SISTEM KEAMANAN TRANSAKSI DATA DENGAN MENERAPKAN XML ENKRIPSI DAN XML SIGNATURE DENGAN MENGGUNAKAN METODE FAST

Slamet Widodo
Jurusan Teknik Komputer Politeknik Negeri Sriwijaya
Jl.Srijaya Negara Bukit Besar Palembang
Telp.0711353414 dan Fax.0711 355918
Email: info@polsri.ac.id/slamet_widodo2003@yahoo.com

ABSTRAK
Perkembangan Sistem Informasi sering disalah gunakan seseorang untuk tindakan kriminal, seperti kemampuan untuk mencuri dan mengubah informasi tersebut. Bank dalam melakukan transaksi keuangannya secara online lebih intensif, sehingga membutuhkan sistem keamanan transaksi data dari kantor cabang ke kantor pusat.Tujuan penelitian ini untuk membangun sistem keamanan transaksi kredit nasabah Bank antar kantor cabang pusat. Salah satu cara untuk melindungi transakasi menggunakan XML enkripsi dan XML signature . Penerapan teknik enkripsi dan tanda tangan digital dengan teknologi web service untuk meningkatkan kerahasiaan, otentikasi dan verifikasi transaksi kredit nasabah pada Bank Perkreditan Rakyat dengan menggunakan metode Framework of Analisis For System Thinking (FAST). Penelitian ini menghasilkan sebuah sistem keamanan pesan SOAP(Simple Object Access Protocol) dengan bahasa XML WSDL(Web Services Description Language) melalui protocol HTTP (Hipertext Transfer Protocol) untuk melindungi data transaksi kredit nasabah dari penyusup (intruder) dalam bentuk pesan rahasia yang dikodekan dan distribusikan menggunakan teknologi web service. Analisa pengujian menunjukan bahwa ukuran kapasitas data(byte) yang dikirim hasil enkripsi XML tanpa kompresi lebih besar dibandingkan hasil enkripsi XML dengan kompresi kapasitas data(byte) menjadi lebih kecil, sehingga terjadi perubahan yang signifikan saat data di transfer sebelum dikompresi dan sesudah melakukan kompresi yaitu waktu proses data yang dikompresi lebih cepat dibandingkan XML enkripsi tanpa kompresi.

Kata kunci: XML Enkripsi, XML Signature dan Metode FAST

1. PENDAHULUAN

Penyimpangan peranan teknologi informasi untuk tindakan kriminal yang dilakukan oleh organisasi atau pribadi seperti kesempatan untuk mencuri dan mengubah informasi dalam distribusi data untuk tujuan kejahatan (Bush : 2005). Mahalnya perangkat lunak sistem keamanan juga menjadi salah satu kendala bagi industri kecil menengah, sehingga mereka kurang memperhatikan perlunya sistem keamanan keadaan ini menjadi peluang penyebab terjadinya kriminalitas. Keamanan selalu menjadi hal yang amat penting khususnya dalam dunia internet.

Teknologi keamanan XML dapat diaplikasikan dalam sistem keamanan *end-to-end* , yang sangat penting saat pesan XML dikirimkan melalui beberapa perantara. Sistem keamanan XML lebih ke arah keamanan materi, sehingga saling melengkapi bila dihubungkan dengan sistem keamanan yang borientasi ke keamanan transportasi misalnya *secure sockets layer* (SSL) / *transport layer security* (TLS) atau *virtual private networks* (VPNs) hanya menyediakan kerahasiaan selama informasi ditransit, dan bukan selama disimpan diserver. Ada beberapa cara untuk melindungi dan mengamankan data yaitu lewat *XML Encryption* (Bilal Siddiqui, 2002).

XML Digital signature digunakan untuk menyediakan kepastian integritas materi dalam dokumen dan untuk membuat serta menguji tandatangan elektronik tersebut. Dengan kepastian integritas materi, pengguna materi dapat mendeteksi perubahan isi materi yang tidak diinginkan, baik karena kesengajaan maupun karena kesalahan system sendiri. Tidak seperti mekanisme *checksum* yang sederhana, tanda tangan digital menghubungkan initisari materi dengan penanda isi materi menggunakan teknik kriptografi. Tanda tangan digital tersebut adalah sebuah angka pendek yang nilainya tetap, khas terhadap isi materi, dan tidak berguna untuk diketahui jika tanpa isi materi itu sendiri. Teknik kriptografi membuat materi dengan tanda tangan digital menjadi lebih susah untuk diubah isi materinya oleh seseorang yang bukan memberi tanda tangan digital itu sendiri tanpa terdeteksi. Kepastian integritas materi tidak hanya memberikan perlindungan dalam transportasi tapi juga dalam penyimpanan dan dalam suatu proses. (Eastlake,2003).

