

Peningkatan *Security* Melalui Kombinasi *Digital Signature* dan *One Time Password* Pada *Service Oriented Architecture* Menggunakan TOGAF

TESIS



Oleh:

Galih Nabihi

1211600364

PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2016

Peningkatan *Security* Melalui Kombinasi *Digital Signature* dan *One Time Password* Pada *Service Oriented Architecture* Menggunakan TOGAF

TESIS

Diajukan untuk memenuhi salah satu persyaratan
Memperoleh gelar Magister Ilmu Komputer (M.Kom)



Oleh:

Galih Nabihi
1211600364

PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2016

Peningkatan *Security* Melalui Kombinasi *Digital Signature* dan *One Time Password* Pada *Service Oriented Architecture* Menggunakan TOGAF

TESIS

Diajukan untuk memenuhi salah satu persyaratan
Memperoleh gelar Magister Ilmu Komputer (M.Kom)



Oleh:

Galih Nabihi

1211600364

Disetujui untuk diajukan dalam sidang tesis

Jakarta, 11 Agustus 2016

Menyetujui

Ir. Teddy Mantoro, M Sc., Phd

Pembimbing



**PROGRAM STUDI: MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : Galih Nabihi
Nomor Induk Mahasiswa : 1211600364
Program Studi : Magister Ilmu Komputer
Program : Rekayasa Komputasi Terapan

Menyatakan bahwa tesis yang berjudul:

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

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

Jakarta, 11 Agustus 2016



(Galih Nabihi)



**PROGRAM STUDI: MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

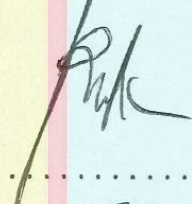
LEMBAR PENGESAHAN TESIS

Nama : Galih Nabihi
Nomor Induk Mahasiswa : 1211600364
Konsentrasi : Rekayasa Komputasi Terapan
Topik/Judul Tesis : **Peningkatan *Security* Melalui Kombinasi *Digital Signature* dan *One Time Password* Pada *Service Oriented Architecture* Menggunakan TOGAF**

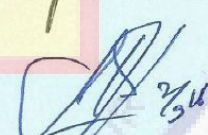
Jakarta, 11 Agustus 2016
Tim Penguji:

Tanda Tangan:

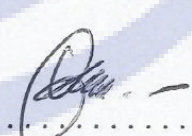
Ketua,
Dr. Ir. Nazori, Az., MT.

 3/8 2016

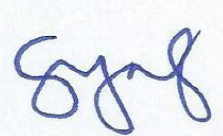
Anggota,
Achmad Solichin, S.kom., M.T.I

 2/8 16

Pembimbing Utama,
Ir. Tedy Mantoro, M Sc., Phd



Ketua Program Studi,



Dr. M. Syafrullah, M Sc.

ABSTRAK

Pada akhir tahun 1990 ditemukan Internet. Dalam perkembangannya Internet memberikan dampak besar dalam perkembangan bisnis transaksi elektronik. Pada awal tahun 2005 transaksi pengiriman uang elektronik (*remittance*) mulai masuk pada pasar bisnis *online* di Indonesia. Sayangnya meskipun sudah menggunakan keamanan pada sistem pengiriman uang elektronik, penggunaannya masih merasa tidak aman terhadap ancaman kejahatan. Terbukti pada tahun yang sama banyak kasus kejahatan yang marak terjadi pada transaksi elektronik, termasuk bisnis *remittance*. Solusi dari permasalahan tersebut adalah dengan melakukan analisis keamanan pada sistem yang berjalan. Analisis tersebut menghasilkan kebutuhan – kebutuhan yang dijadikan standar untuk membuat sistem yang aman. Kebutuhan yang dihasilkan pada penelitian ini menghasilkan pengembangan metode baru, yang diimplementasikan dalam bentuk *web-service*. Penelitian ini menggunakan metode TOGAF, memfokuskan pembahasannya pada *Security Assessment* dengan implementasi pengembangan studi kombinasi otentikasi *digital signature* dengan OTP (*one time password*). Kontribusi penelitian ini adalah mengolah kebutuhan – kebutuhan yang diperlukan agar sebuah sistem dapat dikatakan aman kemudian membuat pengembangan metode otentikasi studi kombinasi *digital signature* dan *one time password* (OTP). Pengembangan metode tersebut diuji untuk mengetahui apakah metode tersebut layak untuk diimplementasikan dengan membandingnya dengan beberapa metode lainnya.

