UNIVERSITAS INDONESIA

POTENSI KOMPETITIF DAN ANALISA STRATEGI PENYEDIAAN LAYANAN KEAMANAN CERTIFICATE AUTHORITY DI ERA KONVERGENSI STUDI KASUS : LEMBAGA SANDI NEGARA

TESIS

Diajukan sebagai Salah Satu Syarat untuk Memperoleh Gelar Magister Tehnik

RINI WISNU WARDHANI
0906495671

FAKULTAS TEKNIK
PROGRAM STUDI TEHNIK ELEKTRO
KEKHUSUSAN MANAJEMEN TELEKOMUNIKASI
UNIVERSITAS INDONESIA
DESEMBER 2010

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Rini Wisnu Wardhani

NPM : 0906495671

Tanda Tangan : _____

Tanggal : Jakarta, Desember 2010

HALAMAN PENGESAHAN

Tesis ini diajukan oleh :

Nama : Rini Wisnu Wardhani
NPM : 0906495671
Program Studi : Manajemen Telekomunikasi
Judul Tesis :

POTENSI KOMPETITIF DAN ANALISA STRATEGI PENYEDIAAN LAYANAN KEAMANAN CERTIFICATE AUTHORITY DI ERA KONVERGENSI STUDI KASUS : LEMBAGA SANDI NEGARA

Telah berhasil dipertahankan dihadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Tehnik pada Program Studi Teknik Elektro, Kekhususan Manajemen Telekomunikasi, Departemen Teknik Elektro, Fakultas Teknik Universitas Indonesia.

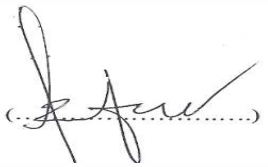
DEWAN PENGUJI

Pembimbing : Prof. Dr. Ir. Dadang Gunawan, M.Eng

Penguji : Ir. Djamhari Sirat M.Sc., Ph.D

Penguji : Dr. Ir. Muhammad Asvial, M.Eng

Penguji : Ir. Arifin Djauhari, MT



Ditetapkan di : Jakarta
Tanggal : 12 November 2010

UCAPAN TERIMAKASIH

Atas segala rahmat yang diberikan, penulis memanjatkan puji syukur kehadirat Tuhan Yang Maha Kuasa, sehingga dapat menyelesaikan penulisan dengan judul: "POTENSI KOMPETITIF DAN ANALISA STRATEGI PENYEDIAAN LAYANAN KEAMANAN CERTIFICATE AUTHORITY DI ERA KONVERGENSI STUDI KASUS : LEMBAGA SANDI NEGARA "

Pada kesempatan ini penulis ingin menyampaikan ungkapan Terima Kasih yang tulus, atas segala bantuan dan dukungannya, terutama kepada:

1. Bapak Prof. Dr. Ir. Dadang Gunawan, M.Eng selaku dosen, wali akademik sekaligus juga sebagai dosen pembimbing tesis yang telah banyak memberikan saran dan arahan selama proses penulisan.
2. Orang Tua dan Keluarga Penulis, yang telah memberikan dukungan sehingga penulis mampu menyelesaikan penulisan ini.
3. Dedy Septono C.P dan Iffah, yang telah memberikan dukungan, cinta dan semangat hingga akhirnya penulisan ini dapat diselesaikan.
4. Endang A.A, Eko Sulist, rekan-rekan Laboratorium STSN dan Tim Litbang Lembaga Sandi Negara yang telah membantu terselesaikannya penulisan ini.
5. Rekan-rekan Mantel 2009, Bapak Agoes, Estina, Gesit, Meivita, Wawan dan Nindi, Tim Depkominfo dan Tim Aviasi atas dukungan selama proses penulisan.
6. Seluruh pihak yang tidak dapat disebutkan satu persatu, yang telah membantu penyelesaian penulisan ini.

Jakarta, Desember 2010

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Rini Wisnu Wardhani

NPM : 0906495671

Program Studi : Manajemen Telekomunikasi

Departemen : Teknik Elektro

Fakultas : Teknik

Jenis karya : Tesis

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul :

POTENSI KOMPETITIF DAN ANALISA STRATEGI
PENYEDIAAN LAYANAN KEAMANAN CERTIFICATE AUTHORITY
DI ERA KONVERGENSI
STUDI KASUS : LEMBAGA SANDI NEGARA

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 28 Desember 2010
Yang menyatakan

(Rini Wisnu Wardhani)

ABSTRAK

Nama : Rini Wisnu Wardhani
Program Studi : Manajemen Telekomunikasi

Judul : POTENSI KOMPETITIF DAN ANALISA STRATEGI PENYEDIAAN LAYANAN KEAMANAN CERTIFICATE AUTHORITY DI ERA KONVERGENSI STUDI KASUS : LEMBAGA SANDI NEGARA

Teknologi telekomunikasi memungkinkan kita untuk selalu terkoneksi dimanapun dan kapanpun. Produk dan jasa dari penyedia layanan infrastruktur telekomunikasi terus memberikan layanan kepada penggunanya untuk dapat melakukan komunikasi lebih mudah, memiliki akses komunikasi cepat dan kapasitas pita yang lebar dengan harga yang terjangkau. Internet yang merupakan media (*platform*) yang melewatkan data menggunakan teknologi berbasis internet protokol (IP), jumlah penggunanya semakin meningkat dan keberadaannya mengubah arah dunia telekomunikasi kearah konvergensi. Konvergensi adalah bersatunya layanan telekomunikasi, teknologi informasi, dan penyiaran.

Dimasa persaingan antar penyedia jasa layanan telekomunikasi saat ini, bisnis telekomunikasi berkembang tidak hanya menjual infrastruktur tetapi juga layanan tambahan (*value added service)*. Salah satunya adalah layanan keamanan CA (*Certificate Authority*) untuk menjamin keamanan dan kebenaran identitas dan data bagi setiap entitas yang melakukan transaksi elektronik.

Lembaga Sandi Negara (Lemsaneg) adalah Lembaga Pemerintahan Non Departemen yang memiliki ruang lingkup pengamanan (informasi) dalam pemerintahan. Dengan besarnya tingkat ancaman keamanan dalam transaksi elektronik, di era konvergensi ini kebutuhan keamanan publik sangat tinggi sehingga terdapat peluang untuk menyediakan layanan keamanan CA untuk memenuhi kebutuhan publik.

Dari hasil analisa potensi kompetitif penyediaan layanan CA di era konvergensi dengan menggunakan model Porter 5 Forces didapatkan hasil potensi kompetitif bernilai Medium. Saat ini posisi Lemsaneg dilihat dari faktor internal eksternal, berada pada Kuadran 1 (pada analisa SWOT) dan Sel 5 (pada matriks IE) yang merupakan arah penerapan strategi tumbuh (*growth)*. Dengan menggunakan Pendekatan Manajemen Strategis, sesuai kondisi industri dan posisi organisasi saat ini didapatkan strategi bagi Lemsaneg adalah melakukan strategi pengembangan dan penetrasi pasar, agar penyediaan layanan CA menjadi layanan yang bernilai strategis bagi organisasi.

Kata Kunci : Internet, Konvergensi, *Certificate Authority, Porter 5 Forces, SWOT, Matrik IE.*

Nama : Rini Wisnu Wardhani
Program Studi : Management Telecommunication

Judul : COMPETITIVE POTENTIAL AND STRATEGIC ANALYSIS TO PROVIDE CERTIFICATE AUTHORITY SERVICE IN CONVERGENCE ERA
CASE STUDY : LEMBAGA SANDI NEGARA

ABSTRACT

Telecommunication technology enable us to be correspondingly connected anywhere and anytime. Products and services of telecommunication provider always provide service to their customers for an easier life, fast communication access and wide bandwidth data at an affordable price. Internet, whose users increase, is passing data using Internet Protocol (IP) Based. It's Presence turns telecommunication world into convergence. Convergence means the composite of telecommunication service, information technology and broadcasting.

During competition among telecommunication provider, the telecommunication businesses expand in sale not only infrastructure but also additional services (Value Added Service). One of those service is Certificate Authority (CA) to ensure the security service in electronic data transaction in convergence.

National Crypto Agency is the government institution which area of work is information pacification in the government area. Along with increase of threat safety in electronic transaction, the need of public safety is getting higher in this convergence era. So that it lent it self to provide CA security service to fulfill public needs.

From the competitive potential analysis result, which uses Porter 5 Force model in the convergence era, the writer obtained Medium Competitive Potential value. At moment, from internal and eksternal factor analysis, Lemsaneg was in first quadrant (in SWOT Analysis) and fifth cell (in IE Matrix), which mean Lemsaneg have to possess growth strategy implementation. With strategic management approach, market development and penetration is the strategy to make CA services as a strategic value of Lemsaneg.

Keyword: Internet, Convergence, Certificate Authority, Porter 5 Forces, SWOT Analysis, IE matrix.

DAFTAR ISI

Halaman Judul ……. i
Halaman Pernyataan Orisinalitas ……ii
Halaman Pengesahan..……...……iii
Kata Pengantar …….……. iv
Halaman Pernyataan Persetujuan Publikasi ……v
Abstrak ……..……..vi
Abstract ……vii
Daftar Isi……..….viii
Daftar Gambar……..…….. xii
Daftar Tabel……..… xiv
Daftar Lampiran …….……. xv
Daftar Singkatan……...…..……xvi

BAB I PENDAHULUAN ……... 1
1.1.Latar Belakang ……. 1
1.2.Identifikasi Masalah …… 8
1.3.Tujuan Kajian …….. 9
1.4.Batasan Masalah ……...….. 9
1.5.Metodologi Penelitian ……...…..10
1.6.Sistematika Penulisan ……...….. 11

BAB II LAYANAN KEAMANAN CERTIFICATE AUTHORITY ….. 12
2. 1. Konvergensi Telekomunikasi …….. 12
2. 2. Keamanan Transaksi Elektronik …….……... 16
2. 3. Layanan CA…….. 21
2. 4. Profil Singkat Organisasi…….. 26

BAB III POTENSI KOMPETITIF LAYANAN CA DI ERA KONVERGENSI ……. 29
3.1. Identifikasi Pemain Dalam Industri ..…… 30
3.2. Identifikasi Faktor Tekanan ……. 33
3.3. Analisa ……. 36
3.3.1. Tekanan Pendatang Baru ……..…… 36
3.3.1.1. Skala Ekonomi ……..…….. 37
3.3.1.2. Diferensiasi Produk ……..…….. 38
3.3.1.3. Identitas Merk Produk ……..…….. 39
3.3.1.4. Biaya Investasi ……..…..… 40
3.3.1.5. Biaya Beralih ke Pemasok ……..……. 41
3.3.1.6. Akses ke Saluran Distribusi ….…….. 42
3.3.1.7. Kebijakan Pemerintah ……..…….. 45
3.3.2. Ancaman Produk Pengganti ……..…… 46
3.3.2.1. Produk Pengganti ……..…….. 46
3.3.2.2. Layanan Produk Pengganti ……..…….. 47
3.3.2.3. Tarif Produk Pengganti ……..…… 48
3.3.2.4. Kualitas Produk Pengganti ……..…… 48
3.3.2.5. Ketersediaan Produk Pengganti ….……. 50
3.3.2.6. Proses Aktifasi ……..…….. 51
3.3.2.7. Biaya Beralih Pemasok ……..……. 51
3.3.2.8. Loyalitas Pelanggan ……..……. 51
3.3.3. Kekuatan Tawar Menawar Pembeli ……..…… 53
3.3.3.1. Pembeli Terpusat ……..…….. 53
3.3.3.2. Kapasitas Pembelian ……..…… 54
3.3.3.3. Differensiasi Produk …….. 56
3.3.3.4. Biaya Beralih ke Pemasok ……..…… 57
3.3.3.5. Orientasi Biaya ……..…… 58
3.3.3.6. Integrasi Balik …… 60
3.3.3.7. Kualitas Produk …….. 61
3.3.3.8. Informasi tentang Produk ……..…….. 65

3.3.4. Kekuatan Tawar Menawar Pemasok …..……. 67
3.3.4.1. Dominasi Pemasok …….…… 67
3.3.4.2. Produk Pengganti …….…….. 69
3.3.4.3. Pasar Pemasok …….…….. 69
3.3.4.4. Kualitas Produk …….. 70
3.3.4.5. Integrasi Maju …….…….. 70
3.3.4.6. Kebijakan Pemerintah …… 70
3.3.5. Persaingan Diantara Perusahaan Eksisting …….. 72
3.3.5.1. Jumlah & Ragam Pesaing …….…. 72
3.3.5.2. Pertumbuhan Industri …….…… 75
3.3.5.3. Differensiasi Produk …….…. 76
3.3.5.4. Penambahan Kapasitas …….……. 77
3.3.5.5. Hambatan Pengunduran Diri ……..… 77
3.4. Potensi Kompetitif Layanan CA di Era Konvergensi ….. 78

BAB IV STRATEGI PENYEDIAAN LAYANAN KEAMANAN CA… 81
4.1. Tahap Input ..……..……. 83
4.1.1. Evaluasi Faktor Internal …….. 87
4.1.1.1. Analisa Faktor Internal …….. 87
4.1.1.2. Skor Bobot Faktor Internal ……. 91
4.1.2. Evaluasi Faktor Eksternal ……..92
4.1.2.1. Analisa Faktor Eksternal…… 93
4.1.2.2. Skor Bobot Faktor Eksternal …….. 96
4.2. Tahap Pencocokan …… 94
4.2.1. Matriks Internal Eksternal ……..... 97
4.2.2. Matriks SWOT……..… 99
4.2.2.1. Kuadran SWOT ……..… 100
4.2.2.2. Analisis SWOT ……..…101
4.3. Tahap Keputusan ……..…..103
4.3.1. Strategi Alternatif Penyediaan Layanan CA ……101
4.3.2. Identifikasi Strategi untuk QSPM …..……. 106
4.3.2.1. Fokus Nilai Terbaik……106

4.3.2.2. Pengembangan Pasar ..……..……..106
4.3.2.3. Integrasi Horizontal ……...107
4.3.3. Perhitungan Matriks QSPM …… 108
4.3.4. Analisa Strategi Penyediaan Layanan CA bagi Lemsaneg……...…111
4.3.4.1. Peningkatan Kompetensi Kompetitif Pelayanan Publik ….……..112
4.3.4.2. Membentuk Identitas & Merk Layanan *Certificate Authority* ……..113
4.3.4.3. Menciptakan *Strategic Partner* …… ….113
4.3.4.4. Penguatan Strategi Marketing …… .. 115

BAB VI KESIMPULAN……...……...…….. 116

DAFTAR REFERENSI

LAMPIRAN

DAFTAR GAMBAR

Gambar 1.1 Tren Telekomunikasi [1] ……1
Gambar 1.2 Infrastruktur Penyedia Jasa Pengiriman Data [2]…… 2
Gambar 1.3 Pengguna Internet di Dunia dan di Asia [1][2][3] ……..…. 3
Gambar 1.4 Grafik Tren Pelanggan dan Pengguna Internet [4][5]……..... 4
Gambar 1.5 Data Sebaran Pelanggan Internet [5]……..…….5
Gambar 2.1 Layanan Industri Telekomunikasi [1]……12
Gambar 2.2 Kebutuhan Konten Elektronik [11] …….. 13
Gambar 2.3 Jaringan Telekomunikasi di Era Konvergensi [1]……. 13
Gambar 2.4 Ekosistem Penyelenggara Telekomunikasi di Era Konvergensi[3] …….. 15
Gambar 2.5 Aplikasi Konten di Era Konvergensi [19] ……17
Gambar 2.6 Pengambilan Informasi dalam Transaksi ……..18
Gambar 2.7 Pengubahan Informasi dalam Transaksi ……...… 18
Gambar 2.8 Tidak ada Pembuktian Pengirim dalam Transaksi ……..…. 19
Gambar 2.9. Pemalsuan Identitas dalam Transaksi ……..……. 19
Gambar 2.10 Dimensi Keamanan Standar ITU [14] …….……. 21
Gambar 2.11 Infrastruktur Kunci Publik [15] …..…….…… 22
Gambar 2.12 Skema Publik Key [16] ……..…….…...… 22
Gambar 2.13 Tanda Tangan Digital untuk Transaksi Elektronik [17] ….…….. 23
Gambar 2.14 Desain Layanan *Certificate Authority* [18] …….……..24
Gambar 2.16 Provider Layanan CA [20] ……...…… 25
Gambar 2.16 Provider Layanan CA Perbankan [21] ……..25
Gambar 2.17 Ruang Lingkup Pengamanan Informasi [23]…….……27
Gambar 3.1 Porter 5 Forces [25] …….……..29
Gambar 3.2 Market Share Layanan CA [28] ……31
Gambar 3.3 Peran di Industri Penyedia Layanan Keamanan CA ……32
Gambar 3.4. Komponen Layanan CA bagi Pendatang Baru [29] ……..….... 49
Gambar 3.5 Standar Layanan Keamanan [31][32] ……..…… 40
Gambar 3.6 Unit Tehnis Persandian [23] …….……..……..….. 42
Gambar 3.6. Lapisan Keamanan [34]……..….. 46
Gambar 3.7. Keamanan dalam Platform IP Network [35] …….…….. 47
Gambar 3.8 Segmentasi Pengguna Layanan CA [36]……..…… 54
Gambar 3.9. Biaya Berlangganan Layanan CA [36] ……..…….. 56
Gambar 3.10. Browser Akses Layanan CA di Sisi Pengguna ……..…….. 57
Gambar 3.11 Tampilan Graphic User Interface Aplikasi CA [37] ……..…….. 58
Gambar 3.12 Pemetaan Kebutuhan Keamanan Infomasi Transaksi Elektronik [39] ……..……. 60
Gambar 3.13 Motif Penggunaan E-commerce [40] ……..……. 62
Gambar 3.14 Manfaat Penerapan E-commerce [40] …….……. 62
Gambar 3.15 Aliran Data Elektronik …….…… 63
Gambar 3.16 Sertifikat Layanan CA [41]…….…….. 64
Gambar 3.17. Data Elektronik dengan Layanan Keamanan …….…….. 64
Gambar 3.18 Isi Sertifikat Layanan Keamanan CA [42] ……..……..65

