BAB II
2. DASAR TEORI

2.1. Keamanan Jaringan

Dalam pembangunan teknologi informasi, sistem keamanan jaringan yang terhubung ke jaringan LAN maupun internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para *hacker*.

Mendeteksi keberadaan dan keamanan yang terbuka atau tanpa pengamanan dan terekamnya *username* dan *password* dapat membahayakan keamanan data para pengguna layanan teknologi informasi berbasis jaringan. Dengan kondisi seperti ini diperlukan peningkatan keamanan yang baik untuk dapat mencegah/menangani serangan *packet sniffing* dan gangguan lebih lanjut.

Terdapat tiga aspek utama ketika berbicara tentang keamanan data yaitu :

1) *Privacy* atau *Confidentiality*, mencakup kerahasiaan informasi. Inti aspek privacy adalah bagaimana menjaga informasi agar tidak dilihat atau diakses oleh orang yang tidak berhak.
2) *Message Integrity*, atau integritas mencakup keutuhan informasi. Inti aspek *integrity* adalah bagaimana menjaga informasi agar tetap utuh atau dapat dikatakan apa yang diterima harus sama dengan apa yang dikirim.
3) *Authentication*, atau otentikasi berkaitan dengan keabsahan pemilik informasi.

SSL biasanya digunakan antara *server* dan *client* untuk mengamankan sambungan. Ketika komputer mengirimkan data melalui jaringan, kemudian data tersebut dikirimkan dalam bentuk paket-paket. Paket *sniffing* adalah teknik pemantauan setiap paket yang melintasi jaringan. Paket *sniffing* adalah bagian dari perangkat lunak atau perangkat keras yang memonitor semua lalu lintas jaringan. Komponen *sniffer* meliputi *hardware, drive program, buffer, packet analysis*. Ini tidak seperti jaringan host standar yang hanya menerima lalu lintas yang dikirim khusus untuk mereka. Ancaman keamanan yang disajikan oleh penyadapan adalah

kemampuan mereka untuk menangkap semua lalu lintas masuk dan keluar, termasuk *password* dan *username* atau bahan sensitif lainnya.

2.2. Hypertext Transfer Protokol (HTTP)

HTTP adalah sebuah protokol meminta atau menjawab antara *client* dan *server*. Sebuh client HTTP seperti *web browser*, biasanya memulai permintaan dengan membuat hubungan TCP/IP ke port tertentu di tuan rumah yang jauh (default port 80).

Sebuah server HTTP yang mendengarkan di port tersebut menunggu client mengirim kode permintaan (request), seperti "GET / HTTP/1.1" (yang akan meminta halaman yang sudah ditentukan), diikuti dengan pesan MIME yang memiliki beberapa informasi kode kepala yang menjelaskan aspek dari permintaan tersebut, diikut dengan badan dari data tertentu.

Beberapa kepala (header) juga bebas ditulis atau tidak, sementara lainnya (seperti tuan rumah) diperlukan oleh protokol HTTP/1.1. Begitu menerima kode permintaan (dan pesan, bila ada), server mengirim kembali kode jawaban, seperti "200 OK", dan sebuah pesan yang diminta, atau sebuah pesan error atau pesan lainnya.

Pengembangan HTTP dikoordinasi oleh Konsorsium *World Wide Web* (W3C) dan grup bekerja *Internet Engineering Task Force* (IETF), bekerja dalam publikasi satu seri RFC, yang paling terkenal RFC 2616, yang menjelaskan HTTP/1.1, versi HTTP yang digunakan umum sekarang ini.

2.3. Hypertext Transfer Protokol Secure (HTTPS)

Hypertext Transfer Protocol Secure memiliki pengertian yang sama dengan http hanya saja https memiliki kelebihan fungsi di bidang keamanan (secure) dengan menggunakan *Secure Socket Layer* (SSL) atau *Transport Layer Security* (TLS) sebagai sub-layer di bawah HTTP.

Teknologi HTTPS protokol mencegah kemungkinan dicurinya informasi penting yang dikirimkan selama proses komunikasi berlangsung antara user dengan web server atau sebaliknya. Secara teknis, website yang menggunakan HTTPS akan

