|  |  |
| --- | --- |
| logomobile.png | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**ĐỒ ÁN MÔN HỌC**

**Môn: BẢO MẬT THÔNG TIN**

SINH VIÊN THỰC HIỆN: Nguyễn Đặng Việt Thái

MSSV 1811060696 18DTHB3

Nguyễn Khánh Triệu

MSSV 1811062328 18DTHB4

TP. HỒ CHÍ MINH, 12/2020

**LỜI CẢM ƠN!**

“Đặc biệt, chúng em xin gửi lời cảm ơn sâu sắc đến giảng viên bộ môn –đã quan tâm hướng dẫn, truyền đạt những kiến thức quý báu cho chúng em trong suốt thời gian học tập vừa qua. Trong thời gian tham gia lớp học Bảo Mật Thông Tin của thầy, chúng em đã có thêm cho mình nhiều kiến thức bổ ích, tinh thần học tập hiệu quả, nghiêm túc. Đây chắc chắn sẽ là những kiến thức quý báu, là hành trang để chúng em có thể vững bước sau này.

Tuy nhiên, do vốn kiến thức còn nhiều hạn chế và khả năng tiếp thu thực tế còn nhiều bỡ ngỡ. Mặc dù, chúng em đã cố gắng hết sức nhưng chắc chắn khó có thể tránh khỏi những thiếu sót và nhiều chỗ còn chưa chính xác, kính mong quý thầy xem xét và góp ý để đồ án của chúng em được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn!”

TP.Thủ Đức, tháng 04 năm 2021

**LỜI NÓI ĐẦU**

Công nghệ Thông tin là một trong những ngành khoa học ngày càng được quan tâm và sử dụng rộng rãi trong mọi lĩnh vực của cuộc sống. Với những ưu điểm mạnh, có thể ứng dụng được nhiều trong cuộc sống

Báo cáo này được thực hiện tại trường Đại học Công Nghệ TP HCM dưới sự hướng dẫn của thầy. Nhóm xin được gửi lời cảm ơn sâu sắc nhất đến thầy đã định hướng, giúp đỡ, quan tâm và tạo mọi điều kiện thuận lợi trong suốt quá trình nghiên cứu để hoàn thành báo cáo này. Nhóm cũng xin được gửi lời cảm ơn đến thầy cũng như các bạn đã mang lại cho tôi những kiến thức vô cùng quý giá và bổ ích trong quá trình học tập tại trường.

Do thời gian và kiến thức có hạn nên không tránh khỏi những thiếu sót. Nhóm rất mong nhận được những góp ý quý báu của thầy cô và các bạn.

**MỤC LỤC**

[CHƯƠNG I: TỔNG QUAN VỀ GIAO THỨC ACME 5](#_Toc70592852)

[**1.1. Khái niệm về giao thức ACME (The Automatic Certificate Management Environment).** 5](#_Toc70592853)

[**1.2. Lịch sử về giao thức ACME.** 5](#_Toc70592854)

[**1.2.1. Tổng quát** 6](#_Toc70592855)

[**1.3. Thiết lập và xác thực** 7](#_Toc70592856)

[**1.4. Cấp, Gia hạn và Thu hồi Chứng chỉ** 7](#_Toc70592857)

[**1.5. Những lời ích** 9](#_Toc70592858)

[**1.5.1 Đại lý ACME phổ biến** 10](#_Toc70592859)

[CHƯƠNG II: Giới thiệu Let's Encrypt 10](#_Toc70592860)

[**2.1 Tổng quan** 10](#_Toc70592861)

[**2.2. Ứng dụng Let's Encrypt** 10](#_Toc70592862)

[**2.3. Nguyên tắt hoạt động** 10](#_Toc70592863)

[**2.4. Xác thực tên miền** 11](#_Toc70592864)

[**2.5. Cấp và Thu hồi Chứng chỉ** 12](#_Toc70592865)

[**2.6. Lý do Let’s Ecrypt thuyết phục người dùng** 14](#_Toc70592866)

[CHƯƠNG III: CÁCH LET’S ENCRYPT TẠO CHỨNG CHỈ SSL 15](#_Toc70592867)

[**3.1. Cách tạo chứng chỉ SSL miễn phí với Let’s Encrypt** 16](#_Toc70592868)

[**3.2. Các cách để có chứng chỉ SSL miễn phí** 17](#_Toc70592869)

[**3.3. Cách tạo SSL certificate với Let’s Encrypt** 17](#_Toc70592870)

[**3.4. Sửa file cấu hình cho website:** 19](#_Toc70592871)

[**3.5. Lỗi gia hạn tự động Let’s Encrypt và cách khắc phục** 20](#_Toc70592872)

[**3.5.1 Nguyên nhân gây ra lỗi** 20](#_Toc70592873)

[**3.5.2. Cách khắc phục lỗi gia hạn tự động Let’s Encrypt** 20](#_Toc70592874)

[**3.6. Kiểm tra việc gia hạn Let’s Encrypt** 21](#_Toc70592875)

[TÀI LIỆU THAM KHẢO 23](#_Toc70592876)

# CHƯƠNG I: TỔNG QUAN VỀ GIAO THỨC ACME

## **1.1. Khái niệm về giao thức ACME (The Automatic Certificate Management Environment).**

Môi trường quản lý chứng chỉ tự động (ACME) là một giao thức tiêu chuẩn để tự động xác thực miền, cài đặt và quản lý chứng chỉ X.509. Giao thức ACME được thiết kế bởi Nhóm Nghiên cứu Bảo mật Internet và được mô tả trong [IETF RFC 8555](https://tools.ietf.org/html/rfc8555). Là một tiêu chuẩn mở, được tài liệu hóa tốt với nhiều triển khai ứng dụng khách có sẵn, ACME đang được áp dụng rộng rãi như một giải pháp tự động hóa chứng chỉ doanh nghiệp.

Giao thức Môi trường quản lý chứng chỉ tự động (ACME) là một giao thức truyền thông để tự động hóa các tương tác giữa tổ chức cấp chứng chỉ và máy chủ web của người dùng, cho phép triển khai tự động cơ sở hạ tầng khóa công khai với chi phí rất thấp.



## **1.2. Lịch sử về giao thức ACME.**

ACME hay môi trường quản lý chứng chỉ tự động được thiết kế bởi ISRG ([Internet Security Research Group](https://www.abetterinternet.org/)) cho dịch vụ certificate authority. Nó cho phép các chứng chỉ do Let’s Encrypt cấp tự động được trưng dụng và được cài đặt trên các máy chủ web.

