Secure Socket Layer

Lindung Siswanto

POLNEP

- **Hypertext Transfer Protocol (HTTP)** ➔ Sebuah protocol aplikasi yang digunakan untuk berkomunikasi antara client dan server
- **Client** yang dimaksud adalah web browser atau device lain yang dapat mengakses, menerima, hingga menampilkan konten web melalui browser
- Server ➔ sistem komputer yang memiliki layanan khusus berupa penyimpanan data. Data yang disimpan melalui **server** berupa informasi dan beragam jenis dokumen yang kompleks
- **Hypertext Transfer Protocol Secure (HTTPS)** ➔ versi HTTP yang lebih aman, karena menggunakan **Secure Socket Layer (SSL)** atau Transport Layer Security (TLS)

- Keamanan Data ➔ HTTP kurang menjamin keamanan data yang ditransmisikan antara client dan server, HTTPS menjamin keamanan data yang dikirimkan
- SSL ➔ HTTP, maka tidak memerlukan sertifikat SSL, HTTPS membutuhkan sertifikat SSL.
- Penggunaan Port ➔ HTTP menggunakan port 80 yang berfungsi sebagai konektivitas web server secara umum dengan client. HTTPS melalui SSL dibutuhkan port 443 sebagai jaringan konektivitasnya
- Bagi Pengguna ➔ HTTP Komunikasi browser ke server atau server ke server tidak dienkripsi. HTTPS Komunikasi browser ke server atau server ke server akan dienkripsi