Kata Kunci: Security Assesment, Digital Signature, One Time Password, Remittance, TOGAF model.

ABSTRACT

At the end of 1990 Internet was found. In the expansion of them, Internet had a major impact in the development of electronic business transactions. In early 2005 remittance transactions started to get in on the business in market of Indonesia. Unfortunately, despite using the security system of electronic money transfer, user still feel unsecure against the threat of crime. It is proved, in the same year a lot of crime happed in electronic transactions, including the remittance business. The solution to these problems is to perform a security analysis on a running system. The analysis resulted in the requirement that used as the standard to make the system safe. The result of this study is developed a new method, which implemented in the form of web-service. This study uses TOGAF, focusing the discussion on the implementation of Security Assessment study the development of a combination of digital signature authentication with OTP (one time password). Contribution of this study is to analyze the system and get the security requirement in order for a system can be said to be safe. This study develops an alternative method that combined digital signature with one time password (OTP). That method is tested to determine whether the method is feasible to be implemented with and compare it with other method.

Keywords: Security Assesment, Digital Signature, One Time Password, Remittance, TOGAF model.

KATA PENGANTAR

Segala puji dan puja hanya untuk Allah SWT, shalawat serta salam semoga tetap tercurahkan kepada nabi besar, Nabi Muhammad SAW. Salam sejahtera semoga sampai kepada para keluarganya, sahabatnya, dan kita umatnya yang senantiasa mengikuti ajaran yang telah beliau sampaikan kepada kita. Amin.

Penulis sangat bersyukur, karena atas rahmat, pertolongan dan bimbingan Allah SWT penulis dapat menyelesaikan penelitian ini dengan judul “**Peningkatan Security melalui kombinasi *Digital Signature* dan *One Time Password* pada *Service Oriented Architecture* menggunakan TOGAF**”.

