**SSL Certificate** là gì ?

**SSL Certificate**(hay còn được gọi là chứng chỉ SSL – **Sercure Socket Layer**) là giao thức bảo mật các thông tin được lưu hành từ website đến các trình duyệt web, các thông tin, dữ liệu trên trang web và khả năng hiển thị, hoạt động của website trên mạng Internet.

Nói theo cách dễ hiểu, **SSL Certificate** giống như một phương tiện “chứng thực” nhằm xác minh đây là một website có bản quyền, thuộc sở hữu của các cá nhân hay tập thể nhất định và chính vì vậy nó được bảo hộ về nội dung cũng như các dữ liệu truyền dẫn.

Ngày nay, **SSL Certificate** còn được các ông lớn trong ngành công nghệ như [Google](https://www.google.com.vn), [Mozilla Firefox](https://www.mozilla.org/vi/firefox/)… xem là một tiêu chuẩn, một công cụ xác định độ tin cậy, an toàn của một website hiện đại.

**Các nhiệm vụ chính cơ bản nhất của chứng chỉ SSL:**

* Xác thực trang web: Các chứng chỉ SSL sẽ làm nhiệm vụ đảm bảo tính xác thực của trang web của bạn. Cụ thể, các trang web có đăng kí SSL sẽ hiển thị giao thức https và có hình ổ khóa phía trước tên miền
* Mã hóa thông tin, dữ liệu: Việc cài đặt SSL Certificate cũng giúp đảm bảo các dữ liệu trên trang web của bạn sẽ không thể truy cập được bởi bên thứ 3, thường là các hacker. Các thông tin truyền dẫn giữa website và các trình duyệt lớn sẽ được mã hóa bằng công nghệ mã hóa hiện đại, chuyên nghiệp nhất. Thao tác này chắc chắn sẽ khắc phục gần như hoàn toàn việc xem trộm thông tin, ăn cắp thông tin, dữ liệu khi lưu truyền trên Internet.
* Toàn vẹn dữ liệu: Đảm bảo các thông tin trao đổi giữa bạn và website được toàn vẹn và không bị thay đổi, chỉnh sửa…

# Các loại chứng chỉ SSL khác nhau là gì?

Có ba loại Chứng chỉ SSL có sẵn ngày hôm nay; Xác thực mở rộng (EV SSL), Xác thực tổ chức (OV SSL) và Xác thực tên miền (DV SSL). Các mức mã hóa là giống nhau cho mỗi chứng chỉ, điều khác biệt là các quy trình kiểm tra và xác minh cần thiết để có được chứng chỉ và giao diện trong thanh địa chỉ trình duyệt.

Trong vài năm qua, số lượng các tổ chức sử dụng Chứng chỉ SSL đã tăng lên đáng kể. Các ứng dụng mà SSL đang được sử dụng cũng đã được mở rộng. Ví dụ:

* bạn có thể cần SSL để bảo mật trong giao tiếp (để đảm bảo bạn không bị rình mò),
* hoặc bạn có thể muốn chứng minh rằng bạn có thể tin tưởng **người** mà bạn đang nói chuyện (danh tính trong giao tiếp riêng tư).

Với mã hóa, bạn có thể ẩn thông tin liên lạc khỏi tin tặc nhưng bạn không thể ngăn chúng chặn các liên lạc và đóng giả làm trang web của bạn để đánh cắp thông tin từ khách hàng của bạn. Khi mọi người tránh xa các cửa hàng gạch và vữa và tăng thói quen mua sắm và ngân hàng trực tuyến, người tiêu dùng phải có thể tin tưởng rằng họ đang truy cập trang web thực sự của cửa hàng họ đang mua sắm. Điều này là khó khăn hơn để chứng minh trực tuyến.

Bạn có thể chứng minh danh tính của mình bằng cách yêu cầu bên thứ ba bên ngoài (như GlobalSign) kiểm tra thông tin cá nhân và công ty của bạn. Dựa trên quy trình xác minh hoặc kiểm tra này, Chứng chỉ SSL có thể được chia thành ba loại.

# Chứng chỉ xác thực mở rộng (EV SSL) **Extended Validation**

Với EV SSL, [Cơ quan cấp chứng chỉ (CA)](https://translate.googleusercontent.com/translate_c?depth=2&hl=vi&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies/&xid=17259,15700021,15700186,15700191,15700256,15700259&usg=ALkJrhgXL_hicwaoyw9Rdi_m5PADstawNg) kiểm tra quyền của người nộp đơn sử dụng một tên miền cụ thể **cộng với** , họ tiến hành kiểm tra **kỹ lưỡng** về tổ chức. Quy trình cấp Chứng chỉ SSL EV được xác định nghiêm ngặt trong Nguyên tắc EV, được chính thức phê duyệt bởi [diễn đàn CA / Trình duyệt](https://translate.googleusercontent.com/translate_c?depth=2&hl=vi&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.globalsign.com/en/ssl-information-center/ca-network-security-practices/&xid=17259,15700021,15700186,15700191,15700256,15700259&usg=ALkJrhhF-9AhuOKLHApC3epidfO9UFdwHQ) vào năm 2007. Tất cả các bước cần thiết cho CA trước khi cấp chứng chỉ được chỉ định tại đây bao gồm:

* xác minh sự tồn tại hợp pháp, vật lý và hoạt động của thực thể,
* xác minh rằng danh tính của thực thể phù hợp với hồ sơ chính thức,
* xác minh rằng thực thể có độc quyền sử dụng tên miền được chỉ định trong Chứng chỉ EV EV,
* và xác minh rằng thực thể đã ủy quyền chính xác việc cấp Giấy chứng nhận EV SSL.