Gambar 3.19 Komputer sebagai alat komputasi pemecahan Kunci dan Sistem Secure Socket Layer [44] …….. 68
Gambar 3.20 Rancangan Undang-undang Konvergensi ……..71
Gambar 3.21 Perangkat Pendukung Layanan di Era Konvergensi …….72
Gambar 3.22 Layanan CA di Indonesia ……..75
Gambar 3.23 Penurunan Merk CA [56] ……. 76
Gambar 3.24 Porter 5 Force Layanan CA di Era Konvergensi …….. 80
Gambar 4.1 Tahapan dalam Manajemen Strategis [26] …… ……. 83
Gambar 4.2 Bidang Pekerjaan Responden ……..……. 84
Gambar 4.3 Matriks IE Penyediaan Layanan CA…… …… 98
Gambar 4.4 Kuadran SWOT Penyediaan Layanan CA …… ……100
Gambar 4.5 Strategi Penyediaan Layanan CA …… …….. 112
Gambar 4.6 Visualisasi Cakupan Layanan ……..……113
Gambar 4.7 Jaring Komunikasi Sandi……..……114

DAFTAR TABEL

Tabel 2.1 Paradigma Telekomunikasi Masa Depan [7] ……..…14
Tabel 2.2 Aspek Setiap Entitas dalam Ekosistem Telekomunikasi [12] ….. 16
Tabel 3.1 Penyedia Layanan Keamanan CA [28] ……..... 30
Tabel 3.2 Variabel dan Indikator Sumber Tekanan model Porter 5 Forces.. 33
Tabel 3.3 Pasal-pasal Kebijakan Pemerintah dalam layanan CA [33]……. 43
Tabel 3.4. Hasil Penilaian Variabel Tekanan Pendatang Baru …… 45
Tabel 3.5. Perbandingan Kualitas Produk Pengganti ……49
Tabel 3.6. Hasil Penilaian Variabel Ancaman Produk Pengganti ……..52
Tabel 3.7 Biaya Berlangganan Layanan Keamanan CA …….. 55
Tabel 3.8 Harga untuk Pengambilan Informasi [38] …… 59
Tabel 3.9. Hasil Penilaian Variabel Kekuatan Tawar menawar Pembeli….. 66
Tabel 3.10 Waktu yang diperlukan untuk Pemecahan Kunci [43] …… 68
Tabel 3.11. Hasil Penilaian Variabel Kekuatan Tawar menawar Pemasok … 72
Tabel 3.12. Layanan CA pada Jasa Perbankan di Indonesia [45] …….. 74
Tabel 3.13. Hasil Penilaian Variabel Persaingan Diantara Perusahaan Eksisting ……... 78
Tabel 3.14 Hasil Analisa Pemodelan Porter 5 Forces terhadap Penyediaan Layanan Keamanan CA di Era Konvergensi ……... 79
Tabel 4.1. Model Jawaban Kuisioner Penyediaan Layanan CA untuk menetapkan Tingkat Pengaruh (Bobot)…… 84
Tabel 4.2. Model Jawaban Kuisioner Penyediaan Layanan CA untuk menetapkan Tingkat Kepentingan (Rating)…….. 86
Tabel 4.3 Matrik IFE Penyediaan Layanan CA ……..….. 92
Tabel 4.4 Matrik EFE Penyediaan Layanan CA ……..…… 96
Tabel 4.5 Strategi Alternatif Penyediaan Layanan CA Sesuai Matriks IE . 99
Tabel 4.6 Pilihan Strategi Alternatif Penyediaan Layanan CA …….. 105
Tabel 4.7 Alternatif Strategi dalam QSPM ……..…….. 107
Tabel 4.8 Matriks QSPM ……..…. 109

.

DAFTAR LAMPIRAN

Lampiran 1	Daftar Perusahaan CA di Dunia……....	L1 (1-8)
Lampiran 2	Detail Market Share Perusahaan CA ……..	L2 1
Lampiran 3	Contoh *Project Milestone* Pembangunan CA ……..…	L3 (1-2)
Lampiran 4	Peringkat Pengguna Layanan CA……...…..…	L4 (1-6)
Lampiran 5	Hasil Monitoring Traffik ID SIRTI …….……....	L5 (1-2)
Lampiran 6	Layanan & Biaya Layanan CA…….……....	L6 (1-3)
Lampiran 7	Contoh Fitur Layanan CA……...…..…	L7 1
Lampiran 8	Permohonan & Contoh Kuisioner Faktor IE…….	L8 (1-6)
Lampiran 9	Contoh Perhitungan Kuisioner …….	L9 (1-3)
Lampiran10	Hasil Perhitungan Kuisioner Faktor IE…….	L10(1-4)
Lampiran 11	Hasil Perhitungan Nilai AS dan Bobot Matriks QSPM	L11(1-4)

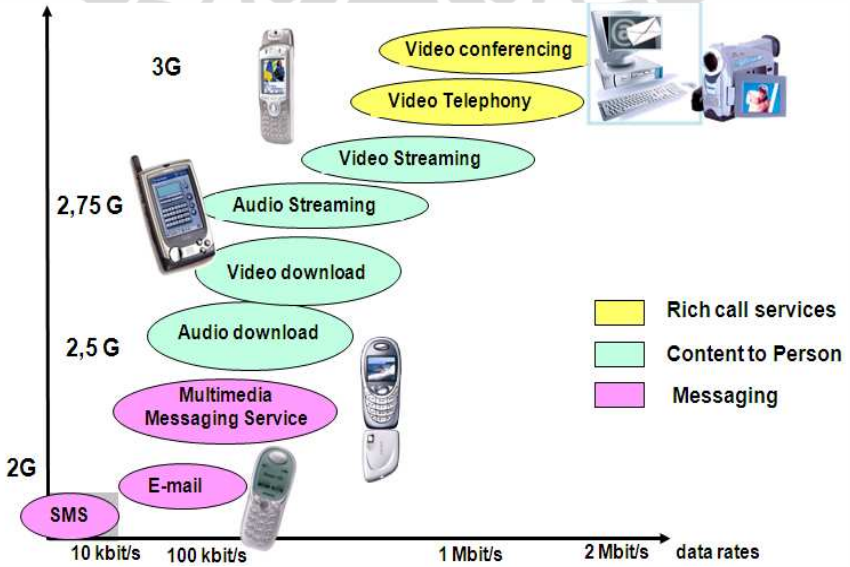
DAFTAR SINGKATAN

AS	*Attractive Score*
CA	*Certificate Authority*
IE	Internal Eksternal
EFE	*External Factor Evaluation*
IFE	*Internal Factor Evaluation*
IP	*Internet Protocol*
ITE	Informasi dan Transaksi Elektronik
Lemsaneg	Lembaga Sandi Negara
RA	*Registration Authority*
SSL	*Secure Socket Layer*
STAS	*Sum Total Attractive Score*
SWOT	*Strength Weakness Opportunity Threat*
TAS	*Total Attractive Score*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TTP	*Trusted Third Party*
UTP	Unit Tehnis Persandian
VPN	*Virtual Private Network*
QSPM	*Quantitative Strategic Planning Matrix*

BAB I
PENDAHULUAN

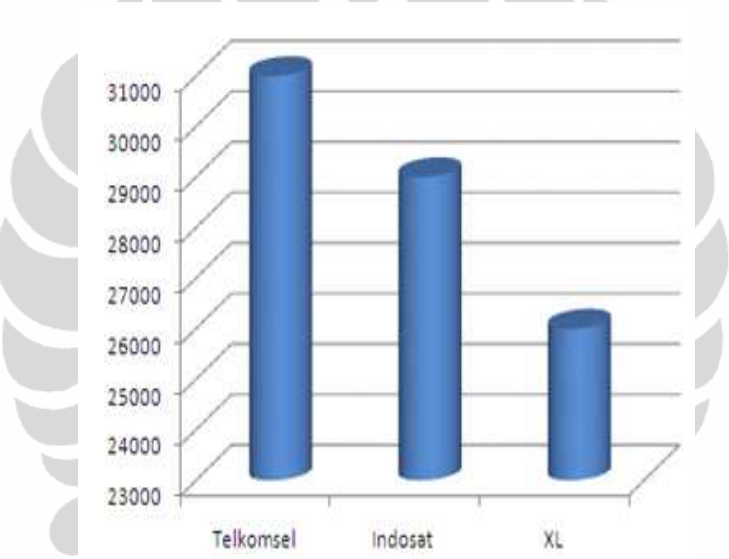
1.1. Latar Belakang

Teknologi telekomunikasi saat ini memungkinkan penggunanya untuk selalu dapat terhubung dimanapun dan kapanpun. Teknologi dan infrastruktur telekomunikasi yang ada saat ini mendukung pengiriman informasi tidak hanya dalam bentuk suara (*voice*) tetapi juga kearah pengiriman data. Produk dan jasa dari penyedia layanan infrastruktur telekomunikasi terus memberikan layanan kepada pelanggannya untuk dapat mencapai kemudahan berkomunikasi, kecepatan akses dan kapasitas lebar pengiriman data dengan harga yang terjangkau. Seperti terlihat pada Gambar 1.1, layanan dari penyedia jasa telekomunikasi berkembang sesuai perkembangan kecepatan transfer data dan aplikasi yang dapat berjalan dalam teknologi telekomunikasi.



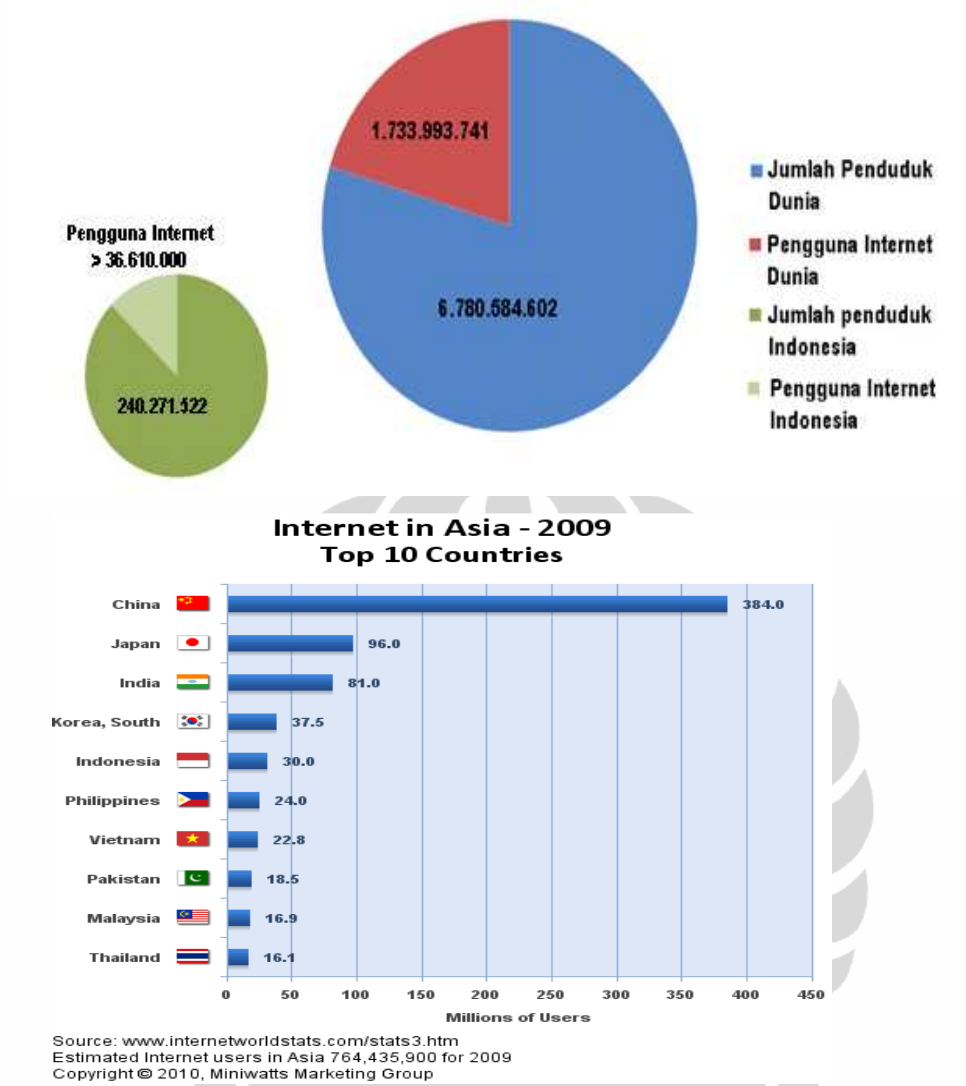
Gambar 1.1 Tren Telekomunikasi [1]

Evolusi pengiriman informasi dalam telekomunikasi terjadi sesuai infrastruktur dan layanan yang dapat diberikan oleh penyedia jasa, mulai dari informasi berupa teks, suara, gambar, data sampai dengan *streaming data*. Data Badan Regulasi Telekomuniksi Indonesia (BRTI) menunjukkan bahwa pada akhir tahun 2009 sebagian besar BTS dari 3 operator selular GSM teratas dalam bisnis telekomunikasi telah siap melayani akses data. Jumlah BTS provider Telkomsel mencapai 31,000 unit, Indosat 29,000 unit dan XL 26,000 unit dengan jangkauan wilayah layanan (*coverage area*) telah mencapai 99% dari 5,300 kecamatan di Indonesia, seperti diperlihatkan pada Gambar 1.2.



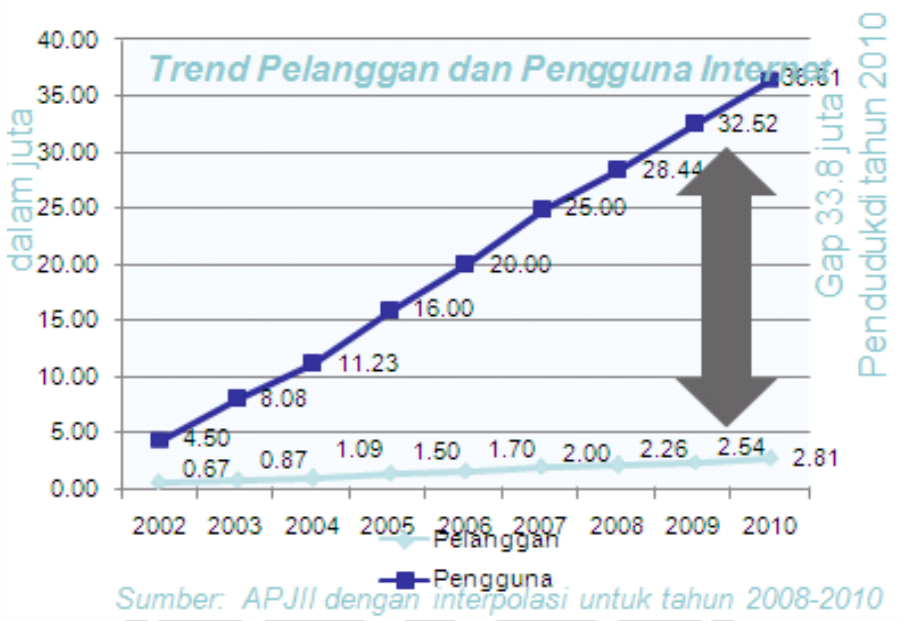
Gambar 1.2 Infrastruktur Penyedia Jasa Pengiriman Data [2]

Didukung berkembangnya infrastruktur layanan data dan harga yang relatif terjangkau saat ini, pertukaran informasi dalam bentuk data menggunakan media internet terus meningkat. Menurut statistik CIA *World Factbook* seperti terlihat pada Gambar 1.3, populasi dunia pada saat ini adalah 6,780,584,602. Sekitar 1,733,993,741 (26%) orang secara teratur telah mengakses Internet. Sedangkan penduduk Indonesia tercatat sejumlah 240,271,522 dengan perkiraan lebih dari 35 juta pengguna Internet [2].