BAB III

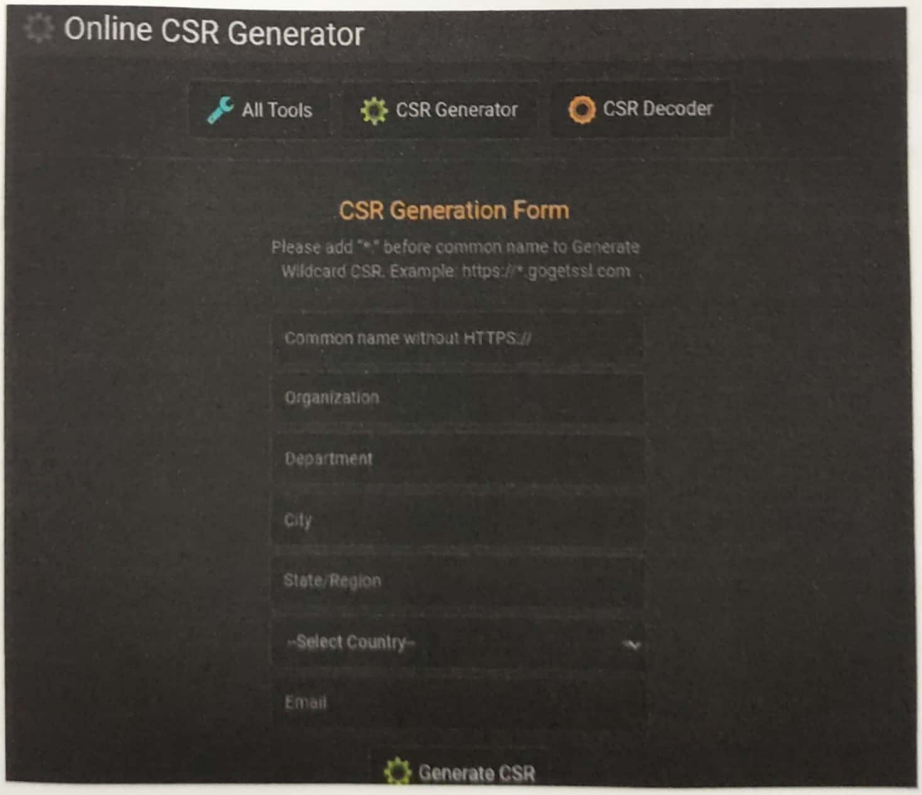
3. PELAKSANAAN PEKERJAAN

3.1. Tahap – Tahap Pembuatan Sertifikat SSL Dan Instalasinya

3.1.1. Generate CSR dan PRIVATE KEY

Certificate Signing Request (CSR) adalah blok teks yang disandikan yang diberikan kepada Otoritas Sertifikat ketika mengajukan permohonan Sertifikat SSL. Biasanya dihasilkan di server tempat sertifikat akan dipasang dan berisi informasi yang akan dimasukkan dalam sertifikat seperti nama organisasi, nama umum (nama domain), lokalitas, dan negara. Sedangkan *Private Key* selalu mengikuti ketika generate CSR.

Ada dua metode proses generate CSR yaitu menggunakan tools yang disediakan oleh pihak vendor jika membeli Certificate SSL berbayar atau menggunakan aplikasi gratis yang sudah disediakan di server. Pada tahap ini, pihak Pemerintah Kabupaten Kebumen menggunakan aplikasi gratis yang sudah tersedia di Server CentOS 7.



Gambar 1 Generate CSR dan Private Key di gogetSSL.com

Generate CSR dan private key dilakukan di terminal menggunakan perintah:

```
#openssl genrsa -out subdomain.kebumenkab.key 2048
```

```
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
```

dan

```
#openssl req -new -key subdomain.kebumenkab.key -out subdomain.kebumenkab.csr
```

