Penggunaan SSL untuk website RSUP Persahabatan

1. Pendahuluan

SSL (Secure Sockets Layer) merupakan teknologi keamanan yang telah menjadi sebuah standar keamanan untuk terjadinya proses enkripsi saat komunikasi antara Komputer Server dengan Komputer client (User) terkoneksi. Contohnya seperti, saat terhubung dengan web server (website) melalui sebuah browser. atau seperti saat terhubung dengan mail server dengan mail client (seperti; Microsoft Outlook, atau Apple Mail, Thunderbird, dll).

Dengan menggunakan SSL, akan memungkinkan terjaminnya keamanan informasi sensitif atau rahasia seperti informasi Kartu Kredit, Informasi User dan Password (login), atau informasi identitas lainnya (KTP, Passport, dll), atau informasi lainnya yang dianggap perlu dijaga kerahasiaannya.

Biasanya, pada saat melakukan browsing dan perlu melakukan input untuk disimpan pada website, browser akan mengirimkan data ke server dengan "polos" (Plain Text). Sadar maupun tidak sadar, hal ini tentunya membuat anda rentan terhadap penyalahgunaan data akibat dari penyadapan selama proses pengiriman data.

Jika saat pengiriman data dari komputer ke server penyadap dapat melihat isi data maupun informasi yang dikirimkan ke server, mereka dapat menggunakan data dan informasi tersebut.

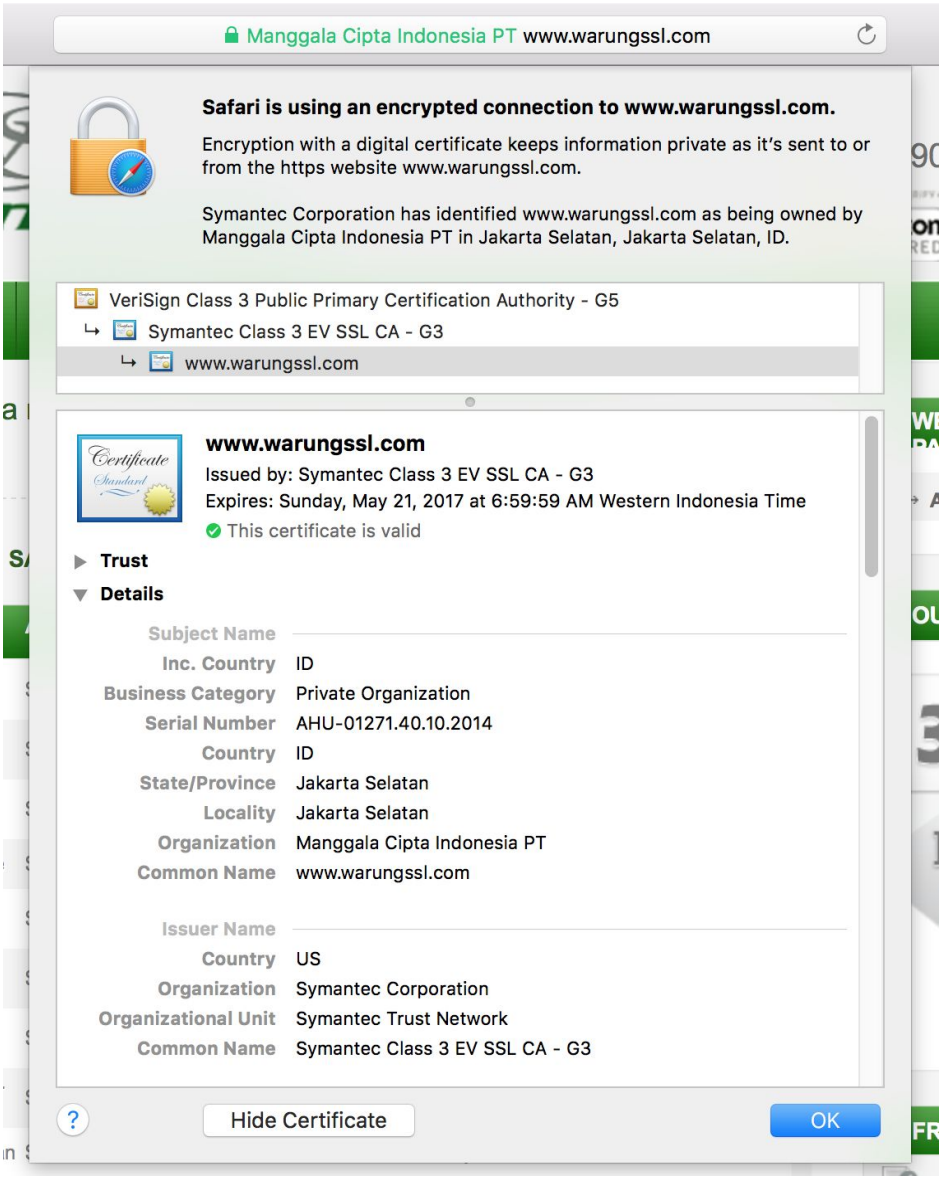
Secara spesifiknya, SSL merupakan sebuah protokol keamanan. Protokol menggambarkan bagaimana sebuah algoritma digunakan. Dalam hal ini, protol SSL menentukan variabel enkripsi untuk keduanya, link yang dituju dan data yang dikirimkan

