác nhau. Điều này có lẽ được minh họa tốt nhất bởi hai nguồn gốc COMODO (nay là Sectigo) gần đầu danh sách đó. Một để tạo chữ ký RSA và cái kia cho chữ ký ECDSA.

Bất kỳ chứng chỉ nào được cấp ra khỏi bất kỳ root nào trong số này sẽ tự động được hệ thống máy tính của chúng ta tin tưởng. Bây giờ, cho đến nay chúng ta đang xem xét điều này một cách quá đơn giản. Giá trị của những root này, và những rủi ro đi kèm với việc có một root bị xâm phạm, có nghĩa là chúng hiếm khi thực sự được sử dụng để cấp chứng chỉ. Thay vào đó, xoay vòng và phát hành dựa vào intermediate.

## Certificate chain là gì?

Trước khi chúng ta có thể đi xa hơn, chúng ta cần tìm hiểu khái niệm về chuỗi chứng chỉ (certificate chain). Hãy để tôi bắt đầu bằng cách đặt ra một câu hỏi: làm thế nào để trình duyệt của bạn biết tin tưởng chứng chỉ SSL của trang web? Chúng ta đã đề cập rằng bất kỳ chứng chỉ con nào của một trusted root, bằng cách mở rộng, đáng tin cậy. Nhưng làm thế nào để điều đó hoạt động ở cấp độ kỹ thuật?

Khi bạn đến một trang web, trình duyệt của bạn sẽ xem chứng chỉ SSL của nó và thực hiện một quy trình nhanh chóng để xác minh tính xác thực của chứng chỉ. Nó kiểm tra ngày hiệu lực của nó, đảm bảo chứng chỉ đã không bị thu hồi và nó xác thực chữ ký số của chứng chỉ.

Những gì trình duyệt của bạn đang làm để xác thực chứng chỉ là theo chuỗi chứng chỉ. Để có được chứng chỉ SSL được cấp, bạn bắt đầu bằng cách tạo Yêu cầu Ký Chứng chỉ (CSR) và private key. Trong lần lặp đơn giản nhất, bạn gửi CSR đến cơ quan chứng chỉ, sau đó nó ký chứng chỉ SSL của bạn bằng private key từ root của nó và gửi lại.

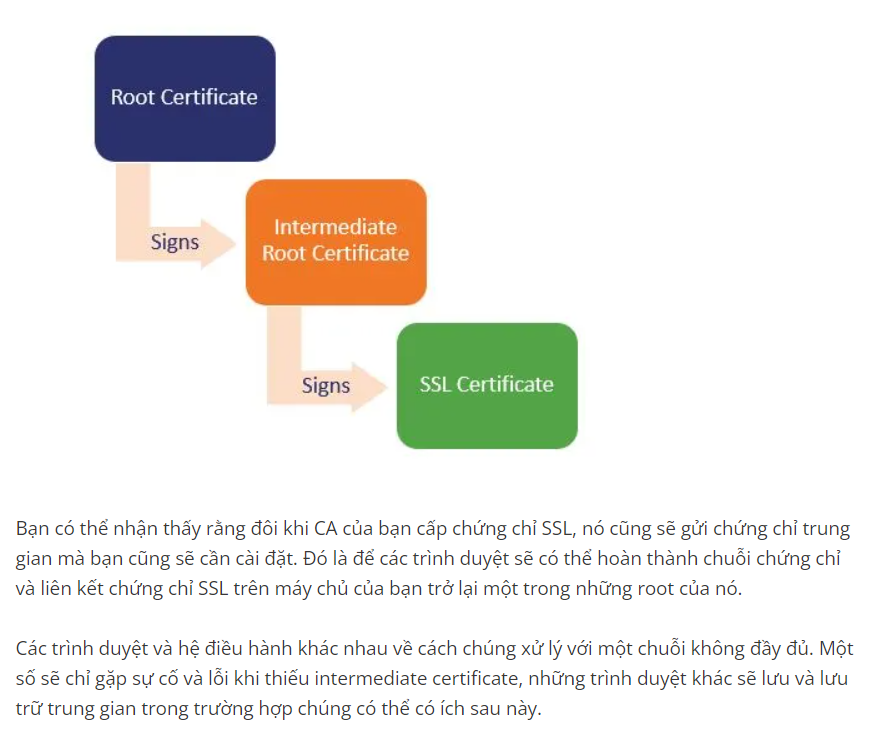
Bây giờ, khi một trình duyệt nhìn thấy chứng chỉ SSL, nó thấy rằng chứng chỉ được cấp bởi một trong những root đáng tin cậy trong root store của nó (hoặc chính xác hơn, được ký bằng private key của root). Vì nó tin tưởng vào root, nó tin tưởng bất kỳ chứng chỉ nào của root.

