PENGAMANAN DATA XML PADA PROSES EDI

(*ELEKTRONIK DATA INTERCHANGE*)

Skripsi

Oleh

Adrianus Barus

22033387

Program Studi Teknik Informatika Fakultas Teknik

Universitas Kristen Duta Wacana

2010 / 2011

PENGAMANAN DATA XML PADA PROSES EDI

(*ELEKTRONIK DATA INTERCHANGE*)

Skripsi

Diajaukan kepada Fakultas Teknik Program Teknik Informatika

Universitas Kristen Duta Wacana

Sebagai salah satu syarat dalam memperoleh gelar

Sarjana Komputer

Disusun Oleh

Adrianus Barus

22033387

Program Studi Teknik Informatika Fakultas Teknik

Universitas Kristen Duta Wacana

2010 / 2011

PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa tugas akhir dengan judul:

PENGAMANAN DATA XML PADA PROSES EDI

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan sarjana Program Studi teknik Informatika, Fakultas Teknik Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika di kemudian hari didapati bahwa skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia menerima sanksi berupa pencabutan gelar kesarjanaan saya.

Yogyakarta, 03Desember2010

(Adrianus Barus)

22033387

HALAMAN PERSETUJUAN

Judul : Pengamanan Data XML Pada Proses EDI

Nama : Adrianus Barus

NIM : 22033387

Mata Kuliah : Tugas Akhir

Senester : Gasal Tahun Akademik : 2010/2011

Telah diperiksa dan disetujui

Di Yogyakarta

Pada Tanggal..... 3 Desember 2010

Dosen Pembimbing I

(..Willy. S. R. SKom, M.Cs)

DosenPembimbing II

(ANDRONICUS RIYAD)

HALAMAN PENGESAHAN

SKRIPSI

PENGAMANAN DATA XML PADA PROSES EDI

Oleh : Adrianus Barus / 22033387

Dipertahankan didepan dewan Penguji Tugas Akhir / Skripsi

Program Studi Teknik Informatika Fakultas Teknik

Universitas Kristen Duta Wacana – Yogyakarta

Dan dinyatakan diterima untuk memenuhi salah satu

Syarat memperoleh gelar

Sarjana Komputer

Pada Tanggal

22 - 12 - 2010

Yogyakarta, 22 - 12 - 2010

Mengesahkan,

Dewan Penguji :

1. Willy Sudiarto R, S.Kom., M.Cs.
2. Andronicus Riyono, M.T.
3. Erick Kurniawan, S.Kom, M.Kom.

Dekan

Ir. Henry Feriadi, M.Sc., Ph. D

Ketua Program Studi

Restyandito, S.Kom,. MSIS.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena atas segala berkat dan rahmat yang Dia berikan sehingga penulis dapat menyelesaikan tugas akhir ini dengan baik.

Tugas akhir merupakan studi akhir yang diwajibkan kepada mahasiswa Jurusan Teknik Informatika Fakultas Teknik Universitas Kristen Duta Wacana Yogyakarta setelah menyelesaikan beberapa tahapan seperti teori, praktikum, KKN, dan Kerja Praktek serta salah satu syarat untuk mendapatkan gelar Sarjana Komputer.

Penulis menyadari bahwa dalam pembuatan tugas akhir ini tidak terlepas dari bantuan berbagai pihak yang telah menyumbangkan pikiran, tenaga, dan bimbingan kepada penulis baik secara langsung maupun tidak langsung. Oleh sebab itu, pada kesempatan ini penulis mengucapkan terima kasih kepada :

Tuhan Yang Maha Esa.

Bapak Restyandito, S.Kom., M.T. selaku Ketua Program Studi Teknik Informatika Fakultas Teknik Universitas Kristen Duta Wacana .

Bapak Willy Hendarto, S.Kom., M.T. selaku Dosen Pembimbing I yang telah meluangkan waktu dan tenaga untuk memberikan bimbingan yang sangat berarti kepada penulis.

Bapak Andronikus Riyono S.T., M.Kom. selaku Dosen Pembimbing II yang telah meluangkan waktu dan tenaga untuk memberikan bimbingan dan masukan yang sangat berarti kepada penulis.

Seluruh dosen Program Studi Teknik Informatika Fakultas Teknik Universitas Kristen Duta Wacana Yogyakarta.