Masalah pokok yang paling sering dihadapi oleh setiap perusahaan yang bergerak dalam bidang usah apapun selalu tidak terlepas dari kebutuhan akan dana (modal) untuk membiayai usahanya. Kebutuhan akan dana ini diperlukan baik untuk modal investasi atau modal kerja. Di sini bank sebagai lembaga keuangan mempunyai kegiatan utama yaitu membiayai permodalan suatu bidang usaha disamping usaha lain seperti menampung uang yang sementara waktu belum digunakan oleh pemiliknya. Jadi fungsi utama bank merupakan

perantara diantara masyarakat yang membutuhkan dana dengan masyarakat yang kelebihan dana. Dalam hal ini diperlukan suatu manajemen kredit yang merupakan pengelolaan kredit yang baik mulai dari perencanaan jumlah kredit, penentuan suku bunga, prosedur pemberian kredit, analisis pemberian kredit sampai kepada pengendalian dan pengawasan kredit yang macet (Kasmir, 2002:71-72)**.** Sehingga untuk mendukung prosedur keamanan transaksi kredit nasabah dibutuhkan sistem keamanan distribusi data nasabah bank yang berbasis web service .

Web service merupakan perkembangan *distributed computing* dengan arsitektur n-tier. Keuntungan yang paling mendasar yang ditawarkan oleh web services adalah integrasi. Usaha untuk mengintegrasikan aplikasi, sistem, maupun platform yang berbeda sering mengalami kesulitan dan memerlukan proses yang panjang. Web services merupakan standar yang tepat sebagai alat pengintegrasian. Web services mampu mengintegrasikan aplikasi dan sistem dari platform yang berbeda karena menggunakan standar protokol web dalam interaksinya seperti TCP/IP, HTTP, XML, SOAP, UDDI. (Gottschalk, 2002).

Teknologi web service tampaknya menjanjikan untuk mendukung sistem keamanan yang cukup memadai *pada* sistem keamanan yang penting. Bank Perkreditan Rakyat Boyolali melakukan transaksi keuangan online yang cukup intensif, sehingga membutuhkan suatu sistem keamanan pada distribusi data transaksi kredit nasabah antar kantor cabang ke manager pusat.

Tesis ini akan membahas penerapan teknik enkripsi dalam XML dan tanda tangan digital dalam XML *dengan* teknologi *web service* untuk meningkatkan kerahasiaan,otentikasi dan verifikasi transaksi kredit nasabah Bank Perkreditan Rakyat dengan metode *Framework of Analisis For System Thinking* (FAST).

2. KEAMANAN WEB SERVICE

Keamanan Web Service merupakan model pengamanan pesan SOAP yang menjadi dasar bagi spesifikasi keamanan *web service*. Keamanan web service berurusan dengan integritas pesan dan kerahasiaan isi pesan SOAP *(simple object application protocol).* Selain itu, keamanan web service juga mengatur cara menyisipkan *security token* dalam pesan SOAP dalam bentuk plainteks maupun dalam bentuk biner (seperti sertifikat X.509). Keamanan web service didesain fleksibel mungkin terhadap tipe *security token* yang dapat disisipkan. Keamanan web service menyediakan keamanan pada pesan SOAP tanpa memperdulikan bagaimana komunikasi pesan tesebut disalurkan ke penerima. Keamanan web service dibangun berdasarkan teknologi-teknologi yang sudah ada sebelumnya. Dua teknologi yang menjadi pondasi utama keamanan adalah enkripsi dalam *XML* dan tanda tangan digital dalam *XML*. Enkripsi dalam *XML* lebih berperan dalam menjaga kerahasiaan isi pesannya SOAP dan tanda tangan digital dalam *XML* berperan dalam menjaga integritas pesan SOAP. (Ilham Gorgun,2004)

2.1 Enkripsi dalam XML

Enkripsi dalam XML merupakan teknologi yang fleksibel untuk mengenkripsi seluruh atau sebagian dokumen XML. Enkripsi dalam *XML* akan membungkus elemen yang dienkripsi menggunakan tag XML penanda. Dalam tag XML penanda tersebut terdapat kunci enkripsi, petunjuk metode yang digunakan untuk melakukan enkripsi, chiperteks, dan properti tambahan lainnya. Tag XML yang menjadi penanda tersebut biasanya berupa tag *EncryptedData* . Enkripsi dalam XML diimplementasikan dalam pesan SOAP berupa tag *EncryptedKey* dan *EncryptedData*. Tag *EncryptedKey* diletakkan sebagai subelemen tag *Security* pada bagian *header* SOAP. Sementara *EncryptedData* dapat diletakkan dalam *header* maupun dalam *body* SOAP. Untuk plainteks berupa data dengan tipe selain teks, tag *EncryptedData* diletakkan dalam *header* SOAP**.** (Ilhami Gorgun,2004).