Vào tháng 3 năm 2019, IETF (Internet Engineering Task Force) là một tổ chức tiêu chuẩn mở về kĩ thuật internet đã chuẩn hóa ACME thành một giao thức cấp chứng chỉ, có thể sử dụng chung cho cộng đồng.

Ngày nay, bất kì một cơ quan cấp chứng chỉ nào hỗ trợ ACME đều có thể cho phép các người dùng có thể tự động hóa các hoạt động chứng chỉ cốt loại trên máy chủ của họ.

Đã có 2 phiên bản API hỗ trợ cho ACME:

API v1 được phát hành vào ngày 12 tháng 4 năm 2016. Nó hỗ trợ cấp chứng chỉ cho các tên miền đơn lẻ, chẳng hạn như example.com hoặc cluster.example.com. Let's Encrypt đề xuất rằng người dùng nên di chuyển sang phiên bản v2 càng sớm càng tốt vì hỗ trợ cho v1 được lên kế hoạch ngừng sử dụng. Nhiều ứng dụng khách ACME đã hỗ trợ v2 trước khi phát hành.

API v2 được phát hành vào ngày 13 tháng 3 năm 2018. Sau khi bị đẩy lùi nhiều lần. ACME v2 không tương thích ngược với v1. Phiên bản 2 hỗ trợ các miền ký tự đại diện, chẳng hạn như \* .example.com, cho phép nhiều miền phụ có SSL đáng tin cậy, ví dụ: https://cluster01.example.com,https://cluster02.example.com, https://example.com, trên các mạng riêng trong một miền duy nhất sử dụng một chứng chỉ "wildcard" được chia sẻ. Một yêu cầu mới chính trong v2 là yêu cầu chứng chỉ ký tự đại diện yêu cầu sửa đổi bản ghi TXT của Dịch vụ tên miền, xác minh quyền kiểm soát đối với miền.

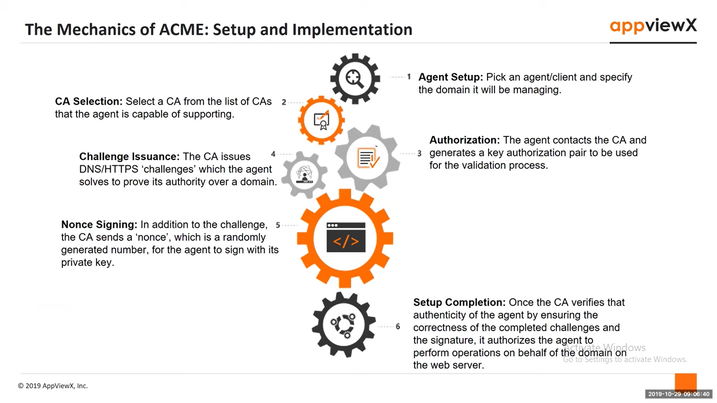
Các thay đổi đối với giao thức ACME v2 kể từ v1 bao gồm:

1. Quy trình cấp phép / phát hành đã thay đổi.
2. Ủy quyền yêu cầu JWS đã thay đổi.
3. Trường "tài nguyên" của các cơ quan yêu cầu JWS được thay thế bằng tiêu đề JWS mới: "url".
4. Đổi tên điểm cuối thư mục / tài nguyên.
5. URI -> Đổi tên URL trong tài nguyên thử thách.
6. Tạo tài khoản và thỏa thuận ToS là một bước thay vì hai bước.
7. Có một loại thử thách mới, TLS-SNI-02 và TLS-SNI-01 đã bị xóa. TLS-SNI-02 không còn được hỗ trợ vì nó có các vấn đề bảo mật giống như TLS-SNI-01, do đó TLS-ALPN-01 đã được giới thiệu.

### **1.2.1. Tổng quát**

ACME đang giải quyết vấn đề quan trọng của việc phải quản lý các chứng chỉ theo cách thủ công. Không có ACME, các hoạt động như tạo CSR, xác minh quyền sở hữu miền, tải xuống chứng chỉ và cài đặt là các quy trình hoàn toàn thủ công. ACME tự động hóa chúng bằng cách cài đặt tác nhân nguồn mở và ủy quyền cho tác nhân thực hiện các hoạt động này theo các khoảng thời gian đã định. Theo mặc định, tác nhân yêu cầu quyền truy cập vào máy chủ web HTTPS hoặc DNS để xác minh rằng nó hoạt động thay mặt cho một miền.

## **1.3. Thiết lập và xác thực**



Tác nhân ACME cần được thiết lập và định cấu hình chính xác trước khi nó có thể bắt đầu yêu cầu và cài đặt chứng chỉ. Dưới đây là danh sách các bước tiêu chuẩn trong quy trình:

1. ***Agent Setup:*** chọn một đại lý/khách hàng và chỉ định miền nó sẽ quản lý
2. ***CA Selection:*** chọn CA (Certificate Authority) từ danh sách CAs mà đại lý có khả năng hổ trợ
3. ***Authorization (ủy quyền):*** người đại diện liên hệ với CA và tạo một ủy quyền khóa được sửa dụng cho quá trình xác nhận
4. ***Challenge Issuance (vấn đề thử thách):*** các vấn đề về CA DNS/HTTPS ‘thử thách’ tác nhân giải quyết để giải quyết quyền hạn của mình đối với một miền
5. ***Nonce Siging:*** ngoài những thử thách CA gửi một “nonce” đây là một số được tạo, để đại lý ký với khóa cá nhân
6. ***Setup Completion (hoàn tất thiết lập) :*** sau khi CA xác minh rằng tính xác thực của đại lý bằng cách đảm bảo tính đúng đắn của các ‘thử thách’ đã hoàn thành và chữ ký nó cho phép người đại diện thực hiện các hoạt động thay mặt cho miền trên wed server

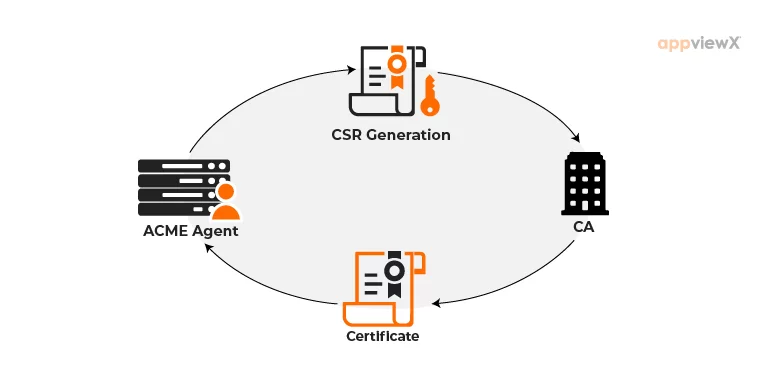
## **1.4. Cấp, Gia hạn và Thu hồi Chứng chỉ**

Khi tác nhân đã được thiết lập và xác minh, các hoạt động chứng chỉ có thể được tự động hóa.