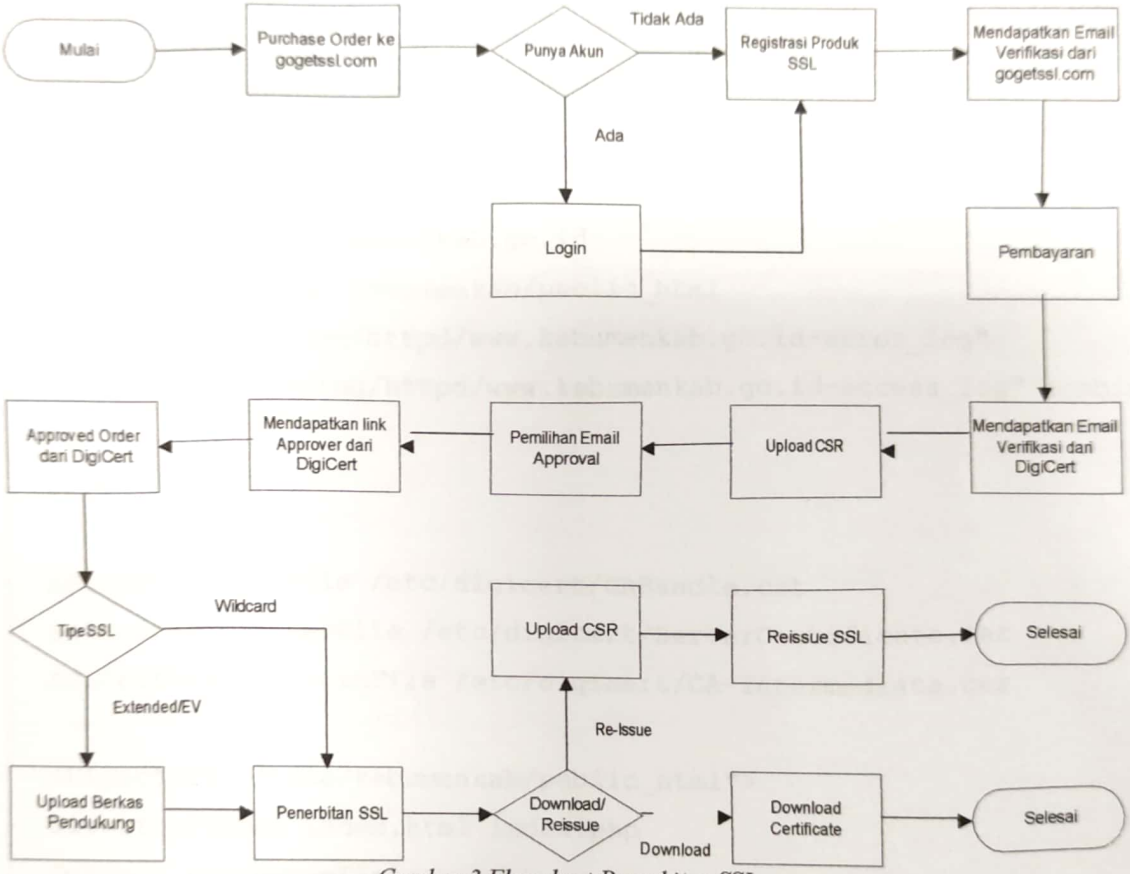
```
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]: ID
State or Province Name (full name) []: Central of Java
Locality Name (eg, city) [Default City]: Kabupaten Kebumen
Organization Name (eg, company) [Default Company Ltd]: Dinas
Komunikasi dan Informatika Kabupaten Kebumen
Organizational Unit Name (eg, section) []: Bidang Telematika
Common Name (eg, your name or your server's hostname) []:
kebumenkab.go.id
Email Address []: webmaster@kebumenkab.go.id

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Setelah perintah diatas dilakukan maka akan tercipta 2 (dua) buah file yang dikirimkan ke pihak vendor untuk issue SSL.

website@simpada:~/SSL