2.2 Tanda Tangan Digital Dalam XML

Tanda tangan digital dalam XML bertugas menjaga Integritas pesan SOAP. Berarti penerima pesan SOAP dapat memastikan bahwa pesan yang diterimanya benar-benar berasal dari pihak tertentu tanpa ada perubahan sedikitpun pada isi pesannya. Dalam keamanan web service , integritas pesan SOAP dijaga menggunakan tanda tangan digital dalam *XML* yang terkadang dilengkapi juga dengan *security token*. Tanda tangan digital dalam *XML* merupakan implementasi *digital signature*. Tanda tangan digital dalam *XML* digunakan dalam keamanan web service , sebab pesan SOAP pada dasarnya merupakan sebuah dokumen XML. Prinsip yang digunakan dalam membuat tanda tangan digital *XML* secara umum sama dengan prinsip pembuatan *digital signature*. (Jeffrey Scott Williams Sr,2009).

2.3 Algoritma AES

Advanced Encryption Standard (AES) merupakan blok cipher diadopsi sebagai standar enkripsi oleh pemerintah USA. AES menjadi penerus resmi untuk DES (Data Encryption Standar) pada bulan Desember 2001. Tidak seperti DES, pendahulunya, AES adalah jaringan substitusi permutasi, bukan sebuah jaringan *Feistel.* AES yang cepat di kedua perangkat lunak dan hardware, relatif lebih mudah diterapkan , dan membutuhkan memori kecil. AES memiliki ukuran blok tetap 128 bit dan ukuran kunci 128, 192 atau 256 bit, sedangkan AES atau Rijndael dapat ditentukan dengan ukuran kunci dan blok dalam setiap

beberapa 32 bit, dengan minimal 128 bit dan maksimum 256 bit. Karena ukuran blok tetap 128 bit, AES beroperasi pada array 44 byte, disebut state. Kebanyakan perhitungan AES dilakukan khusus dalam *finite field* (Nagireddy Sreenivasulu:2008). AES menggunakan blok *input* atau blok data dengan ukuran 128 bit, panjang kunci yang digunakan adalah 128, 192, dan 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah *round* atau putaran pada algoritma AES. Di bawah ini adalah tabel perbedaan kunci algoritma tersebut.

Parameter algoritma AES terdiri dari tiga bagian :

1. *Plaintext* : *array* berukuran 16 *byte* merupakan data masukan
2. *Ciphertext* : *array* berukuran 16 *byte* merupakan hasil *enkripsi*
3. *Cipher Key* : *array* berukuran 16 *byte* merupakan kunci *enkripsi*

Masing-masing tipe menggunakan kunci internal yang berbeda yaitu roundkey untuk setiap proses putaran. Proses putaran enkripsi AES-128 dikerjakan sebnayka 10 kali (a=10), yaitu sebagai berikut:

1. Addroundkey
2. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap putaran adalah SubBytes, ShiftRows, MixColumns, dan AddRoundKey.
3. Final round, adalah proses untuk putaran terakhir yang meliputi SubBytes, ShiftRows, dan AddRounKey

Sedangkan pada proses dekripsi AES-128, proses putaran juga dikerjakan sebanyak 10 kali (a=10) yaitu sebagai berikut :

1. Addroundkey
2. Putaran sebanyak a-1 kali, dimana pada setiap putaran dilakukan proses : InverseShiftRows, Inverse SubBytes, , AddRounKey dan InverseMixColumns,
3. Final round, adalah proses untuk putaran terakhir yang meliputi InverseShiftRows, Inverse SubBytes, , AddRoundKey

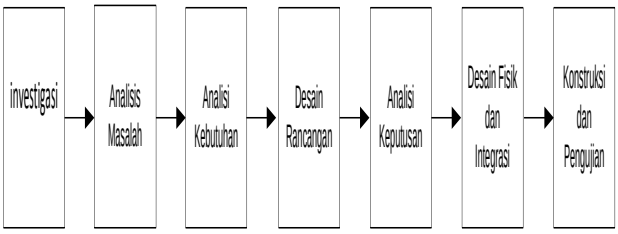
Pada enkripsi dan dekripsi AES-192 proses putaran dikerjakan 12 kali (a=12), sedangkan untuk AES-256 proses putaran dikerjakan 14 kali (a=14).

Fungsi algorithma AES pada penelitian ini digunakan untuk mengenkripsi dan mendekripsi query XML pada transaksi kredit nasabah. Dengan langkah-langkah sebagai berikut:

a. Proses dimulai dengan mengambil transaksi kredit nasabah dalam query database dengan format teks.
b. Kemudian format teks tersebut diberi tanda tangan digital menggunakan kunci private untuk memberikan kepastian bahwa query database yang dikirim memang benar berasal dari kantor pusat .
c. Selanjutnya dilakukan proses enkripsi menggunakan Algorithma AES menggunakan public key milik kantor cabang yang akan dikirim ke Manager Pusat.