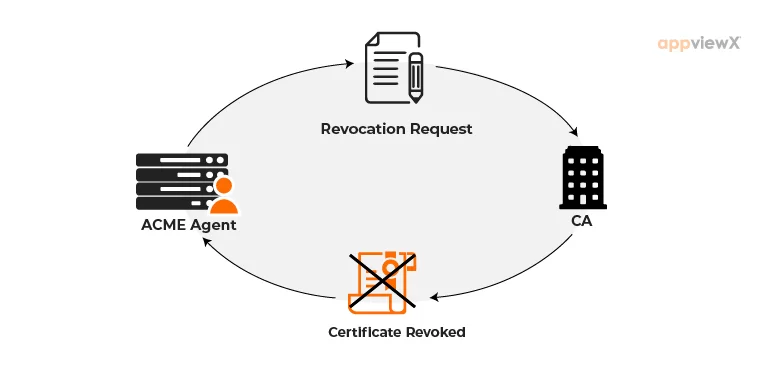
**Phát hành / Gia hạn:** Trong một chu kỳ gia hạn điển hình do ACME tạo điều kiện, máy chủ web có cài đặt tác nhân ACME. Tác nhân tạo CSR, chuyển nó cho CA và CA cấp nó. Quá trình này có thể được tận dụng để cấp chứng chỉ mới hoặc gia hạn chứng chỉ hiện có sắp hết hạn. Chúng ta hãy xem xét kỹ hơn chu kỳ.

Như với tất cả các hoạt động PKI, tác nhân tạo CSR và khóa công khai, ký cả hai bằng khóa cá nhân của máy chủ và gửi chúng đến CA phát hành. CA xác minh cả hai chữ ký và gửi chứng chỉ tới tác nhân, người này sẽ tiến hành cài đặt nó trên máy chủ.

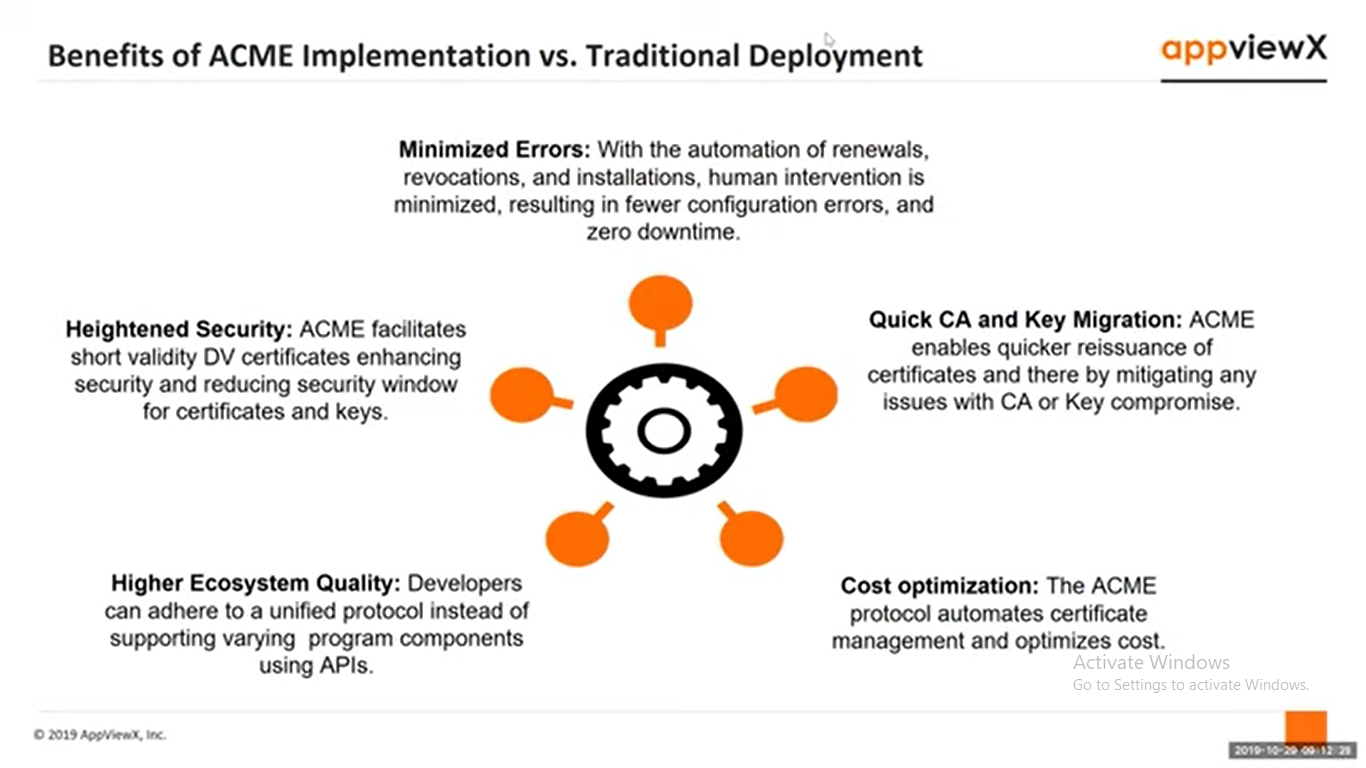
Gia hạn hoạt động theo cách tương tự. Tác nhân phải được định cấu hình để thực hiện các yêu cầu định kỳ tới CA theo các khoảng thời gian đã định, cho phép nó xoay các khóa và chứng chỉ theo mong muốn của quản trị viên.



