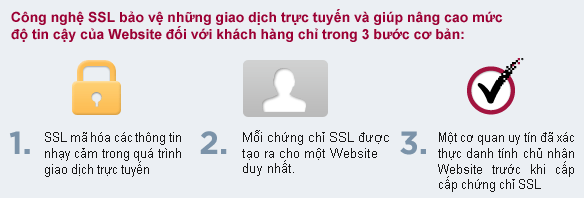
**[SSL](https://www.matbao.net/bao-mat-website/geotrust-ssl.html" \o "SSL" \t "_blank)** là một chuẩn công nghiệp được sử dụng bởi hàng triệu trang web trong việc bảo vệ các giao dịch trực tuyến với khách hàng của họ. **SSL** đảm bảo rằng tất cả các dữ liệu được truyền giữa các máy chủ web và các trình duyệt được mang tính riêng tư, tách rời.

**SSL là gì?**

Chắc rằng bạn cũng đã nghe nhắc đến cụm từ [chứng chỉ SSL](https://www.matbao.net/bao-mat-website/geotrust-ssl.html) (SSL Certificate) trên các website, vậy chứng chỉ SSL là gì?

Trước tiên, chúng ta nên biết rằng **Giao thức bảo mật – SSL** là viết tắt của từ Secure Sockets Layer. Đây là một tiêu chuẩn an ninh công nghệ toàn cầu tạo ra một liên kết được mã hóa giữa máy chủ web và trình duyệt. Liên kết này đảm bảo tất cả các dữ liệu trao đổi giữa máy chủ web và trình duyệt luôn được bảo mật và an toàn.

SSL đảm bảo rằng tất cả các dữ liệu được truyền giữa các máy chủ web và các trình duyệt được mang tính riêng tư, tách rời. SSL là một chuẩn công nghiệp được sử dụng bởi hàng triệu trang web trong việc bảo vệ các giao dịch trực tuyến với khách hàng của họ.

Chứng thư số SSL cài trên website của doanh nghiệp cho phép khách hàng khi truy cập có thể xác minh được tính xác thực, tin cậy của website, đảm bảo mọi dữ liệu, thông tin trao đổi giữa website và khách hàng được mã hóa, tránh nguy cơ bị can thiệp.

## Một số định nghĩa, thuật ngữ SSL thường gặp

Để hiểu rõ hơn, chúng ta cần phải biết **Certificate Authority (CA)** là gì?

CA là tổ chức phát hành các chứng thực các loại chứng thư số cho người dùng, doanh nghiệp, máy chủ ([server](https://www.matbao.net/cloud-server-linux.html)), mã code, phần mềm. Nhà cung cấp chứng thực số đóng vai trò là bên thứ ba (được cả hai bên tin tưởng) để hỗ trợ cho quá trình trao đổi thông tin an toàn.

Trong bài viết này, chúng tôi đơn cử **Global Sign** – một trong những doanh nghiệp đầu tiên trên thế giới được công nhận là nhà cung cấp dịch vụ chứng thực chữ ký số công cộng cung cấp tất cả các loại chứng thư, gói chứng thư, giải pháp chứng thư số cho các ngành tài chính – ngân hàng, y tế, giáo dục và các lĩnh vực kinh doanh khác.

* Chứng thư tiêu chuẩn toàn cầu.
* Tương thích với 99% các trình duyệt.
* Cung cấp bởi một trong những CA uy tín nhất thế giới.
* Định hướng doanh nghiệp với tất cả các dòng sản phẩm SSL.
* Tiết kiệm cho doanh nghiệp với lựa chọn Wildcard, SAN.

**Domain Validation (DV SSL)**: chứng thư số SSL chứng thực cho Domain Name – Website. Khi 1 Website sử dụng DV SSL thì sẽ được xác thực tên domain, website đã được mã hoá an toàn khi trao đổi dữ liệu.

**Organization Validation (OV SSL)**: chứng thư số SSL chứng thực cho Website và xác thực doanh nghiệp đang sở hữu website đó .

**Extended Validation (EV SSL)**: cho khách hàng của bạn thấy Website đang sử dụng chứng thư SSL có độ bảo mật cao nhất và được rà soát pháp lý kỹ càng. Với thanh địa chỉ sang màu xanh với hiển thị đầy đủ thông tin của công ty, cung cấp một cấp độ cao hơn tin tưởng vào website của bạn

**Subject Alternative Names (SANs SSL)** – Nhiều tên miền hợp nhất trong 1 chứng thư số:

* Một chứng thư số SSL tiêu chuẩn chỉ bảo mật cho duy nhất một tên miền đã được kiểm định. Lựa chọn thêm SANs chỉ với chứng thư duy nhất bảo đảm cho nhiều tên miền con. SANs mang lại sự linh hoạt cho người sử dụng, dễ dàng hơn trong việc cài đặt, sử dụng và quản lý chứng thư số SSL. Ngoài ra, SANs có tính bảo mật cao hơn Wildcard SSL, đáp ứng chính xác yêu cầu an toàn đối với máy chủ và làm giảm tổng chi phí triển khai SSL tới tất cả các tên miền và máy chủ cần thiết.
* Chứng thư số SSL SANs có thể tích hợp với tất cả các loại chứng thư số SSL của GlobalSign bao gồm: *Chứng thực tên miền (DV SSL)*, *Chứng thực tổ chức doanh nghiệp (OV SSL)* và *Chứng thực mở rộng cao cấp (EV SSL)*.