```
[website@simpada SSL]$ ls -l
total 8
-rw-r--r-- 1 root root 1175 Apr  2 16:04 subdomain.kebumenkab.csr
-rw-r--r-- 1 root root 1679 Apr  2 16:02 subdomain.kebumenkab.key
[website@simpada SSL]$
```

Gambar 2 Output CSR dan Private Key



Gambar 3 Flowchart Penerbitan SSL

3.1.2. Instalasi Sertifikat SSL

Instalasi sertifikat SSL dilakukan di 2 (dua) server yang berbeda. Server utama untuk domain utama www.kebumenkab.go.id dan server untuk subdomain. Sertifikat SSL untuk domain utama menggunakan tipe EV sehingga pada address bar di browser terdapat indikator hijau yang tertulis "Dinas Komunikasi dan Informatika Kabupaten Kebumen".

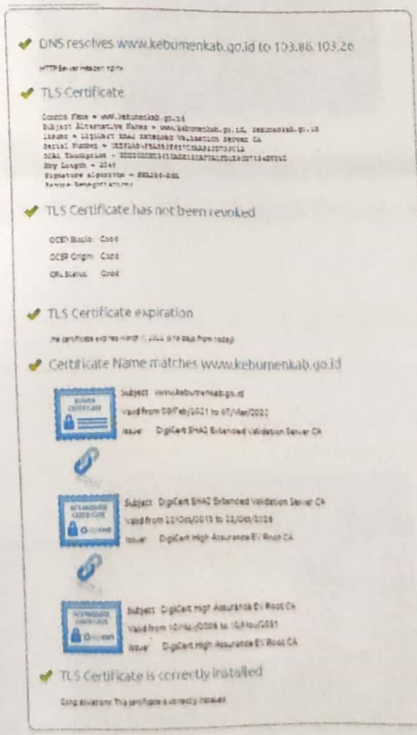
3.1.3. Pengujian Hasil Implementasi

Tahap akhir instalasi adalah pengujian instalasi sertifikat SSL. Karena menggunakan SSL berbayar yang disediakan oleh DigiCert maka proses pengujian dilakukan pada domain DigiCert yang dapat diakses melalui https://www.digicert.com/help/.

Gambar 4 Pengujian Sertifikat SSL di DigiCert.com

1. Domain www.kebumenkab.go.id

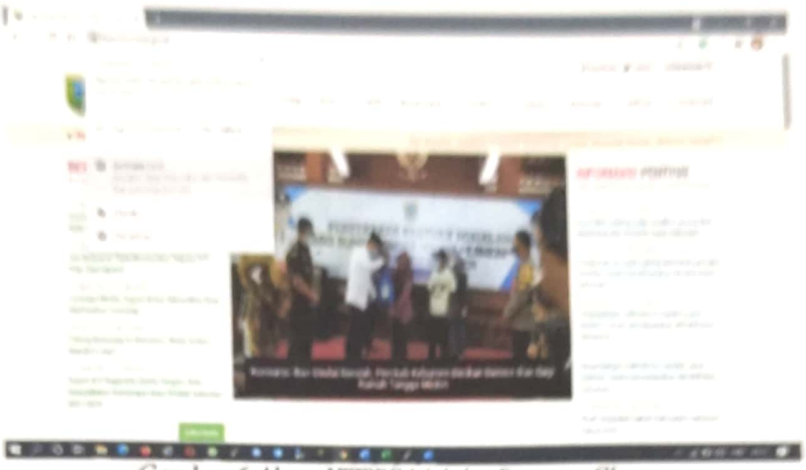
Pengujian sertifikat hanya perlu memasukan alamat website yang sudah terpasang sertifikat SSL. Pada hal ini adalah domain utama www.kebumenkab.go.id dan subdomain.kebumenkab.go.id. selain itu, jika instalasi berhasil, pada address bar domain www.kebumenkab.go.id terdapat tulisan "Dinas Komunikasi dan Informatika Kabupaen Kebumen [ID]". Hal ini menyebutkan bahwa SSL yang terpasang adalah tipe EV.



Gambar 5 Verifikasi SSL melalui DigiCert.com

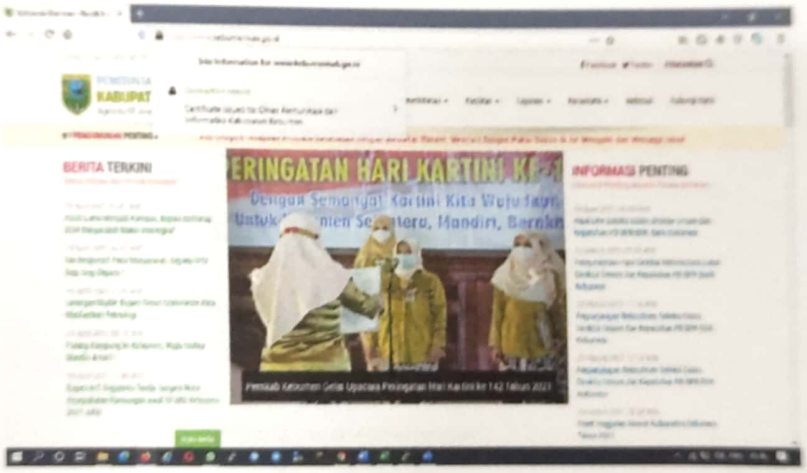
Pada proses verifikasi diatas tampak instalasi sudah sesuai dan terpasang dengan benar. Tahap selanjutkan adalah akses domain www.kebumenkab.go.id apakah title sertifikat muncul di address bar jika diakses menggunakan browser.

