

METODE PENGAMANAN DATA DALAM WEBSERVICE MENGGUNAKAN METODE XML SIGNATURE DAN XML ENCRYPTION

TESIS



Oleh :

CHaidir Kurnia Thoullah Soedaryono

1111600977

PRORAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2014

METODE PENGAMANAN DATA DALAM WEBSERVICE MENGGUNAKAN METODE XML SIGNATURE DAN XML ENCRYPTION

TESIS

**Diajukan Untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (MKOM)**



Oleh:

**CHAIDIR KURNIA THOULLAH SOEDARYONO
1111600977**

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA TEKNOLOGI INFORMASI
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2014**



PROGRAM STUDI : MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : CHAIDIR KURNIA THOULLAH S
Nomor Induk Mahasiswa : 1111600977
Konsentrasi : Teknologi Sistem Informasi
Jenjang Studi : Strata Dua (S2) Komputer
Judul : **METODE PENGAMANAN DATA DALAM
WEBSERVICE MENGGUNAKAN METODE XML
SIGNATURE DAN XML ENCRPTION**

Jakarta, 15 Agustus 2014

Tim Penguji

Ketua,

Dr.Moedjiono, M.Sc

Moderator,

Dr.Ir.Nazori Az, M.T

Penguji I

Ir.Wendi Usino, MM.,M.Sc.,Ph.D

Tanda Tangan

[Handwritten signatures of the examiners]

Ketua Program Studi

[Handwritten signature of Dr. Ir. Nazori Az]
Dr.Ir.Nazori Az, M.T



PROGRAM STUDI : MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama Mahasiswa : CHAIDIR KURNIA THOULLAH S

Nomor Induk Mahasiswa : 1111600977

Konsentrasi : Sistem Informasi

Jenjang Studi/Program : PASCASARJANA

Menyatakan bahwa Thesis yang berjudul:

**METODE PENGAMANAN DATA DALAM WEBSERVICE MENGGUNAKAN
METODE XML SIGNATURE DAN XML ENCRPTION**

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. Saya ijin untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila dikemudian hari pernyataan ini tidak benar.

Jakarta, 15 Agustus 2014



(Chaidir Kurnia Thoullah Soedaryono)

ABSTRAK

Saat ini perkembangan teknologi di dunia sangat berkembang pesat dengan bermunculannya teknologi informasi yang semakin moderen dan canggih , semakin banyak pula permintaan dan kebutuhan komunikasi data dengan cepat dan aman melalui web , salah satu metode yang sedang berkembang saat ini adalah *webservice* , *webservice* menjadi trend dalam teknologi web karena teknologi ini dapat melakukan komunikasi *multiplatform* , perantara antar *multiplatform* ini menggunakan *eXtensible Markup Language* (XML) dalam berkomunikasi, karena XML mudah untuk dibaca oleh macam-macam bahasa pemograman seperti ASP.Net, PHP dll, dikarnakan komunikasi data tersebut sangat mudah dibaca , maka dengan itu semakin mudah juga XML ini dimanipulasi seperti serangan yang dilakukan berupa pengintaian, perusakan maupun pencurian data, salah satu penyelesaian terbaik adalah dengan membuat data tersebut tidak dapat dibaca orang lain dan dilakukan validasi chek apakah data tersebut sama pada saat dikirim dan diterima, Pengamanan tersebut dapat dilakukan dengan menggunakan salah satu teknik kriptografi yaitu enkripsi, dan untuk menjaga ke-absahan data yang dikirim sama dengan data yang diterima kita akan menambahkan XML Signature untuk menambah keamanan data tersebut , XML Signature digunakan untuk menyediakan kepastian terhadap integritas data (*Content of message*) dalam dokumen serta membuat data dan menguji tandatangan elektronik tersebut (*digital signature*), dengan Prototipe aplikasi ini akan dikembangkan menggunakan UML (*Unified Modeling Language*) dan metode *Prototyping*, *Protoyping* ini akan diuji dengan *Fungsional test* dan *User Accepted*, dan penelitian ini diharapkan akan menjaga kerahasiaan data dalam *webservice* khususnya untuk menjaga kevalidan data dan kerahasiaan data pada saat pengiriman data.