Buat Bapak dan Mamak, terima kasih buat didikan, kasih sayang, dan doanya, serta kepercayaan yang sudah diberikan kepadaku. Dan buat adekku Nova Linda Barus terimakasih atas kepercayaan yang diberikan kepadaku.

Buat Abangku Musti Barus dan Kakak iparku Lenti, serta adekku Murniati Barus terima kasih buat doanya dan dukungan yang diberikan kepadaku. Dan buat keponakanku Alicia Mayria Chabrina Barus dan Yoel Egidio Hagata Sitanggang terimakasih atas kehadiran kalian dalam keluarga dan tetap menjadi anak yang baik.

Sahabat dan teman seperjuangan yang memiliki andil yang sangat besar dalam proses penyelesaian tugas akhir ini : Paul, Papianta, Sanusi, Rabbi, Nasdi, Ivo, Arifin, Christina Oktaviani, Agustina, Almira, dan K'Inna , terima kasih atas semangat, bantuan dan perhatian kalian.

Sahabat seperjuangan dikampus : semua angkatan 2003 Teknik Informatika UKDW yang dulu sering nongkrong di depan Biro 2.

Temen-temen yang sering nongkrong dikontrakan janti gang vetran 2 no 36 : Fransius (csQ), Junus(impalQ), Astri(koncoQ), Doanta, Qnoy, dan adek-adek : Roy, Amos, Morris, Alek, Rindy, Eva, Eke, Keke, Priska Natalia Sembiring, Tere Sinulingga,Vander, Putri, Ita, Emma, Iyan, Andri, Elfin, dan Dia yang ku cintai Terima kasih atas dukungan dan perhatiannya selama ini.

KBMK Merga Silima terima kasih buat dukungannya. .

Keluarga besar Gereja Batak Karo Protestan Yogyakarta, penulis mengucapkan banyak terima kasih atas bimbingan dan dukungan serta sudah diberikan kepercayaan kepada saya untuk bisa melaksanakan Kerja Praktek dilokasi gereja.

Semua pihak yang tidak dapat penulis sebutkan satu persatu, yang telah membantu dalam penyelesaian tugas akhir ini.

Demikian laporan tugas akhir ini dibuat dengan usaha terbaik dari penulis. Tetapi jika masih ada kekurangan karena keterbatasan waktu dan pengetahuan yang dimiliki penulis, maka kritik dan saran yang bersifat membangun sangat diharapkan demi kesempurnaan laporan ini. Semoga apa yang ada di laporan ini dapat bermanfaat bagi semua pihak yang membutuhkan.

Yogyakarta, 23 Agustus 2010

Adrianus Barus

ABSTRAKSI

Keamanan data merupakan merupakan salah satu aspek terpenting dalam sebuah system informasi. Keamanan menjaga dan melindungi data dari pengakses yang tidak sah.Keamanan data dimaksud memastikan kerahasiaan data sekaligus melindungi data pribadi dan data perusahaan untuk keperluan bisnis. Model bisnis sekarang ini banyak yang sudah berbasis internet terutama penggunaan website membuat pertukaran sangat rawan akan adanya perubahan dan kehilangan data.

Data dalam bentuk XML saat ini telah digunakan secara luas dalam dunia teknologi informasi. Peranan XML dalam transaksi bisnis pun cukup besar. Hal ini dikarenakan fitur yang diberikan XML, antara lain data yang tersimpan secara terstruktur, semantik yang dapat didefinisikan sesuai kebutuhan, berbasis teks, dan *web-ready*. Seiring dengan perkembangan *web-services* sebagai *middleware* untuk integrasi aplikasi antar perusahaan, XML digunakan pula sebagai format data yang dipertukarkan melalui *web-services.* Semua data yang dikirm aman dari orang yang tidak bertanggung jawab dengan menyembunyikan data memakai algoritma kriptografi.

Dalam penulis tugas akhir ini, penulis focus kepada implementasi keamanan dokumen XML melalui web-service. Banyak solusi yang ditawarkan untuk metode pengamana data, yaitu XML *Digital Signature* dan XML *Encryption.* XML *Digital Signature* memastikan data sampai ketujuan aman tanpa termodifikasi dan XML *Encryption* menyembunyikan atau membungkus data yang sudah diberi XML *Digital Signature* tanda bisa terlihat oleh orang lain. Ada beberapa algoritma kriptografi yang digunakan dalam pengimplementasian XML *Digital Signature* dan XML *Encryption*, yaitu RSA dan Rijndael.