a. Browser Chrome



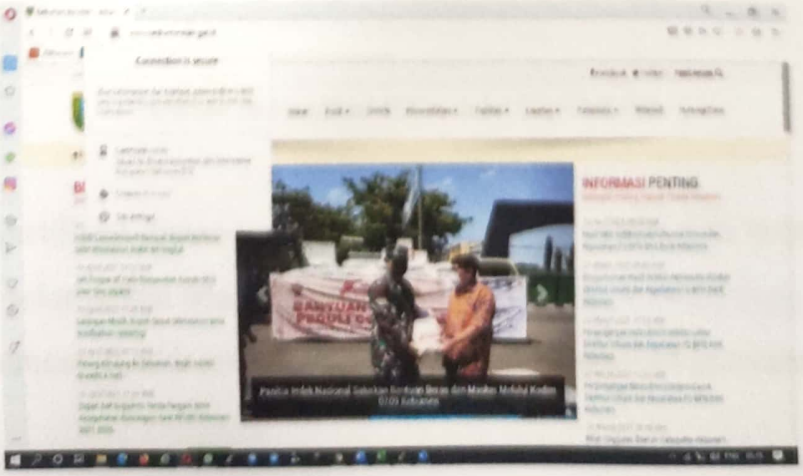
Gambar 6 Akses HTTPS Melalui Browser Chrome

b. Browser Mozilla Firefox



Gambar 7 Akses HTTPS Melalui Browser Mozilla

c. Browser Opera



Gambar 8 Akses HTTPS Melalui Browser Opera

BAB IV

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Dari hasil pekerjaan ini, pelaksana teknis telah merumuskan beberapa kesimpulan, yaitu :

1. Implementasi SSL pada domain dan subdomain kebumenkab.go.id sudah berhasil dilakukan.
2. Dengan mengimplementasikan metode SSL(*Secure Socket Layer*), maka website ini lebih terjaga keamanan informasi dan data yang ada di dalamnya.
3. Dari hasil percobaan yang dilakukan HTTP lebih rentan terhadap sniffing dibandingkan dengan HTTPS, karena HTTP tidak menggunakan metode enkripsi dalam pengiriman maupun penerimaan paket data yang dilakukan antara device dengan server.

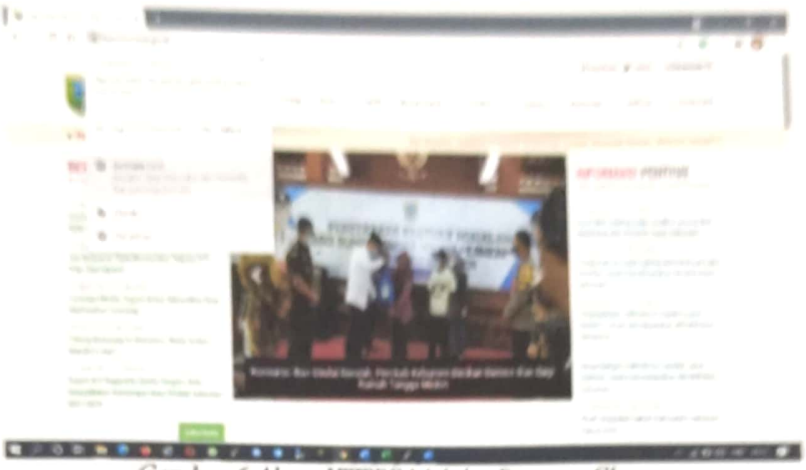
4.2. Saran

Pelaksana Teknis/Penyedia Jasa memberikan saran atas atas pekerjaan ini, yaitu sebagai berikut :

1. Sertifikat SSL(*Secure Socket Layer*) yang digunakan sudah berlisensi yang memiliki masa berlaku. Hal ini perlu diperhatikan batas waktu expired date agar sertifikat SSL dapat terus digunakan.
2. Pada domain dan subdomain yang berisi data transaksi atau terhubung dengan data penting lain, diharapkan menambah level keamanan pada proses otentikasi seperti token.
3. Membatasi akses pada domain dan subdomain yang berisi data rahasia. Karena setinggi apapun keamanan jaringan, hacker masih berpeluang untuk menyusup.

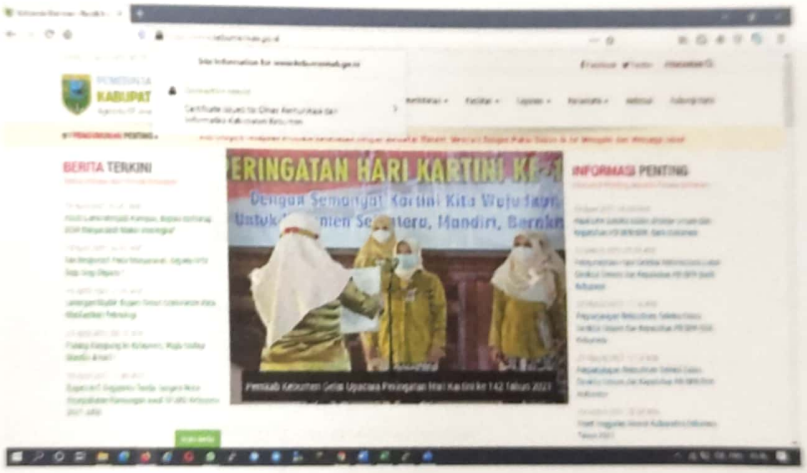