**Thu hồi:** Khi một chứng chỉ cần được thu hồi, tác nhân sẽ ký yêu cầu thu hồi bằng khóa của nó và CA sử dụng chữ ký này để xác minh xem yêu cầu đó có hợp pháp hay không. Nếu đúng như vậy, nó sẽ xuất bản thông tin thu hồi trực tuyến (CRL, OCSP, v.v.), để các trình duyệt và các bên khác tham khảo.



## **1.5. Những lời ích**



* ***Minimized Errors (Ít lỗi cấu hình hơn):*** Ít lỗi cấu hình hơn Sự can thiệp của con người được loại bỏ, dẫn đến không có lỗi tiềm ẩn trong việc cấp, gia hạn, cài đặt và thu hồi chứng chỉ. Điều này cũng có thể làm giảm thời gian chết thực.
* ***Heightened Security*** ***(bảo mật nâng cao):*** Giao thức tạo điều kiện cho việc sử dụng chứng chỉ DV có giá trị thấp, thu hẹp chu kỳ thay thế, do đó tăng cường bảo mật.
* ***Highter Ecossystem Quality*** ***(Chất lượng hệ sinh thái cao hơn):*** Các nhà phát triển có thể tuân thủ một giao thức thống nhất thay vì hỗ trợ các thành phần chương trình khác nhau bằng cách sử dụng API.
* ***Quick CA và Key Migration:*** Với nhiều CA thương mại hỗ trợ ACME, người dùng có thể nhanh chóng chuyển sang một CA khác trong trường hợp có sự xâm phạm, tác nhân thậm chí có thể thay thế tất cả các chứng chỉ cũ bằng chứng chỉ mới từ CA mới***.***
* ***Cost optimization (tối ưu hóa chi phí):*** Việc tự động hóa các quy trình chứng chỉ giúp tiết kiệm thời gian và công sức, và do đó, chi tiêu. Hơn nữa, giao thức là mã nguồn mở và sử dụng miễn phí.

### **1.5.1 Đại lý ACME phổ biến**

Có rất nhiều tác nhân ACME có sẵn, dựa trên nguồn gốc mã nguồn mở của nó, nhưng đây là một số ứng dụng khách đáng chú ý hỗ trợ ACME v2. Không cần phải nói rằng v2 là phiên bản duy nhất nên được sử dụng, do sự mất giá sắp xảy ra và các thâm hụt bảo mật rõ ràng của v1.

* Certbot
* GetSSL
* Posh-ACME
* Caddy
* ACMESharp
* Nginx ACME

# CHƯƠNG II: Giới thiệu Let's Encrypt

## **2.1 Tổng quan**

Let’s Encrypt là chứng nhận (CA) mở, miễn phí và tự động, hoạt động vì lợi ích cộng đồng. Đây là dịch vụ được cung cấp bởi Internet Security Research Group (ISRG).

## **2.2. Ứng dụng Let's Encrypt**

cung cấp cho mọi người các chứng chỉ kỹ thuật số họ cần để kích hoạt HTTPS (SSL/TLS) cho các trang web, miễn phí, theo cách thân thiện nhất với người dùng mà chúng tôi có thể. Chúng tôi làm điều này bởi vì chúng tôi muốn tạo ra một trang web an toàn và bảo mật hơn.

## **2.3. Nguyên tắt hoạt động**

+ Miễn phí: Bất cứ ai sở hữu một tên miền có thể dùng Let’s Encrypt để có được một chứng chỉ tin cậy với chi phí bằng không.

+ Tự động: Phần mềm chạy trên máy chủ web có thể tương tác với Let’s Encrypt để lấy chứng chỉ một cách dễ dàng, cấu hình an toàn để sử dụng và tự động gia hạn.

+ An toàn: Let’s Encrypt sẽ phục vụ như một nền tảng để thúc đẩy các thực hành tốt nhất về bảo mật TLS, cả về phía CA và bằng cách giúp những người vận hành trang web bảo mật đúng cách các máy chủ của họ.

+ Trong suốt: Tất cả các chứng chỉ được cấp hoặc thu hồi sẽ được ghi lại công khai và có sẵn cho bất kỳ ai muốn kiểm tra.

+ Mở: Giao thức phát hành và gia hạn tự động sẽ được công bố như một tiêu chuẩn mở mà những người khác có thể áp dụng.

Hợp tác: Giống như các giao thức Internet cơ bản, Let’s Encrypt là một nỗ lực chung nhằm mang lại lợi ích cho cộng đồng, vượt ra ngoài tầm kiểm soát của bất kỳ một tổ chức nào.

Mục tiêu của Let’s Encrypt và giao thức ACME là giúp bạn có thể thiết lập máy chủ HTTPS và để máy chủ này tự động nhận được chứng chỉ được trình duyệt tin cậy mà không cần bất kỳ sự can thiệp nào của con người. Điều này được thực hiện bằng cách chạy tác nhân quản lý chứng chỉ trên máy chủ web.

Để hiểu cách hoạt động của công nghệ, hãy cùng tìm hiểu quy trình thiết lập https://example.com/ với đại lý quản lý chứng chỉ hỗ trợ Let’s Encrypt.

Có hai bước cho quá trình này. Đầu tiên, tác nhân chứng minh với CA rằng máy chủ web kiểm soát một miền. Sau đó, đại lý có thể yêu cầu, gia hạn và thu hồi chứng chỉ cho miền

## **2.4. Xác thực tên miền**

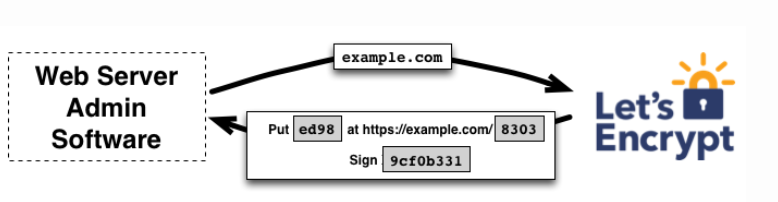
Let’s Encrypt xác định quản trị viên máy chủ bằng khóa công khai. Lần đầu tiên phần mềm tác nhân tương tác với Let’s Encrypt, nó sẽ tạo ra một cặp khóa mới và chứng minh với Let’s Encrypt CA rằng máy chủ kiểm soát một hoặc nhiều miền. Điều này tương tự như quy trình CA truyền thống là tạo tài khoản và thêm miền vào tài khoản đó.