2. Manfaat SSL

Alasan utama mengapa menggunakan SSL adalah untuk menjaga informasi sensitif selama dalam proses pengiriman melalui Internet dengan cara dienkripsi, sehingga hanya penerima pesan yang dapat memahami dari hasil enkripsi tersebut. Hal ini sangat penting, karena informasi yang kita kirimkan di Internet membutuhkan proses perjalanan dari komputer ke komputer sampai mencapai server tujuan. Komputer lain yang ada diantara Anda dan server dapat melihat nomor Kartu Kredit Anda, username dan passwords, dan informasi sensitive lainnya bila hal ini tidak dienkripsi dengan Sertifikat SSL. Ketika sertifikat SSL digunakan, informasi menjadi tidak dapat terbaca oleh siapapun kecuali ke

server yang memang dituju saat mengirim informasi tersebut. Hal ini melindungi informasi tersebut dari hackers dan pencuri identitas sekaligus menambah kepercayaan terhadap pelanggan anda.

Web browser memberikan isyarat secara visual, seperti ikon kunci atau bar yang berwarna hijau, untuk memastikan dan memberitahu kepada pengunjung web bahwa mereka berada pada koneksi yang telah diberi pengamanan. Ini berarti bahwa mereka akan lebih mempercayai website Anda ketika mereka melihat isyarat ini dan akan lebih cenderung untuk membeli dari Anda. Penyedia SSL juga akan memberikan Anda sebuah segel kepercayaan yang bertujuan untuk menanamkan rasa lebih percaya pada pelanggan Anda.



Contoh Memanfaatkan SSL

Kekurangan dari SSL

Dengan begitu banyaknya keuntungan, mengapa masih ada yang tidak menggunakan SSL ? Apakah ada kerugian untuk menggunakan SSL ? Biaya adalah merupakan kerugian yang memang jelas. Penyedia SSL perlu mempersiapkan infrastruktur terpercaya dan memvalidasi identitas mereka, itu sebabnya biaya mereka menjadi begitu tinggi. Karena sebagian dari penyedia SSL sudah begitu cukup dikenal, harga mereka bisa menjadi sangat tinggi. Performa adalah kelemahan lain untuk SSL. Karena informasi yang Anda kirim harus melewati proses enkripsi lebih dahulu pada server, ini membutuhkan sumber daya tambahan pada server dimana informasi yang Anda kirim mesti di–encrypt oleh server. Perbedaan performa hanya terlihat pada website yang memiliki jumlah pengunjung yang sangat besar namun hal ini masih dapat diminimalkan dengan hardware khusus.

Secara keseluruhan, kelemahan menggunakan sertifikat SSL lebih sedikit dibanding dengan keuntungan yang diraih. Sangat penting agar Anda mengirimkan segala informasi sensitif ke semua website dengan menggunakan sertifikat SSL yang tepat. Penggunaan sertifikat SSL yang tepat akan membantu melindungi pelanggan Anda, melindungi Anda, dan membantu untuk mendapat kepercayaan pelanggan terhadap Anda sehingga Anda dapat lebih banyak menjual.

3. Fiture SSL

Terdiri dari 3 Fiture diantaranya:

1. *Domain Validasi (DV)*

Untuk Domain Validasi (DV) tidak memerlukan legal dokument hanya saja mengapprove email yang dikirimkan oleh vendor hosting melalui email yang terdapat pada whois record, dan untuk Secure atau gembok hijau yang terpasang jika diklik **tidak menampilkan nama perusahaan.**

2. *Organization Validasi (OV)*

Untuk Organization Validasi (OV) dapat **menampilkan nama perusahan** ketika diklik, dikarenakan untuk produk tipe Organization Validation(OV) membutuhkan legal dokument-dokument yang di perlukan agar dapat menampilkan nama perusahaan pada Secure yang ada terpasang. Dan untuk produk Organization Validation(OV) membutuhkan waktu 3-7 hari kerja tergantung respon dari End User.

Untuk tipe produk **Organization Validation(OV)** membutuhkan legal dokument seperti,sebagai berikut:

1. **Surat Ijin Usaha Perdagangan (SIUP) atau ijin sejenisnya.**
2. **Tanda Daftar Perusahaan (TDP)**
3. **NPWP Perusahaan**
4. **Tagihan telepon terakhir**

3. Extended Validasi (EV)

Untuk Extended Validation(EV) yang dapat menampilkan Green Bar atau nama perusahaan yang terdapat pada Adress Bar, Akan tetapi untuk produk Extended Validation(EV) memerlukan legal dokument yang lengkap seperti, sebagai berikut:

1. **Dasar Pendirian atau Akta pendirian perusahaan atau akta perubahaannya (bila ada)**
2. **Surat Ijin Usaha Perdagangan (SIUP) atau ijin sejenisnya.**
3. **Tanda Daftar Perusahaan (TDP)**
4. **NPWP Perusahaan**
5. **Tagihan telepon terakhir**
6. **Scan KTP Pimpinan Perusahaan atau kepala bagian**
7. **Scan KTP Administrative Contact Details (PIC saat verifikasi dilakukan, termasuk penerima SSL Certificate saat diterbitkan)**
8. **Kop Rekening Koran**

Dan untuk produk Extended Validation(EV) Memiliki Trust yang tinggi terhadap pengguna atau pengunjung website bapak dan untuk produk dari produk EV tersebut memerlukan 7–14 hari kerja tergantung respon dari end user (Pengelola Hosting).

4. Harga SSL

Contact:

LiveChat di https://www.warungssl.com
email di cs@warungssl.com
telepon di 021 2904 1500.