**HTTP (Hypertext Transfer Protocol)**

* Là giao thức truyền tải siêu văn bản
* Dùng để truyền tải dữ liệu dưới dạng văn bản, âm thanh, hình ảnh, video từ Web Server tới trình duyệt web của người dùng và ngược lại
* Hoạt động theo mô hình Client (Khách) – Server (Chủ)

A picture containing text, electronics, computer, screenshot

Description automatically generated

**HTTPS (Hypertext Transfer Protocol Secure)**

* Là giao thức truyền tải siêu văn bản an toàn
* Thực chất, đây chính là giao thức HTTP nhưng được bổ sung thêm chứng chỉ **SSL (Secure Sockets Layer – tầng ổ bảo mật)** hoặc **TLS (Transport Layer Security – bảo mật tầng truyền tải),**  nhằm mã hóa các thông điệp giao tiếp để tăng tính bảo mật. Cả hai giao thức TLS và SSL đều sử dụng hệ thống PKI (Public Key Infrastructure- hạ tầng khóa công khai) không đối xứng. Một hệ thống không đối xứng sử dụng hai “khóa” để mã hóa thông tin liên lạc, khóa “công khai” và khóa “riêng”. Bất cứ thứ gì được mã hóa bằng khoá công khai (public key) chỉ có thể được giải mã bởi khóa riêng (private key) và ngược lại. Khóa “riêng” cần được bảo vệ nghiêm ngặt và chỉ truy cập được bởi chủ nhân của khóa riêng. Trong trường hợp một trang web, khóa riêng được giữ kín trên máy chủ web, khóa công khai được phân phối cho bất kỳ ai cần để có thể giải mã thông tin đã được mã hoá bằng khóa riêng.
* Có thể coi, HTTPS là phiên bản HTTP an toàn, bảo mật hơn. Có thể nghĩ một cách đơn giản như này, khi sử dụng HTTP tức là đang phô diễn mọi thứ trên website một cách trần trụi nhất, khi nhìn vào người ta biết website đó có gì. Còn giao thức HTTPS là lúc đó mọi thông tin dữ liệu trên website đã được che khuất, được bảo vệ bởi một chữ “S” (Sercure – an toàn).

Graphical user interface, Word

Description automatically generated

**HTTPS hoạt động thế nào ?**

Quá trình giao tiếp giữa Client và Server thông qua HTTPS như sau:

1. Client truy cập cho 1 trang web https. Ví dụ https://abc.com
2. Server của abc.com sẽ trả về certificate để chứng thực rằng website user đang truy cập là website chính thức.

Certificate là một khối dữ liệu bao gồm rất nhiều thông tin về payment.com. Các thông tin này bao gồm:

* Tên miền
* Tên công ty sở hữu
* Thời gian certificate được cấp
* Thời hạn certificate
* Public key

1. Client (web browser) tiến hành xác thực certificate này bằng cách kiểm tra tính hợp lệ chữ ký số của CA([Certificate Authority](https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq#cert)) được kèm theo certificate

CA là ai ?

CA là **người chứng minh certificate mà abc.com cung cấp là thật.** CA **bán dịch vụ chứng thực** đó bằng cách ký chứng minh rằng certificate của abc.com là thật

Certificate chứng thực cho abc.com sẽ được CA **ký** bằng **khóa bí mật** của CA. Khóa này chỉ có CA biết và do vậy việc chữ ký là an toàn. abc.com sẽ gửi cho user certificate đã được ký bởi CA cùng với khóa công khai tương ứng của khóa bí mật mà CA dùng để ký certificate. Browser sẽ tiến hành kiểm tra certificate này như bình thường dùng khóa công khai của CA.

1. Sau khi kiểm chứng được certificate, browser sẽ tự sinh ra 1 khóa K. Sau đó sử dụng public key (lấy trong certificate) để mã hóa khóa K và gửi về cho server. (Khóa K sẽ được dùng để mã hóa tất cả các liên lạc giữa client và abc.com sau này. Do quá trình mã hóa các gói tin dùng mã đối xứng, khóa K cần được gửi trở lại abc.com vì nếu không có K, server không thể nào giải mã được gói tin)
2. Server sử dụng private key của mình (tương ứng với public key trong certificate ở trên) để giải mã ra khóa K ở trên.
3. Sau đó, cả server và client đều sử dụng khóa K để mã hóa/giải mã toàn bộ dữ liệu liên lạc sau này.