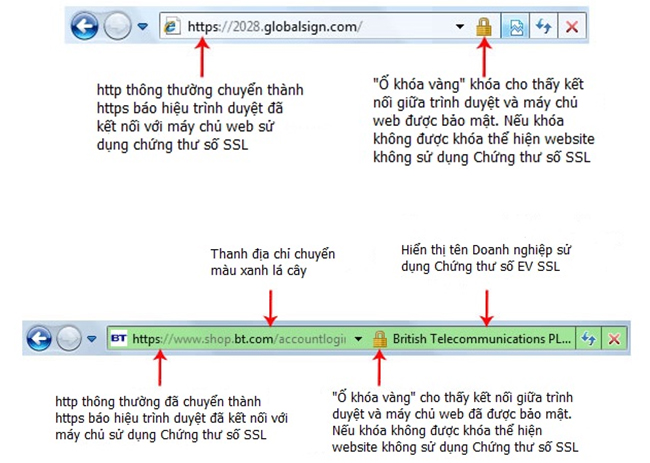
**Wildcard SSL Certificate (Wildcard SSL)**: sản phẩm lý tưởng dành cho các cổng thương mại điện tử. Mỗi e-store là một sub-domain và được chia sẻ trên một hoặc nhiều địa chỉ IP. Khi đó, để triển khai giải pháp bảo bảo mật giao dịch trực tuyến (đặt hàng, thanh toán, đăng ký & đăng nhập tài khoản,…) bằng SSL, chúng ta có thể dùng duy nhất một chứng chỉ số Wildcard cho tên miền chính của website và tất cả sub-domain.

## Trình duyệt làm thế nào để kiểm tra một SSL là có thực hay không?

Khi Website gởi cho trình duyệt một chứng chỉ SSL, Trình duyệt sẽ gởi chứng chỉ này đến một máy chủ lưu trữ các chứng chỉ số đã được phê duyệt. Các máy chủ này được thành lập bởi những công ty uy tín như GlobalSign, [VeriSign](http://www.verisign.com/).

Về mặt kỹ thuật, SSL sử dụng mã hóa công khai. Kỹ thuật này giúp cho Website và Trình duyệt tự thỏa thuận (bước 4 ở hình trên) một bộ khóa sẽ dùng trong suốt quá trình trao đổi thông tin sau đó.

Bộ khóa sẽ thay đổi theo mỗi trong lần giao dịch kế tiếp, một người khác sẽ không thể giải mã ngay cả khi có được dữ liệu của máy chủ lưu trữ chứng chỉ số nói trên.



## Tại sao nên sử dụng SSL?

Khi bạn [đăng ký tên miền](https://www.matbao.net/ten-mien/dang-ky-ten-mien.html) để sử dụng các dịch vụ website, email v.v… luôn có những lỗ hổng bảo mật cho hacker tấn công, **SSL** bảo vệ website và khách hàng của bạn.

* **An toàn dữ liệu:** dữ liệu không bị thay đổi bởi hacker.
* **Bảo mật dữ liệu:** dữ liệu được mã hóa và chỉ người nhận đích thực mới có thể giải mã.
* **Chống chối bỏ:** đối tượng thực hiện gửi dữ liệu không thể phủ nhận dữ liệu của mình.

Tiêu chuẩn xác thực – SSL chỉ được cung cấp bởi các đơn vị cấp phát chứng thư (CA) có uy tín trên toàn thế giới sau khi đã thực hiện xác minh thông tin về chủ thể đăng ký rất kỹ càng mang lại mức độ tin cậy cao cho người dùng Internet và tạo nên giá trị cho các website, doanh nghiệp cung cấp dịch vụ.

## Lợi ích khi sử dụng SSL?

* Xác thực website, giao dịch.
* Nâng cao hình ảnh, thương hiệu và uy tín doanh nghiệp.
* Bảo mật các giao dịch giữa khách hàng và doanh nghiệp, các dịch vụ truy nhập hệ thống.
* Bảo mật webmail và các ứng dụng như Outlook Web Access, Exchange, và Office Communication Server.
* Bảo mật các ứng dụng ảo hó như Citrix Delivery Platform hoặc các ứng dụng điện toán đám mây.
* Bảo mật dịch vụ FTP.
* Bảo mật truy cập control panel.
* Bảo mật các dịch vụ truyền dữ liệu trong mạng nội bộ, file sharing, extranet.
* Bảo mật VPN Access Servers, Citrix Access Gateway …
* Website không được xác thực và bảo mật sẽ luôn ẩn chứa nguy cơ bị xâm nhập dữ liệu, dẫn đến hậu quả khách hàng không tin tưởng sử dụng dịch vụ.

## ****Công cụ kiểm tra SSL đã cài đặt đúng hay chưa.****

Quý khách có thể **kiểm tra SSL** đã được cài đặt đúng hay chưa, có tin cậy với các trình duyệt hay không.

Các công cụ này cũng cung cấp các thông tin: Tên miền sử dụng SSL, loại và thời hạn còn lại của SSL, SSL đã được cài đặt đầy đủ và chính xác các mã CA hay không.