Sự tiến bộ mới nhất và có thể là quan trọng nhất trong công nghệ SSL kể từ khi thành lập ban đầu tuân theo các nguyên tắc Xác thực mở rộng được tiêu chuẩn hóa. Các trình duyệt bảo mật cao mới như Microsoft Internet Explorer 7+, Opera 9.5+, Firefox 3+, Google Chrome, Apple Safari 3.2+ và iPhone Safari 3.0+ xác định Chứng chỉ SSL mở rộng và kích hoạt các cải tiến bảo mật giao diện trình duyệt, như thanh màu xanh lá cây hoặc phông chữ màu xanh lá cây. Đối với những khách hàng muốn khẳng định mức độ xác thực cao nhất, đây là giải pháp lý tưởng.

Chứng chỉ EV SSL có sẵn cho tất cả các loại hình doanh nghiệp, bao gồm cả các tổ chức chính phủ và cả các doanh nghiệp hợp nhất và chưa hợp nhất. Bộ hướng dẫn thứ hai, Nguyên tắc kiểm toán EV, chỉ định các tiêu chí theo đó CA cần được kiểm tra thành công trước khi cấp Chứng chỉ EV SSL. Các cuộc kiểm toán được lặp lại hàng năm để đảm bảo tính toàn vẹn của quy trình phát hành. Ví dụ về Chứng chỉ EV SSL

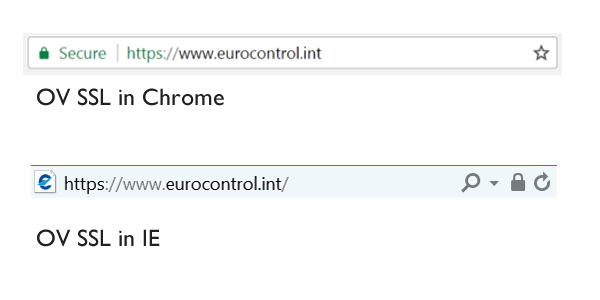
## Ví dụ về Chứng chỉ EV SSL



# Giấy chứng nhận tổ chức (OV SSL) **Organization Validation**

CA kiểm tra quyền của người nộp đơn sử dụng một tên miền cụ thể PLUS mà họ tiến hành một số kiểm tra của tổ chức. Thông tin công ty được hiệu đính bổ sung được hiển thị cho khách hàng khi nhấp vào [Dấu trang web bảo mật](https://translate.googleusercontent.com/translate_c?depth=2&hl=vi&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.globalsign.com/en/ssl-information-center/using-secure-site-seal/&xid=17259,15700021,15700186,15700191,15700256,15700259&usg=ALkJrhhMJEClc-KkkfY1WXn16HfxwuNgCA) , mang lại khả năng hiển thị nâng cao ở phía sau trang web và niềm tin được tăng cường liên quan. Tên tổ chức cũng xuất hiện trong chứng chỉ dưới trường BẬT.

## Ví dụ về Chứng chỉ SSL OV

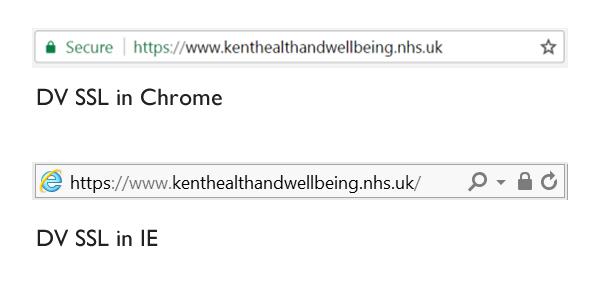


# Chứng chỉ xác thực tên miền (DV SSL) **Domain Validation**

CA kiểm tra quyền của người nộp đơn sử dụng một tên miền cụ thể. Không có thông tin nhận dạng công ty nào được hiệu đính và không có thông tin nào được hiển thị ngoài thông tin mã hóa trong Dấu trang web bảo mật. Mặc dù bạn có thể chắc chắn rằng thông tin của mình được mã hóa, nhưng bạn không thể chắc chắn ai thực sự ở cuối nhận thông tin đó.

Chứng chỉ DVSSL được hỗ trợ đầy đủ và chia sẻ cùng một nhận dạng trình duyệt với OV SSL, nhưng đi kèm với lợi thế là được cấp gần như ngay lập tức và không cần phải nộp giấy tờ công ty. Điều này làm cho DV SSL lý tưởng cho các doanh nghiệp cần SSL chi phí thấp một cách nhanh chóng và không cần nỗ lực gửi tài liệu của công ty.

## Ví dụ về chứng chỉ DV SSL



### Tại sao bạn nên mua Chứng chỉ Xác thực Tên miền (DV)?

* **Giá thấp hơn** - Giá của chứng chỉ xác thực tên miền (DV) ở phía thấp hơn so với chứng chỉ được xác thực (OV) và chứng thực mở rộng (EV).
* **Được cấp trong vòng vài phút** - Cơ quan cấp chứng chỉ Các chứng chỉ SSL được xác thực (DV) trong vòng vài phút sau khi quá trình xác minh tên miền được thực hiện.
* **Không có giấy tờ để xác nhận** - Cơ quan cấp chứng chỉ không yêu cầu bất kỳ tài liệu nào trong quá trình xác minh tên miền.
* **Lợi ích xếp hạng của Google** - Google gần đây đã công bố cung cấp lợi ích xếp hạng cho các trang web hỗ trợ SSL. Vì vậy, DV SSL sẽ giúp bạn tăng lưu lượng truy cập trang web của bạn, điều này chắc chắn có thể thúc đẩy doanh nghiệp của bạn.
* **Tăng sự tin cậy của người dùng** - HTTPS và con dấu trang web là các chỉ số tin cậy cho phép người dùng biết rằng trang web được bảo mật và thông tin của họ được an toàn.