Kata Kunci : *Prototyping*, *Web Service* , *XML Signature* , *Kriptografi*, *XML Encription*

ABSTRAK

Currently, the development of technology in the world is growing rapidly with the emergence of information technology will increasingly modern and sophisticated, the more the demand and need for data communications quickly and securely over the web, webservice becomes a trend in web technology because this technology can perform multi-platform communication, multiplatform intermediaries between these uses eXtensible Markup language (XML) to communicate, because XML is easy to read by a variety of programming languages such as ASP.Net, PHP etc., dikarnakan data communication is very easy to read, then the easier it is manipulated as XML also conducted a reconnaissance attack, destruction or theft of data, one of the best solution is to make these data can not be read by other and performed validation check whether the data is the same at the time sent and received, the security can be done by using one of the techniques of cryptography is encryption, and to keep to the invalidity of data that is sent together with the data received we will add an XML Signature to add security these data, XML Signature is used to provide assurance of the integrity of data (Content of message) in the document as well as making the data and test the electronic signature (digital signature), the prototype of this application will be developed using UML (Unified Modeling Language) and methods Prototyping, Prototyping this will be tested with a test Functional and User Accepted, and this study is expected to maintain the confidentiality of data in a particular webservice to validan to maintain confidentiality of data and to the data during data transmission.

Keyword : Prototyping, Web Service , XML Signature , Kriptografi, XML Encryption

KATA PENGANTAR

Puji syukur alhamdulillahirobbil'alamin penulis panjatkan ke hadirat Allah SWT yang telah melimpahkan rahmat, taufik dan hidayahnya, shalawat serta salam senantiasa selalu penulis panjatkan kepada Nabi besar Muhammad SAW beserta keluarga dan para sahabat, sehingga penulis dapat menyelesaikan penulisan Tesis dengan judul "METODE PENGAMANAN DATA DALAM WEBSERVICE MENGGUNAKAN METODE XML SIGNATURE DAN XML ENCRYPTION".

Tesis ini disusun untuk memenuhi sebagian persyaratan mencapai derajat Magister pada Program Studi Ilmu Komputer, Program Pascasarjana, Universitas Budi Luhur Jakarta.

Pada Kesempatan ini penulis menyampaikan rasa hormat dan terima kasih yang sebesar-besarnya atas bantuan, bimbingan dan dukungan dari berbagai pihak yang ikut serta dalam penyusunan tesis ini kepada :

1. Kedua Orang tua, keluarga, calon istriku Afrila(anna) dan teman-teman tercinta yang telah memberikan kasih sayang dan perhatian yang tulus serta do'a yang selalu menyertai.
2. Dr. Moedjiono, MSc., selaku Direktur Pascasarjana Universitas Budi Luhur
3. Dr.Ir.Nazori AZ,MT, selaku Pembimbing dan Kepala Program Pascasarjana Teknologi Informasi / Kepala Program Studi Magister Komputer Universitas Budi Luhur, yang telah melayani serta memberikan fasilitas bagi kelancaran studi.
4. Seluruh Dosen Magister Komputer Universitas Budi Luhur yang telah berkenan mentransfer dan membuka cakrawala ilmu pengetahuan kepada penyusun.
5. Semua pihak yang tidak dapat penulis sebut satu persatu yang telah membantu selama penulis studi hingga penyelesaian Tesis ini.

Penulis senantiasa menyadari bahwa penulisan tesis ini masih jauh dari sempurna, untuk itu segala saran dan kritik yang sifatnya membangun sangat penulis harapkan untuk tujuan yang lebih baik kedepan, Silahkan hubungi penulis di email chaidirkurnia@gmail.com semoga tesis ini dapat bermanfaat bagi kita semua serta dapat menambah khasanah kepustakaan ilmiah bagi Universitas Budi Luhur pada khususnya dan seluruh masyarakat pada umumnya.Amin.