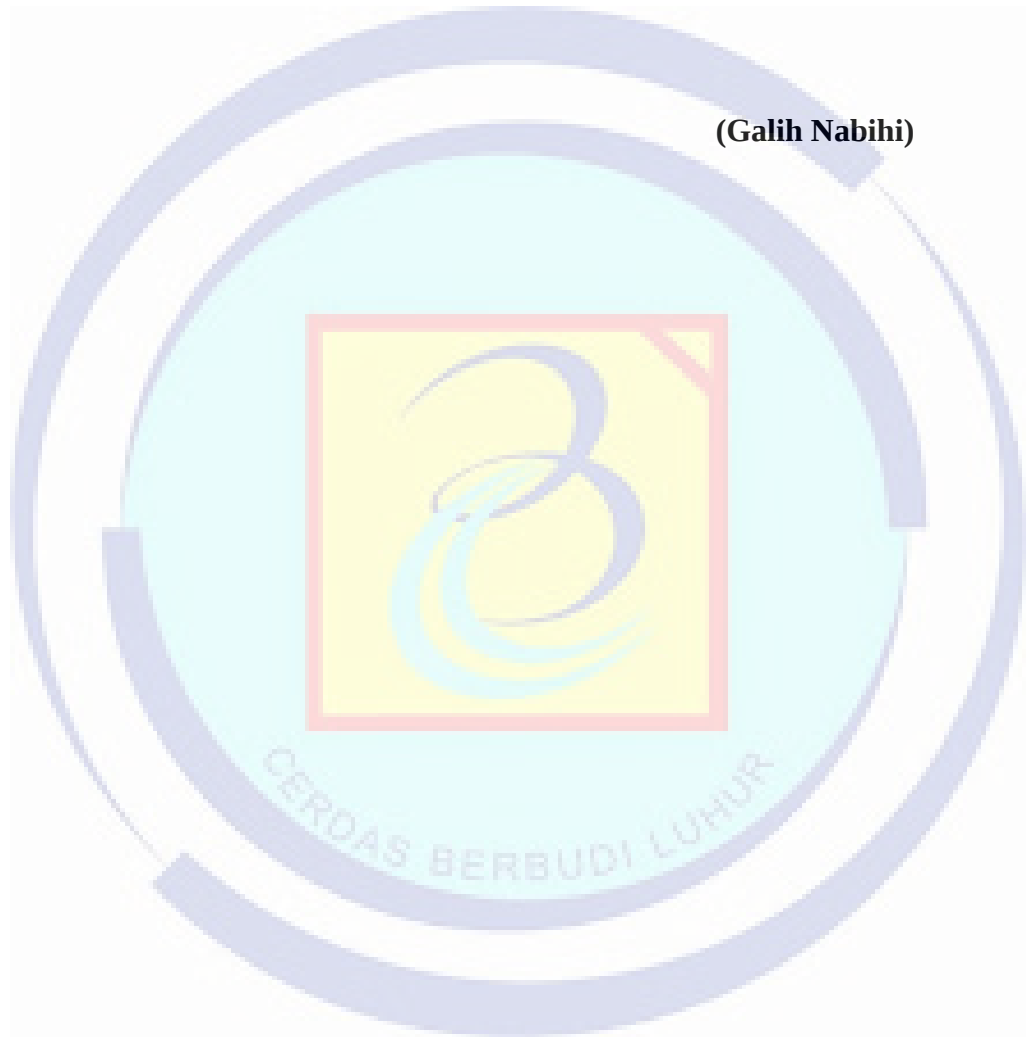
Pada kesempatan ini penulis menyampaikan rasa hormat dan ucapan terima kasih yang sangat mendalam kepada semua pihak, terutama atas doa, dukungan dan motivasi yang begitu besar, terimakasih yang sebesar-besarnya kepada:

1. Bapak Dr. Sugiharto, M Sc., M.Fin selaku Direktur Program Pascasarjana Universitas Budi Luhur.
2. Bapak Dr. M.Syafrullah, M Sc. selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur.
3. Bapak Ir. Teddy Mantoro, M sc., Phd. sebagai pembimbing tesis yang dengan kesabaran dan ketulusan hati terus memberikan bimbingan, dorongan dan motivasi untuk menyelesaikan penelitian ini.
4. Bapak dan Ibu Dosen beserta seluruh staf Program Studi Magister Ilmu Komputer Universitas Budi Luhur yang tidak dapat penulis cantumkan satu persatu atas dukungan dan motivasinya.
5. Seluruh Teman – teman XK yang telah banyak membantu kelancaran dari penelitian ini
6. Istriku Ayu kharisma dan anaku alfath untuk bantuanya sehingga saya dapat menyelesaikan penelitian ini

Dengan kerendahan hati, penulis menyadari bahwa penelitian ini yang akan disusun nanti merupakan sebuah karya yang belum sempurna mengingat keterbatasan pengetahuan dan wawasan penulis.