Diagram

Description automatically generated

**Chữ ký số**

### Chữ ký số hoạt động dựa trên PKI(Public Key Infrastructure)

PKI là gì?

* Hạ tầng khóa công khai là cơ chế bảo mật do một bên thứ 3 (thường là CA(nhà cung cấp chứng thư số)) cung cấp và xác thực định danh các bên tham gia vào quá trình trao đổi thông tin
* PKI cho phép người dùng internet có thể trao đổi thông tin một cách an toàn thông qua việc sử dụng cặp khóa private key và public key được cấp chứng nhận bởi nhà cung cấp chứng thư số CA.

Diagram

Description automatically generated

Một PKI hoàn chỉnh gồm những thành phần cơ bản sau:

* **Certification Authority** – Cơ quan chứng nhận (CA): Thực hiện nhiệm vụ phát hành, quản lý và thu hồi chứng thư số là thực thể quan trọng trong một PKI
* **Registration Authority** – Cơ quan đăng ký (RA): Đảm nhiệm xác thực cá nhân, tổ chức đăng kí chứng thư số; kiểm tra tính chính xác của thông tin do cá nhân, tổ chức cung cấp
* **Certificate Repository** – Kho lưu trữ chứng thư số (CR): Đảm nhiệm công việc lưu trữ chứng thư số
* **Certificate Policy** – Chính sách về chứng thư số (CP): Là chính sách chỉ ra những phạm vi sử dụng của một chứng thư số. Certificate policy đóng vai trò quan trọng, nó giống như lời hứa của nhà cung cấp dịch vụ dành cho khách hàng để họ có thể yên tâm rằng quyền lợi của họ được đảm bảo.
* **Certification Practice Statement** – Thủ tục chứng nhận (CPS): Là quy định về các thủ tục trong việc ban hành chứng thư số. Ví dụ như thủ tục quản lý chứng thư số bao gồm việc công bố và lưu trữ, thu hồi, cấp mới hay thay đổi cặp khóa.
* **PKI Applications** – Ứng dụng PKI: Bao gồm người sử dụng các dịch vụ PKI và các phần mềm hỗ trợ cài đặt sử dụng chứng thư số như các trình duyệt web, các ứng dụng Email chạy bên client.

Triển khai chữ ký số như thế nào?

A picture containing timeline

Description automatically generated

Dữ liệu của người kí🡪 thuật toán băm🡪 băm ra các mã nhị phân🡪mã hóa nó nhờ khóa riêng của người kí🡪 tạo ra chữ kí số.

Từ chữ kí số đó🡪+ nhờ thuật toán băm->băm dãy mã nhị phân(1)

+giải mã nhờ khóa công khai 🡪 băm ra dãy mã nhị phân(2)

(1)=(2)🡪 valid

# no valid

### 

Khi người ký ký điện tử vào một tài liệu, chữ ký được tạo bằng cách sử dụng khóa riêng của người ký, khóa này luôn được người ký giữ an toàn. Thuật toán toán học hoạt động giống như một mật mã, tạo ra dữ liệu khớp với tài liệu đã ký, được gọi là hàm băm và mã hóa dữ liệu đó. Dữ liệu được mã hóa đó là chữ ký số.

. Chữ ký cũng được đánh dấu bằng thời gian mà tài liệu được ký. Nếu tài liệu thay đổi sau khi ký, chữ ký điện tử sẽ mất hiệu lực.

Ví dụ: Jane ký thỏa thuận bán lượt chia sẻ bằng khóa riêng của mình. Người mua nhận được tài liệu. Người mua nhận được tài liệu cũng nhận được một bản sao của khóa công khai của Jane. Nếu khóa công khai không thể giải mã chữ ký (thông qua mật mã mà từ đó các khóa được tạo), điều đó có nghĩa là chữ ký không phải của Jane, hoặc đã bị thay đổi kể từ khi nó được ký. Chữ ký sau đó được coi là không hợp lệ.

Để bảo vệ tính toàn vẹn của chữ ký, PKI yêu cầu các khóa phải được tạo, tiến hành và lưu một cách an toàn và thường yêu cầu các dịch vụ của [Tổ chức phát hành chứng chỉ (CA)](https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq#cert) đáng tin cậy . Các nhà cung cấp chữ ký số, như DocuSign, đáp ứng các yêu cầu của PKI để ký số an toàn.