3. METODE FAST *(FRAMEWORK ANALYTICAL SYSTEM OF THINGKING)*

Dalam penelitian ini perangkat lunak yang dihasilkan adalah untuk mengenkripsi dalam xml query transaksi kredit nasabah bank dari web server ke web service kantor pusat atau sebaliknya dan mendistribusikan kunci yang digunakan untuk membukannya secara aman. Selain itu terdapat juga fasilitas tanda tangan digital dalam xml dan memverifikasinnya. Pembuatan system atau perangkat lunak pada penelitian ini mengikuti langkah-langkah penegembangan perangkat lunak model FAST (Whitten L.jeffrey,2004), seperti dalam bentuk blok diagram gambar 3.30 berikut ini:

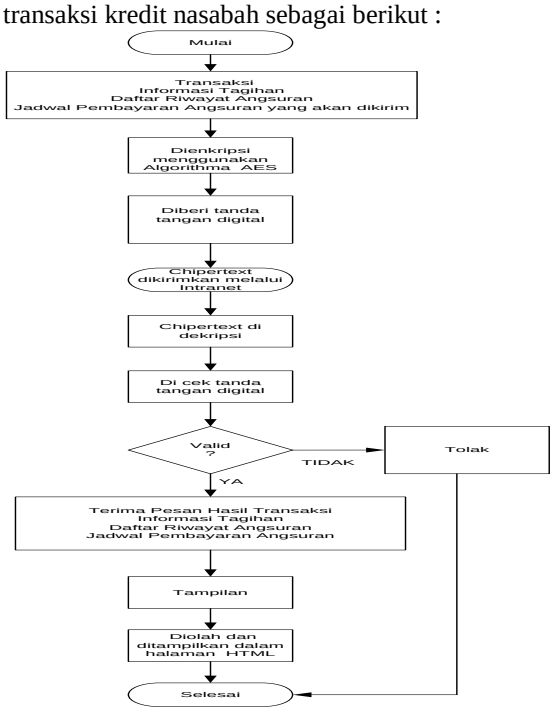


Gambar 3. Blok Diagram Metode FAST (Whitten L.jeffrey,2004 : hal 89)

1. Investigasi
   Pada tahap ini dilakukan kegiatan untuk mengetahui adanya masalah, peluang, dan kesempatan yang memicu pengembangan system keamanan serta menetapkan ruang lingkup pengembangan sistem.
2. Analisa Masalah
   Dengan proses sistem keamanan transaksi kredit dengan menggunakan *secure socket layer* masih memberi peluang orang yang tidak bertanggung jawab untuk melihat bahkan masuk ke sistem pada saat terjadi distribusi data transaksi dari web server (kantor pusat) ke web service dengan komputer cabang (browser).
3. Analisa Kebutuhan
   Beberapa bahan yang dibutuhkan dalam pengembangan sistem keamanan transaksi kredit dan tabungan nasabah adalah :
   Data-data pada transaksi informasi tagihan kredit Individual dan kolektif, daftar riwayat angsuran nasabah, dan jadwal pembayaran angsuran kredit nasabah dengan menyesuaikan status dan identitas nasabah. Sedangkan langkah-langkah yang digunakan dalam memenuhi kebutuhan

adalah dengan cara wawancara dan studi literatur.

4. Desain Logic
   Dalam Desain Logic ini menggunakan flowchart diagram untuk proses enkripsi dan tanda tangan digital dalam xml transaksi kredit nasabah sebagai berikut :



Gambar 4. Diagram Enkripsi /Dekripsi dan Signature

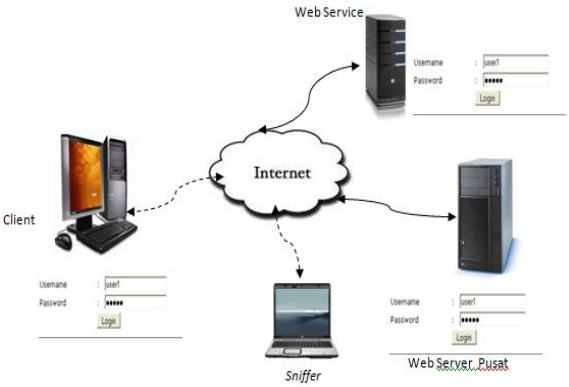
   a. Proses dimulai dengan mengambil transaksi Informasi Tagihan Kredit Nasabah, Daftar Riwayat Angsuran, dan jadwal Pembayaran angsuran dalam query database dengan format request parameter teks.
   b. Kemudian request parameter teks tersebut dienkripsi menggunakan chiper key milik pengirim menggunakan algorithma AES untuk memberikan keamanan data selama dikirim dari web server ke web service kantor pusat dengan komputer klien(browser) atau sebaliknya.
   c. Selanjutnya dilakukan membubuhi tanda tangan digital dalam xml menggunakan private key milik server menggunakan algorithma RSA untuk member kepastian memang chiper text yang dikirim benar berasal dari server pusat.
   d. Kemudian web service melakukan proses verifikasi tanda tangan digital dalam xml yang dikirimkan menggunakan public key milik server pusat.
   e. Selanjutnya mendecrypt chiper text yang dikirim menggunakan private key milik server pusat menggunakan chiper key pada AES.
   f. Kemudian apabila hasilnya sesuai request parameter yang dikirim maka proses selanjutnya data diolah untuk ditampilkan dalam bentuk halaman HTML. .