Gambar 1.3 Pengguna Internet di Dunia dan di Asia [1][2][3]

Diperkirakan pada tahun 2010 terdapat 36.61 juta pengguna internet di Indonesia dengan jumlah pelanggan internet sebesar 2.81 juta pelanggan. Terdapat perbedaan sebesar 33.8 juta orang yang merupakan pengguna internet tetapi tidak menjadi pelanggan internet [4].

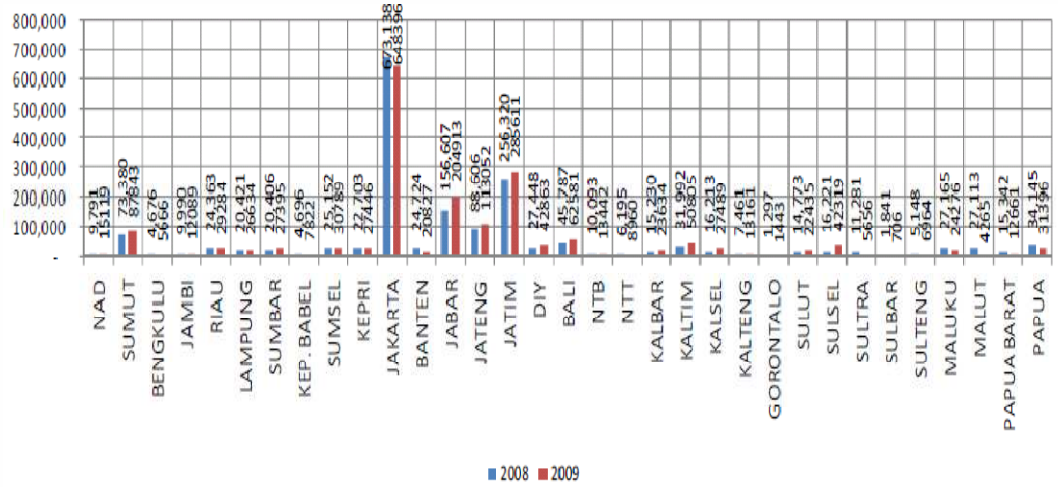


Gambar 1.4 Grafik Tren Pelanggan dan Pengguna Internet [4][5]

Perbedaan (*gap*) antara pelanggan dan pengguna internet pada 2010 diperkirakan mencapai 33.8 juta jiwa, seperti dapat dilihat pada Gambar 1.4. Pada pertengahan (kuartal kedua) tahun 2010, APJII (Assosiasi penyelenggara Jasa Internet) menyatakan bahwa bulan Juni 2010 ada sekitar 45 juta pengguna internet, angka tersebut didapat dari pengakses internet melalui komputer dan ponsel.

Kompilasi data survey pasar menunjukkan : Indonesia memiliki rasio kepemilikan perangkat akses internet tertinggi, kenaikan jumlah perangkat paling banyak dan penurunan tarif layanan (termasuk paket data Internet) paling tajam di kawasan ASEAN (*Association of South East Asian Nations*) walau di tengah isu resesi ekonomi [6][7]. Sektor telekomunikasi mengalami pertumbuhan yang sangat pesat baik dari sisi teknologi, struktur industri, nilai bisnis dan ekonomi, maupun dampaknya bagi kehidupan sosial.

Internet merupakan media (*platform*) yang melewatkan data menggunakan teknologi berbasis *internet protokol* (IP), keberadaannya mengubah arah dunia telekomunikasi kearah konvergensi. Seperti diperlihatkan pada Gambar 1.5, saat ini propinsi-propinsi di Indonesia telah dapat menggunakan atau berlangganan internet [5], dilihat dari jumlah *Network Access Provider*.



Gambar 1.5 Data Sebaran Pelanggan Internet [5]

Konvergensi merupakan integrasi yang progresif dari beberapa platform jaringan yang berbeda untuk menyalurkan layanan yang serupa dan atau layanan-layanan yang berbeda yang disalurkan pada platform jaringan yang sama [7]. Konvergensi adalah bersatunya layanan telekomunikasi, teknologi informasi, dan penyiaran. Dalam era ini tidak hanya antar perangkat telekomunikasi seperti telepon tetapi juga menggabungkan teknologi komputer dan sistem informasi menjadi sebuah kesatuan utuh untuk mendukung interkoneksi sesuai kebutuhan penggunanya.

Pemanfaatan teknologi informasi, media dan komunikasi telah menyebabkan hubungan dunia tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi dan budaya secara signifikan berlangsung cepat.

Transaksi elektronik adalah salah satu aplikasi atau layanan yang menggunakan infrastruktur telekomunikasi dalam era konvergensi. Salah satu aplikasi transaksi elektronik dalam bidang bisnis adalah *e-commerce. E-commerce* dapat didefinisikan sebagai kegiatan bisnis secara elektronik melalui suatu jaringan (biasanya internet) dan komputer [8]. Fasilitas *e-commerce* atau layanan transaksi elektronik dapat diakses menggunakan perangkat telekomunikasi seperti telepon, fax, ATM, telepon selular dan lain-lain. Selain *e-commerce*, bentuk transaksi elektronik yang dapat diaplikasi adalah *e-procurement , e-payment , e-buy, e-trading, e-markets, e-banking, m-commerce, e-government, e-health, e-ticketing* dan lain-lain.

Di era konvergensi, dimana layanan data dapat berjalan dengan baik, transaksi elektronik merupakan alternatif pilihan untuk berhubungan satu sama lain dibandingkan dengan melakukan pertemuan/transaksi dengan metode konvensional. Transaksi elektronik dalam kegiatan perdagangan melalui sistem elektronik telah menjadi bagian dari perniagaan nasional dan internasional. Kenyataan ini menunjukkan bahwa konvergensi dibidang teknologi informasi, media dan informatika (telematika) berkembang terus tanpa dapat dibendung.

Saat ini globalisasi komunikasi yang semakin terpadu membuat dunia menjadi tanpa batas (*borderless*), terutama dengan semakin maraknya pemanfaatan internet (*interconnection networking*). Salah satu aktivitas dunia maya yang paling berkembang dalam kaitan dengan penggunaan internet adalah transaksi elektronik. Aplikasi transaksi elektronik telah dilakukan diseluruh dunia, bahkan menjadi alat kesepakatan atau alat pembayaran utama. Sesuai target Hasil Simposium APEC bahwa *e-commerce & paperless trading* dapat menjadi realita di negara maju APEC pada tahun 2005 dan tahun 2010 di negara berkembang (termasuk Indonesia) [9].

Namun, semakin tingginya penggunaan teknologi informasi di era globalisasi komunikasi ini, semakin meningkat pula resiko yang dihadapi, terutama dari sisi kualitas dan keamanannya. Berbagai ancaman terhadap suatu data atau informasi yang dipetukarkan melalui jaringan internet menuntut suatu solusi keamanan yang salah satunya dengan menggunakan sertifikat elektronik yang dikeluarkan oleh pihak ketiga terpercaya (*Trusted Third Party*) atau lazim disebut CA (Certification Authority).

Kesepakatan internasional melalui organisasi *Asia-Pacific Economic Cooperation (*APEC) dalam hal penggunaan telekomunikasi untuk perekonomian global adalah untuk melakukan langkah [9] :

i. Memulai penyimpanan secara elektronis
ii. Kebijakan menggunakan e-mail untuk berkomunikasi;
iii. Identitas, tanda tangan digital, hak cipta;
iv. Penggunaan teknologi *certificate authority (CA)* sebagai Kepercayaan Pihak Ketiga (*Trusted Third Party).*

CA (*Certificate Authority*) atau TTP (*Trusted Third Party*) adalah sebuah badan hukum yang menyediakan layanan keamanan yang dapat dipercaya oleh para pengguna dalam menjalankan pertukaran informasi secara elektronis [7]. Suatu pertukaran informasi melalui media elektronik yang terkait dengan transaksi bisnis atau perdagangan secara elektronik memerlukan pengamanan melalui infrastruktur kunci publik agar informasi yang dipertukarkan hanya dapat dibaca oleh pihak yang berhak, identitas yang benar atau dijamin otentikasinya, informasi yang tidak berubah dan pihak yang terkait dapat diketahui atau dijamin otentitasnya [10].

Beberapa aspek keamanan yang ditawarkan oleh layanan CA adalah *Confidentiality*, menyangkut kerahasiaan dari data atau informasi, dan perlindungan bagi informasi tersebut dari pihak yang tidak berwenang,. *Authenticity*, menyangkut kemampuan seseorang, organisasi, atau komputer untuk membuktikan identitas dari pemilik yang sesungguhnya dari informasi tersebut. *Integrity*, menyangkut perlindungan data terhadap upaya pemodifikasian oleh pihak-pihak yang tidak bertanggung jawab, baik selama data itu disimpan maupun selama data itu dikirimkan kepada pihak lain. *Non Repudiation*, menyangkut perlindungan terhadap suatu pihak yang terlibat dalam suatu transaksi atau kegiatan komunikasi yang di belakang hari pihak tersebut menyanggah bahwa transaksi atau kegiatan tersebut benar telah terjadi.

Layanan seperti transaksi elektronik dalam era konvergensi memungkinkan setiap entitas dapat saling berhubungan satu dengan yang lainnya tanpa melakukan pertemuan. Layanan keamanan dalam transaksi elektronik diperlukan tidak hanya untuk melindungi data digital yang dikirimkan tetapi juga memberikan validasi setiap entitas yang melakukan transaksi. Potensi kompetitif untuk menyediakan layanan CA menjadi lebih tinggi karena setiap entitas yang melakukan transaksi tidak hanya berada di dalam negeri tetapi juga diluar negeri.

Lembaga Sandi Negara adalah Organisasi Lembaga Pemerintahan Non Departemen yang salah satu misinya adalah Menyusun kebijakan nasional dalam bidang persandian sektor pemerintahan & publik serta menyelenggarakan operasional pengamanan informasi. Lemsaneg bergerak di bidang pengamanan informasi melalui persandian, dalam hal ini adalah mengamankan jalur

komunikasi yang digunakan instansi pemerintah. Saat ini ruang lingkup pengamanan (informasi) yang di tangani masih diwilayah pemerintahan dan VVIP kenegaraan.

Salah satu fungsi penyedia layanan CA adalah sebagai sebuah entitas yang mengeluarkan sertifikat digital (aplikasi penyandian) yang dapat digunakan oleh pihak-pihak lainnya. CA merupakan contoh pihak-pihak yang dapat dipercayai, khususnya dalam transaksi secara *online* di Internet. Saat ini penyedia Layanan CA yang digunakan untuk memenuhi kebutuhan keamanan berbasis IP di Indonesia adalah perusahaan asing yang bersifat komersial. Untuk menggunakan jasanya, sebuah entitas, baik itu perseorangan ataupun organisasi, harus membayar jasa mereka. Hal ini harus ditempuh karena di Indonesia belum memiliki CA yang memiliki jangkauan nasional ataupun global, sedangkan persyaratan perekonomian global adalah adanya penjamin pihak ketiga. Hal ini dapat menimbulkan kerentanan dalam hal keamanan informasi mengingat seluruh data pengguna CA diproses (untuk kebutuhan pengamanan) dalam perangkat-perangkat milik perusahaan penyedia jasa CA di negara lain.

Penulisan ini mengukur bagaimana potensi kompetitif penyediaan layanan CA di era konvergensi serta bagaimana strategi yang perlu dilakukan Lembaga Sandi Negara untuk menyediakan layanan ini kepada publik, dalam hal ini pengguna transaksi elektronik di era konvergensi.

1.2. Identifikasi Masalah

Dari uraian latar belakang dapat diidentifikasikan beberapa hal sebagai berikut :

1. Transaksi elektronik merupakan salah satu aplikasi berbasis digital (*IP Based*) yang dapat dilakukan dalam era konvergensi. Besarnya tingkat penggunaan transaksi elektronik juga menimbulkan ancaman keamanan terhadap pengiriman data secara digital tersebut. Oleh karena itu salah satu layanan yang diperlukan adalah berupa jaminan keamanan bagi setiap entitas yang melakukan transaksi (telekomunikasi) secara elektronik.
2. Lembaga Sandi Negara adalah perangkat pemerintahan yang bertugas di bidang keamanan informasi. Salah satu layanan keamanan yang

dimungkinkan untuk diselenggarakan bagi keperluan publik di era konvergensi adalah penyediaan layanan keamanan CA.

3. Saat ini di Indonesia belum ada organisasi/lembaga/perusahaan yang mampu berdiri sebagai pihak ketiga yang memberikan jaminan keamanan CA untuk mengamankan transaksi elektronik secara global. Padahal layanan ini mutlak diperlukan di era konvergensi dalam setiap transaksi elektronik dalam praktek perekonomian dan telekomunikasi baik skala nasional, regional maupun internasional.

Dari identifikasi masalah diatas, didapatkan perumusan masalah sebagai berikut :

1. Layanan CA adalah salah satu solusi untuk melindungi keamanan transaksi elektronik dalam era konvergensi telekomunikasi. Bagaimana potensi kompetitif (peluang) penyediaan layanan ini dalam lingkungan industri telekomunikasi di era konvergensi (global).
2. Lembaga Sandi Negara adalah salah satu organisasi pemerintah dibidang keamanan informasi dalam lingkup pemerintahan. Bagaimana pengaruh internal dan eksternal organisasi untuk menyelenggarakan layanan CA bagi keperluan publik.
3. Bagaimana strategi untuk membuat layanan CA menjadi layanan yang bernilai strategis bagi organisasi.

1.3. Tujuan Kajian

Tujuan yang ingin dicapai dari penelitian ini adalah menganalisa potensi kompetitif penyediaan layanan keamanan CA di era konvergensi dan menyusun perencanaan strategi dalam menyediakan layanan keamanan CA untuk keperluan publik bagi Lembaga Sandi Negara.

1.4. Batasan Masalah

Untuk menghindari meluasnya materi pembahasan penelitian ini, maka penulis membatasi permasalahan sebagai berikut :

1. Penelitian ini membahas mengenai penyediaan layanan keamanan CA dengan metode keamanan CA - *Publik Key Infrastruktur*.

2. Perencanaan strategi penyediaan layanan CA di era konvergensi dilakukan dalam studi kasus Lembaga Sandi Negara, yang dalam hal ini sebagai sebuah lembaga yang telah memiliki kompetensi dibidang pengamanan informasi sehingga memungkinkan untuk membentuk layanan CA bagi keperluan publik.
3. Penulisan tidak mencakup strategi dalam hal menentukan biaya dan struktur fungsional organisasi untuk menyediakan layanan CA kepada publik.
4. Hasil akhir penelitian perencanaan strategi tidak akan sampai ke tahap pelaksanaan dan pengujian.

1.5. Metodologi Penelitian

Penelitian ini diawali dengan identifikasi masalah kemudian dilanjutkan dengan tahapan-tahapan sebagai berikut :

1. Pengumpulan Data

   Metode pengumpulan data untuk penelitian ini dilakukan dengan cara sebagai berikut :

   a. Studi Literatur

      Studi literatur dilakukan untuk memahami konsep teori dan untuk mendapatkan informasi-informasi yang dapat mendukung penelitian. Sumber dari studi literatur dapat berupa buku, jurnal ilmiah, peraturan dan data internal serta artikel-artikel yang relevan dengan topik penelitian.

   b. Survey dan wawancara dengan pihak terkait penelitian.

      Survey kuisioner dan wawancara dilakukan untuk mendapatkan justifikasi manajemen mengenai faktor internal,eksternal dan penentuan strategi terkait penelitian.