Để bắt đầu quá trình, đại lý hỏi Let’s Encrypt CA những gì nó cần làm để chứng minh rằng nó kiểm soát example.com. Let’s Encrypt CA sẽ xem xét tên miền được yêu cầu và đưa ra một hoặc nhiều bộ thử thách. Đây là những cách khác nhau mà đại lý có thể chứng minh quyền kiểm soát miền. Ví dụ: CA có thể cho người đại diện một trong hai lựa chọn:

Cấp phép bản ghi DNS trong example.com hoặc

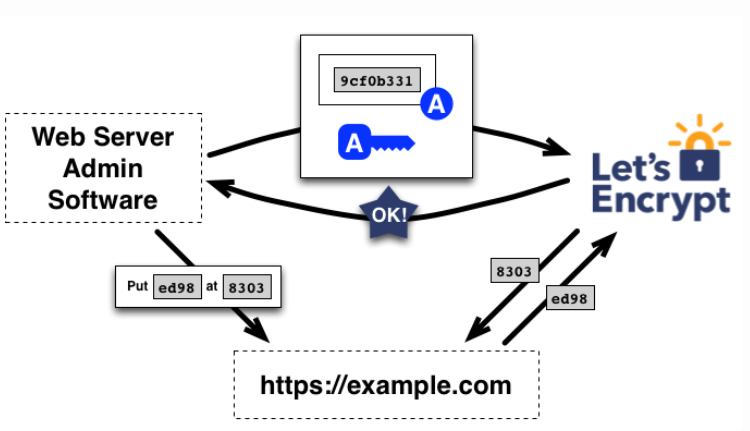
Cấp phép tài nguyên HTTP trong một URI nổi tiếng trên http://example.com/

Cùng với những thách thức, Let’s Encrypt CA cũng đưa ra quy định bắt buộc rằng tác nhân phải ký bằng cặp khóa riêng tư của mình để chứng minh rằng họ kiểm soát cặp khóa.



Phần mềm đại lý hoàn thành một trong những bộ thử thách được cung cấp. Giả sử nó có thể hoàn thành nhiệm vụ thứ hai ở trên: nó tạo một tệp trên một đường dẫn cụ thể trên trang web http://example.com. Người đại diện cũng ký nonce được cung cấp bằng khóa riêng của nó. Khi tác nhân đã hoàn thành các bước này, tác nhân sẽ thông báo cho CA rằng họ đã sẵn sàng hoàn tất quá trình xác thực.

Sau đó, nhiệm vụ của CA là kiểm tra xem các thử thách đã được thỏa mãn chưa. CA xác minh chữ ký trên nonce và nó cố gắng tải xuống tệp từ máy chủ web và đảm bảo rằng nó có nội dung như mong đợi.



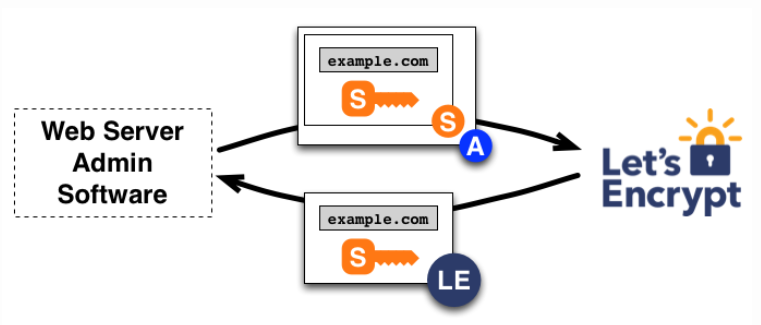
Nếu chữ ký trên nonce là hợp lệ và các thử thách được kiểm tra, thì tác nhân được xác định bằng khóa công khai được ủy quyền thực hiện quản lý chứng chỉ cho example.com. Chúng tôi gọi cặp khóa mà tác nhân đã sử dụng “cặp khóa được ủy quyền” cho example.com.

## **2.5. Cấp và Thu hồi Chứng chỉ**

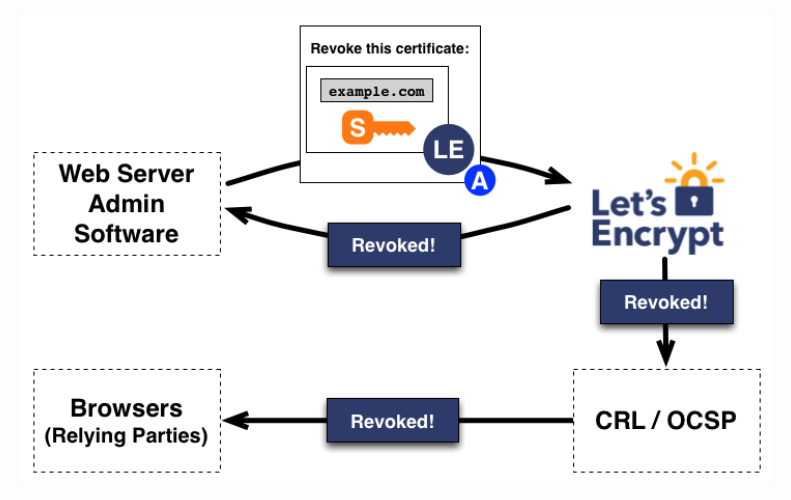
Sau khi tác nhân có cặp khóa được ủy quyền, việc yêu cầu, gia hạn và thu hồi chứng chỉ rất đơn giản — chỉ cần gửi thông báo quản lý chứng chỉ và ký chúng bằng cặp khóa được ủy quyền.

Để có được chứng chỉ cho miền, tác nhân tạo Yêu cầu ký chứng chỉ PKCS # 10 yêu cầu Let’s Encrypt CA cấp chứng chỉ cho example.com với một khóa công khai được chỉ định. Như thường lệ, CSR bao gồm chữ ký bằng khóa riêng tương ứng với khóa công khai trong CSR. Người đại diện cũng ký toàn bộ CSR bằng khóa được ủy quyền cho example.com để Let’s Encrypt CA biết nó được ủy quyền.

Khi Let’s Encrypt CA nhận được yêu cầu, nó sẽ xác minh cả hai chữ ký. Nếu mọi thứ có vẻ ổn, nó sẽ cấp chứng chỉ cho example.com với khóa công khai từ CSR và trả lại cho đại lý.