Penulis

(Galih Nabihi)



DAFTAR ISI

LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN TESIS	ii
ABSTRAK	iii
ABSTRACT	iv
KATA PENGANTAR	v
DAFTAR GAMBAR	x
DAFTAR TABLE	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Masalah Penelitian	2
1.2.1 Identifikasi Permasalahan	2
1.2.2 Pembatasan 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 Sistematika Penulisan	5
1.5 Glosari	6
BAB II LANDASAN TEORI DAN KERANGKA KONSEP	8
2.1 Tinjauan Pustaka	8
2.1.1 <i>Security and Information Assurance</i>	8
2.1.2 <i>Risk Management</i>	10
2.1.3 <i>Software Oriented Architecture</i>	14
2.1.4 <i>Konsep Service Oriented</i>	15
2.1.5 <i>Komponen-komponen SOA</i>	17
2.1.6 <i>Penerapan SOA pada Web-service</i>	18

2.1.7	Komponen <i>Web-service</i>	19
2.1.8	<i>Web Security Pattern</i>	19
2.1.9	TOGAF (<i>The Open Group Architecture Framework</i>) ..	22
2.1.10	Hubungan SOA, TOGAF dan Teori Otentikasi	29
2.1.11	SKKNI Tentang <i>Enterprise Architecture Design</i>	30
2.2	Tinjauan Studi.....	34
2.3	Tinjauan Obyek Penelitian	37
2.4	Kerangka Pemikiran	38
2.5	Hipotesis	40
BAB III	METODOLOGI DAN RANCANGAN PENELITIAN	41
3.1	Metode Penelitian	41
3.2	Sampling / Metode Pemilihan Data	44
3.2.1	Bentuk Penelitian.....	44
3.2.2	Jenis Data.....	45
3.2.3	Sumber Data	45
3.3	Metode Pengumpulan Data	45
3.3.1	Metode Observasi	45
3.3.2	Studi Pustaka	46
3.4	Instumentasi.....	46
3.5	Metode Pendekatan dan Pengembangan Sistem	46
3.5.1	Metode Pendekatan Sistem.....	46
3.5.2	Metode Pengembangan Sistem.....	47
3.5.3	Pengujian Sistem	48
3.6	Langkah – Langkah Penelitian	49
3.7	Jadwal Penelitian	50
BAB IV	ANALISIS DAN INTERPRETASI DATA	52
4.1	Analisis Masalah.....	52
4.1.1	Fase Pendahuluan (<i>Preliminary Parse</i>).....	52
4.1.2	Pemahaman Arsitektur (<i>Architecture Vision</i>).....	54
4.1.3	Arsitektur Bisnis (<i>Bussiness Architecture</i>).....	55

4.1.4	Sistem Informasi Arsitektur (<i>Information System Architecture</i>).....	61
4.1.5	<i>Technology Architecture</i>	69
4.1.6	<i>Oportunities and Solution</i>	75
4.1.7	<i>Migration Planning</i>	75
4.1.8	<i>Implementation Governance</i>	76
4.1.9	<i>Architecture Change Management</i>	86
BAB V	KESIMPULAN DAN SARAN	87
5.1	Kesimpulan.....	87
5.2	Saran	87
	DAFTAR PUSTAKA	89
	LAMPIRAN TESIS	92