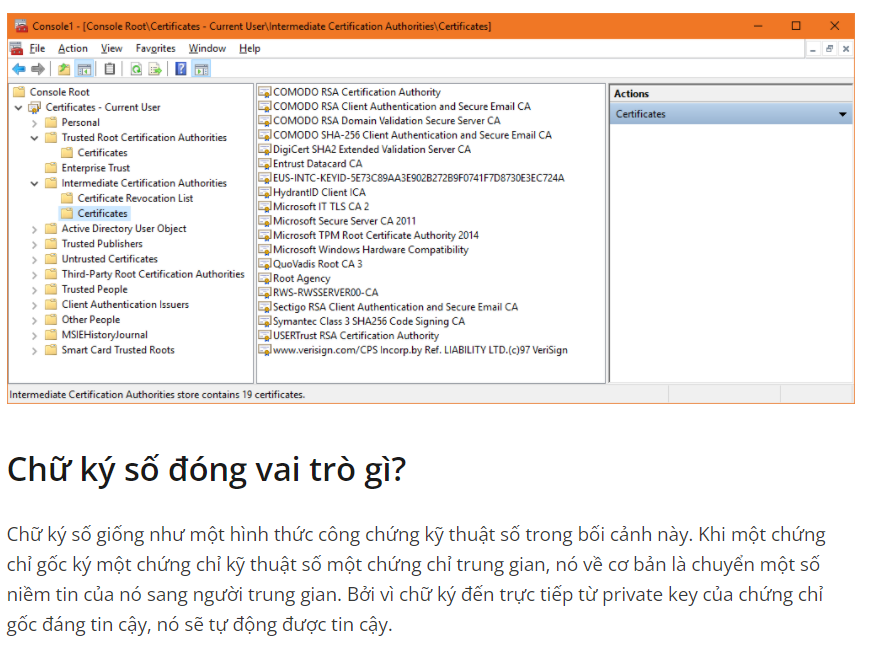
## Chứng chỉ trung gian (intermediate certificate) là gì?

Như đã nêu ở trên, Cơ quan cấp chứng chỉ không cấp chứng chỉ máy chủ (chứng chỉ SSL của người dùng cuối) trực tiếp từ root của chúng. Những root đó quá có giá trị và có quá nhiều rủi ro.

Vì vậy, để tự cách ly, CAs thường phát hành những gì được gọi là root trung gian. CA ký vào root trung gian bằng private key của nó, điều này làm cho nó đáng tin cậy. Sau đó, CA sử dụng private key của chứng chỉ trung gian để ký và cấp chứng chỉ SSL của người dùng cuối. Quá trình này có thể diễn ra nhiều lần, trong đó một root trung gian ký một trung gian khác và sau đó CA sử dụng điều đó để ký chứng chỉ. Những liên kết này, từ root đến trung gian đến cuối tạo thành chuỗi chứng chỉ.

Đây là hình dung về chuỗi chứng chỉ. Ví dụ, chúng ta sẽ chỉ sử dụng một trung gian để giữ cho nó đơn giản. Chuỗi chứng chỉ trong thế giới thực thường phức tạp hơn nhiều.





Đoạn này sẽ hơi đi sâu về công nghệ một chút. Bất cứ khi nào trình duyệt hoặc thiết bị được chỉ định chứng chỉ SSL, nó sẽ nhận được chứng chỉ cũng như public key liên quan đến chứng chỉ. Sử dụng public key, nó xác minh chữ ký số và xem nó được tạo bởi ai – chứng chỉ nào đã ký nó. Bạn có thể bắt đầu ghép điều này lại với nhau ngay bây giờ. Khi trình duyệt của bạn đang xác thực chứng chỉ SSL của người dùng cuối trên một trang web, nó sử dụng public key được cung cấp để xác minh chữ ký và di chuyển một liên kết lên chuỗi. Nó tiếp tục lặp lại quá trình này – xác thực chữ ký và theo chuỗi vào chứng chỉ đã ký – cho đến khi cuối cùng nó đến một trong những chứng chỉ gốc trong root store tin cậy của trình duyệt.

Nếu nó không thể liên kết đến một trong những root đáng tin cậy của nó, nó sẽ không được tin tưởng chứng chỉ đó.

## Ok, vậy sự khác biệt giữa Root CA và Intermediate CA là gì?

Điều này thực sự khá đơn giản. Root CA là Cơ quan Chứng nhận sở hữu một hoặc nhiều root đáng tin cậy. Điều đó có nghĩa là họ có root từ các root store của các trình duyệt lớn. Intermediate CA là Cơ quan cấp giấy chứng nhận phát hành Intermediate root (root trung gian). Nó không có nguồn gốc từ các root store của trình duyệt, thay vào đó chuỗi Intermediate root của nó sẽ trở lại root của bên thứ ba đáng tin cậy. Điều này đôi khi được gọi là cross-signing.

Bây giờ, đây là nơi nó có thể có một chút khó hiểu. Như chúng ta đã thảo luận trước đó, CA không phát hành trực tiếp từ root của chúng. Họ thêm các lớp bảo mật bằng cách cấp trung gian (Intermediate) và sau đó ký chứng chỉ với nó. Điều này giúp giảm thiểu và phân chia thiệt hại trong trường hợp phát hành sai hoặc sự kiện bảo mật. Thay vì thu hồi chứng chỉ root và theo nghĩa đen là mọi chứng chỉ mà nó đã ký bằng phần mở rộng, bạn chỉ cần thu hồi trung gian (Intermediate), điều này chỉ ảnh hưởng đến 1 số nhóm chứng chỉ được cấp bởi trung gian đó bị vô hiệu hóa.