Thu hồi hoạt động theo cách tương tự. Tác nhân ký yêu cầu thu hồi bằng cặp khóa được ủy quyền cho example.com và Let’s Encrypt CA xác minh rằng yêu cầu được ủy quyền. Nếu vậy, nó xuất bản thông tin thu hồi vào các kênh thu hồi thông thường (tức là OCSP), để các bên phụ thuộc như trình duyệt có thể biết rằng họ không nên chấp nhận chứng chỉ đã thu hồi.



## **2.6. Lý do Let’s Ecrypt thuyết phục người dùng**

**Hoàn toàn miễn phí:** chỉ cần sở hữu một tên miền bạn có thể sử dụng Let’s Encrypt để có được chứng chỉ tin cậy mà không phải bỏ ra bất kì chi phí nào

**Dể dàng cài đặt:** thông qua Control Panel phổ biến như cPanel, DirectAdmin và Plesk

Không yêu cầu chứng thực qua email…

Không yêu cầu sử dụng trên địa chỉ IP riêng (có phát sinh phí khi đăng ký thêm IP)

**Mở rộng hợp tác không hạn chế:** với tính chất mở, giao thức phát hành và gia hạn tự động sẽ được công bố như một tiêu chuẩn công khai và người khác có thể áp dụng. Giống như những giao thức Internet cơ bản khác, Let’s Encrypt nổ lực để mang lại lợi ích cho cộng đồng và không nằm dưới sự kiểm soát của bất kì tổ chức nào

**Được tin cậy bới các trình duyệt:** hoạt động như một nền tảng thức đẩy những TLS tốt nhất, cả về phía CA (Certificate Authority), Let’s Encrypt giúp các nhà khai thác trang wed đảm bảo an toàn cho máy chủ một cách đúng đắn

**Độ rõ ràng và minh bạch:** tất cả các chứng chỉ được ban hành hoặc thu hồi sẽ được ghi công khai và bất kì ai cũng có thể kiểm tra

**Tính tự động cao:** phần mềm chạy trên máy chủ wed có thể tương tác với Let’s Encrypt để có được chứng chỉ một cách nhanh chóng cấu hình an toàn sẳn sàng sửa dụng và tự động thy mới khi cần. Song song đó chứng chỉ SSL của Let’s Encrypt theo chuẩn Domain Validation, do đó bạn cần tên miền và sử dụng chúng bất kì máy chủ nào.

# CHƯƠNG III: CÁCH LET’S ENCRYPT TẠO CHỨNG CHỈ SSL

Mục tiêu của Let’s Encrypt và giao thức ACME là thiết lập máy chủ HTTPS và để nó tự động có được chứng nhận đáng tin cậy trên trình duyệt mà không cần có bất kỳ sự can thiệp nào của con người. Điều này được thực hiện bằng cách chạy một trình quản lý chứng chỉ trên máy chủ web.

Để hiểu công nghệ của Let’s Encrypt làm việc như thế nào, hãy cùng tìm hiểu quá trình thiết lập trang web https:.//example.com/ với trình quản lý chứng chỉ hỗ trợ Let’s Encrypt.

Có 2 bước trong quá trình này. Đầu tiên, trình quản lý sẽ chứng minh với CA rằng máy chủ web đang kiểm soát một [tên miền](https://www.semtek.com.vn/). Sau đó, trình quản lý có thể yêu cầu, đổi mới hoặc thu hồi chứng chỉ cho [tên miền](https://www.semtek.com.vn/) đó.

**Xác nhận tên miền**

Let’s Encrypt xác định quyền quản trị máy chủ bằng khóa công khai. Lần đầu tiên, phần mềm quản lý tương tác với Let’s Encrypt, nó tạo ra một cặp khóa mới và chứng minh với Let’s Encrypt CA rằng máy chủ đang kiểm soát một hoặc vài [tên miền](https://www.semtek.com.vn/). Điều này cũng tương tự như quá trình CA truyền thống tạo tài khoản và thêm tên miền vào tài khoản đó.

Để khởi động quá trình này, trình quản lý yêu cầu Let’s Encrypt CA cung cấp thông tin cần thiết để chứng minh rằng nó đang kiểm soát example.com. Let’s Encrypt sẽ xem xét và đưa ra các yêu cầu, bạn cần hoàn thành nó để chứng minh mình có quyền kiểm soát tên miền.

Bạn có hai lựa chọn:

Cung cấp một bản ghi DNS dưới tên example.com

Cung cấp nguồn HTTP dưới URL được biết đến trên

Sau khi hoàn thành các yêu cầu, Let’s Encrypt sẽ cung cấp cho trình quản lý chứng chỉ một cặp khóa riêng để chứng minh rằng nó kiểm soát cặp khóa.

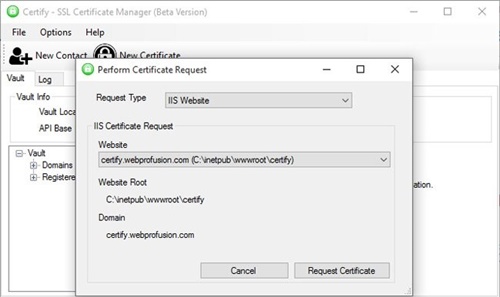
Đến đây, trình quản lý đặt một tập tin trên đường dẫn được chỉ định trên trang web . Trình quản lý cũng ký một khóa riêng, sau khi hoàn thành sẽ thông báo cho CA rằng nó đã hoàn thành xác nhận.

Công việc tiếp theo của CA là kiểm tra xem các yêu cầu đưa ra đã được thỏa mãn hay chưa. CA xác minh chữ ký, cố gắng tải về tập tin từ máy chủ web và chắc chắn rằng nó sẽ lấy được nội dung mong muốn.

Nếu chữ ký hợp lệ, các yêu cầu đã được thỏa mãn, trình quản lý được xác định bằng khóa công khai được ủy quyền để làm quản lý chứng chỉ cho example.com. Cặp khóa mà trình quản lý sử dụng cho example.com được gọi là “cặp khóa ủy quyền”.

Phần mềm quản lý chứng chỉ SSL trên máy chủ Windows – Certify

Let’s Encrypt là dịch vụ miễn phí để tạo chứng chỉ SSL tin cậy cho tên miền của bạn, nhưng hầu hết các công cụ chỉ là dòng lệnh. Nếu bạn đang sử dụng máy chủ Windows thì hãy cài thêm Certify. Phần mềm này mang đến giao diện người dùng đơn giản để quản lý chứng chỉ SSL. Chỉ cần bật Certify trên máy chủ web IIS để bắt đầu.



