

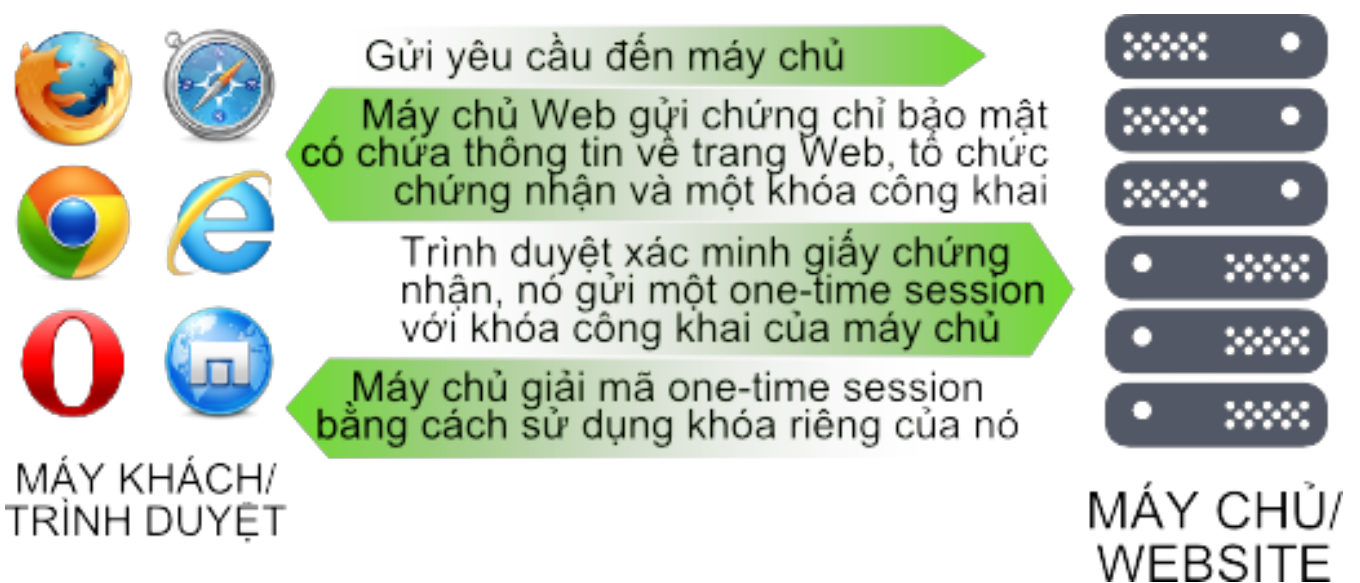
# Ch?ng ch? s? SSL là gì?

**SSL (Secure Sockets Layer) là công nghệ bảo mật tiêu chuẩn cho việc thiết lập kết nối giữa mã hóa giữa máy chủ web và trình duyệt. Kết nối này đảm bảo rằng tất cả các dữ liệu được truyền giữa các máy chủ web và các trình duyệt vẫn còn riêng tư và an toàn. SSL là một chuẩn công nghiệp và được sử dụng bởi hàng triệu trang web trong việc bảo vệ các giao dịch trực tuyến của họ với khách hàng của họ.**

## 1. SSL là gì?

SSL – Secure Sockets Layer – một tiêu chuẩn an ninh công nghệ toàn cầu tạo ra một kết nối giữa mã hóa giữa máy chủ web và trình duyệt. Kết nối này đảm bảo tất cả các dữ liệu trao đổi giữa máy chủ web và trình duyệt luôn được bảo mật và an toàn.

Ch?ng th? s? SSL cài trên website của doanh nghiệp cho phép khách hàng khi truy cập có thể xác minh 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.



## 2. Tại sao nên sử dụng SSL?

Bạn đang ký tên miền và sử dụng các dịch vụ website, email v.v... ? Luôn có những lợi ích bảo mật và nguy cơ bị tấn công ? SSL bảo vệ website và khách hàng của bạn.

- Bảo mật dữ liệu: dữ liệu được mã hóa và chỉ người nhận đích thực mới có thể giải mã.
- Toàn vẹn dữ liệu: dữ liệu không bị thay đổi bất kỳ tin tức.
- Chứng chỉ bất biến: người tấn công thực hiện giả mạo dữ liệu không thể phá vỡ được dữ liệu của mình.

### 3. 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 cập hệ thống
- Bảo mật webmail và các ứng dụng như Outlook Web Access, Exchange, và Office Communication Server;
- Bảo mật các ứng dụng ảo hóa 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 truy cập 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 nhận được nguy cơ bị xâm nhập dữ liệu, dẫn đến hậu quả khách hàng không tin tưởng sử dụng dịch vụ.

### 4. CA là gì?

- Certificate Authority ( CA ): là tổ chức phát hành các chứng thực các loại chứng thư số cho người dùng, doanh nghiệp, máy chủ (server), mã nguồn, phần mềm. Nhà cung cấp chứng thực sẽ 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.