Đây là một ví dụ thực tế, Google và các trình duyệt khác gần đây đã không tin tưởng chứng chỉ SSL thương hiệu Symantec CA. Lúc đầu, có vẻ như là một sự kiện khá hoành tráng, không tin tưởng hàng triệu chứng chỉ SSL của người dùng cuối. Trên thực tế, nó rất đơn giản. Họ vừa loại bỏ tất cả các nguồn gốc của Symantec CA khỏi các trusted root store của họ. Bây giờ bất kỳ chứng chỉ nào được liên kết tới những root đó đều thất bại và không được tin tưởng. (Điều đáng chú ý là DigiCert đã làm sạch Symantec, nhưng điều này phục vụ như một ví dụ thực tế tốt cho cuộc thảo luận này.)

## Sự khác biệt giữa một chained root và một single root là gì?

Điều đó thực sự trở lại câu hỏi cuối cùng của chúng ta. Một root duy nhất được sở hữu bởi một CA. Nó có thể cấp chứng chỉ trực tiếp, làm cho nó đơn giản hơn nhiều để triển khai chứng chỉ và đơn giản hóa cài đặt. Một chained root là những gì một Sub CA sử dụng để phát hành chứng chỉ. Đó là một chứng chỉ trung gian (Intermediate certificates), nhưng, bởi vì Sub CA không có root đáng tin cậy của riêng mình là phải liên kết với CA của bên thứ ba có.

Điều này cũng tạo ra sự khác biệt. Đây là lý do tại sao:

* Chained root làm cho các cài đặt phức tạp hơn vì Root Intermediate cần phải được tải vào mọi máy chủ và ứng dụng lưu trữ chứng chỉ.
* Chained root không có quyền kiểm soát root, vì vậy nếu Root CA hết kinh doanh, nó cũng sẽ không hoạt động.
* Chứng chỉ Roots và Intermediate cũng sẽ hết hạn. Mặc dù trên các mốc thời gian dài, intermediate phải hết hạn trước root của nó, điều này làm tăng thêm sự phức tạp.

## Một từ cuối cùng về Roots and Intermediates

Những gì chúng ta vừa mô tả – mô hình ủy thác liên quan đến Cơ quan chứng chỉ, chuỗi chứng chỉ và chữ ký mật mã – về cơ bản là PKI (Public Key Infrastructure). Chúng ta đã tránh sử dụng thuật ngữ đó quá nhiều cho đến bây giờ bởi vì nó có vẻ rất trừu tượng cho đến khi bạn đi sâu vào các chi tiết cụ thể một chút.

Nhưng, khi ai đó đề cập đến PKI, đây là những gì họ muốn đề cập tới. Và với ý nghĩ đó, bạn có thể tìm ra cách thức một CA riêng tư và chứng chỉ tự ký được triển khai trong một Doanh nghiệp. Làm việc cùng với một CA đáng tin cậy, một tổ chức tạo ra một chứng chỉ gốc và private key. Tổ chức sau đó thêm root vào các root store của riêng mình, trên tất cả các hệ thống và thiết bị của mình. Và từ thời điểm đó, tổ chức có thể tự ký chứng chỉ X.509 của riêng mình bằng cách sử dụng private key từ private root của nó và chúng sẽ được tin cậy trên mạng của mình.