Tính năng chính của Certify:

Dễ dàng cài đặt

Dễ dàng tạo yêu cầu chứng chỉ, ủy quyền, đổi chứng chỉ mới

Quản lý các chứng chỉ và những thông tin liên quan

Tính năng IIS Lockdown giúp dễ dàng theo dõi những SSL tốt nhất cho việc vô hiệu hóa các giao thức và mật mã không an toàn

## **3.1. Cách tạo chứng chỉ SSL miễn phí với Let’s Encrypt**

Hiện nay hầu hết các trang web đều đã hỗ trợ SSL (Secure Socket Layer). Nó mã hóa [dữ liệu](https://www.semtek.com.vn/du-lieu-la-gi/#Du_lieu_lon_-_Big_Data_tai_sao_duoc_nhac_den_ngay_cang_nhieu) truyền đi giữa máy chủ web và trình duyệt và làm tăng tính bảo mật cho website.

Ngoài ra, việc sử dụng SSL certificate (chứng chỉ SSL) là cần thiết bởi hiện tại Google đã ưu tiên xếp hạng website dựa theo giao thức https (HTTP + SSL), những website mà chỉ sử dụng giao thức http sẽ bị coi là “unsafe” (không an toàn).

Có nhiều loại chứng chỉ SSL cung cấp các mức độ bảo mật khác nhau. Ví dụ chúng ta có thể mua một chứng chỉ SSL tại Namecheap với các mức giá khác nhau tùy từng loại. Tuy nhiên trong bài viết này chúng ta sẽ chỉ nói đến loại cơ bản nhất và làm thế nào để có được nó một cách miễn phí

## **3.2. Các cách để có chứng chỉ SSL miễn phí**

Sử dụng Cloudflare: Đây là một website cung cấp dịch vụ tăng tốc và bảo mật website, họ có cung cấp chứng chỉ SSL ở gói Free. Việc đăng ký rất dễ dàng nên mình sẽ không hướng dẫn ở đây.  
Chú ý là với website chỉ phục vụ người dùng tại Việt Nam thì chạy qua Cloudflare có thể sẽ chậm hơn 1 chút do sử dụng CDN server ngoài Việt Nam.

Sử dụng Let’s Encrypt: Sử dụng dịch vụ này chúng ta sẽ tự tạo SSL certificate cho riêng mình và hoàn toàn miễn phí.

## **3.3. Cách tạo SSL certificate với Let’s Encrypt**

Giả sử chúng ta đang sử dụng 1 server Ubuntu với tài khoản [truy cập](https://www.semtek.com.vn/kiem-tra-luot-truy-cap-website/) có quyền sudo và sử dụng [web server](https://www.semtek.com.vn/web-server-la-gi/) là Nginx.

**Bước 1: Cài đặt gói letsencrypt (với bản mới sẽ đổi tên là certbot và dùng lệnh certbot thay cho letsencrypt)**

sudo apt-get update

sudo apt-get install letsencrypt

hoặc làm theo hướng dẫn tại trang chủ

**Bước 2: Tạo SSL certificate**

Thêm đoạn cấu hình sau vào block server của file cấu hình cho website (thường nằm trong /etc/nginx/sites-enabled hoặc /etc/nginx/conf.d) để cho phép [truy cập](https://www.semtek.com.vn/kiem-tra-luot-truy-cap-website/) vào thư mục ẩn (.well-known) phục vụ cho việc xác thực:

…

location ~ /.well-known {

allow all;

}

…

Khởi động lại Nginx (sau khi khởi động xong nhớ kiểm tra lại xem website còn hoạt động không  ):

sudo systemctl restart nginx

Tạo SSL certificate (thay example.com bằng tên miền của bạn và /var/www/example.com là đường dẫn đến thư mục gốc của website):

sudo letsencrypt certonly -a webroot –webroot-path=/var/www/example.com -d example.com -d www.example.com

Nếu thành công output sẽ trông như sau:

IMPORTANT NOTES:

– If you lose your account credentials, you can recover through

e-mails sent to sammy@digitalocean.com

– Congratulations! Your certificate and chain have been saved at

/etc/letsencrypt/live/example.com/fullchain.pem. Your

cert will expire on 2016-03-15. To obtain a new version of the

certificate in the future, simply run Let’s Encrypt again.

…

**Bước 3: Cấu hình SSL cho website**

Để tăng tính bảo mật, tạo Strong Diffie-Hellman Group (dùng cho Nginx) :

sudo openssl dhparam -out /etc/[ssl](https://www.semtek.com.vn/ssl-la-gi/)/certs/dhparam.pem 2048

Tạo 1 snippet cho Nginx để có thể tái sử dụng được khi muốn cấu hình cho nhiều website:

sudo nano /etc/nginx/snippets/[ssl](https://www.semtek.com.vn/ssl-la-gi/)-params.conf

Nội dung file như sau:

ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_prefer\_server\_ciphers on;

ssl\_ciphers “EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH”;

ssl\_ecdh\_curve secp384r1;

ssl\_session\_cache shared:SSL:10m;

ssl\_stapling on;

ssl\_stapling\_verify on;

ssl\_dhparam /etc/[ssl](https://www.semtek.com.vn/ssl-la-gi/)/certs/dhparam.pem;

resolver 8.8.8.8 8.8.4.4 valid=300s;

resolver\_timeout 5s;

add\_header Strict-Transport-Security “max-age=63072000; includeSubdomains”;

add\_header X-Frame-Options DENY;

add\_header X-Content-Type-Options nosniff;

## **3.4. Sửa file cấu hình cho website:**

Tạo [redirect](https://www.semtek.com.vn/redirect-la-gi/#Tim_hieu_ve_redirect_la_gi_trong_SEO) 301 cho block server listen 80 (http) nếu bạn chỉ muốn support https (khi người dùng truy cập với giao thức http sẽ tự động chuyển thành https)

server {

listen      80;

server\_name example.com www.example.com;

return      301 https://$server\_name$request\_uri;

}

Tạo thêm 1 block server listen 443 (https)

server {

listen      443 ssl http2;

server\_name example.com www.example.com;

ssl\_certificate     /etc/letsencrypt/live/example.com/fullchain.pem;

ssl\_certificate\_key /etc/letsencrypt/live/example.com/privkey.pem;

include snippets/ssl-params.conf;

root /var/www/example.com;

location ~ /.well-known {

allow all;

}

}

Chú ý thay toàn bộ example.com bằng domain của mình và đường dẫn root /var/www/example.com giống bước tạo SSL certificate.