RSA merupakan salah satu teknik cryptography yang menerapkan metode Asymmetric key, sehingga dibutuhkan 2 macam kunci yaitu kunci private dan kunci public. Masing-masing pengguna akan selalu memiliki sepasang kunci tersebut. RSA digunakan untuk melakukan tanda tangan dan mengenkripsi session key yang dihasilkan dari perhitungan menggunakan algoritma Rijndael.

Algoritma Rijndael mengasilkan session key, dan session key yang dihasilkan digunakan untuk mengenkripsi dokumen XML.

Kata Kunci : XML, XML *Digital Signature*, XML *Encryption*, RSA, dan Rijndael.

DAFTAR ISI

\

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi keamanan mempunyai peran yang sangat penting dalam dunia bisnis khususnya dalam pertukaran data yang dimana aspek keamanan tersebut berguna untuk memberikan perlindungan kerahasiaan serta menjamin informasi digunakan secara benar. Model bisnis sekarang ini banyak yang sudah berbasis internet terutama penggunaan website membuat pertukaran sangat rawan akan adanya perubahan dan kehilangan data. Selain memperhatikan aspek kerahasiaan data, perlu diperhatikan pula aspek keamanan lain seperti otentikasi, integritas data, dan anti-penyangkalan *(non-repudiation).*

Data dalam bentuk XML saat ini telah digunakan secara luas dalam dunia teknologi informasi. Peranan XML dalam transaksi bisnis pun cukup besar. Hal ini dikarenakan fitur yang diberikan XML, antara lain data yang tersimpan secara terstruktur, semantik yang dapat didefinisikan sesuai kebutuhan, berbasis teks, dan *web-ready*. Seiring dengan perkembangan *web-services* sebagai *middleware* untuk integrasi aplikasi antar perusahaan, XML digunakan pula sebagai format data yang dipertukarkan melalui *web-services.*

Tidak dapat dipungkiri bahwa XML sangat fleksibel dalam pertukaran data khususnya dalam pertukaran data elektornik melalui internet.Namun dari semua itu terdapat beberapa kelemahan yang ditemukan pada XML, antara lain:

1. XML memisahkan antara bagian data(*content)* dengan bagaimana data ditampilkan secara terstruktur, secara terstruktur, hal ini menyebabkan data dapat dimanipulasi oleh siapapun yang membacanya.
2. XML berbasis teks, mudah dibaca oleh manusia (human-readable), maka dokumen XML mudah untuk di-debug dan dilewatkan melalui firewall.

Untuk mengatasi kelemahan-kelemahan pada XML, beragam standar telah direkomendasikan oleh W3C, diantaranya adalah XML Encryption yang menjaga kerahasiaan data dan XML Digital Signature untuk otentikasi.Namun aplikasi yang memanfaatkan standar tersebut untuk pertukaran data belum banyak ditemui.

1.2 Rumusan Masalah

Masalah yang timbul dapat dirumuskan sebagai berikut:

1. Bagaimana memastikan otentikasi dari data elektronik yang dipertukarkan?
2. Bagaimana mengimplementasikan keamanan data XML pada proses pertukaran data elektronik dengan menggunakan XML *Digital Signature XML Encryption*?

1.3 Batasan Masalah

Adapun yang menjadi batasan dari pembangunan Perangkat Lunak ini yaitu :

1. Studi kasus yang digunakan antara Toko Buku dan Penerbit serta data yang digunakan hanya simulasi, bukan data yang sebenarnya dan proses pertukaran menggunakan satu Toko Buku dan satu Penerbit.
2. Fokus utama penulisan ini adalah penerapan keamanan data XML menggunakan XML *Digital Signature* dan XML *Encryption* pada proses pertukaran data elektronik (EDI).
3. Pengiriman data menggunakan protokol HTTP.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai penulis dari pembuatan tugas akhir ini adalah untuk mengimplementasikan XML *Digital Signature* dan XML *Encryption* sebagai bagian dalam keamanan data XML pada proses pertukaran data elektronik sehingga data yang dipertukarkan dapat terjamin keamanan dan keasliannya.