2. Tahap Analisa

   Tahap ini dilakukan analisa terhadap data yang terkumpul, sehingga dapat dijadikan dasar setiap tekanan kompetitif bagi penyusunan strategi bersaing layanan keamanan (CA) di era konvergensi.

1.6. Sistematika Penulisan

Penulisan ini menggunakan sistematika sebagai berikut :

BAB I PENDAHULUAN

Bagian ini menjelaskan latar belakang penulisan, perumusan masalah, tujuan penulisan, pembatasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II LAYANAN KEAMANAN CERTIFICATE AUTHORITY

Pada bab ini dipaparkan mengenai konvergensi telekomunikasi, kebutuhan keamanan transaksi elektronik, layanan keamanan CA serta profil singkat organisasi.

BAB III POTENSI KOMPETITIF LAYANAN CA DI ERA KONVERGENSI

Pada bab ini dipaparkan mengenai potensi kompetitif penyediaan layanan keamanan CA di era konvergensi dengan model analisa *Porter 5 Forces.*

BAB V STRATEGI PENYEDIAAN LAYANAN KEAMANAN CA

Bab ini memaparkan mengenai tahapan penyusunan strategi bagi Lembaga Sandi Negara dalam penyediaan layanan keamanan CA kepada publik di era konvergensi dengan menggunakan Pendekatan Manajemen Strategis.

BAB VI PENUTUP

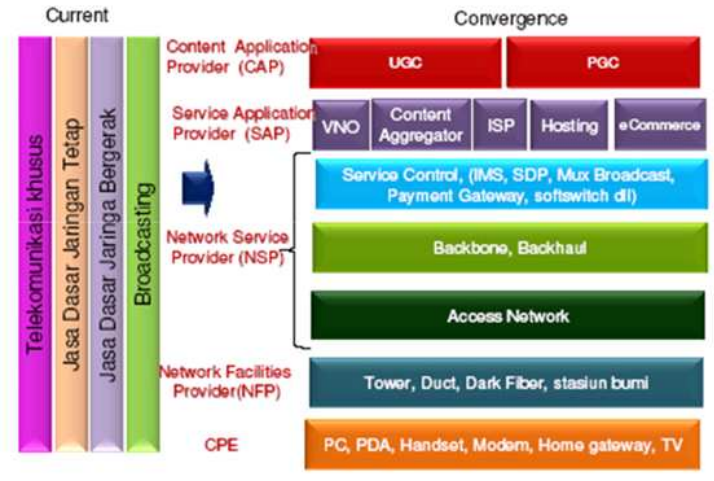
Berisi kesimpulan dari penulisan ini.

BAB II
LAYANAN KEAMANAN
CERTIFICATE AUTHORITY

2.1. Konvergensi Telekomunikasi

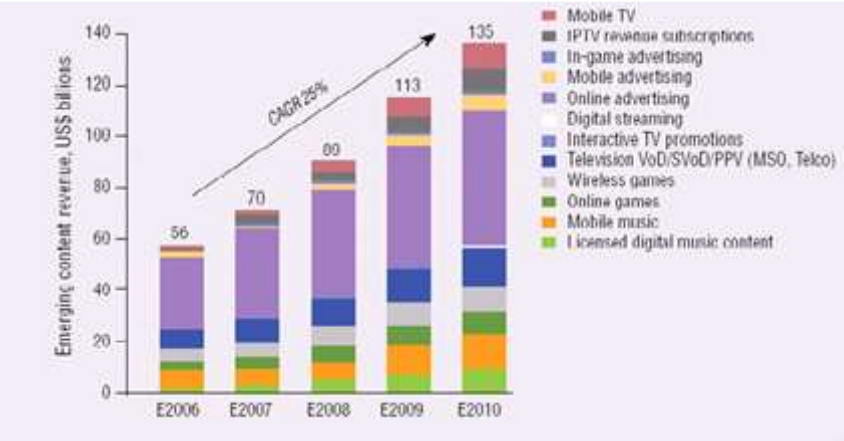
Telekomunikasi saat ini tidak lagi menjadi kebutuhan tetapi juga menjadi sebuah keharusan. Telekomunikasi tidak hanya memberikan mobilitas yang tidak terikat ruang dan waktu, tetapi juga memberikan layanan bagi pelanggannya hingga mengubah cara hidup masyarakat dunia. Infrastruktur telekomunikasi yang mampu melewatkan informasi dalam kecepatan tinggi dan kanal yang lebar mengakibatkan evolusi pengiriman informasi yang awalnya hanya berbentuk *voice* (suara) menjadi kearah transfer data dengan kecepatan tinggi dan *bandwidth* yang lebar.

Perubahan segmentasi layanan Industri telekomunikasi di era konvergensi tidak hanya menyediakan infrastruktur telekomunikasi (*Network Facilities)* tetapi juga menyelenggarakan konten atau aplikasi yang dapat berjalan di platform tersebut *Network Service* dan *Content Aplication*. Pada Gambar 2.1 diperlihatkan perbedaan segmentasi layanan di era konvergensi telekomunikasi.



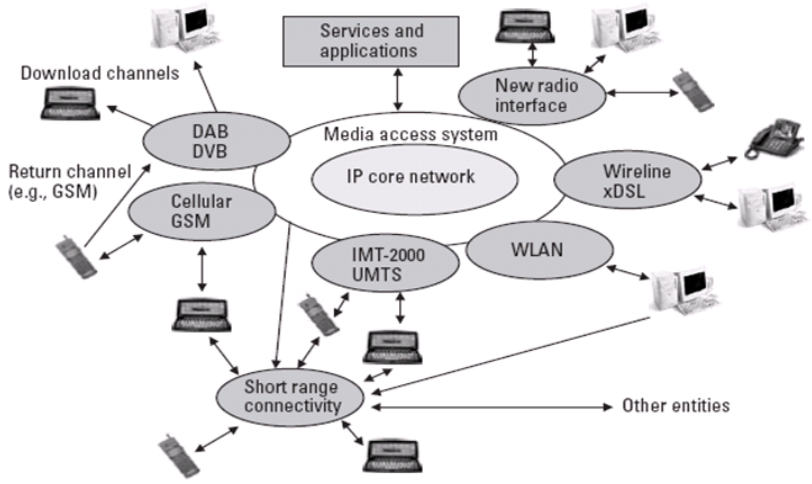
Gambar 2.1 Layanan Industri Telekomunikasi [1]

Evolusi mengiriman informasi kearah data melalui media telekomunikasi dan komputer mengakibatkan semakin besar kebutuhan dan peluang penyelenggaraan konten elektronik, seperti terlihat pada Gambar 2.2.



Gambar 2.2 Kebutuhan Konten Elektronik [11]

Dalam era konvergensi, tidak hanya antar perangkat telekomunikasi saja yang dapat saling berhubungan, tetapi juga menggabungkan teknologi komputer dan sistem informasi menjadi sebuah kesatuan utuh untuk mendukung interkoneksi sesuai kebutuhan penggunanya. Pada Gambar 2.3 diperlihatkan layanan yang dapat diakses melalui perangkat-perangkat yang berbeda dalam suatu jaringan telekomunikasi.



Gambar 2.3 Jaringan Telekomunikasi Era Konvergensi [1]

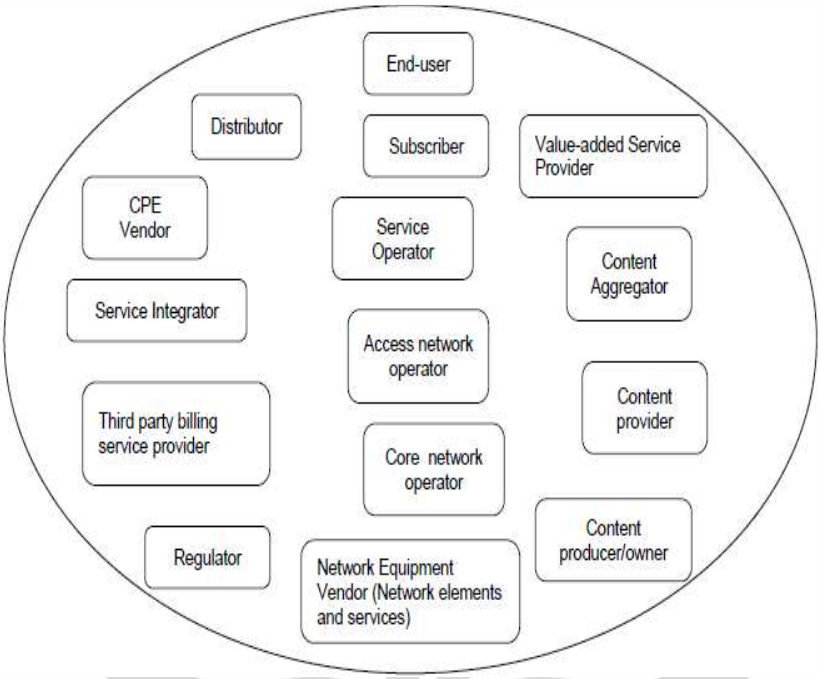
Konvergensi merupakan integrasi yang progresif dari beberapa platform jaringan yang berbeda untuk menyalurkan layanan yang serupa dan atau layanan-layanan yang berbeda yang disalurkan pada platform jaringan yang sama [7]. Tabel 2.1 memberikan perbandingan paradigma teknologi informasi dan telekomunikasi saat ini dan di masa depan. Kedepan infrastruktur akan lebih kearah digital dan didominasi oleh *Packet Switched* (*IP Based*).

Tabel 2.1 Paradigma Telekomunikasi Masa Depan [7]

Item	Paradigma Saat Ini	Paradigma Ke Depan
Pasar	Kompetisi Terbatas	Kompetisi Penuh
Regulasi	Ketat dan Parsial	*Light touch regulation* dan terintegrasi
Infrastruktur	Telekomunikasi	Informasi
Struktur Industri	Vertikal	Horisontal
Penyaluran Informasi	format terpisah untuk Suara, Data, Teks, Gambar	format Multimedia (konvergensi)
Infrastruktur	Hybrid Analog dan Digital	Seluruhnya Digital
Major Infrastruktur	*Circuit-Switched*	*Packet-Switched* (IP Based)
Jaringan akses	Didominasi saluran narrowband	Dominasi oleh saluran broadband
Skema pentarifan	berdasarkan waktu dan jarak	berdasarkan volume (byte)
Basis Industri	Industrial Economy	Knowledge based Economy

Meningkatnya penggunaan transaksi elektronik memberikan peluang bagi perusahaan atau organisasi dalam industry telekomunikasi untuk menciptakan *value added service* kearah penyediaan jasa konten untuk mendukung transaksi elektronik termasuk juga layanan untuk mengamankan transaksi yang berjalan dalam platform IP tersebut.

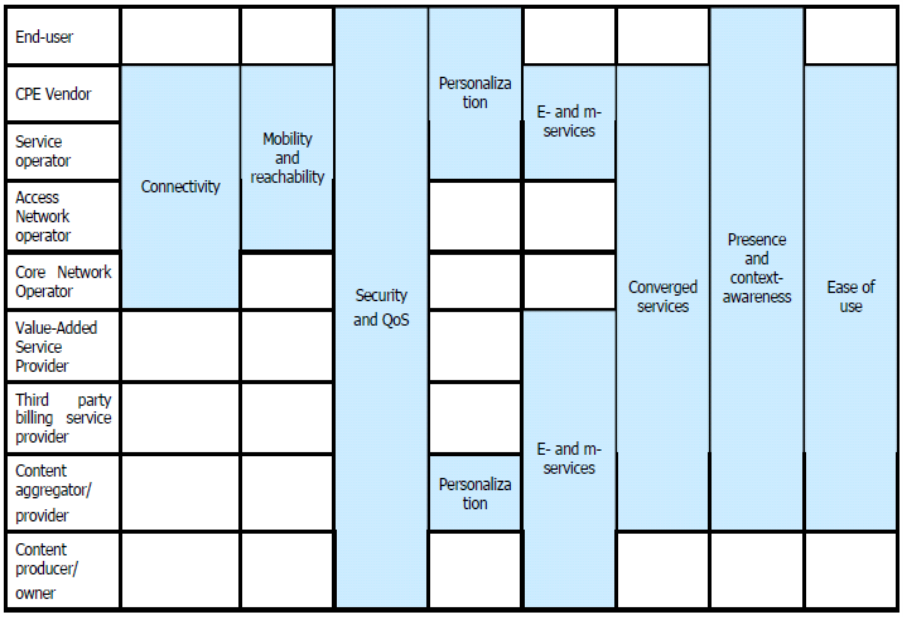
Besarnya kebutuhan penyelenggaraan elektronik dan hadirnya konvergensi secara global mengakibatkan bervariasinya penyediaan layanan. Pada dokumen *celtic initiative* disebutkan bahwa ekosistem penyelenggaraan jasa telekomunikasi akan terdiri dari ekosistem seperti digambarkan pada Gambar 2.4.



Gambar 2.4 Ekosistem Penyelenggara Telekomunikasi di Era Konvergensi [12]

Pada Gambar tersebut digambarkan bahwa pemain bisnis dalam industri telekomunikasi di era konvergensi tidak hanya penyedia jasa jaringan, tetapi juga entitas lain yang berhubungan dengan setiap layanan yang diberikan. Setiap komponen ekosistem telekomunikasi menyediakan jenis layanan (konten) sesuai dengan fungsi dari entitas ekosistem. Dalam memberikan layanan seperti transaksi elektronik, setiap entitas tersebut saling berhubungan satu dengan yang lainnya. Layanan keamanan dalam transaksi elektronik diperlukan tidak hanya untuk melindungi data digital yang dikirimkan tetapi juga memberikan validasi setiap entitas yang melakukan transaksi. Kebutuhan layanan keamanan ini menjadi tinggi di era konvergensi mengingat setiap entitas tidak hanya berada di dalam negeri tetapi juga diluar negeri. Dari sumber *ecosys celtic initiative* dikatakan bahwa setiap entitas dalam ekosistem penyelenggara telekomunikasi di era konvergensi akan memerlukan aspek pengamanan.

Tabel 2.2 Aspek Setiap Entitas Ekosistem Penyelenggara Telekomunikasi [12]



Pada Tabel 2.2 diperlihatkan aspek yang dicakup oleh setiap entitas dalam ekosistem penyelenggara telekomunikasi di era konvergensi. Diperlihatkan bahwa setiap entitas tersebut membutuhkan aspek keamanan dan harus memperhatikan *Quality of Service* (QoS) layanan yang diberikan.

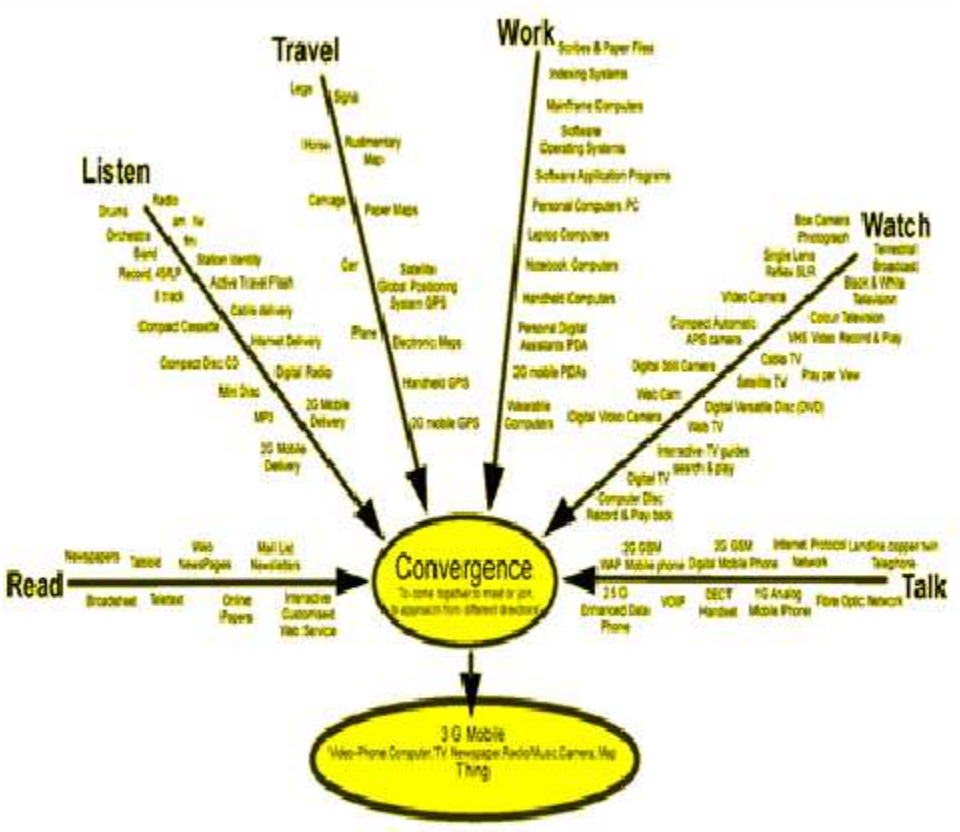
2.2. Keamanan Transaksi Elektronik

Transaksi Elektronik merupakan satu set dinamis teknologi, aplikasi dan proses bisnis yang menghubungkan perusahaan, konsumen dan komunitas tertentu melalui transaksi elektronik dan perdagangan barang, pelayanan dan informasi yang dilakukan secara digital**.** Dari sumber "*The Canadian Electronic Commerce Strategy*" didefinisikan transaksi e-Commerce sebagai berikut [13] :

Definisi luas: segala bentuk transaksi yang menggunakan teknologi digital, meliputi jaringan terbuka (Internet), jaringan tertutup (*Electronic Data Interchange*), *credit card* dan *debit card*.