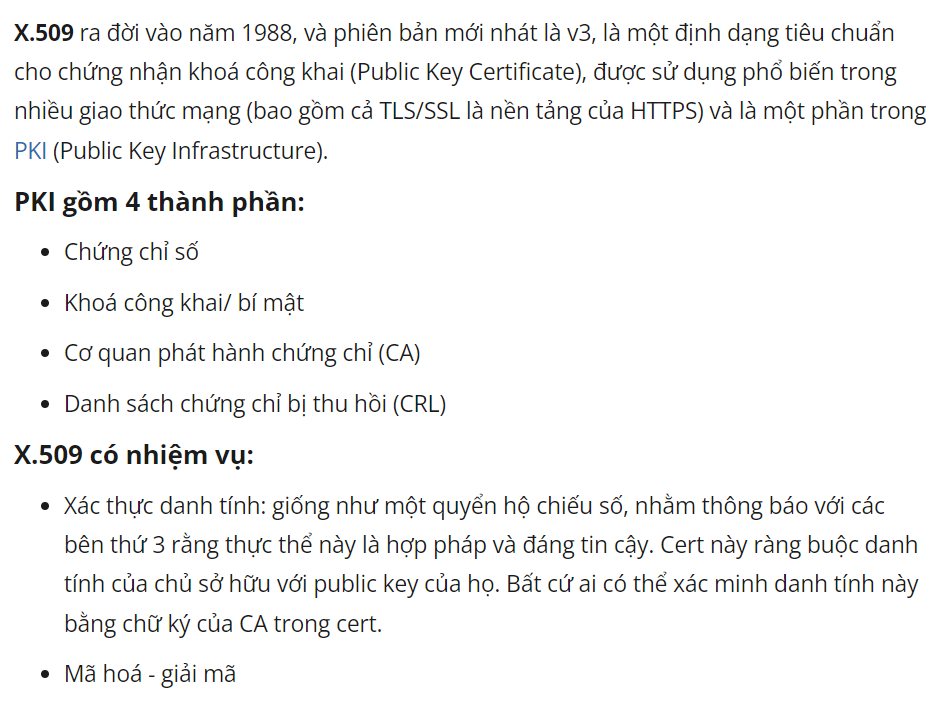
# Tài liệu chuẩn CA

X.509: Certificate được sử dụng hàng ngày.

Trong quá trình mình tìm hiểu mạng blockchain Hyperledger Fabric, mình có biết được một loại chứng chỉ là X.509.  
Tuy nhiên, sau khi tìm hiểu mình mới phát hiện ra là X.509 không hề xa lạ mà vẫn được ta sử dụng hàng ngày trong việc lướt web. Vậy nên bài viết này sẽ giải thích rõ về X.509 !

CA là bên thứ 3, nhà cung cấp chứng chỉ số như kiểu google, microsoft

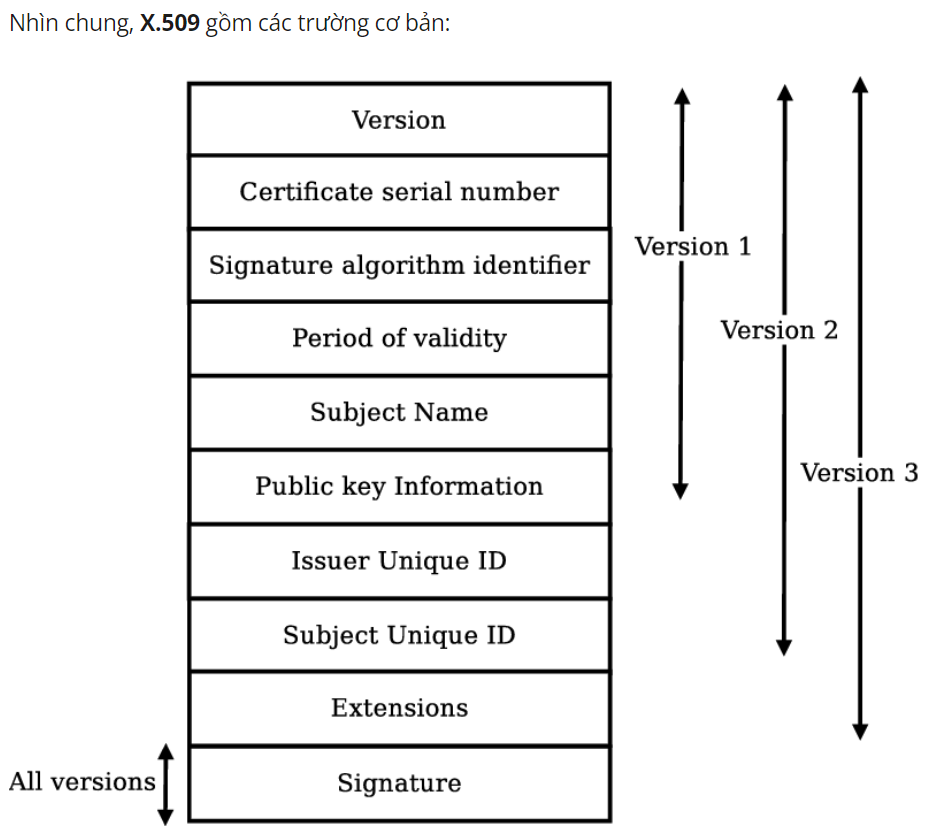
## 1. X.509 là gì ?