Jakarta, 6 Juni 2014

Penulis

(Chaidir Kurnia Thoullah .S)

DAFTAR ISI

Lembar Judul Luar	i
Lembar Judul Dalam	ii
Lembar Pernyataan.....	iii
Lembar Pengesahan	iv
Abstrak	v
Kata Pengantar	vi
Lembar Persembahan	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	ix
DAFTAR TABEL	x
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Masalah Penelitian.....	2
1.2.1. Identifikasi Masalah.....	2
1.2.2. Batasan Masalah.....	3
1.2.3. Rumusan Masalah.....	3
1.3. Tujuan dan Manfaat Penelitian	4
1.3.1. Tujuan Penelitian.....	4
1.3.2. Manfaat Penelitian... ..	4
1.4. Tata Urut Penulisan	4
1.4.1. Sistematika Penulisan... ..	4
1.5. Daftar Pengertian	
1.5.1. XML (eXtensible Markup Language).....	5

1.5.2. XML Signature....	5
1.5.3. Web Service....	6
1.5.4. Kriptografi....	6
1.5.5. SOAP....	6
BAB II LANDASAN TEORI DAN KERANGKA KONSEP	7
2.1. Tinjauan Pustaka/Teori.....	7
2.1.1. Definisi Service Oriented Architecture....	7
2.1.2. Teknologi Web Service.....	10
2.1.3. Arsitektur Web Service.....	13
2.1.3.1. Simple Object Access Protokol (SOAP).....	14
2.1.3.2. Web Service Discription Language (WSDL)....	15
2.1.3.3. Universal Description , Discovery and Integration (UDDI).....	16
2.1.4. Management Pengujian Perangkat Lunak.....	17
2.1.4.1. Tujuan Pengujian Perangkat Lunak....	18
2.1.4.2. Proses – Proses Pengujiaan Perangkat Lunak.....	19
2.1.4.3. Jenis – Jenis Pengujian Perangkat Lunak.....	20
2.1.5. Jaringan Komputer.....	21
2.1.5.1. LAN (Local Area Network).....	22
2.1.5.2. MAN (Metropolitan Area Network).....	23
2.1.5.3. WAN (Wide Area Network).....	23
2.1.6. XML Signature.....	25
2.1.7. Enkripsi dalam XML.....	28
2.1.8. Client Server.....	28
2.2. Tinjauan Studi.....	29
2.2.1. Literature Review.....	30
2.3. Tinjauan Obyek Penelitian	37
2.3.1. Tinjauan PT.Rabobank Internasional Indonesia....	37
2.3.2. Produk dan Layanan.....	37
2.4. Kerangka Pemikiran....	38
2.5. Hipotesis.....	39

BAB III METODOLOGI DAN RANCANGAN PENELITIAN	40
3.1. Metode Penelitian	40
3.1.1. Studi Pendahuluan... ..	41
3.1.1.1. Tinjauan Lapangan... ..	41
3.2. Metode Pengumpulan Data... ..	42
3.3. Metode Perancangan... ..	43
3.4. Instrumentasi... ..	44
3.5. Alur Proses Webservice... ..	46
3.6. Teknik Analisa Data... ..	46
3.7. Langkah – Langkah Penelitian.. ..	48
3.8. Pengujian Teknis... ..	50
3.8.1. Tahapan – Tahapan Pengujian... ..	51
3.9. Jadwal Penelitian... ..	52
BAB IV PEMBAHASAN HASIL PENELITIAN.....	53
4.1. Analisis dan Interpretasi.....	53
4.1.1. Analisis Pendahuluan... ..	53
4.1.2. Pengujian dan Relibilitas Instrumen... ..	58
4.1.2.1. Data Hasil Penelitian... ..	58
4.2. Analisi, Perancangan Prototipr model dan Pengujian Prototipe.....	59
4.2.1. Analisis Kebutuhan... ..	59
4.2.2. Perancangan Prototipe XML Signature dan XML Encription.	62
4.2.2.1. Sequence Diagram.....	62
4.2.2.2. Prototipe Model.	64
4.2.3. Pengujian Model Prototipe.	66
4.2.3.1. Functional Testing.	66

4.2.3.2. Acceptance Testing.....	68
4.3. Pengujian Hipotesis.	74
4.3.3. FGD (Focus Group Discusion).....	74
4.4. Implikasi Hasil Peneliian Terhadap Implementasi.....	76
4.4.3. Aspek Sistem.	76
4.4.4. Aspek Perangkat Keras.....	76
4.4.5. Aspek Perangkat Lunak.....	77
4.4.6. Infrastruktur Network.	77
4.4.7. Sumber Daya Manusia.....	77
4.5. Rencana Implementasi Sistem.....	77
BAB V PENUTUP.....	81
DAFTAR PUSTAKA.....	**
LAMPIRAN-LAMPIRAN.....	***