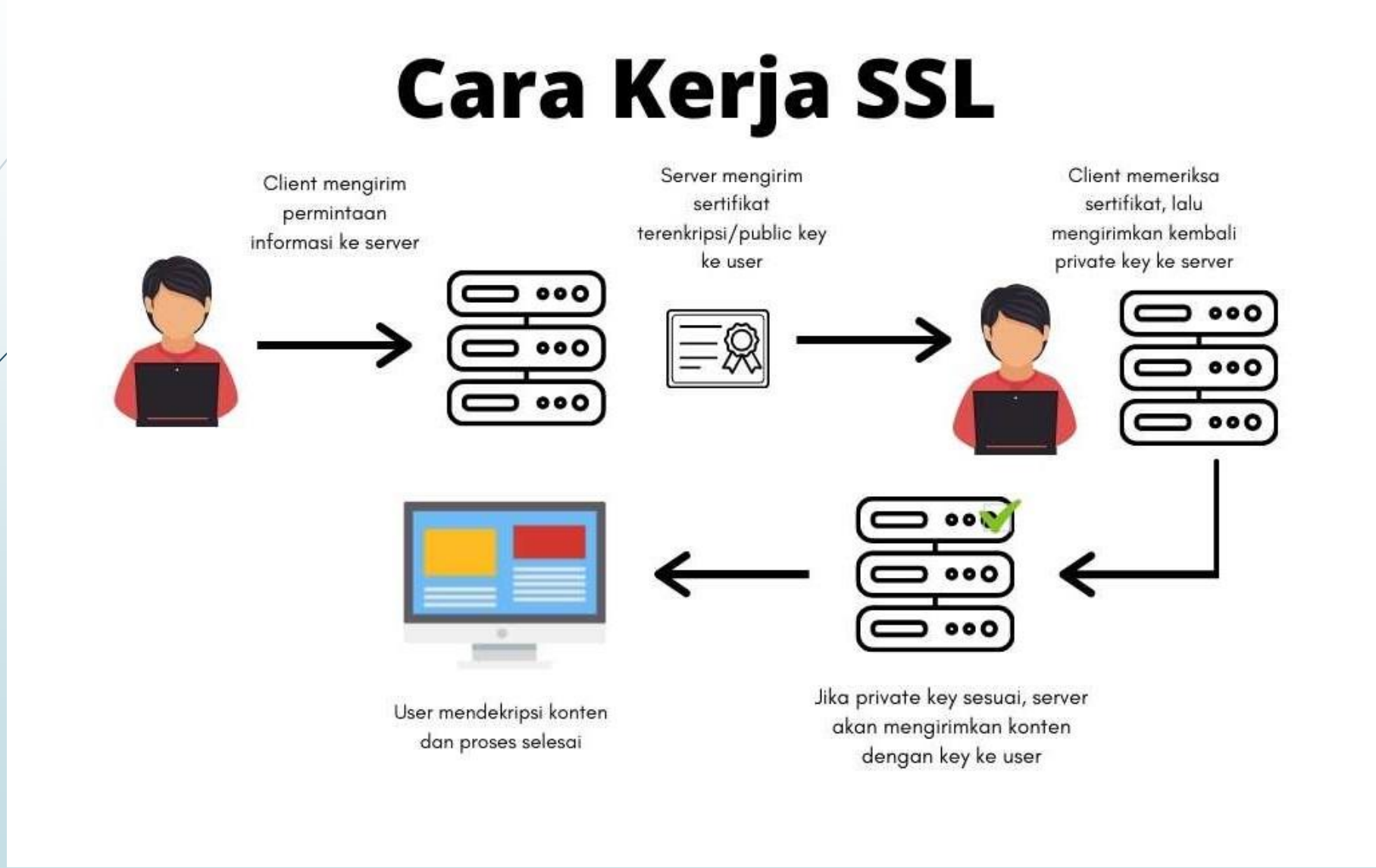
SSL VS TLS

- Secure Socket Layer ➔ sebuah lapisan keamanan terenkripsi yang memiliki fungsi sebagai pengaman data pribadi. SSL bekerja ketika pengunjung website melakukan transaksi data antar server melalui web browser
- Sertifikat SSL ➔ merupakan sebuah file berisi kode yang diinstal pada situs asal. File ini berisi informasi terkait **public key** dan identitas pemilik website
- *Transport Layer Security* ➔ teknologi TLS lebih baik karena lebih baru dan merupakan upgrade dari SSL

FUNGSI SSL

- **Mengenkripsi Informasi Sensitif ➔** Saat informasi tersebut dikirimkan, SSL akan mengenkripsi dan mengacak informasi tersebut sehingga tidak akan bisa dibaca kecuali oleh alamat tujuan saja. SSL sangat berguna untuk informasi yang menyangkut akun, kata sandi, nama, alamat, hingga kartu kredit, dan data penting lainnya.
- **Menyediakan Authentication ➔** Memastikan bahwa informasi pribadi yang dikirimkan pada alamat yang benar bukan pada oknum penipu yang berusaha mencuri data pribadi milik Anda
- **Memberikan Kepercayaan ➔** Kepercayaan yang SSL berikan kepada pelanggannya berupa website yang diberikan logo gembok atau green bar pada halaman url-nya, ini berlaku untuk SSL yang berbayar dan juga yang gratis
- **Kepatuhan pada PCI ➔** PCI atau Payment Card Industry membuat syarat berupa, jika website yang Anda miliki menggunakan transaksi kartu kredit haruslah menggunakan SSL

Cara Kerja SSL



Cara Kerja SSL

- Browser terhubung ke website yang aman, dan meminta identitas server.
- Server mengirimkan salinan Sertifikat SSL dengan kunci publiknya.
- Browser memverifikasi sertifikat masih aktif dalam artian tidak kedaluwarsa atau dicabut dan berasal dari CA tepercaya.
- Jika semuanya sudah jelas, browser akan membuat, mengenkripsi, dan mengirim kembali kunci sesi ke website menggunakan kunci publik server.
- Server penerima kemudian mendekripsi kunci sesi menggunakan kunci privatnya. Ini kemudian mengirimkan kunci pengakuan dan sesi untuk memulai sesi terenkripsi.
- Semua data yang dikirimkan antara browser dan server sekarang dienkripsi dengan kunci sesi.

Jenis-Jenis SSL

- **Domain Validation SSL ➔** SSL Certificate yang digunakan untuk kelas entry level dengan tingkat validitas yang mudah dan proses yang memakan waktu paling cepat. Untuk menerbitkan SSL jenis ini diperlukan verifikasi domain dan email Anda saja, jenis ini lebih cocok digunakan oleh website personal, blog, portfolio, dan lainnya yang sejenis
- **Organization Validation ➔** untuk website yang membutuhkan user password serta yang menyimpan data pelanggan, untuk kecocokannya Organization Validation atau OV SSL ini merujuk pada website toko online, E-Commerce atau organisasi
- **Extended Validation ➔** EV atau Extended Validation adalah SSL dengan standar tertinggi, jika Anda memiliki website toko online atau E-Commerce yang ingin highest trust level

Penyedia SSL

Let's Encrypt

- Let's Encrypt adalah CA (Certificate Authority) yang memberikan sertifikat SSL gratis untuk enkripsi TLS melalui prosedur otomatis.
- Didukung banyak perusahaan seperti Google, Facebook, Cisco, Automattic, Mozilla telah berkumpul untuk mendukung Let's Encrypt untuk meningkatkan tingkat keamanan secara keseluruhan di Internet.
- ISRG (Internet Security Research Group) mempertahankannya. Lingkungan Pengelolaan Sertifikat Otomatis atau Automatic Certificate Management Environment (ACME) memungkinkan untuk menginstal sertifikat hanya dengan beberapa perintah.