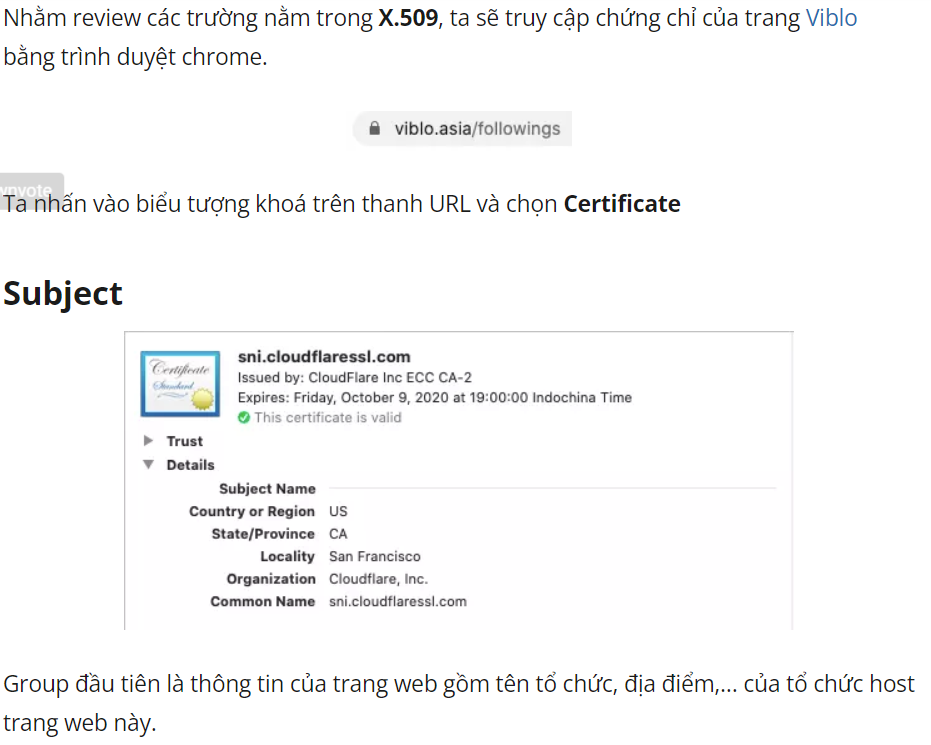


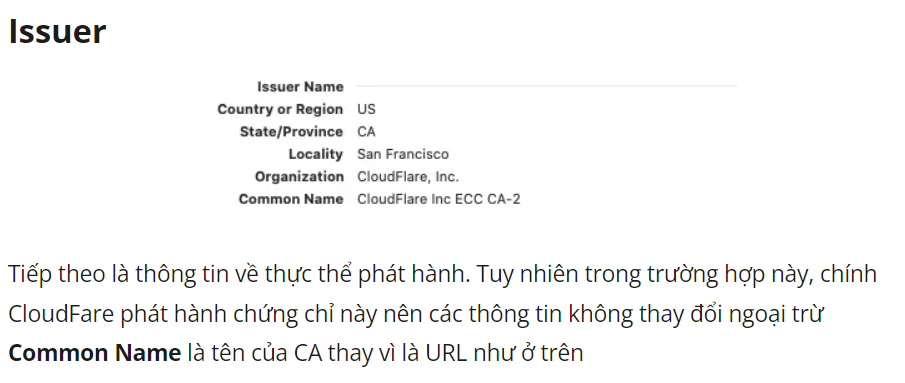
## 2. Cặp khoá và chữ ký số

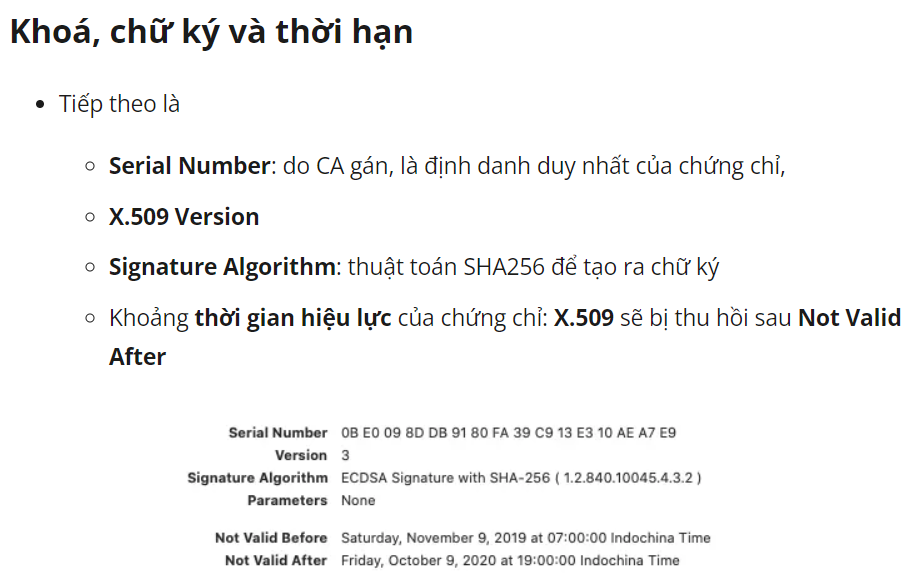


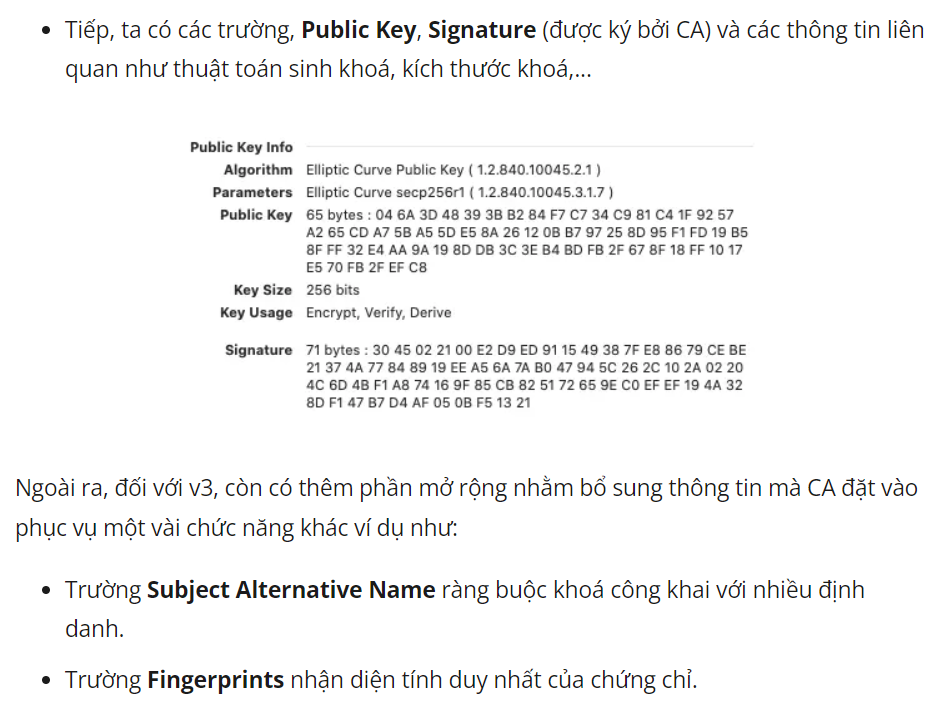