Definisi sempit: segala transaksi yang menggunakan TCP/IP (*Transmission Control Protocol/Internet Protocol*) (sehingga dalam definisi ini e-Commerce hanyalah merupakan aplikasi Internet).

Transaksi Elektronik dalam era konvergensi memanfaatkan teknologi dari berbagai jenis teknologi (platform) yang berbeda dapat saling terkoneksi dalam bentuk aplikasi dan proses komunikasi bisnis yang menghubungkan perusahaan, organisasi, konsumen dan komunitas tertentu. Aplikasi atau konten yang diselenggarakan disesuaikan dengan kebutuhan konsumen, seperti pemetaan yang diperlihatkan pada Gambar 2.5.



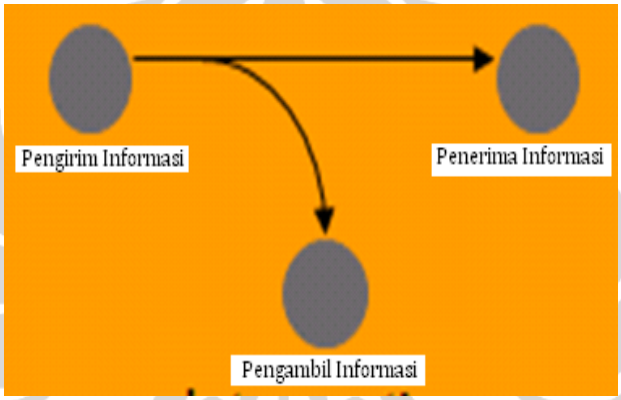
Gambar 2.5 Aplikasi Konten di Era Konvergensi [19]

Electronic Commerce sebagai salah satu layanan transaksi elektronik yang dapat berjalan pada platform konvergensi mencakup perdagangan elektronik baik barang atau jasa, pengiriman data secara online, transfer dana secara elektronik, *electronic share trading, electronic bill of landing, commercial auctions, direct consumer marketing*. *Electronic Commerce* adalah melakukan aktivitas bisnis yang diarahkan pada pertukaran nilai melalui jaringan telekomunikasi [20]. Transaksi elektronik dapat dilakukan untuk menggantikan pola transaksi

konvensional. Dalam perniagaan konvensional, setiap penjual dan pembeli dipertemukan dalam satu tempat yang sama untuk melakukan transaksi-transaksi perniagaan atau perdagangan.

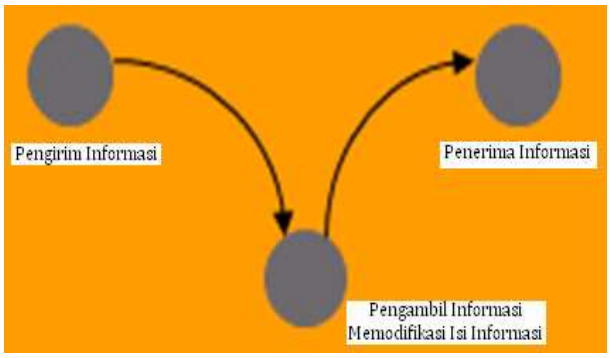
Dalam transaksi elektronik menggunakan jaringan berbasis IP (internet), ancaman (*vulnerabilities*) dapat muncul dengan metode-metode berikut :

a) Ancaman berupa penyadapan data, pencurian arsip elektronik, akses yang tidak sah. Pengambilan data informasi yang sedang dikirim (*interception*) dilakukan oleh pihak yang tidak berkepentingan, diperlihatkan pada Gambar 2.6.



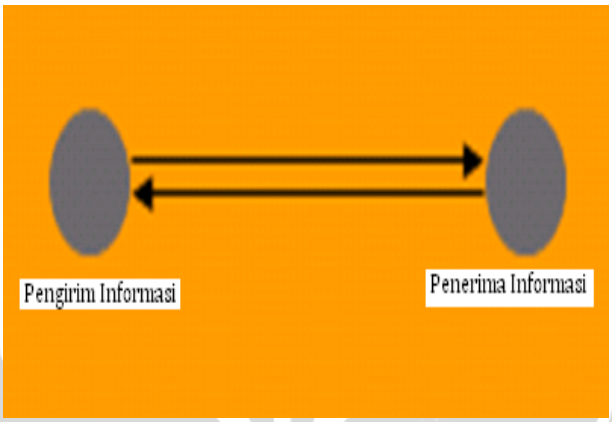
Gambar 2.6. Pengambilan Informasi dalam Transaksi

b) Ancaman terhadap keutuhan data yang dikirim melalui media elektronik, misalnya terjadi perubahan informasi oleh pihak lain untuk kepentingan tertentu. Pengambilan Informasi dan perubahan data informasi (*modification*) oleh pihak yang tidak berkepentingan diperlihatkan pada Gambar 2.7.



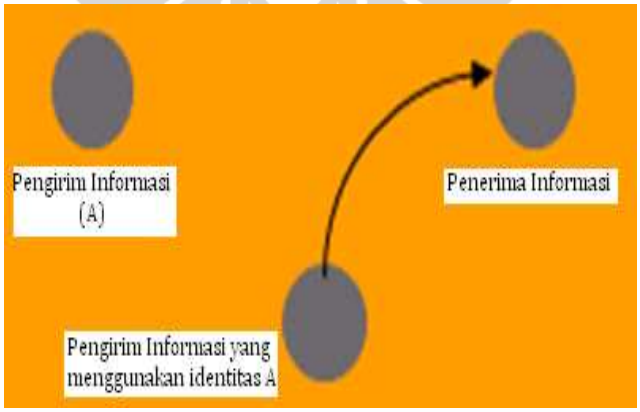
Gambar 2.7. Pengubahan Informasi dalam Transaksi

c) Dalam transaksi secara elektronik, pengirim data dapat dengan mudah menyangkal telah mengirimkan informasi. Seperti diperlihatkan pada Gambar 2.8, Penerima data informasi tidak memiliki bukti nyata bahwa yang mengirim informasi adalah pengirim yang benar.



Gambar 2.8. Tidak ada Pembuktian Pengirim dalam Transaksi

d) Secara umum pihak-pihak yang bertransaksi secara elektronik tidak bertemu seperti dalam transaksi konvensional. Oleh karena itu transaksi elektronik rentan terhadap pemalsuan identitas oleh pihak lain. Pemalsuan identitas untuk mengirim data informasi kepada pihak tertentu dalam transaksi diperlihatkan pada Gambar 2.9.



Gambar 2.9. Pemalsuan Identitas dalam Transaksi

Dalam Standar *International Telecommunication Union* (ITU-T) dikatakan bahwa dimensi keamanan yang harus di cakup dalam sebuah komunikasi yang dapat dikatakan aman (*secure telecommunication*) ada 8 dimensi yaitu;

2.2.1. *Access Control* (Pengendali Akses)

Hanya yang memiliki wewenang yang dapat mengakses aplikasi yang dilindungi.

2.2.2. *Authetication* (Autentikasi)

Artinya para pihak yang berkomunikasi benar adalah pihak yang dimaksud.

2.2.3. *Non Repudiation* (Nir-Sangkal)

Artinya pihak pengirim tidak dapat menyangkal telah mengirimkan informasi tertentu pada waktu tertentu.

2.2.4. *Confidential* (Konfidensialitas)

Artinya informasi terjaga kerahasiaannya sehingga hanya diketahui pengirim dan penerima.

2.2.5. Keamanan dalam berkomunikasi (*Communication Security*)

Keamanan dalam komunikasi merupakan jaminan keamanan saat komunikasi dilakukan.

2.2.6. *Integrity* (Integritas)

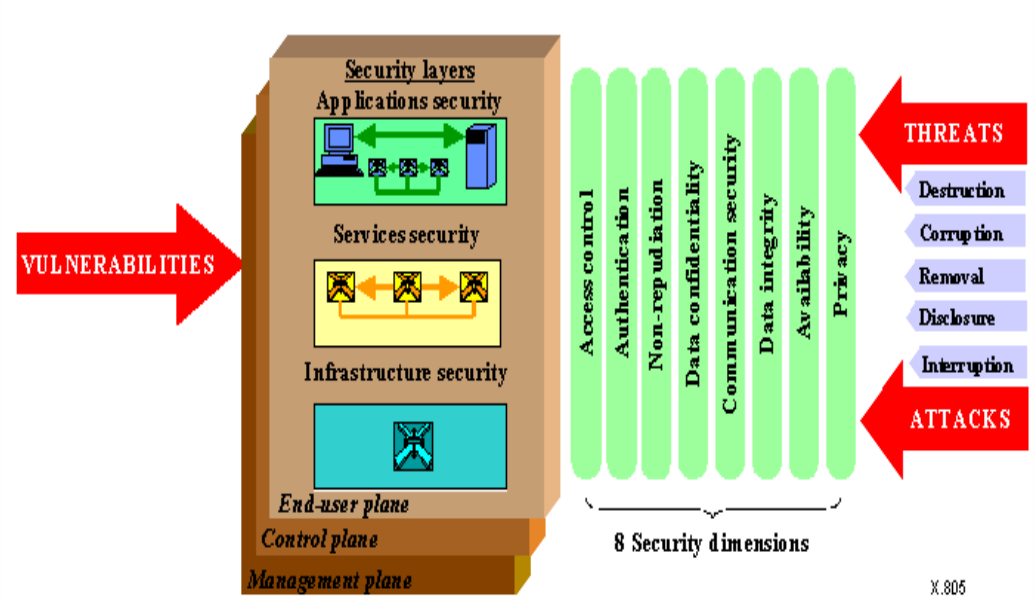
Artinya informasi tidak terganggu keasliannya baik sengaja maupun tidak sengaja selama dalam perjalanannya.

2.2.7. *Availability* (Ketersediaan)

Jaminan bahwa jaringan atau aplikasi yang ada dijaringan tersebut memiliki ketahanan terhadap ancaman yang mungkin terjadi.

2.2.8. *Privacy*

Jaminan keamanan terhadap penyimpanan data yang dilakukan oleh pengguna dalam jaringan komunikasi.

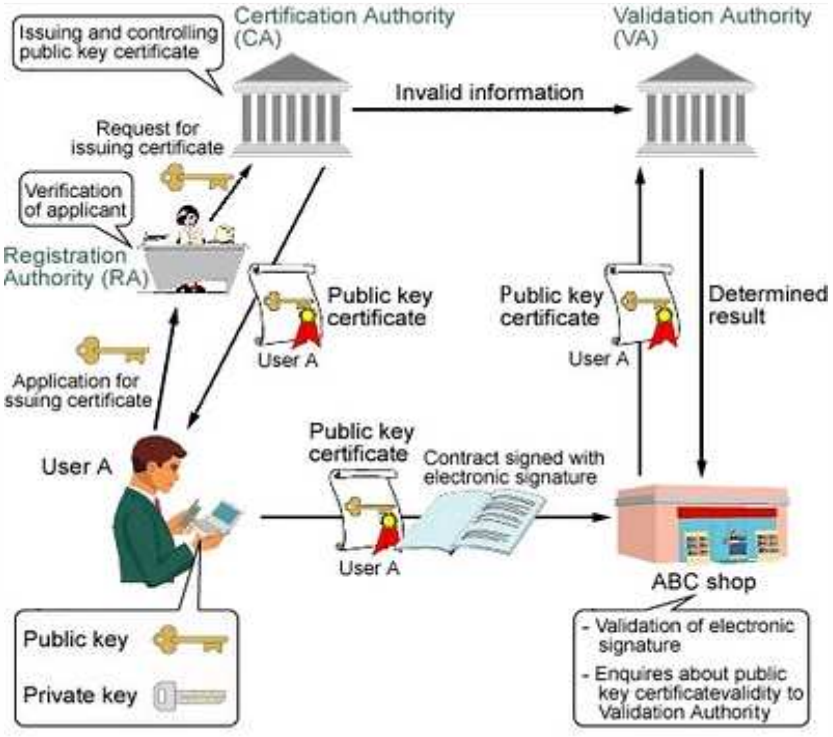


Gambar 2.10 Dimensi Keamanan Standar ITU [14]

Pada Gambar 2.10 diperlihatkan dimensi keamanan yang harus di cakup dalam sebuah komunikasi yang dapat dikatakan aman (*secure telecommunication*) sesuai standar *International Telecommunication Union* untuk Telekomunikasi (ITU-T).

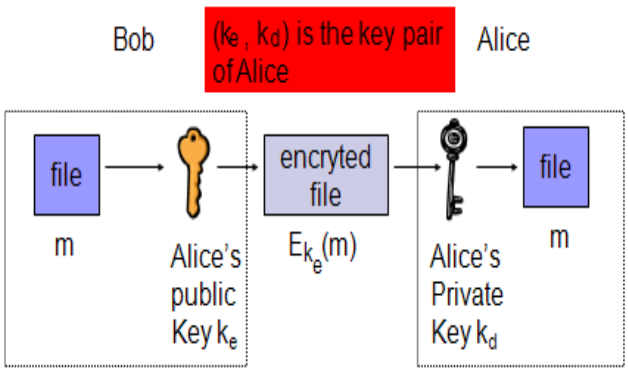
2.3. Layanan CA

Certificate Authority (CA) secara umum didefinisikan sebagai pihak ketiga yang terpercaya dalam sebuah komunikasi aman. CA merupakan sebuah *body / entity* dalam pihak-pihak transaksi yang memberikan dan mengelola sertifikat digital yang dibutuhkan dalam setiap transaksi elektronik. CA berhubungan erat dengan pengelolaan infrastruktur kunci publik (*public key infrastructure*). Pada Gambar 2.11 diperlihatkan bagaimana kunci yang akan digunakan dalam berkomunikasi secara elektronik diatur oleh sebuah *Certificate Authority*.



Gambar 2.11 Infrastruktur Kunci Publik [15]

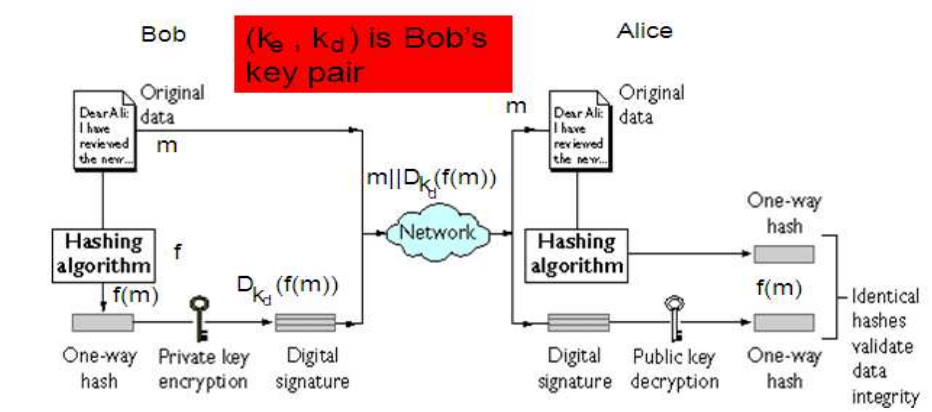
Publik Key Infrastruktur (PKI) merupakan salah satu mekanisme keamanan untuk melakukan komunikasi pesan rahasia dalam sebuah sistem atau jaringan. Pada Gambar 2.12 berikut, dijelaskan ada dua pihak yang akan berkomunikasi dengan melakukan penyandian menggunakan metode *publik key*. Sebelum melakukan komunikasi data/informasi yang akan dikirimkan diubah dengan menggunakan perhitungan secara matematis (algoritma), agar pesan yang dikirim tidak merupakan pesan asli.