Sau khi cấu hình xong thì khởi động lại Nginx

sudo systemctl restart nginx

Truy cập thử website để xem thành quả hoặc kiểm tra bằng trang sau:

Gia hạn SSL certificate với Let’s Encrypt

SSL tạo theo cách sử dụng Let’s Encrypt sẽ hết hạn sau 90 ngày và chúng ta sẽ phải gia hạn bằng lệnh sau:

sudo certbot renew

Để tự động hóa việc này chúng ta có thể cấu hình cronjob để tự động gia hạn chứng chỉ.

Ví dụ cấu hình cronjob để tự động gia hạn mỗi 60 ngày:

sudo crontab -e

Thêm vào dòng sau (đặt lịch cứ mỗi 2 tháng tự động chạy lệnh renew vào lúc 0h30):

30 0 1 \*/2 \* /usr/bin/letsencrypt renew && /bin/systemctl reload nginx

## **3.5. Lỗi gia hạn tự động Let’s Encrypt và cách khắc phục**

### **3.5.1 Nguyên nhân gây ra lỗi**

Tên miền của bạn đang trỏ về IP khác

Một trong các yêu cầu bắt buộc trước khi cài Let’s Encrypt bằng tính năng AutoSSL (SSL/TLS Status) trong cPanel là tên miền của bạn phải được trỏ về đúng IP của host. Sau khi cài đặt thành công, nếu bạn vô tình hay hữu ý trỏ tên miền sang một địa chỉ IP khác thì hệ thống sẽ gặp lỗi khi gia hạn tự động.

Tên miền của bạn đang redirect sang một tên miền khác

Nếu bạn cài Let’s Encrypt trên các tên miền phụ và thiết lập [redirect](https://www.semtek.com.vn/redirect-la-gi/#Tim_hieu_ve_redirect_la_gi_trong_SEO) 301 (bằng file .[htaccess](https://www.semtek.com.vn/htaccess-la-gi-2/" \t "_self) chẳng hạn) sang tên miền chính thì việc này cũng sẽ dẫn đến lỗi không thể gia hạn tự động Let’s Encrypt trên các tên miền phụ.

Bạn đang sử dụng CloudFlare CDN

Sử dụng CloudFlare làm CDN đồng nghĩa với việc địa chỉ IP của host sẽ bị tự động thay thế bằng địa chỉ IP của CloudFlare. Điều này dẫn đến việc hệ thống sẽ xác định tên miền đang không được trỏ về IP của host và không thể tiến hành gia hạn SSL được.

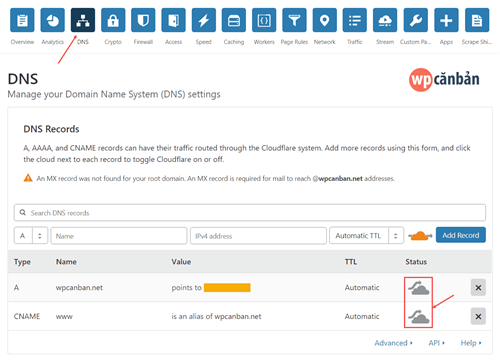
### **3.5.2. Cách khắc phục lỗi gia hạn tự động Let’s Encrypt**

Từ những nguyên nhân kể trên, chúng ta có thể khắc phục lỗi gia hạn Let’s Encrypt bằng các phương pháp đơn giản như sau:

Trỏ tên miền về đúng IP của host

Nếu bạn đang trỏ tên miền về một địa chỉ IP khác, hãy kiểm tra và trỏ nó về đúng IP của host. Bạn có thể sử dụng các công cụ như intoDNS hay IP Checker để kiểm tra địa chỉ IP mà tên miền đang được trỏ.

Nếu bạn đang sử dụng CloudFlare, tạm thời hãy tắt tính năng CDN của nó đi, bằng cách truy cập vào tài khoản CloudFlare => chọn tên miền tương ứng => chọn tab DNS => Click vào các [đám mây](https://www.semtek.com.vn/luu-tru-du-lieu-tren-dam-may/) màu cam trong cột Status để chuyển nó sang màu xám.



Đợi khi hệ thống gia hạn SSL thành công, hãy lặp lại các bước kể trên để chuyển các đám mây màu xám sang màu cam (kích hoạt lại CloudFlare CDN).

Vô hiệu hóa tính năng redirect tên miền

Nếu bạn đang [redirect](https://www.semtek.com.vn/redirect-la-gi/#Tim_hieu_ve_redirect_la_gi_trong_SEO) tên miền muốn gia hạn Let’s Encrypt sang một tên miền khác, hãy vô hiệu hóa tính năng [redirect](https://www.semtek.com.vn/redirect-la-gi/) cho đến khi việc gia hạn thành công. Ví dụ, tôi đang [redirect](https://www.semtek.com.vn/redirect-la-gi/) tên miền wpcanban.net sang tên miền wpcanban.com bằng file .[htaccess](https://www.semtek.com.vn/htaccess-la-gi-2/" \t "_self), tôi sẽ vô hiệu hóa tính năng này bằng cách đổi tên file .[htaccess](https://www.semtek.com.vn/htaccess-la-gi-2/) thành .htaccess\_old.

## **3.6. Kiểm tra việc gia hạn Let’s Encrypt**

Để biết liệu tên miền đã được gia hạn Let’s Encrypt thành công hay chưa, đối với các hosting cPanel được trang bị AutoSSL, các bạn có thể truy cập vào mục SSL/TLS Status để xem kết quả.

Thông thường, hệ thống sẽ mất khoảng 1 ngày để tự động gia hạn Let’s Encrypt. Nếu bạn không muốn chờ lâu hay SSL của bạn đã hết hạn, không thể chờ thêm được nữa, hãy click vào nút Run AutoSSL để tiến hành gia hạn ngay lập tức. Quá trình có thể mất từ vài phút đến vài tiếng, do đó hãy kiên nhẫn chờ đợi cho đến khi hoàn tất nhé.

# TÀI LIỆU THAM KHẢO

[**https://blog.tinohost.com/**](https://blog.tinohost.com/)

[**https://hungcoi.com/**](https://hungcoi.com/)

# 