## 3. Các trường và phần mở rộng

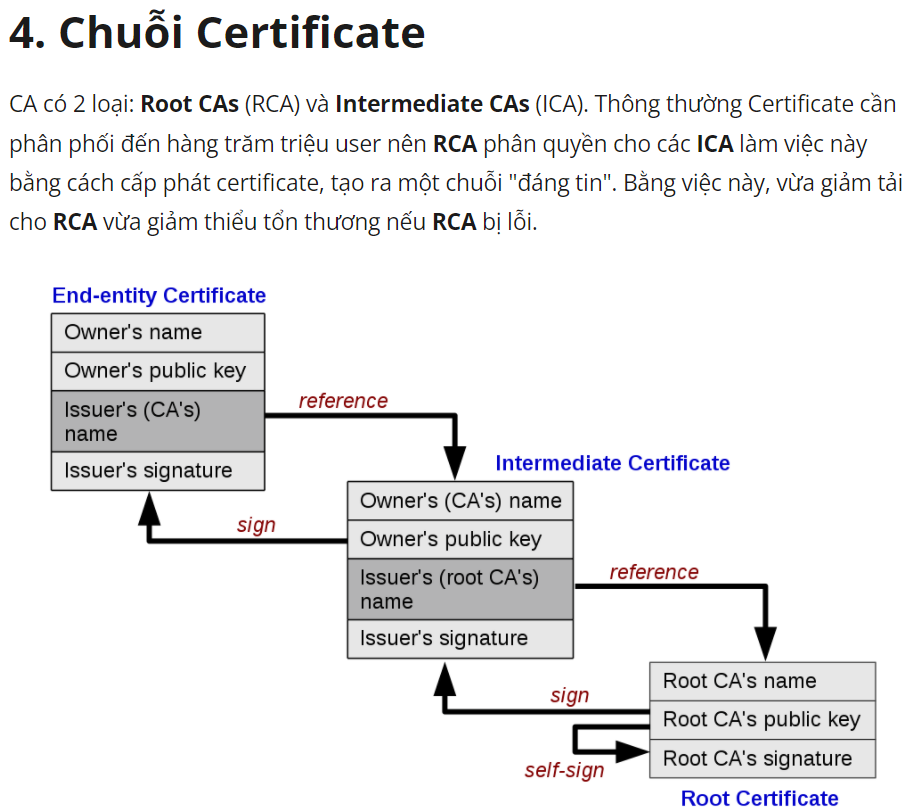


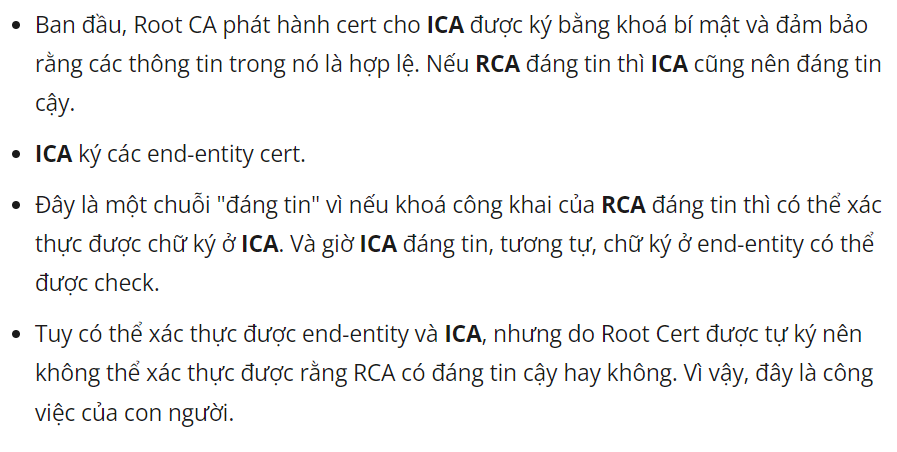


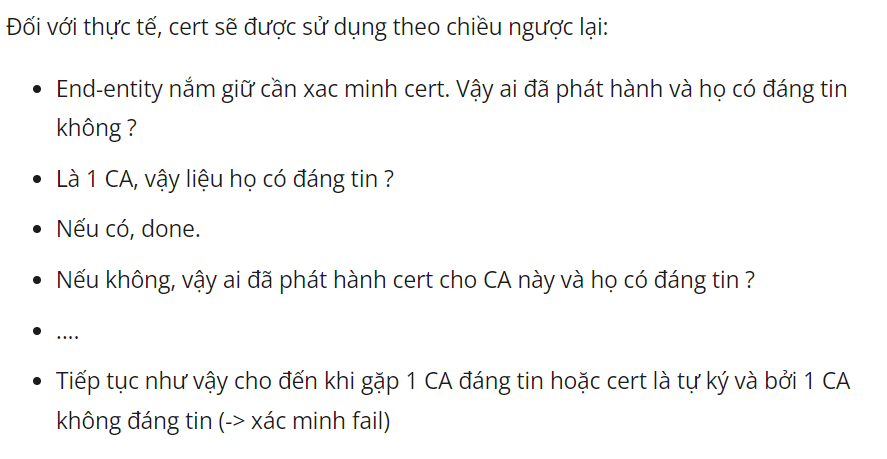


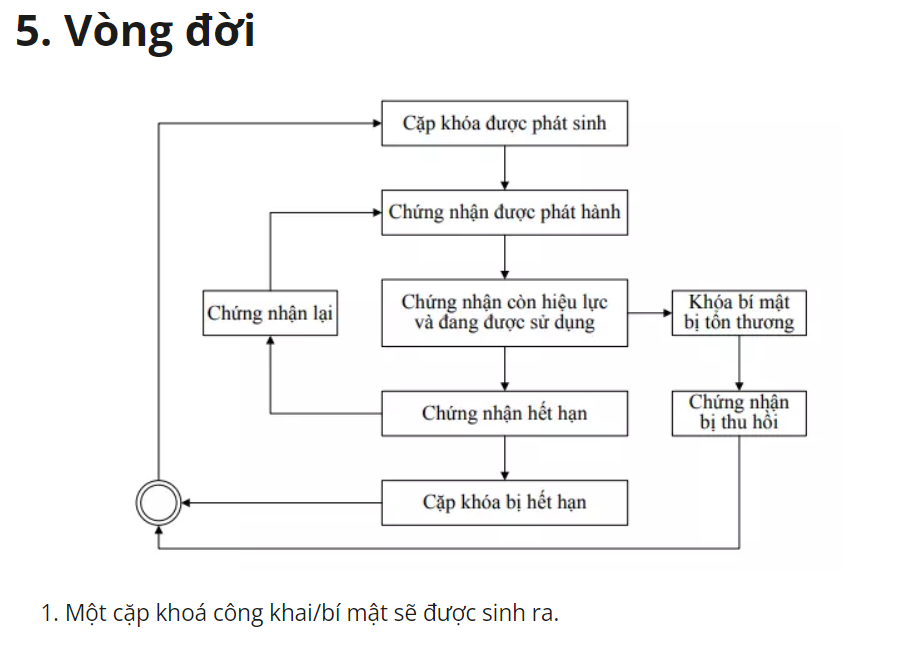




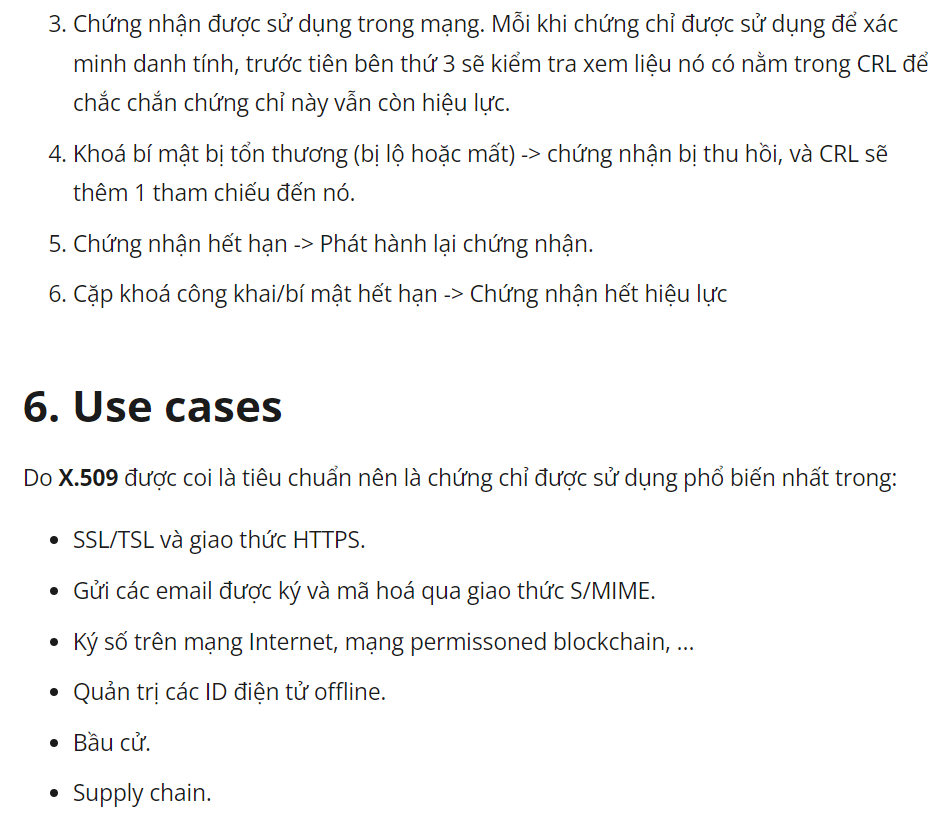