Gambar 2.12. Skema *Publik Key* [16]

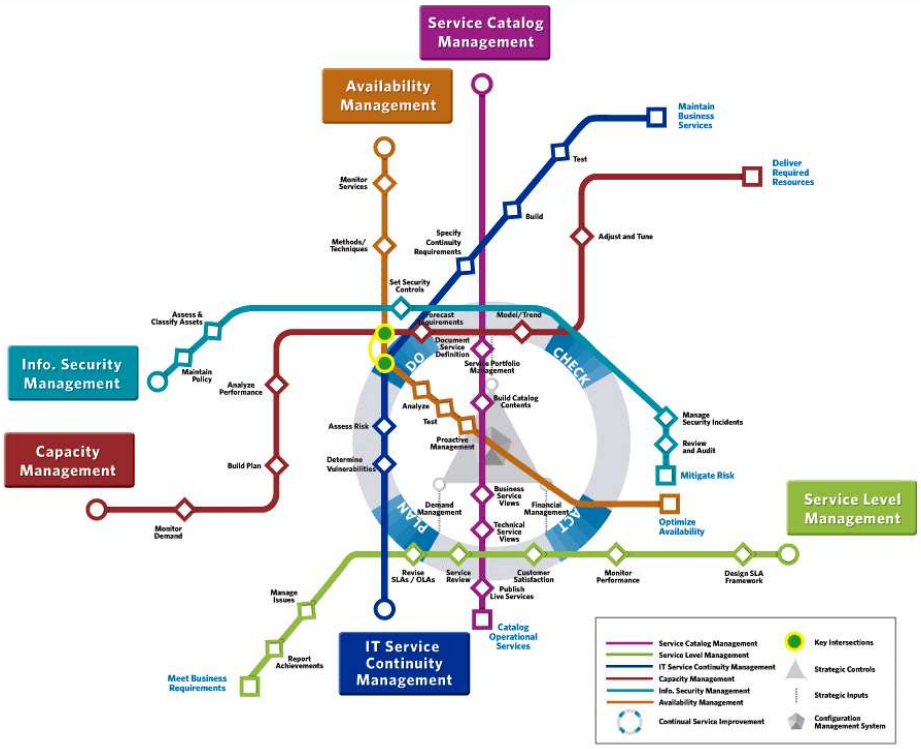
Dalam skema *Publik Key*, setiap pihak (Alice dan Bob) memiliki 2 kunci yaitu kunci publik (kunci yang diumumkan) dan kunci rahasia (kunci *private* yang digunakan untuk melakukan penyandian). Kunci *private* dan kunci publik merupakan pasangan kunci yang sebelumnya di bangkitkan (*generate*). Pembangkitan dilakukan sesuai algoritma (perhitungan matematis) yang telah disepakati untuk digunakan dalam komunikasi "rahasia" yang akan dilakukan.

Sama halnya dengan penyandian sebuah informasi, metode yang sama dilakukan untuk melakukan penanda tanganan pesan secara elektronik. Gambar 2.13 adalah salah satu contoh skema tanda tangan digital (*Digital Signatures*). Tanda tangan digital dilakukan dengan menghitung nilai *hash* menggunakan algoritma *hash* yang disepakati. Setelah didapat hasil perhitungan, dilakukan penyandian dengan kunci *private* pengirim. Dari hasil keseluruhan perhitungan didapat nilai-nilai yang menjadi tanda tangan digital untuk kemudian dikirimkan bersama pesan yang terkirim pada jaringan.



Gambar 2.13. Tanda Tangan Digital untuk Transaksi Elektronik [17]

CA (*Certificate Authority*) adalah sebuah badan hukum yang menyediakan layanan keamanan yang dapat dipercaya oleh para pengguna dalam menjalankan pertukaran informasi secara elektronis. Secara sederhana layanan CA adalah sebagai pihak ketiga yang mengatur bagaimana kunci dan algoritma dihasilkan, diatur, dimusnahkan dan diperbaharui untuk setiap transaksi elektronik yang dilakukan. Contoh desain layanan CA diperlihatkan pada Gambar 2.14 berikut.



Gambar 2.14. Desain Layanan *Certificate Authority* [18]

Layanan dasar yang diberikan pada penyedia layanan CA adalah sebagai berikut [19] ;

a) Layanan Manajemen Kunci seperti layanan pembuatan kunci, layanan pendaftaran kunci, layanan penyimpanan kunci, layanan *revocation* kunci, layanan penghancuran/penghentian kunci.

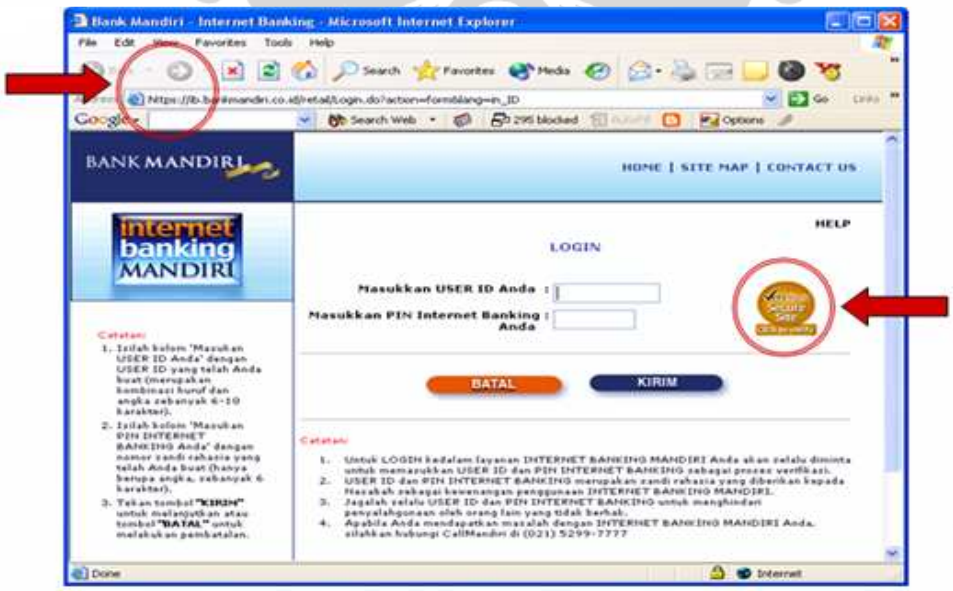
b) Layanan Manajemen Sertifikat seperti layanan sertifikasi kunci publik (identitas pengguna, panjang kunci, masa berlaku, algoritma tanda tangan, unik serial number, profil sertifikat, metode penyandian), layanan *Online Authentication Service*, layanan *revocation* sertifikat.

c) Layanan Materai waktu (*Time Stamping*) seperti Otoritas pemberi materai waktu (*Time Stamping Authority*) yang menandai kapan terjadi transaksi dan layanan *Non-repudiation*.

Pada Gambar 2.15 diperlihatkan contoh perusahaan penyedia layanan CA , diantaranya Verisign, Thawte, Cacert dan Geotrust.

Gambar 2.15 Provider Layanan CA [20]

Perusahaan CA yang saat ini ada adalah perusahaan layanan keamanan yang bersifat internasional. Untuk bisa dijadikan sebagai pihak ketiga terpercaya di Indonesia, perusahaan ini harus terdaftar di Indonesia (sesuai Undang-undang Penyelenggaraan CA). Besarnya kebutuhan dan tuntutan dalam perdagangan global membuat perusahaan atau organisasi mulai menggunakan jasa CA. Beberapa perusahaan dan organisasi mulai membentuk layanan sejenis, seperti PT.Telkom membentuk i-trust untuk aplikasi *cyber notary* internal. Beberapa perusahaan Indonesia misal di bidang perbankan menggunakan layanan CA Luar Negeri, seperti diperlihatkan pada Gambar 2.16 berikut, salah satu contoh bank yang menggunakan layanan CA.



Gambar 2.16 Provider Layanan CA Perbankan [21]

Dalam Undang-undang Penyelenggaraan CA, infrastruktur sebuah CA harus terdapat fungsi-fungsi *Policy Authority*, *Certification Authority* dan *Registration Authority. Policy Authority* adalah unit/organisasi dalam bisnis layanan CA yang bertanggung jawab terhadap penentuan, pemberlakukan, pengembangan dan pengadministrasian kebijakan sertifikasi. *Certification Authority* adalah unit yang memiliki kewenangan untuk memberikan sertifikat digital yang berisi identitas pengguna dimana sertifikat tersebut ditanda tangani secara digital. *Registration Authority* adalah suatu unit yang memiliki otoritas untuk melaksanakan fungsi-fungsi pendaftaran pemohon sertifikat.

2.4. Profil Singkat Organisasi

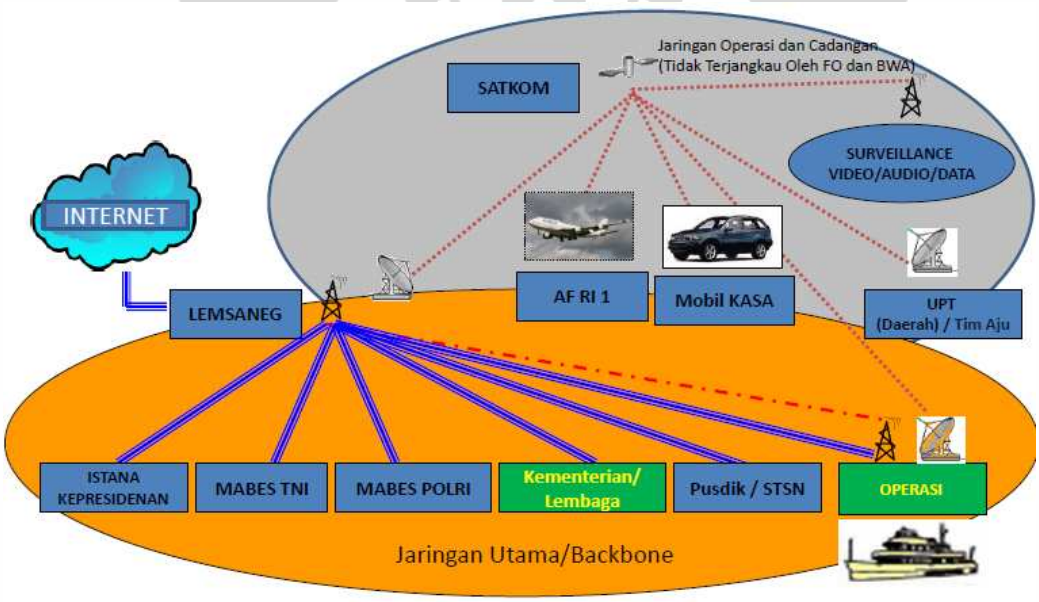
Lembaga Sandi Negara (Lemsaneg) adalah Lembaga Pemerintahan non Departemen yang bergerak di bidang pengamanan informasi melalui persandian. Berdasarkan Keputusan presiden republik Indonesia Nomor 103 Tahun 2001 Tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi dan Tata kerja Lembaga Pemerintahan Non Departemen, tugas Lemsaneg adalah melaksanakan tugas pemerintahan dibidang persandian sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

Lembaga Sandi Negara adalah Lembaga Pemerintahan non Departemen yang didirikan pada tanggal 4 April 1946, yang kemudian melembaga menjadi "Djawatan Sandi" dengan Surat Keputusan Menteri Pertahanan nomor 11/MP/1949 pada tanggal 2 September 1949. Melalui SK Presiden RIS nomor 65/1950, pada tanggal 14 Februari 1950, terjadi pemisahan struktur organisasi persandian dari Kementerian Pertahanan, Pada 22 Februari 1972 menjadi "Lembaga Sandi Negara" dengan Keppres No. 7/1972. Sejalan dengan konsolidasi/penataan struktur kelembagaan Pemerintah, terjadi perubahan landasan hukum Lembaga Sandi Negara, berturut-turut pada 18 Juli 1994 dengan Keppres Nomor 54/1994, pada 7 Juli 1999 dengan Keppres Nomor 77/1999, dan terakhir dengan Keppres Nomor 103/2001.

Bertugas dibidang Pertahanan Negara, Visi Lembaga Sandi Negara adalah "Terpercaya, Profesional dan Mandiri dalam Persandian". Sedangkan Misi Lembaga Sandi Negara adalah [22]:

- Menyusun kebijakan nasional dalam bidang persandian sektor pemerintahan dan publik ;
- Menyiapkan dan meningkatkan aparatur Negara yang profesional/ahli dalam bidang persandian;
- Mengoptimalkan potensi nasional dalam hal penelitian dan pengembangan di bidang persandian untuk mendukung kepentingan nasional;
- Menyelenggarakan operasional pengamanan informasi;
- Menyelenggarakan pencarian dan pengupasan informasi bersandi;
- Optimalisasi manajemen perkantoran secara akuntabel.

Ruang lingkup pengamanan informasi yang ditangani oleh Lembaga Sandi Negara adalah Unit Tehnis Persandian Departemen/Lembaga Pemerintahan dan VVIP Negara seperti Presiden, Menteri Negara, Perutusan Tetap Republik Indonesia dan Perwakilan Luar Negeri, seperti terlihat pada Gambar 2.17.



Gambar 2.17 Ruang Lingkup Pengamanan Informasi [23]

Dalam Tujuan Hankam [24] disebutkan bahwa tujuan pertahanan negara adalah meningkatnya kemampuan pertahanan negara, aktifitas masyarakat, dunia usaha untuk dapat berlangsung secara aman, nyaman serta menjaga agar kondisi keamanan dalam negeri kondusif.

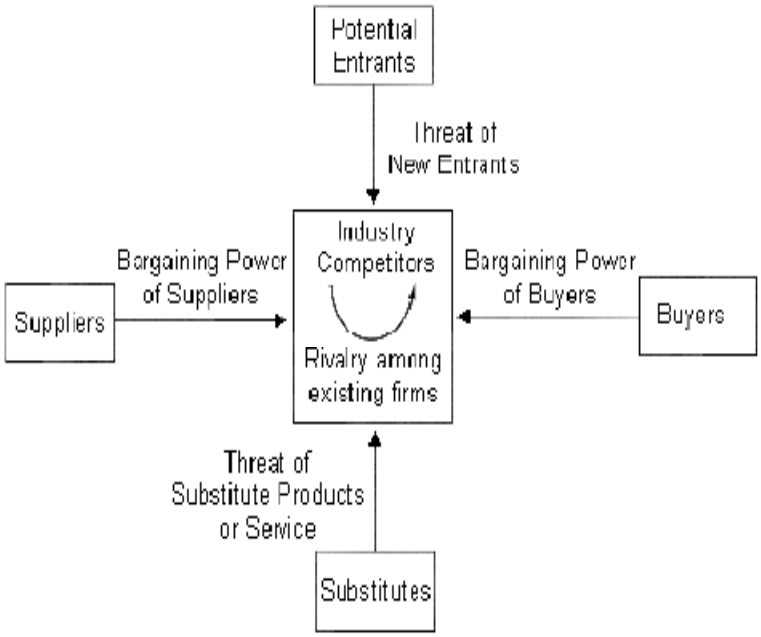
Dalam kerangka meningkatkan ketahanan masyarakat dan dunia usaha sangat dimungkinkan untuk mulai melakukan pelayanan publik sesuai kebutuhan di era konvergensi. Saat ini Lembaga Sandi Negara belum mengembangkan layanan keamanan bagi kebutuhan publik. Meskipun secara tidak langsung ikut serta dalam pembangunan aplikasi keamanan bagi media-media telekomunikasi termasuk layanan CA diberbagai instansi pemerintahan.

Keamanan dalam bertransaksi elektronik seperti e-commerce adalah hal yang sangat dibutuhkan oleh publik. Salah satu solusi keamanan yang dapat dilakukan adalah dengan menyelenggarakan layanan keamanan CA. Dalam penelitian ini, ada 2 bahasan utama yang akan dianalisa, yaitu:

1). Potensi kompetitif penyediaan layanan kemanan CA ke publik (pengguna transaksi elektronik) dalam industri telekomunikasi di era konvergensi global dengan menggunakan model Porter 5 Forces.
2). Penyusunan strategi penyediaan layanan keamanan CA bagi Lembaga Sandi Negara dengan menggunakan pendekatan Manajemen Strategis.