1.5 Metodologi Penelitian

1. Metode Observasi atau Pengamatan

   Metode ini dilakukan dengan melakukan pengamatan dan pencatatan secara langsung terhadap objek yang berkaitan dengan maksud mendapatkan data yang sesuai dengan kondisi sebenarnya.

2. Metode Studi Pustaka

   Data-data yang berkaitan dengan Keamanan Pertukaran Data secara Elektronik dan XML didapat dan dikumpulkan dengan cara membaca dan memahami buku-buku referensi.

3. Pembangunan Perangkat Lunak
   a. Analisis

      Mengumpulkan data-data yang dibutuhkan oleh perangkat lunak, kemudian melakukan analisa kebutuhan yang diperlukan oleh sistem.

   b. Design

      Merancang perangkat lunak berdasarkan analisis yang telah dilakukan.

   c. Implementasi

      Membangun perangkat lunak secara lengkap dengan mengimplementasikan *design* ke dalam *Tools* yang telah dipilih.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini berisi penjelasan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan, dan sistematika Penulisan Laporan.

BAB II LANDASAN TEORI

Bab dua ini berisi dasar teori, pendapat, prinsip-prinsip dan sumber-sumber lain yang dapat dipertanggungjawabkan secara ilmiah dan dapat dipergunakan sebagai pembanding atau acuan di didalam pembahasan masalah.

BAB III PERANCANGAN SISTEM

Bab ini berisi uraian mengenai *use case*,desain antarmuka, serta algoritma-algoritma yang digunakan oleh sistem.

BAB IV IMPLEMENTASI DAN ANALISIS SISTEM

Bab ini berisi pengimplementasian sistem yang dituangkan dalam penjelasan masing-masing form yang telah dibuat dan analisis hasil sistem.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang dapat diambil dari penyusunan Tugas Akhir, serta saran - saran

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari penelitian yang telah dilakukan dapat ditarik kesimpulan sebagai berikut:

XML *Digital Signature* dan XML *Encryption* bisa digunakan sebagai bagian dalam keamanan data XML pada proses pertukaran data elektronik. Data elektronik yang dipertukarkan dalam bentuk XML, dan ukuran data bisa lebih besar, karena data yang dipertukarkan adalah data transaksi antara Toko Buku dan Penerbit. Algoritma yang digunakan adalah *asymmertric key* menggunakan RSA. Kunci RSA 1024 bit, besar data yang bisa diproses untuk dienkripsi adalah 128 *byte*s. Data yang lebih dari 128 *bytes* tidak bisa diproses untuk dienkripsi. Jadi, untuk bisa mengenkripsi data dalam jumlah besar dengan menggabungkan algoritma RSA dengan kunci *symmetric*. Kunci *symmetric* digunakan untuk mengenkripsi data dengan menggunakan *session key* dari algoritma *symmetric* yang menghasilkan *session key*. RSA digunakan untuk mengenkripsi *session key*.

5.2 Saran

Saran yang dapat diberikan untuk penelitian selanjutnya adalah :

1. Menambah daftar toko, atau menggunakan lebih dari satu toko.
2. Dapat ditambahkan *form create new key* untuk menghasilkan *session key* yang berbeda pada tiap toko.
3. Data buku yang digunakan data yang sebenarnya, bukan simulasi.

DAFTAR PUSTAKA

Aiyus, Dony. 2006. Kriptografi Keamanan Data Dan Komunikasi. Graha Ilmu : Yogyakarta.

Dournaee, Blake. 2002. *XML Security.* McGraw-Hill Osborne

Nugroho, Adi. 2009. Algoritma dan Struktur Data dengan C#. ANDI : Yogyakarta

Rusiawan, Dwi . 2003. *Tinjauan Aspek Keamanan Sistem Web Service*. Institut Teknologi Bandung

Seda, Jan. *Dot Net in Sample* . http://www.scribd.com/doc/196716/Dot-Net-in-Samples# .

Short, Scott. 2003. *Building XML Web Service For The Microsoft.Net Platform.* PT Elex Media Komputindo : Jakarta

Sibarani,Elisa, Inte Bu'ulolo, Rosni Lumbantoruan. 2006. *XML Security.* Institut Teknologi Bandung

Susanto, Budi. 2007. *XML Security*. http://budsus.file.wordpress.com/2007/08

Wicaksana Nugraha, Simeon. 2003. *Tinjauan Keamanan Dokumen XML (eXtensible Markup Language).* Institut Teknologi Bandung