Pada proses verifikasi diatas tampak instalasi sudah sesuai dan terpasang dengan benar. Tahap selanjutkan adalah akses domain www.kebumenkab.go.id apakah title sertifikat muncul di address bar jika diakses menggunakan browser.

a. Browser Chrome



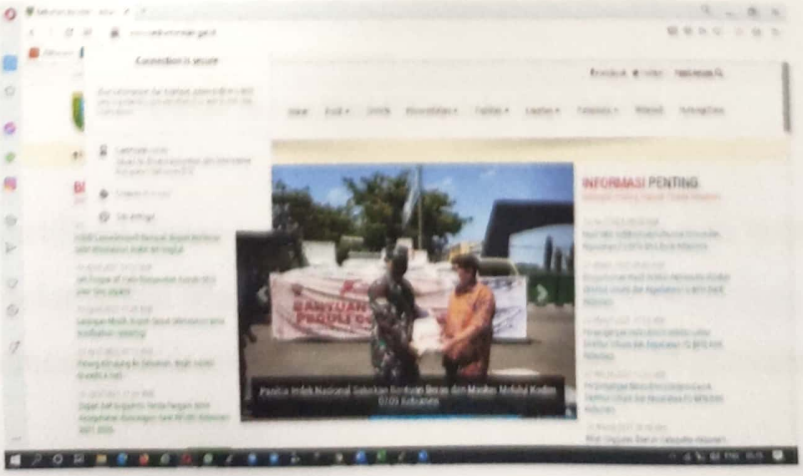
Gambar 6 Akses HTTPS Melalui Browser Chrome

b. Browser Mozilla Firefox



Gambar 7 Akses HTTPS Melalui Browser Mozilla

c. Browser Opera



Gambar 8 Akses HTTPS Melalui Browser Opera

BAB IV

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Dari hasil pekerjaan ini, pelaksana teknis telah merumuskan beberapa kesimpulan, yaitu :

1. Implementasi SSL pada domain dan subdomain kebumenkab.go.id sudah berhasil dilakukan.
2. Dengan mengimplementasikan metode SSL(*Secure Socket Layer*), maka website ini lebih terjaga keamanan informasi dan data yang ada di dalamnya.
3. Dari hasil percobaan yang dilakukan HTTP lebih rentan terhadap sniffing dibandingkan dengan HTTPS, karena HTTP tidak menggunakan metode enkripsi dalam pengiriman maupun penerimaan paket data yang dilakukan antara device dengan server.

4.2. Saran

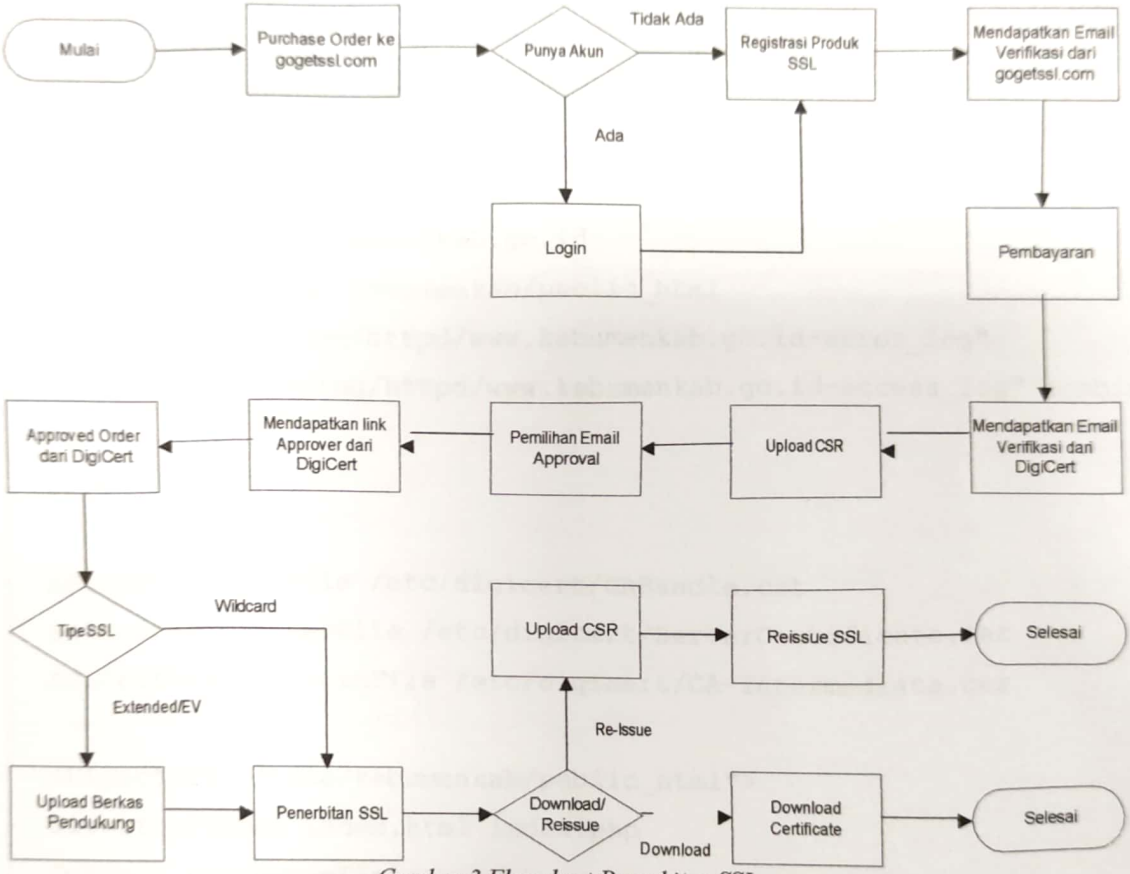
Pelaksana Teknis/Penyedia Jasa memberikan saran atas atas pekerjaan ini, yaitu sebagai berikut :

1. Sertifikat SSL(*Secure Socket Layer*) yang digunakan sudah berlisensi yang memiliki masa berlaku. Hal ini perlu diperhatikan batas waktu expired date agar sertifikat SSL dapat terus digunakan.
2. Pada domain dan subdomain yang berisi data transaksi atau terhubung dengan data penting lain, diharapkan menambah level keamanan pada proses otentikasi seperti token.
3. Membatasi akses pada domain dan subdomain yang berisi data rahasia. Karena setinggi apapun keamanan jaringan, hacker masih berpeluang untuk menyusup.

website@simpada:~/SSL