5. Analisa Keputusan
   Melihat dari perkembangan bahasan diatas maka akan dikembangkan sebuah sistem kemanan database transaksi kredit nasabah dengan enkripsi dan dekripsi menggunakan bahasa XML *(Extensible Markup Languange)*, selanjutnya dengan memberi verifikasi keabsahan pengiriman transaksi kredit menggunakan digital signature atau tanda tangan digital XML *(Exstensible Markup languange)* dari web server server pusat ke web service atau sebaliknya dengan komputer client atau cabang(browser) menggunakan teknologi ASP.NET dengan bahasa pemrograman C#, database MySQL dan WebServernya IIS.
6. Desain Fisik dan Integrasi
   Tiga langkah yang dilakukan yaitu pembuatan user interface, memberi enkripsi dan dekripsi pada transaksi informasi tagihan kredit, daftar riwayat angsuran, dan jadwal pembayaran angsuran, kemudian memberi tanda tangan digital dalam xml untuk menghasilkan data transaksi kredit nasabah yang sudah diverifikasi dan selanjutnya diproses untuk dijadikan halaman HTML
7. Konstruksi dan Pengujian
   Membangun dan menguji sebuah sistem yang memenuhi persyaratan sistem keamanan dan spesifikasi desain fisik, dan mengimplementasikan setiap interface. Adapun yang harus dibangun dan diujikan adalah proses pemberian keamanan encrypt dan decrypt untuk mendapatkan teks rahasia dan tanda tangan digital dalam xml pada request parameter transaksi kredit nasabah untuk verifikasi dan memberi proteksi untuk otentikasi.

4. SKENARIO PENGUJIAN MENGGUNAKAN PROGRAM ALTOVA XMLSPY 2011 R.2 PADA BROWSER KE WEB SERVER

Percobaan berikut dilakukan komunikasi antara web server kantor pusat ke kantor cabang dengan menggunakan web browser pada komputer client dan dimonitor oleh sniffer dengan menggunakan

program wireshark seperti pada gambar 5. dibawah ini :



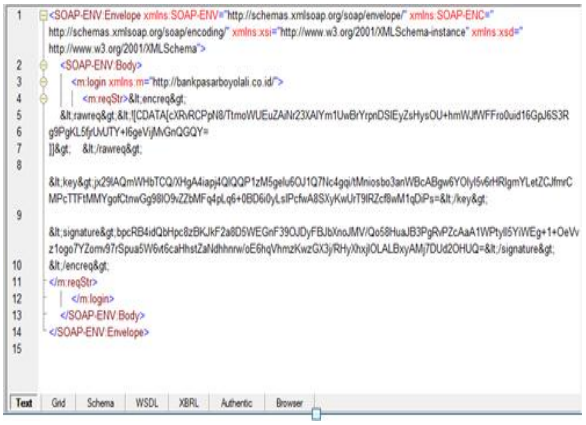
Gambar 5. Skenario Komunikasi Web Server dan Web Browser

4.1 Pengujian Kinerja Web Service ke Web Server

4.1.1 Pengujian Login Tidak Aman (Tanpa Kompresi) username password:

Pengujian kinerja web service terhadap web server dengan melihat hasil *encrypt plain text*, *chiper key* , dan *signature* Login tanpa kompresi dalam bentuk *request string* data XML tanpa kompresi yang terenkripsi saat Login data yang

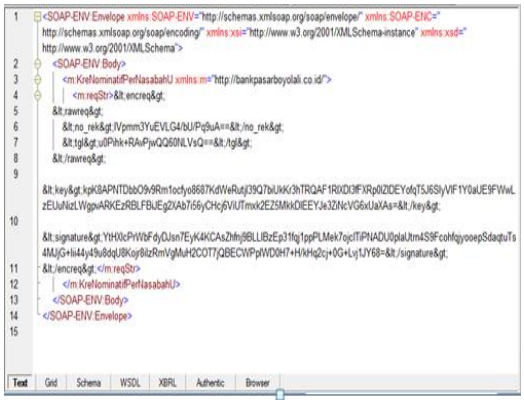
Gambar 6. Hasil Pengamatan Paket Data Enkripsi XML dan Signature XML Login Tanpa kompresi Menggunakan Altova XMLSPY 2011 r.2