DAFTAR GAMBAR

Gambar

Hal

II-1 Enkapsulasi Fungsi logic proses bisnis oleh service.....	8
II-2 Model Konseptual SOA.....	9
II-3 Lingkungan Kerja Web Service.....	12
II-4 Cycle Proses dalam Web Service.....	13
II-5 Arsitektur Web Service.....	14
II-6 Jaringan LAN.....	22
II-7 Jaringan MAN.....	23
II-8 Jaringan WAN.....	24
II-9 Digital Signature Flowchart.....	25
II-10 Enveloped Digital Signature Skema.....	26
II-11 Enveloping Digital Signature Skema.....	27
II-12 Detached Digital Signature Skema.....	28
II-13 Konsep dan Kerangka Kerja dan Penelitian.....	39
III-1 Alur Proses Web Service.....	46
IV-1 Permohonan Kuesioner.....	54
IV-2 Petunjuk Pengisian Kuesioner.....	54
IV-3 Identitas Kuesioner.....	55
IV-4 Pertanyaan Kuesioner.....	55
IV-5 Pertanyaan Kuesioner.....	55
IV-6 Pertanyaan Kuesioner.....	56

IV-7 Sequence Proses XML Signature & XML Encryption.	63
IV-8 Menu Register Prototype Internet Banking.	64
IV-9 Menu Login Prototype Internet Banking.	65
IV-10 Menu Check Saldo Prototype Internet Banking.	66



DAFTAR TABEL

Table

Hal

II-1 Faktor –Faktor Kualitas Perangkat Lunak	19
II-2 Tinjauan Studi.	35
III-1 Pembobotan Skala Linkert.	45
III-2 Langkah-Langkah Penelitian.	48
III-3 Jadwal Penelitian.	52
IV-1 Data Responden Penelitian.	57
IV-2 Data Rekapitulasi hasil Kuesioner.	58
IV-3 List Kategori.	59
IV- 4 Skenario Pengujian Functional Testing.	67
IV-5 Skenario Pengujian Acceptance Testing.	68
IV-6 Profile Peserta FGD.	74
IV-7 Hasil Kuesioner Penerapan Manfaat.	75
IV-8 Rancangan Implementasi.	78

DAFTAR PUSTAKA

- [Ahmad 2012] Ahmad Gunawan H, “Kajian Model Implementasi Mikrotik Router-OS untuk mengelola kecepatan akses internet bagi setiap civitas akademika : Studi Kasus STMIK Pasim Sukabumi”, Tesis, Jakarta : Universitas Budi Luhur.2012
- [Ari 2011] Ari Muzakir,”Rancang Bangun keamanan webservice dengan metode WS-Security” Jakarta
- [Arisandi 2011] Arisandi, Fachry, Prof. Dr. Ir. Harso Supangkat M. Eng, “Implementasi Service Oriented Architecture (SOA) pada pengembangan Sistem Pembelajaran Mobile”. Konferensi Teknologi Informasi dan Komunikasi Untuk Indonesia e-Indonesia Initiative (eII2011), CGET, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Email : if17027@student.if.itb.ac.id. 2011
- [Bernard 2010] Bernard Renaldy Suteja, S.Kom, M.Kom,” Implementasi XML Signature pada dokumen XML untuk Transkrip Nilai Online”,Univeritas Kristen Maranatha, bernard.rs@eng.maranatha.edu, bernardjogja@gmail.com
- [Estlake 2003] Eastlake D. E. XML Security. <http://www.motorola.com>. 22 January 2003.10:20:52
- [Ilham 2004] Ilhami Gorgun, 2004. Deploying dan Invoking Secure Web Service Over JXTA Framework. The Graduate School of Natural dan Applied Sciences Of Middle East Technical University.
- [Josuttis 2007] Josuttis, Nicloai M., “SOA In Practice”, O’Reilly, pp 210.2007
- [Meridith 2003] Meredith, L.G., Bjorg, S, “Contract and types, Communication of ACM”, 46(10) ,pp.41-47.2003
- [Papazoglou 2003] Papazoglou,M.P Georgakopoulos, D., “Service Oriented Computing : Introduction,Communication of the ACM”, 46(10), pp. 25-28. Prentice Hall. 2003