DAFTAR GAMBAR

Gambar II- 1: Mapping hubungan <i>treat</i> , <i>risk</i> dan <i>countermeasure</i> (Cloe & Krutz, 2015)	12
Gambar II- 2: Enkapsulasi Business Proses dengan <i>Service</i>	16
Gambar II- 3: Pola Penerapan SOA (Erl, 2005)	18
Gambar II- 4: <i>Web Security Pattern</i>	20
Gambar II- 5: <i>Direct Authentication</i> (Hogg et al., 2005).....	20
Gambar II- 6: <i>Kerberos Authentication</i> (Hogg et al., 2005)	21
Gambar II- 7: <i>Digital Signature Authentication</i> (Hogg et al., 2005)	21
Gambar II- 8: <i>Token Authentication</i> (Hogg et al., 2005)	22
Gambar II- 9: <i>Fase Architecture Devopment Method</i> (Harrison, 2009).	26
Gambar II- 10: Kerangka Pemikiran.....	39
Gambar III- 1: TOGAF <i>Security ADM</i> (Harrison, 2009).....	41
Gambar III- 2: <i>Prototyping Paradigm</i> (Munawar, 2005)	47
Gambar III- 3: Langkah Penelitian	49
Gambar IV- 1: Rantai Nilai Perusahaan <i>Remittance</i> (Brown, 2009).....	53
Gambar IV- 2: Arsitektur Digram <i>Remittance Transfer System</i>	55
Gambar IV- 3: <i>Usecase Diagram Remittance Transfer System</i>	57
Gambar IV- 4: <i>Activity Diagram</i> Proses Pendaftaran Rekening (<i>Cash to Account</i>)	58
Gambar IV- 5: <i>Activity Diagram</i> Proses Transfer	58
Gambar IV- 6: <i>Attack Tree Remittance Transfer System from Outside</i>	61
Gambar IV- 7: <i>Attack Tree Remittance Transfer System (from Internal)</i>	62
Gambar IV- 8: <i>Miss-Usecase Remittance Transfer System (from outside)</i> (MU01).....	62
Gambar IV- 9: <i>Miss-Usecase Remittance Transfer System (from internal)</i> (MU02).....	63
Gambar IV-10: Studi kombinasi <i>Digital Dignature</i> dengan <i>OTP Authentication</i>	69
Gambar IV-11: Simpel <i>Mapping XML ke Original Message</i>	69
Gambar IV-12: Hasil Randomisasi <i>Original Message</i> pada proses validasi	70

Gambar IV-13: Proses mapping <i>Digital Signature</i> sebelumnya.....	71
Gambar IV-14: Proses Validasi <i>Signature</i>	71
Gambar IV-15: <i>Mapping OTP</i> dengan PIN number	72
Gambar IV-16: Proses Validasi dan Penghasilan <i>random index</i>	72
Gambar IV-17: Proses <i>Mapping Digital Signature</i> usulan	73
Gambar IV-18: Proses Dekripsi metode usulan <i>Digital Signature</i> dan OTP	73
Gambar IV-19: Contoh <i>Maaping tag XML</i> menjadi index array	74
Gambar IV-20: Contoh <i>Response Random Token</i> yang telah dienkripsi dgn OTP	74
Gambar IV-21: Contoh <i>Request Service</i> dengan <i>random token</i> yang sudah dijadikan parameter.	75
Gambar IV-22: Grafik Persebaran Hasil <i>Response Time Server Apache</i>	79
Gambar IV-23: Grafik Persebaran Hasil <i>Response Time Server IIS</i>	80
Gambar IV-24: Grafik Kenaikan Presentasi pada server <i>Apache (Open Souce evniroment)</i>	81
Gambar IV-25: Grafik Kenaikan Presentase Pada server <i>IIS (.NET)</i>	82
Gambar IV-26: Halaman <i>Service remittance</i>	83
Gambar IV-27: <i>Back-end Request</i> Otentikasi OTP	83
Gambar IV-28: <i>Back-end Response</i> Otentikasi OTP	84
Gambar IV-29: <i>Back-end Request Create Account</i>	84
Gambar IV-30: <i>Back-end Response Create Account</i>	84
Gambar IV-31: Tampilan <i>Front-end remittance</i> pendaftaran pelanggan	85
Gambar IV-32: Tampilan <i>Front-end remittance</i> pendaftaran pelanggan sukses.	85
Gambar IV-33: Tampilan <i>Front-end remittance</i> otentikasi OTP <i>failed</i>	85
Gambar IV-34: Tampilan <i>Front-end remittance</i> otentikasi OTP <i>Success</i>	86
Gambar IV-35: Tampilan <i>Front-end remittance transfer</i>	86