Gambar 7. Hasil Pengamatan Paket Data Enkripsi XML dan Signature XML Login dengan Kompresi Menggunakan Altova XMLSPY 2011 r.2

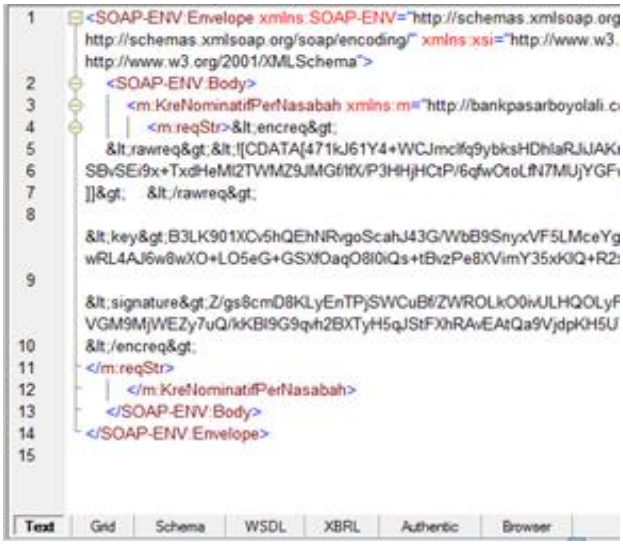
4.2 Pengujian Parameter Procedur KreNominatifNasabah Tidak Aman (Tanpa Kompresi) dan Pengujian yang Aman(Dengan Kompresi) :

Pengujian kinerja web service terhadap web server dengan melihat hasil *encrypt plain text*, *chiper key*, dan *signature* KreNominatifNasabah tanpa kompresi dalam bentuk *request string*. Dengan menggunakan program Wireshark v1.4.2 dan Altova XMLSPY 2011 r.2 seorang *intruder* informasi yang diterima berupa paket yang terenkripsi ,namun bagi intruder masih mengenal entri point **no_rek** nasabah hasil tangkapan data yang dikirim dari web service ke web server Bank seperti Gambar 8 dibawah ini:



Gambar 8 di atas menampilkan hasil pengamatan paket data Login tanpa kompresi dengan menggunakan program Wireshark v1.4.2 dan Altova XMLSPY 2011 r.2 seorang *intruder* informasi yang diterima berupa paket yang terenkripsi dari entri point no_rek menjadi *strings* sehingga agak sulit *intruder* membaca data terenkripsi dan menyatakan data yang dikirimkan tidak aman

 ISSN: 1907-5022



Gambar 9 Hasil Pengamatan Paket Data Enkripsi XML dan Signature XML KreNominatifNasabah dengan kompresi Menggunakan Altova XMLSPY 2011 r.2

Gambar 9 di atas menampilkan hasil pengamatan paket data KreNominatifNasabah tanpa kompresi dengan menggunakan program Wireshark v1.4.2 dan Altova XMLSPY 2011 r.2 seorang *intruder* informasi yang diterima berupa paket yang terenkripsi dari entri point no_rek menjadi *strings* sehingga agak sulit *intruder* membaca data terenkripsi dan menyatakan data yang dikirimkan aman.

.**Tabel 1.** Pengujian Kenerja Enkripsi dalam XML dan Tanda Tangan Digital dalam XML pada Parameter Store Prosedur Login :

Parameter : Login								
	Tanpa Kompresi				**Dengan Kompresi**			
No.Uji	Enkripsi XML		Signature XML		Enkripsi XML		Signature XML	
	Kapasitas (Byte)	Waktu (detik)	Kapasitas (Byte)	Waktu (detik)	Kapasitas (Byte)	Waktu (detik)	Kapasitas (Byte)	Waktu (detik)
1	284	469	172	469	224	60	172	60
2	284	130	172	130	222	100	172	100
3	284	180	172	180	224	70	172	70
4	284	120	172	120	224	40	172	40
5	284	50	172	50	224	70	172	70
Rata - rata	**284**	**189.8**	**172**	**189.8**	**223.6**	**68**	**172**	**68**

Tabel 1. Hasil Waktu Kinerja Login Web server
Pengujian Pertama tabel 1.. diatas Store Prosedur Login terjadi perbedaan hasil proses enkripsi XML dan signature XML dokumen (tanpa melakukan kompresi) dengan dokumen XML yang terkompresi yaitu hasil enkripsi XML data awal kapasitas 284.6(byte) dengan waktu 189.8(detik) setelah dilakukan kompresi berubah menjadi 223.6 (byte) dengan waktu 68(detik), sedangkan data awal signature XML dengan kapasitas 172(byte) dan waktu rata-rata 189.8(detik) setelah dilakukan kompresi berubah menjadi kapasitas 172 (byte) dengan waktu rata-rata 68 (detik) .