- Chứng thư tiêu chuẩn toàn cầu;
- Tỷ lệ thích ứng 99% các trình duyệt;

- Cung cấp bằng chứng trong danh sách CA uy tín nhất thế giới;
- Những hãng doanh nghiệp với tất cả các dòng sản phẩm SSL;
- Tất cả các loại chứng chỉ doanh nghiệp với loại chứng chỉ Wildcard, SAN

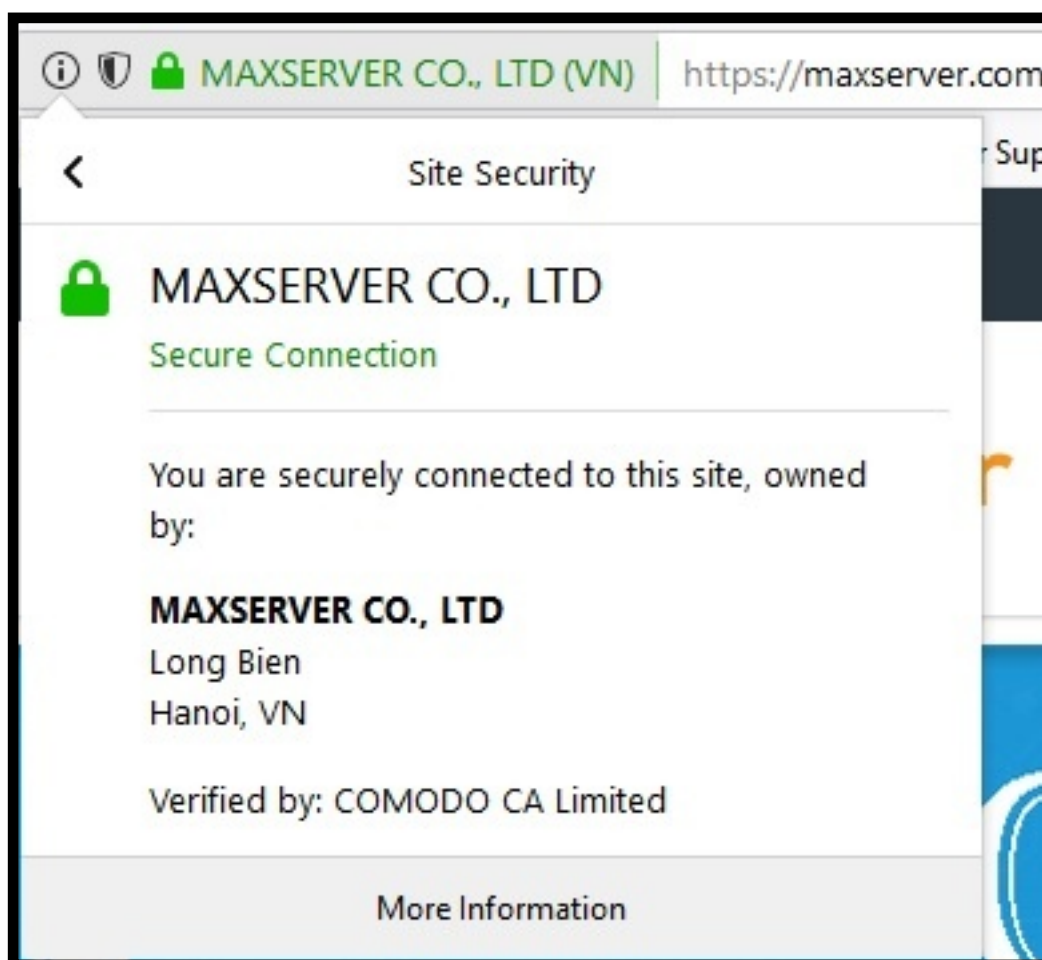
## 5. DV-SSL:

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

## 6. OV-SSL:

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

## 7: EV-SSL:



Extended Validation (EV) : cho khách hàng c?a b?n th?y Website ?ang s? d?ng ch?ng th? SSL có ?? b?o m?t cao nh?t và ???c rà soát pháp lý k? càng v?i thanh ??i ch? sáng màu xanh, hi?n th? ??y ?? thông tin c?a công ty, cung c?p m?t c?p ?? cao h?n tin t???ng vào website c?a b?n.

## 8. Wildcard SSL:

(Wildcard SSL Certificate) : s?n ph?m lý t???ng dành cho các c?ng th???ng m?i ?i?n t?. Các website d?ng này th???ng có th? t?o ra các trang e-store dành cho các ch? c?a hàng tr?c tuy?n, m?i e-store là m?t sub domains và ???c chia s? trên m?t ??a ch? IP duy nh?t. Khi ?ó, ?? tri?n khai gi?i pháp b?o b?o m?t giao d?ch tr?c tuy?n (khi ??t hàng, thanh toán, ??ng ký & ??ng nh?p tài kho?n,...) b?ng SSL, chúng ta có th? dùng duy nh?t m?t ch?ng ch? s? Wildcard cho tên mi?n chính c?a website và dùng chung m?t ??a ch? IP duy nh?t ?? chia s? cho t?t c? m?i sub domains .

Online URL: <https://huongdan.maxserver.com/article-44.html>