BAB III
POTENSI KOMPETITIF LAYANAN CA DI ERA KONVERGENSI

Dalam penelitian ini akan dilakukan analisa terhadap Potensi Kompetitif Penyediaan Layanan Kemanan CA ke publik dalam industri telekomunikasi di era konvergensi global dengan menggunakan model Porter 5 Forces yang dikembangkan oleh Michael Porter. Metode *Porter 5 Forces* merupakan metode yang mengarah pada analisa industri dari luar perusahaan/organisasi dan mencoba untuk melihat potensi kedalam organisasi untuk menganalisa tingkat ketertarikan industri [25].



Gambar 3.1 Porter 5 Forces [25]

Seperti terlihat pada Gambar 3.1 menurut Michael Porter, ada 5 kekuatan persaingan dasar yang mempengaruhi keadaan persaingan yang kemudian dikenal sebagai *Porter 5 Forces* [25]. yaitu ;

1). sisi pendatang baru (*threat of new entrant*),

2). sisi produk atau jasa pengganti (*threat of substitute product*),

3). sisi pemasok (*bargaining power of supplier*),

4). sisi pembeli (*bargaining power of buyer*)

5). sisi pemain bisnis yang sudah ada di pasar (*the rivalvy among the exiting competitors*).

Kelima kekuatan persaingan seperti diilustrasikan pada Gambar 3.1 mencerminkan bahwa situasi persaingan dalam suatu industri tidak terbatas dipengaruhi hanya oleh pemain yang ada saja melainkan karena gabungan lima kekuatan yang bersama-sama menentukan intensitas persaingan dan profitabilitas dalam industri.

3.2.1. Identifikasi Pemain dalam Industri

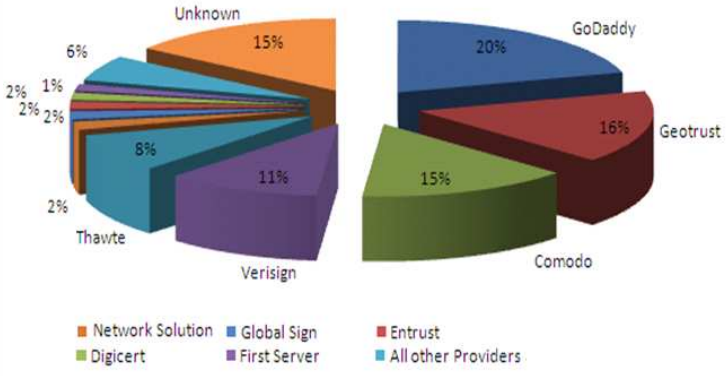
Langkah awal dari melakukan analisis potensi kompetitif penyediaan layanan keamanan CA di era konvergensi adalah menentukan yang menjadi pemain atau yang berperan dalam industri penyediaan layanan CA saat ini. Hasil identifikasi penyedia jasa layanan CA saat ini diperlihatkan pada Tabel 3.1.

Tabel 3.1 Penyedia Layanan Keamanan CA [28]

Peringkat	Nama Provider	Market Share	Total User Certificate	Website	Negara
1.	GoDaddy	20,52%	421.854	http://www.godaddy.com/	USA
2.	Geotrust	16,28%	334.668	http://www.geotrust.com	USA
3.	Comodo	14,66%	301.308	http://www.comodo.com	Washington, United States
4.	Verisign	10,71%	220.117	http://www.verisign.com	North America

5.	Thawte	8,57%	176.078	http://query.thawte.com/	Afrika Selatan
6.	Network Solution	1,86%	38.332	http://www.networksolutions.com/	Canada
7.	GlobalSign	1,84%	37.794	http://www.globalsign.com/	USA
8.	Entrust	1,67 %	34.333	http://www.entrust.com/	Australia
9.	Digicert	1,61 %	33.145	http://www.digicert.com/	Lindon, Utah, USA
10.	Firstserver	1,52%	31.235	http://www.fsv.jp/	Jepang
-	Provider lain	5,75%	118.120	-	-
-	Unknown	15,02%	308.715	-	-

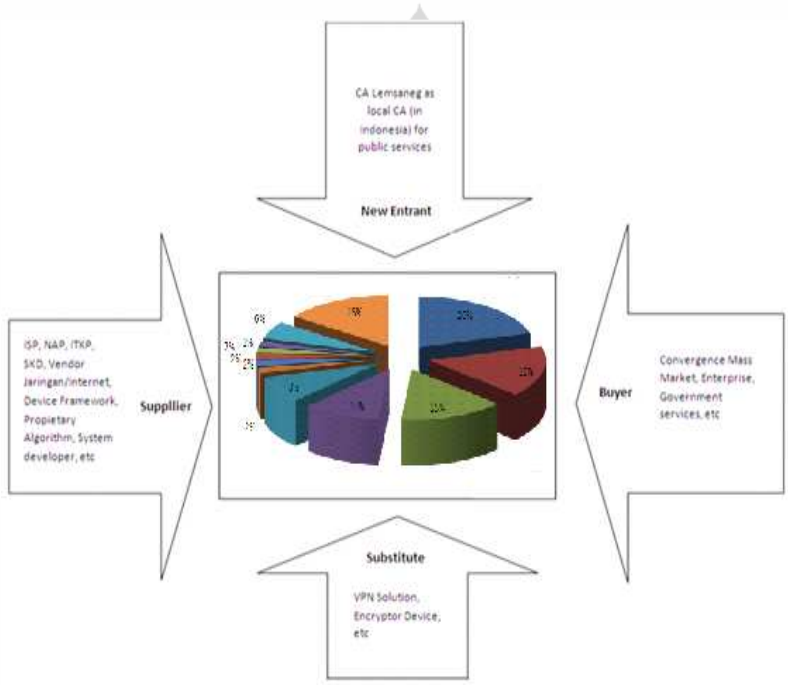
Sebagai pihak ketiga dalam setiap transaksi elektronik sebuah layanan CA harus bersifat hadir mendunia (*global presence*). Pada Lampiran 1 ditunjukan daftar perusahaan-perusahaan penyedia jasa CA yang ada didunia. Komposisi *market share* layanan keamanan CA hingga tahun 2010 diseluruh dunia diperlihatkan pada Gambar 3.2.



Gambar 3.2. Market Share Layanan CA [28]

Pada Gambar 3.2 tersebut memperlihatkan 10 besar perusahaan/organisasi layanan CA diseluruh dunia. Pada Lampiran 2 diperlihatkan detail peringkat total market share pada 10 penyedia jasa keamanan CA didunia.

Sampai akhir tahun 2009 layanan CA yang digunakan di Indonesia hanya beberapa perusahan besar penyedia layanan keamanan CA dari *market share* tersebut. Di Indonesia telah ada beberapa perusahaan penyedia jasa layanan CA meskipun hanya dalam internal organisasi, perusahaan atau regional tertentu.



Gambar 3.3. Peran di Industri Penyedia Layanan Keamanan CA

Setelah diketahui pemain dalam lingkungan industri penyedia layanan keamanan CA (Tabel 3.1), maka tahapan selanjutnya dari analisa kompetitif penyediaan layanan CA adalah pendefinisian peran sesuai model Porter 5 Forces pada Gambar 3.3. Pendefinisian peran dalam model Porter 5 Forces pada industri penyediaan layanan keamanan CA sesuai Gambar 3.3 dijabarkan sebagai berikut :

1. Pendatang Baru didefinisikan disini adalah penyedia layanan CA lokal (Indonesia) yang akan masuk dalam industri layanan keamanan berbasis IP di era konvergensi, dalam penulisan ini adalah penyediaan Layanan CA dari Lembaga Sandi Negara.

2. Produk Pengganti adalah layanan-layanan keamanan lain yang mungkin diterapkan pada lingkungan berbasis IP seperti Solusi *Virtual Private Network* (VPN), Peralatan Penyandi berbasis IP (*Encryptor Devices*). Meskipun dari sisi teknologi saat ini tidak ada solusi keamanan yang dapat disetarakan dengan sistem keamanan seperti pada layanan CA.
3. Pembeli adalah pelanggan yang menjadi target dan segmen pengguna jasa keamanan CA, dalam hal ini adalah pengguna transaksi elektronik di dalam/luar negeri yang akan bertransaksi di era konvergensi nantinya. Pengguna dapat berupa individu, organisasi, komunitas atau korporasi diberbagai bidang yang membutuhkan transaksi secara elektronik.
4. Pemasok adalah vendor penyedia perangkat hardware/software, konten, penyedia aplikasi CA, pembuat dan sertifikasi algoritma, penerbit alat pembayaran di sisi pelanggan maupun penyedia jasa.
5. Persaingan antar pesaing industri disini adalah persaingan antar penyedia jasa layanan CA.

3.2.2. Identifikasi Faktor Tekanan

Pada analisa potensi kompetitif penyediaan layanan CA akan dibahas setiap variabel dan indikator-indikator spesifik terkait yang berpengaruh menjadi sumber tekanan dalam industri penyediaan layanan keamanan di era konvergensi. Pada Tabel 3.2 berikut diberikan variabel dan indikator tekanan model Porter 5 Forces.

Tabel 3.2 Variabel dan Indikator Sumber Tekanan model Porter 5 Forces

1. Ancaman Pendatang Baru (*Treat of New Entrant*)		
No. Variabel	**Variabel**	**Indikator**
1.1	Skala Ekonomi	Layanan CA dilakukan dalam skala relatif besar (global)
1.2	Differensiasi Produk (yang ditawarkan oleh Pendatang Baru)	Produk dari Pesaing tidak memiliki diferensiasi produk (dalam hal propietary algorithm)
1.3	Identitas Merk Produk	layanan CA Lemsaneg (CA lokal Indonesia) belum memiliki identitas merk layanan CA dalam cakupan nasional dan Global kepada publik

1.4	Biaya Investasi (untuk Modal Produksi)	Biaya investasi untuk sebuah keamanan sangat tinggi, salah satunya adalah litbang dalam hal sistem pengamanan yang akan digunakan
1.5	Biaya Beralih Pemasok (bagi Pendatang baru)	Biaya beralih pemasok tinggi untuk penyediaan algoritma dan sistem pengamanan/penyandian
1.6	Akses ke Saluran Distribusi	Lemsaneg telah memiliki saluran distribusi layanan CA (dalam negeri dan luar negeri)
		lemsaneg belum memiliki strategic Partner untuk aktifasi layanan CA ke publik
1.7	Kebijakan Pemerintah	Pemerintah mendukung berkembangnya CA sebagai Pihak Ketiga dalam setiap transaksi elektronik melalui UU ITE, UU penyelenggaraan CA dan RUU Pengawasan Badan CA
2. Ancaman Produk Pengganti (*Treat of Substitute*)		
No. Variabel	**Variabel**	**Indikator**
2.1	Produk Pengganti	Saat ini tidak Ada produk pengganti setara dengan sistem keamanan layanan CA (dalam hal cakupan keamanan dan integrasi manajemen didalamnya), namun ada alternatif pengamanan berbasis IP
2.2	Layanan Produk Pengganti	Terdapat fitur layanan Produk Pengganti hampir sama (dalam hal *user interface*) tetapi tidak selengkap layanan CA
2.3	Tarif Produk Pengganti	Produk pengganti tidak lebih murah
2.4	Kualitas Produk Pengganti	Kualitas produk pengganti tidak lebih baik dari solusi keamann layanan CA
2.5	Ketersediaan Produk Pengganti	Meski tidak selengkap solusi keamanan CA, Produk Pengganti relatif lebih mudah didapat dari solusi CA
2.6	Proses Aktifasi	Produk Pengganti relatif lebih praktis (dalam hal aktifasi)
2.7	Biaya Beralih Pemasok (ke Produk Pengganti)	Produk pengganti membutuhkan *switching cost* yang tinggi
2.8	Loyalitas Pelanggan	Pelanggan dapat "diwajibkan" menggunakan CA (sesuai UU ITE) dan tingginya kebutuhan di era konvergensi
3. Kekuatan Tawar Menawar Pembeli *(Bargaining Power of Buyer)*		
No. Variabel	**Variabel**	**Indikator**
3.1	Pembeli Terpusat	Pembelian produk dilakukan oleh kelompok pembeli dalam area global (konvergen)
3.2	Kapasitas Pembelian	Pembelian Produk layanan CA merupakan pengeluaran yang relatif diperlukan (penting bagi pembeli) dan besar sehingga pembeli akan lebih selektif

3.3	Differensiasi Produk (bagi Pembeli)	Produk yang dibeli adalah produk terdifferensiasi, sesuai kebutuhan dari sisi fitur, algoritma dan lain-lain.
3.4	Biaya Beralih ke Pemasok (bagi Pembeli)	Biaya beralih pemasok rendah
3.5	Orientasi Biaya	Pembeli cenderung tidak menekan biaya untuk kebutuhan keamanan
3.6	Integrasi Balik (Integrasi Kebelakang)	Pembeli tidak (kecil kemungkinan) melakukan integrasi balik
3.7	Kualitas Produk (bagi Pembeli)	Kualitas Produk industri keamanan layanan CA mempengaruhi kualitas produk atau jasa dari pembeli
3.8	Informasi tentang Produk	Pembeli memiliki informasi yang lengkap tentang produk yang akan dibeli
4.Kekuatan Tawar Menawar Pemasok (*Bargaining Power of Supplier*)		
No. Variabel	**Variabel**	**Indikator**
4.1	Dominasi Pemasok	Pemasok perangkat layanan tidak didominasi oleh beberapa perusahaan terpusat,
		Penyedia algoritma dan sistem pengamanan didominasi terpusat
4.2	Produk Pengganti	Terdapat produk pemasok pengganti untuk beberapa komponen CA
4.3	Pasar Pemasok	Industri layanan keamanan berbasis IP merupakan pasar potensial yang penting bagi kelompok pemasok
4.4	Kualitas Produk (dari Pemasok)	Kualitas produk pemasok sangat penting bagi operator jasa layanan CA
4.5	Integrasi Maju (Integrasi Ke Depan)	Pemasok tidak (kecil kemungkinan) melakukan integrasi maju
4.6	Kebijakan Pemerintah (bagi Pemasok)	Pemerintah mendukung masuknya pemasok, misal dalam RUU konvergensi dan program yang disediakan untuk membangun pemasok di era konvergensi
5.Persaingan Antara Perusahaan Eksisting (*Rivalry Among Competitor*)		
No. Variabel	**Variabel**	**Indikator**
5.1	Jumlah dan Ragam Pesaing	Jumlah Pesaing yang seimbang
		Pesaing dalam indutri keamanan yang beragam
5.2	Pertumbuhan Industri	Pertumbuhan industri yang pesat
5.3	Diferensiasi Produk (dalam Persaingan Industri)	Kurangnya Differensiasi produk (dalam hal algoritma), Layanan CA yang ada saat ini menggunakan algoritma standar.
5.4	Penambahan Kapasitas	Penambahan kapasitas dalam jumlah besar dan selalu dibutuhkan proses pembaruan (update)

		untuk komponen layanan keamanan CA
5.6	Hambatan Pengunduran Diri	Hambatan pengunduran diri dari industri tinggi, akibat tingginya investasi dan permintaan yang tinggi

Asumsi pembobotan yang digunakan untuk membantu menganalisis indikator dari setiap variabel adalah sebagai berikut [25] :

a) Untuk kesesuaian indikator-indikator dengan industri penyedia jasa keamanan yang dapat diaplikasi di era konvergensi, dimana hasilnya adalah :

   0 : apabila tidak sesuai dengan kondisi indikator

   1 : apabila sesuai dengan kondisi indikator

b) Untuk pembobotan tekanan, prosentase dari angka 1 terhadap keseluruhan menyatakan nilai kuantitatif dari tekanan yang ada pada satu sumber tekanan, kemudian hasilnya diklasifikasikan menjadi tiga, yaitu :

   - Rendah (*low)* : 0 – 33.33%
   - Sedang (*Medium*) : 33.34%– 66.66%
   - Tinggi (*High*) : 66.67%– 100%

Dari hasil identifikasi dan pembobotan tekanan setiap variabel dalam Porter 5 Forces, dilakukan penggambaran secara visual dari hasil analisa setiap tekanan yang ada dalam industri penyediaan layanan keamanan CA di era konvergensi.