Tabel 2. Pengujian Kenerja Enkripsi dalam XML dan Tanda tangan digital dalam XML pada Parameter store Prosedur KreNominatifPernasabah sebagai berikut :

Parameter : KreNominatifPerNasabah								
	Tanpa Kompresi				**Dengan Kompresi**			
No.Uji	Enkripsi XML		Signature XML		Enkripsi XML		Signature XML	
	Kapasitas (Byte)	Waktu (detik)	Kapasitas (Byte)	Waktu (detik)	Kapasitas (Byte)	Waktu (detik)	Kapasitas (Byte)	Waktu (detik)
1	2738	110	172	110	1747	180	172	180
2	2738	110	172	110	1748	70	172	70
3	2738	170	172	170	1748	100	172	100
4	2738	90	172	90	1748	100	172	100
5	2738	80	172	80	1748	80	172	80
Rata - rata	**2738**	**112**	**172**	**112**	**1747.8**	**106**	**172**	**106**

Tabel 2. Hasil waktu kinerja parameter store prosedurKreNominatifPernasabah

Pengujian 2. diatas Store Prosedur KreNominatifNasabah terjadi perbedaan hasil proses enkripsi dalam XML dan tanda tangan digital dalam XML dokumen (tanpa melakukan kompresi) dengan dokumen XML yang terkompresi yaitu hasil enkripsi dalam XML data awal kapasitas rata-rata 2378(byte) dengan waktu 112(detik) setelah dilakukan kompresi berubah menjadi 1747.8(byte) dengan waktu 106(detik), sedangkan data awal tanda tangan digital dalam XML dengan kapasitas 172(byte) dan waktu rata-rata 112(detik) setelah dilakukan kompresi berubah menjadi kapasitas 172 (byte) dengan waktu rata-rata 106(detik) .

Berdasarkan analisa hasil tabel pengujian diatas , Tabel 1 menjelaskan waktu kinerja entri point parameter procedur Login terjadi perubahan nilai waktu enkripsi dalam XML tanpa kompresi dan dikompresi sebesar 121,8 (detik) dengan kapasitas data sebesar 60,4(byte) . Tabel 2. entri point parameter prosedur KreNominatifNasabah sebesar 6 (detik) dengan kapasitas data sebesar 990,2 (byte) Dari seluruh hasil analisa menunjukan bahwa kapasitas data(byte*)* hasil enkripsi dalam XML dan tanda tangan digital dalam XML terjadi perubahan yang signifikan saat data di transfer tanpa kompresi yaitu lebih lambat waktunya(detik) dibandingkan enkripsi dalam XML dan tanda tangan digital dalam XML dikompresi dengan waktu proses yang lebih cepat. Dengan tanda tangan digital dalam XML kapasitas data (byte) tetap sebelum dan sesudah dikompresi sedangkan terjadi perubahan kecepatan proses sesudah melakukan kompresi tanda tangan digital dalam XML .

Dari segi keamanan, dengan memanfaatkan XML enkripsi dan XML signature melalui pesan SOAP menjadikan dokumen data yang dikirimkan terintegritas dan terjamin kerahasiaanya .

5. KESIMPULAN

Setelah melakukan serangkaian kegiatan mulai dari perancangan, implementasi dan pengujian terhadap sistem keamanan dalam penelitian ini, maka dapat diambil beberapa kesimpulan, di antaranya adalah sebagai berikut:

1. Pengiriman data terenkripsi dalam XML dan tanda tangan digital dalam XML membatasi ruang gerak *intruder* untuk membaca isi dokumen pesan SOAP melalui protocol http web server ke web service atau sebaliknya, sehingga data yang dikomunikasikan lebih aman.
2. Dokumen transaksi yang diamankan dalam bentuk enkripsi dalam XML dan tanda tangan digital dalam XMLdikirim dan dibandingkan kapasitas data*(byte)* hasil dari proses enkripsi tanpa kompresi dan dilakukan kompresi dalam bentuk karakter *string* dengan *hexa* pada setiap entri point parameter store procedur masing-masing .
3. Hasil analisa menunjukan bahwa kapasitas data*(byte)* hasil enkripsi dalam XML dan tanda tangan digital dalam XML terjadi perubahan yang signifikan saat data di transfer tanpa kompresi yaitu lebih lambat waktunya(detik) dibandingkan dengan enkripsi dalam XML dan tanda tangan digital dalam XML dikompresi dengan waktu proses yang lebih cepat.
4. Sistem keamanan yang menggunakan fasilitas XML *web service* selain dapat berjalan dalam jaringan global (internet), juga dapat berjalan dalam jaringan lokal (LAN/intranet).
5. Untuk mengintegrasikan beberapa sistem yang berbeda kedalam sebuah jaringan lokal yang besar maupun internet, web service merupakan pilihan teknologi yang tepat , karena tidak perlu merubah sistem yang telah ada secara total.
6. Aplikasi yang menggunakan XML sebagai basis pertukaran informasi antar aplikasi yang berbeda baik *platform* aplikasi maupun database, tidak dapat diketahui proses yang terjadi di dalamnya oleh *end-user*. *End-user* hanya menerima hasil output dalam bentuk HTML.