DAFTAR TABLE

Table II - 1 : Pemetaan SKKNI Bidang <i>Enterprise Architecture Design</i>	32
Table II - 2 : Table Tinjauan Studi Penelitian.....	34
Table III - 1 : Jadwal Penelitian Penelitian.....	50
Table IV - 1 : Mengidentifikasi Aset.....	59
Table IV - 2 : <i>Type Security Issue</i>	59
Table IV - 3 : <i>Likelihood</i>	59
Table IV - 4 : Dampak Acaman	59
Table IV - 5 : <i>Table Risk Analysis</i>	60
Table IV - 6 : <i>Qsualitative Risk Analysis Matrix</i>	61
Table IV - 7 : <i>List Requirement Analysis</i>	63
Table IV - 8 : Table Prioritas Kebutuhan Keamanan.....	64
Table IV - 9 : Analisis kondisi keamanan saat ini	65
Table IV- 10: Set Kategori Rekomendasi Kebutuhan Kemanan	66
Table IV -11: <i>List Table Experiments</i>	77

DAFTAR LAMPIRAN

LAMPIRAN 1 :	93
LAMPIRAN 2 :	94
LAMPIRAN 3 :	95
LAMPIRAN 4 :	96
LAMPIRAN 5 :	97
LAMPIRAN 6 :	98
LAMPIRAN 7 :	99
LAMPIRAN 8 :	104
LAMPIRAN 9 :	109
LAMPIRAN 10:	110
LAMPIRAN 11:	111
LAMPIRAN 12:	112
LAMPIRAN 13:	114

DAFTAR PUSTAKA

- Alexandre, R., & Fernandes, D. A. (2012). *Modelling Access Control Mechanisms in Enterprise Architecture*. Technical of Lisboa.
- Bieberstein, N., Bose, S., Walker, L., & A., L. (2005). Impact of service-oriented architecture on enterprise systems, organizational structures. *IBM Systems Journal*, 44(4), 691–708.
- Brown, G. W. (2009). Value Delivery Chains. *BPTrends*, (April), 1–12. Retrieved from <http://www.bptrends.com/publicationfiles/FOUR 04-009-ART-Value Chains-Brown.pdf>
- Bruegge, B., & Dutoit, A. H. (2006). Sysiphus: Enabling informal collaboration in global software development. In *Proceedings - 2006 IEEE International Conference on Global Software Engineering, ICGSE 2006* (pp. 139–148). <http://doi.org/10.1109/ICGSE.2006.261227>
- Buc, D., Corbier, J., & Deronzier Eric, Jouas Jean-Philippe, Molines Gerard, R. J.-L. (2009). Risk Management - Concepts and Methods. *Journal Information Security French*, 1(1), 1–40.
- Chappell, D., & Jewell, T. (2002). *Java Web Services*. Retrieved from <http://books.google.com/books?id=wiXOyXdvHO8C\npapers://6b27418f-98b1-4a55-9d4a-81387a1148b8/Paper/p12>
- Chen, S., Zic, J., Tang, K., & Levy, D. (2007). Performance Evaluation and Modeling of Web Services Security. *Web Services, 2007. ICWS 2007. IEEE International Conference on*, (JANUARY), 431–438. <http://doi.org/10.1109/ICWS.2007.139>
- Cloe, E., & Krutz, R. (2015). *Network Security Bible*. CEUR Workshop Proceedings (1st ed., Vol. 1542). Indiana: Wiley Publishing. <http://doi.org/10.1017/CBO9781107415324.004>
- Colombi, M. D. (2005). Modeling Security Architectures for the Enterprise. *11Th International Command and Control Research and Technology Symposium*, 1(1), 1–20. Retrieved from http://www.dodccrp.org/events/11th_ICCRTS/html/papers/020.pdf
- Emadi, S., & Hanza, R. H. (2013). Critical Factors in the Effective of Service-Oriented Architecture. *Advances in Computer Science: An International Journal*, 2(3), 26–30.
- Erl, T. (2005). *Service-Oriented Architecture: Concepts, Technology, and Design*. City.
- Ertaul, L., Movasseghi, A., & Kumar, S. (2015). Enterprise Security Planning with TOGAF-9. *Journal Math and Computer Science CSU*, 1(1), 2–7.
- Fikri, M., Santoso, A. F., Hanafi, R., & Fikri, M. (2014). Analisis dan Perancangan