```
[website@simpada SSL]$ ls -l
total 8
-rw-r--r-- 1 root root 1175 Apr  2 16:04 subdomain.kebumenkab.csr
-rw-r--r-- 1 root root 1679 Apr  2 16:02 subdomain.kebumenkab.key
[website@simpada SSL]$
```

Gambar 2 Output CSR dan Private Key



Gambar 3 Flowchart Penerbitan SSL

3.1.2. Instalasi Sertifikat SSL

Instalasi sertifikat SSL dilakukan di 2 (dua) server yang berbeda. Server utama untuk domain utama www.kebumenkab.go.id dan server untuk subdomain. Sertifikat SSL untuk domain utama menggunakan tipe EV sehingga pada address bar di browser terdapat indikator hijau yang tertulis "Dinas Komunikasi dan Informatika Kabupaten Kebumen".

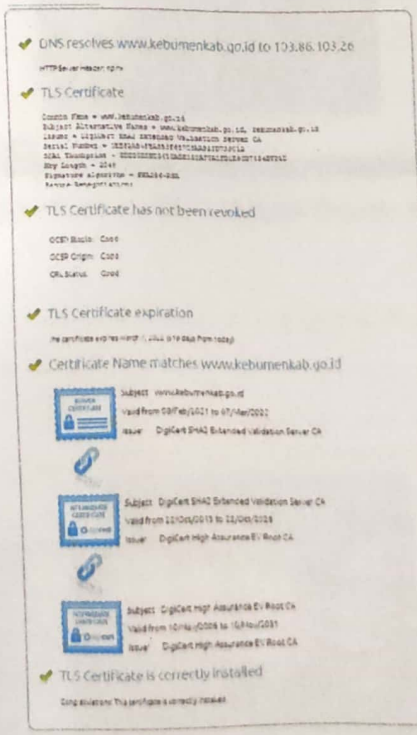
3.1.3. Pengujian Hasil Implementasi

Tahap akhir instalasi adalah pengujian instalasi sertifikat SSL. Karena menggunakan SSL berbayar yang disediakan oleh DigiCert maka proses pengujian dilakukan pada domain DigiCert yang dapat diakses melalui https://www.digicert.com/help/.

Gambar 4 Pengujian Sertifikat SSL di DigiCert.com

1. Domain www.kebumenkab.go.id

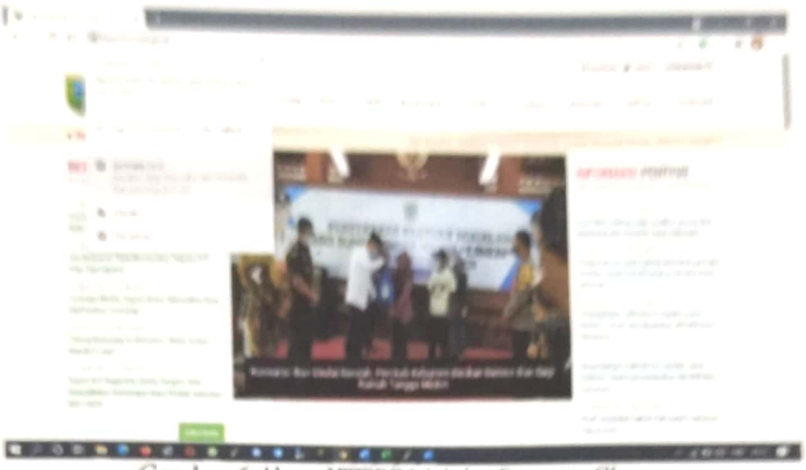
Pengujian sertifikat hanya perlu memasukan alamat website yang sudah terpasang sertifikat SSL. Pada hal ini adalah domain utama www.kebumenkab.go.id dan subdomain.kebumenkab.go.id. selain itu, jika instalasi berhasil, pada address bar domain www.kebumenkab.go.id terdapat tulisan "Dinas Komunikasi dan Informatika Kabupaen Kebumen [ID]". Hal ini menyebutkan bahwa SSL yang terpasang adalah tipe EV.



Gambar 5 Verifikasi SSL melalui DigiCert.com

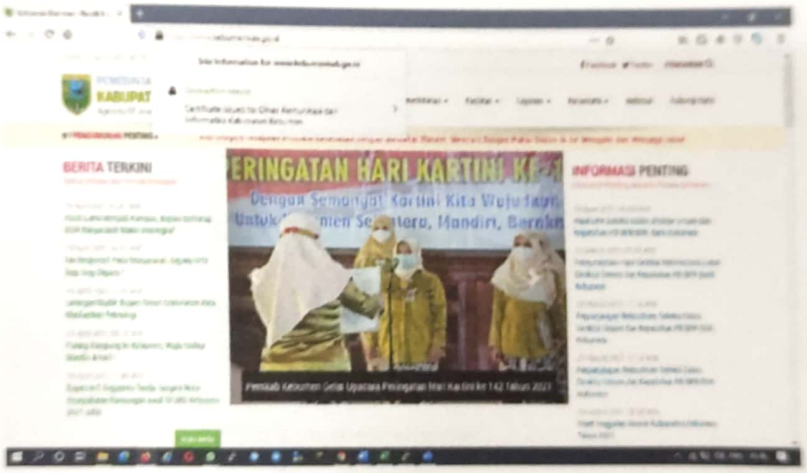