PUSTAKA

1. Bush, George W. 2005. "Executive Order 13388 of October 25, 2005–*Further Strengthening the Sharing of Terrorism Information to Protect Americans*", Federal Register Vol. 70 No. 207 Retrieved August 2009 from http://www.archives.gov/federal-register/executive-orders/2005.html.
2. Douglas Rodrigues. 2011. *Analysis of Security and Performance Aspects in Service-Oriented Architectures.* Institute of Mathematics and Computer Science University of São Paulo São Carlos - SP, Brazil
3. Douglas Robert Stinson. 2002. *Cryptography:Theory and Practice*. Second Edition.Chapman & Hall/CRC.
4. D,Eastlake; J,Reagle; and D,Solo. 2002 . *XML-Signature Syntax and Processing, W3C Recommendation, http://www.w3.org/TR/xmldsig-core*
5. Gu Yue-sheng, Ye Meng-tao, Gan Yong. 2010. *Web Services Security Based on XML Signature and XML Encryption*. Journal of Network s , Vol. 5, No. 9, September 2010. Henan Institute of Science and Technology, Xinxiang, China
6. George Kambourakis. 2008. *Enabling the provision of secure web based m-health services utilizing XML based security models.* Security Comm. Networks. 1:375–388 Published online 2 September 2008 in Wiley Inter Science, Greece.
7. *http://www.w3.org/Encryption/2002/02-xenc-interop.html*
8. Internet Engineering Task Force (IETF).*http://www.ietf.org*
9. Ilhami Gorgun. 2004. *Deploying and Invoking Secure Web Service Over JXTA Framework*. The Graduate School of Natural And Applied Sciences Of Middle East Technical University.
10. Jeffrey Scott Williams Sr. 2009. Document *Based Message Centric Security Using XML Authentication and Encryption For Coalition and Interagency*. Naval PostGraduate School Monterey.
11. Jogiyanto.2004. *Pengenalan Komputer*. Yogyakarta: C.V.ANDI OFFSET.
12. Kasmir, 2003. Manajemen Perbankan. Jakarta : PT. Raja Grafindo Persada
13. L,Whitten.2004. Metode Desaian and Analisis Sistem. McGraw Hill Education.Edition 6.
14. Matthew MacDonald. 2002. *Beginning ASP.NET 3.5 in C# 2008.* From Novice to Professional netbooks.wordpress.com Second Edition *Start your journey into ASP.NET with a renowned author* Codered @ Updatesofts.com
15. Paraskevas Stefas. 2005. *Decentralized Authorization for Web Services*. A dissertation submitted to the University of Dublin, in partial fulfilment of the requirements for the degree of Master of Science in Computer Science.
16. Rinaldi Munir. 2006. Kriptography. Informatika Bandung.
17. Sherif Sakr. 2009. *XML Compression Techniques: A Survey and Camparison*. Journal

of Computer and System Sciences. National ICT Australia (NICTA),Sydney Australia.

18. Sreenivasulu Nagireddy. 2008. *Pattern Recognition Approach To Block Cipher Identification*. Department of Computer Science and Engineering Indian Institute of Technology Madras.
19. Siddiqui,Bilal.2003. *Exploring XML Encryption*. http://www. ibm.com/ developerworks /xml /library /x-encrypt. Tanggal akses : 21 Maret.
20. Tapan,P; D,James. 2003. *XML Data Standards for Microfinance Information Exchange***.** Grameen Foundation Technology Center Seattle, WA USA tparikh@gfusa.org
21. T,Bray; J, Paoli; S,McQueen; and E, Maler. 2002. *Extensible Markup Language (XML) 1.0 (Second Edition).* W3C Recommendation. *http://www.w3.org/TR/2000/REC-xml*
22. T,Imamura; A,Clark; H,Maruyama. 2003. *A Stream-based Implementation of XML Encryption*. IBM Research, Tokyo Research Laboratory 1623-14, Shimotsuruma, Yamato, Kanagawa 242-8502, Japan +81-46-215-4479
23. William Stalings. 2003. *Cryptography and Network Security*. Edition 3.
24. Walsh,Norman.1998. A Technical Introduction to XML http: //www. xml.com /pub /a /98/ 10/guide0.html. Tanggal akses : 30 Maret .2009
25. World Wide Web Consortium (W3C). *http://www.w3.org*
26. Zein Radwan. 2008. *Policy-driven and Content-based Web Services Security Gateway*. Department of Electrical and Computer Engineering, American University of Beirut ,1107 2020, Lebanon (Email: chehab@aub.edu.lb)