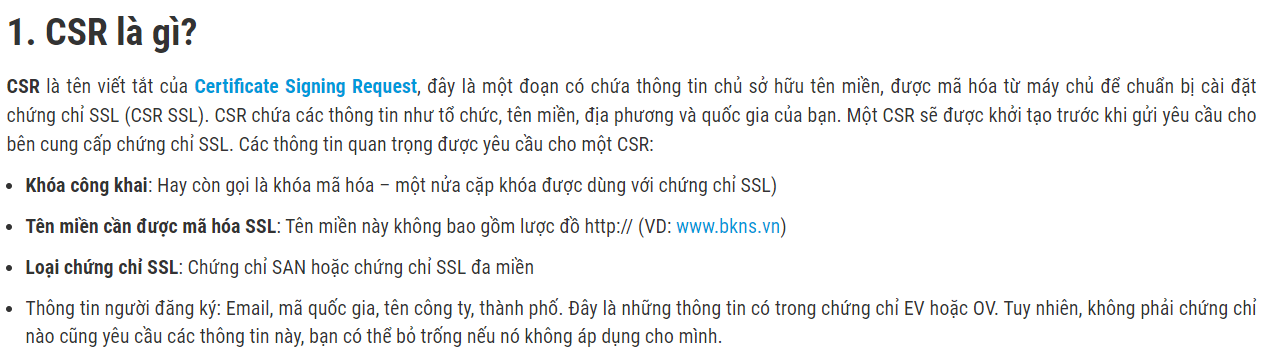








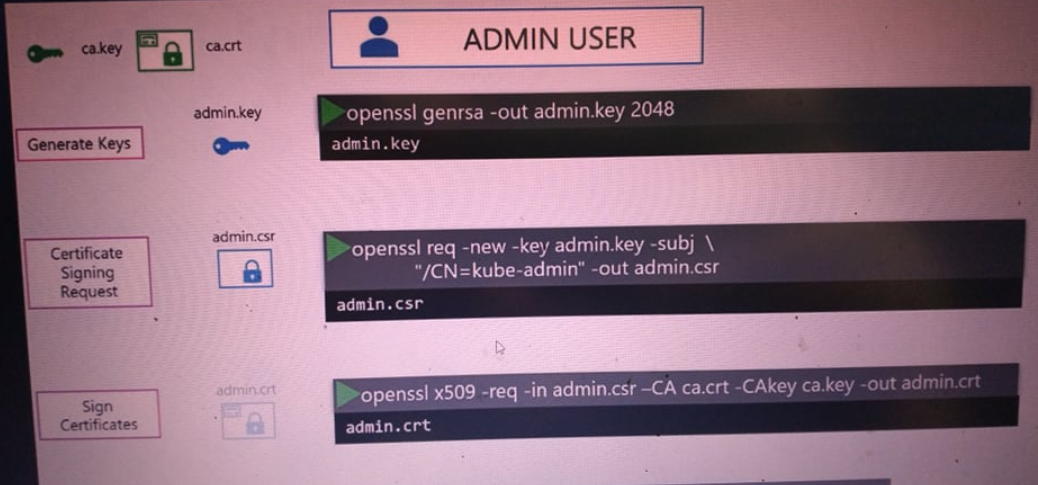
1. Phát hành chứng nhận bao gồm khoá công khai và chữ kỹ sinh ra từ khoá bí mật.

\



Đây là thông tin đăng ký của cert, nó là csr, được cấp bởi ECC CA-3 với domain là sni.cloud….

Csr chỉ là thông tin đăng ký chi tiết



Cái đầu tạo key

Cái thứ 2 là tạo thông tin của key

Cái thứ 3 là tạo cert chứa đầy đủ thông tin của 2 cái đầu **file.crt**