Pada proses verifikasi diatas tampak instalasi sudah sesuai dan terpasang dengan benar. Tahap selanjutkan adalah akses domain www.kebumenkab.go.id apakah title sertifikat muncul di address bar jika diakses menggunakan browser.

a. Browser Chrome



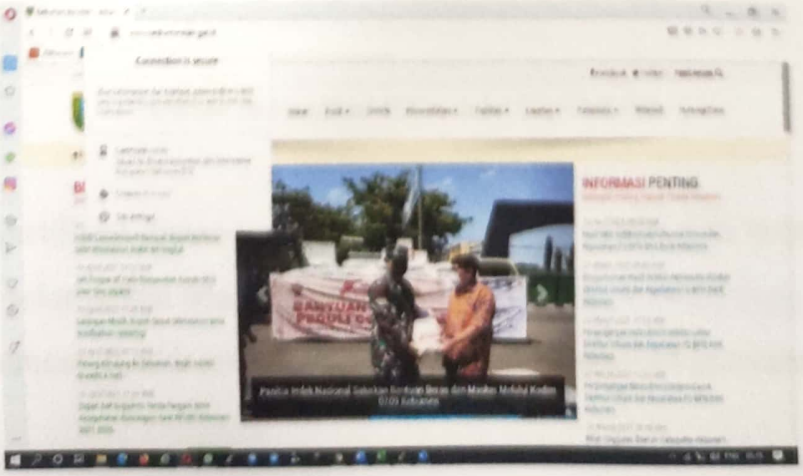
Gambar 6 Akses HTTPS Melalui Browser Chrome

b. Browser Mozilla Firefox



Gambar 7 Akses HTTPS Melalui Browser Mozilla

c. Browser Opera



Gambar 8 Akses HTTPS Melalui Browser Opera

BAB IV

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Dari hasil pekerjaan ini, pelaksana teknis telah merumuskan beberapa kesimpulan, yaitu :

1. Implementasi SSL pada domain dan subdomain kebumenkab.go.id sudah berhasil dilakukan.
2. Dengan mengimplementasikan metode SSL(*Secure Socket Layer*), maka website ini lebih terjaga keamanan informasi dan data yang ada di dalamnya.
3. Dari hasil percobaan yang dilakukan HTTP lebih rentan terhadap sniffing dibandingkan dengan HTTPS, karena HTTP tidak menggunakan metode enkripsi dalam pengiriman maupun penerimaan paket data yang dilakukan antara device dengan server.

4.2. Saran

Pelaksana Teknis/Penyedia Jasa memberikan saran atas atas pekerjaan ini, yaitu sebagai berikut :

1. Sertifikat SSL(*Secure Socket Layer*) yang digunakan sudah berlisensi yang memiliki masa berlaku. Hal ini perlu diperhatikan batas waktu expired date agar sertifikat SSL dapat terus digunakan.
2. Pada domain dan subdomain yang berisi data transaksi atau terhubung dengan data penting lain, diharapkan menambah level keamanan pada proses otentikasi seperti token.
3. Membatasi akses pada domain dan subdomain yang berisi data rahasia. Karena setinggi apapun keamanan jaringan, hacker masih berpeluang untuk menyusup.