3.2.3. Analisa

3.3.6. Tekanan Pendatang Baru

Analisis Ancaman pendatang baru ditujukan untuk melihat kemungkinan sebuah perusahaan baru untuk masuk kedalam industri, apakah ada penghalang masuk (*entry barrier*) ataupun reaksi dari pesaing yang sudah eksisting. Keberadaan pendatang baru dengan maksud untuk memperoleh keuntungan dan porsi pasar (*market share*), akan menambah tingkat kompetisi dalam suatu industri karena keberadaannya dapat memaksa terjadinya penurunan harga dan

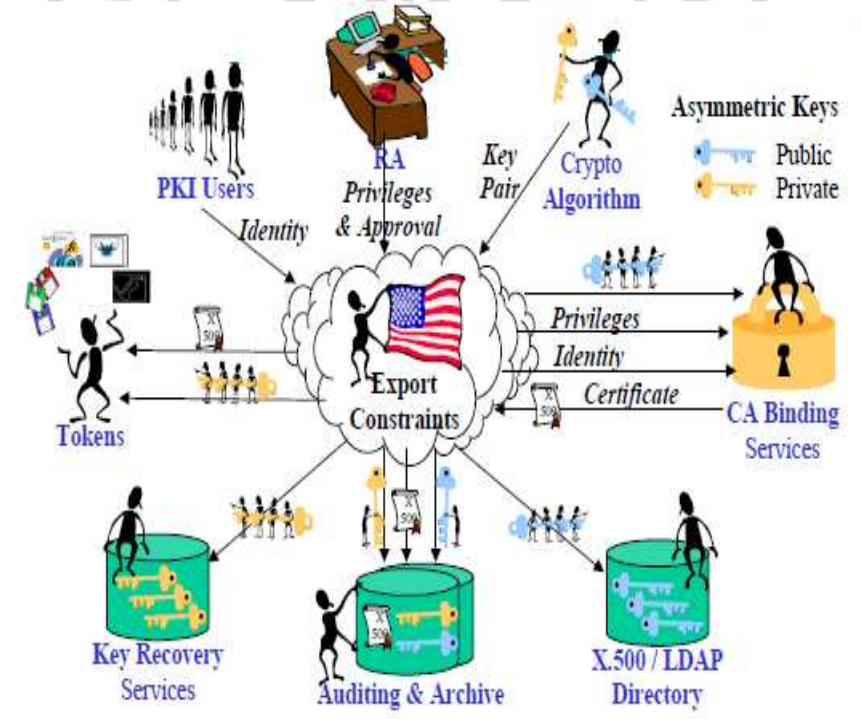
menimbulkan tekanan terhadap keuntungan. Besarnya ancaman pendatang baru ke dalam suatu industri tergantung pada situasi dari variabel sumber tekanan berikut :

3.3.1.8. Skala Ekonomi

Jika dibutuhkan skala ekonomi besar untuk dapat masuk ke pasar yang sama, maka pesaing baru akan diperhadapkan pada situasi yang tidak menguntungkan ketika pesaing baru tersebut harus mempersiapkan produknya dalam skala volume besar, dibandingkan pesaing yang sudah eksisting di area layanan yang sama.

Kondisi :

Lemsaneg merupakan pendatang baru dalam industri layanan keamanan CA, lemsaneg harus mempersiapkan produk dalam volume nasional/global, maka tekanan produk CA Lemsaneg kepada pesaing eksisting rendah.



Gambar 3.4. Komponen Layanan CA bagi Pendatang Baru [29]

Pada Gambar 3.4 diperlihatkan komponen yang harus dipenuhi oleh pendatang baru yang akan menyediakan jasa CA bagi pendatang baru seperti Lembaga Sandi Negara. Pada pelaksanaan pengelolaan keamanan (*Security Management Practices*) diperlukan komponen-komponen berikut [30] :

a. Sistem dan Metodologi Pengendalian Akses (*Access Control Systems and Methodology*).
b. Keamanan Telekomunikasi dan Jaringan (*Telecommunications and Network Security*).
c. Kriptografi (*Cryptography*).
d. Model dan Arsitektur Keamanan (*Security Architecture & Models*).
e. Keamanan Pengoperasian (*Operations Security*).
f. Keamanan Aplikasi dan Pengembangan Sistem (*Application and Systems Development Security*).
g. Rencana Kesinambungan Usaha dan Pemulihan Bencana (*Disaster Recovery and Business Continuity Plan - DRP/BCP*).
h. Hukum, Investigasi, dan Etika (*Laws,Investigations and Ethics*).
i. Keamanan Fisik (*Physical Security*).
j. Audit (*Auditing*).

Pada Lampiran 3 diberikan salah satu contoh project pembangunan CA. Akibat banyaknya komponen dan besarnya biaya investasi yang harus diperhatikan serta tuntutan bahwa layanan ini harus bersifat mendunia (*global presence*), penilaian untuk parameter ini adalah 0 (nol).

3.3.1.9. Diferensiasi Produk (yang ditawarkan Pendatang Baru)

Pendatang baru akan mengalami kesulitan untuk meraih target pasar jika produk pesaing eksisting sudah memiliki diferensiasi produk yang variatif, hal ini membuat pendatang baru mengeluarkan biaya yang besar untuk menciptakan differensiasi produk/jasa untuk mendapatkan kepercayaan pelanggan.

Kondisi :

Dalam layanan CA terdapat beberapa nilai differensiasi pada sisi pelaksanaan pengelolaan keamanan, contohnya adalah algoritma yang digunakan apakah kuat dan dapat dipercaya, fitur kompatibitas browser yang digunakan oleh pengguna, fitur pilihan cakupan jasa (misal pendaftaran layanan,dll), level validitas, ada tidaknya aplikasi gratis sebelum berlangganan produk jasa. Contoh differensiasi produk yang ditawarkan diperlihatkan pada Lampiran 6.

Produk eksisting di industri layanan CA yang ada di Indonesia, dari sisi algoritma tidak terdifferensiasi, layanan CA yang digunakan di Indonesia hanya terdaftar dan berada di Luar Negeri. Bila Lemsaneg tampil sebagai CA lokal di Indonesia dan memiliki sistem pengamanan yang *propietary* akan memberikan tekanan yang kuat pada produk pesaing, dari informasi ini maka nilai untuk parameter ini adalah 1 (satu).

3.3.1.10. Identitas Merk Produk

Pesaing baru akan sulit bersaing jika belum memiliki produk layanan sejenis ataupun yang lainnya yang sudah eksis ataupun memiliki reputasi keunggulan pada industri sejenis ataupun industri lainnya, sehingga memerlukan biaya tambahan yang besar untuk advertising dan aktifitas promosi lainnya.

Kondisi :

Produk yang dihasilkan oleh beberapa perusahaan eksisting sudah dikenal oleh masyarakat pengguna transaksi elektronik dan memiliki penilaian yang baik sehingga relatif lebih mudah diterima. Lemsaneg meskipun telah berkiprah di layanan keamanan (dalam jangka waktu relatif lama) namun belum memberikan layanan ini kepada publik secara langsung sehingga relatif akan membutuhkan strategi yang baik untuk membuat identitas dikenal secara luas. Untuk bisa diterima tidak hanya didalam negeri, selain strategi marketing yang baik, penyedia jasa layanan

CA harus memenuhi standar internasional. seperti diperlihatkan pada Gambar 3.5.

Gambar 3.5 Standar Layanan Keamanan [31][32]

Dari informasi ini maka nilai untuk parameter Identitas Merk Produk adalah 0 (nol).

3.3.1.11. Biaya Investasi (untuk Modal Produksi)

Semakin besar biaya investasi yang dibutuhkan oleh pesaing baru untuk bisa masuk kedalam pasar yang sama, maka semakin kecil peluang bagi pesaing baru untuk dapat menjadi ancaman bagi pemain eksisting di industri.

Kondisi :

Indikator pada variabel biaya investasi adalah besarnya investasi yang dibutuhkan untuk membuat pengelolaan layanan keamanan CA. Dilihat dari sistem yang diperlukan untuk membangun sebuah CA, maka penilaian untuk parameter ini adalah 0(nol), karena Lemsaneg sebagai

pendatang baru membutuhkan investasi yang besar sehingga relatif tidak memberikan tekanan yang kuat pada pesaing eksisting.

3.3.1.12. Biaya Beralih ke Pemasok (bagi Pendatang Baru)

Semakin rendah biaya beralih pemasok, maka semakin mudah pembeli untuk berpindah dengan demikian meningkatkan ancaman masuknya pendatang baru dalam industri.

Kondisi :

Pada industri penyediaan layanan CA, biaya beralih pemasok bagi penyedia jasa layanan CA tinggi. Pada industri layanan keamanan CA, untuk membentuk layanan ini dibutuhkan pemasok atau penyedia jasa seperti :

a. Penyedia Jasa Jaringan, Intranet, Internet (ISP, NAP, ITKP)
b. Aplikasi /Konten Browser
c. Sofftware Aplikasi CA atau VPN
d. Algoritma Penyandian, Algoritma Sistem, *Key Generator, Key Management System*
e. System Developer , Server, Database

Layanan keamanan CA merupakan layanan yang sangat bergantung pada kualitas jaringan pemasok dan pemasok algoritma atau sistem pengamanan. Pemasok sistem pengamanan sangat jarang dan dibutuhkan penelitian dan pengembangan dalam hal pengamanan informasii. Semakin tinggi biaya beralih pemasok, maka semakin tidak mudah untuk berpindah pemasok, dengan demikian menurunkan ancaman masuknya layanan CA lokal di industri ini, dengan demikian nilai untuk variabel ini adalah 0 (nol).

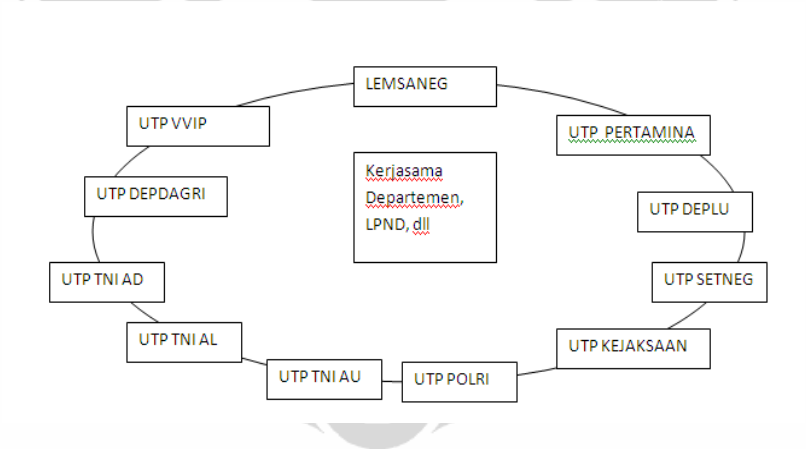
3.3.1.13. Akses ke Saluran Distribusi

Apabila pendatang baru memiliki kemudahan akses ke saluran distribusi pemasok dan akses distribusi ke pembeli, maka produk dari pendatang baru akan memiliki kekuatan tinggi untuk menekan pesaingnya.

Kondisi :

Apabila pendatang baru seperti Lemsaneg memiliki kemudahan akses ke saluran distribusi pemasok dan akses distribusi ke pembeli, maka produk layanan CA baru dari Lemsaneg akan memiliki kekuatan tinggi untuk menekan pesaingnya.

Terdapat 2 parameter yang diperhatikan, yaitu Lemsaneg telah memiliki akses distribusi ke daerah ataupun perwakilan luar negeri melalui setiap unit tehnis persandian (UTP). Pada Gambar 3.6 berikut diperlihatkan secara umum unit tehnis persandian.



Gambar 3.6 Unit Tehnis Persandian [23]

Namun Lemsaneg belum memiliki *strategic partner* untuk mendistribusikan layanan CA langsung ke publik. *Strategic partner* adalah potensial partner untuk dijadikan saluran pendistribusi layanan yang akan dibuat.

Dengan demikian penilaian untuk parameter ini adalah 1 (satu) untuk adanya akses distribusi di Indonesia dan di Luar Negeri, namun

bernilai 0 (nol) untuk belum adanya *strategic partner* yang dapat memudahkan akses distribusi ke publik secara langsung.

3.3.1.14. Kebijakan Pemerintah

Apabila pemerintah mengeluarkan regulasi untuk mendukung masuk dan berkembangnya penyedia jasa dalam industri dan tidak membatasi area kerja maka akan meningkatkan ancaman masuknya pendatang baru.

Kondisi :

Pemerintah mendukung berkembangnya transaksi elektronik dan penyediaan layanan keamanan CA sebagai Pihak Ketiga dalam setiap transaksi elektronik melalui Undang-undang Republik Indonesia nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

UU ITE memiliki azas kepastian hukum, manfaat, kehati-hatian, itikad baik dan netral teknologi. Beberapa tujuan dibuatnya Undang-undang ini adalah untuk mengembangkan perdagangan dan perekonomian, meningkatkan efektifitas & efisiensi pelayanan publik serta memberikan rasa aman, keadilan dan kepastian hukum. Pada Tabel 3.3 Berikut diperlihatkan beberapa pasal yang mendukung untuk penyediaan layanan CA di Indonesia.

Tabel 3.3 Pasal-pasal Kebijakan Pemerintah dalam layanan CA [33]

Pasal	Ayat	Isi
9		Pelaku usaha yang menawarkan produk melalui sistem elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen dan produk yang ditawarkan.
10	1	Setiap Pelaku usaha yang menyelenggarakan Transaksi elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan.
11	1	Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan
12	1	Setiap orang yang terlibat dalam tanda tangan elektronik

		berkewajiban memberikan pengamanan atas tanda tangan elektronik yang digunakan.
13	1	Setiap orang berhak menggunakan jasa penyelenggara sertifikasi elektronik untuk pembuatan tanda tangan elektronik.
13	2	Penyelenggara sertifikasi elektronik harus memastikan keterkaitan suatu tanda tangan elektronik dengan pemiliknya
13	3	Penyelenggara elektronik terdiri atas : Penyelenggara Sertifikasi Elektronik Indonesia dan Penyelenggara Sertifikasi Elektronik Asing.
13	4	Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.
13	5	Penyelenggara Sertifikasi Elektronik Asing yang beroperasi di Indonesia harus terdaftar di Indonesia.
14		Penyelenggara sertifikasi Elektronik harus menyediakan informasi yang akurat, jelas dan pasti kepada setiap pengguna jasa.
18	1	Transaksi Elektronik yang dituangkan kedalam kontrak elektronik mengikat para pihak.
18	4	Para pihak memiliki kewenangan untuk menetapkan forum pengadilan, arbitrase atau lembaga penyelesaiann sengketa alternative lainnya yang berwenang menangani sengketa yang mungkin timbul dari transaksi elektronik internasional yang dibuatnya.
18	5	Jika tidak melakukan pemilihian seperti pada pasal 18 ayat 4 tersebut, penyelesaian sengketa didasarkan pada Hukum Perdata Internasional

Dalam UU ITE dibahas mengenai Informasi, Dokumen dan Tanda Tangan Elektronik pada Bab 3, Penyelenggaraan Sertifikasi Elektronik pada Bab 4 dan Bab 5 mengenai Sistem Elektronik. Dalam undang-undang ini dibahas bahwa penyelenggara sistem elektronik wajib menyediakan informasi yang akurat, jelas dan pasti serta mengatur hak setiap orang dalam menggunakan jasa layanan CA. selain UU ITE, pemerintah juga mengeluarkan peraturan pemerintah mengenai penyelenggaraan CA dan peraturan menteri mengenai Badan Pengawas CA. Dengan informasi ini, maka nilai asumsi parameter bernilai 1 (satu).

Dari hasil perhitungan setiap variabel dalam Tekanan Pendatang Baru didapatkan hasil dalam skala medium (37,5%), seperti terlihat pada Tabel 3.4 berikut.

Tabel 3.4. Hasil Penilaian Variabel Tekanan Pendatang Baru

i. Ancaman Pendatang Baru (*Treat of New Entrant*) ii.			
No. Variabel	**Variabel**	**Indikator**	**Nilai**
1.1	Skala Ekonomi	Layanan CA dilakukan dalam skala relatif besar (global)	0
1.2	Differensiasi Produk (yang ditawarkan oleh Pendatang Baru)	Produk dari Pesaing tidak memiliki diferensiasi produk (dalam hal propietary algorithm)	1
1.3	Identitas Merk Produk	layanan CA Lemsaneg (CA lokal Indonesia) belum memiliki identitas merk layanan CA dalam cakupan nasional dan Global kepada publik	0
1.4	Biaya Investasi (untuk Modal Produksi)	Biaya investasi untuk sebuah keamanan sangat tinggi, salah satunya adalah litbang dalam hal sistem pengamanan yang akan digunakan	0
1.5	Biaya Beralih Pemasok (bagi Pendatang baru)	Biaya beralih pemasok tinggi untuk penyediaan algoritma dan sistem pengamanan/penyandian	0
1.6	Akses ke Saluran Distribusi	Lemsaneg telah memiliki saluran distribusi layanan CA (dalam negeri dan luar negeri)	1
		lemsaneg belum memiliki strategic Partner untuk aktifasi layanan CA ke publik	0
1.7	Kebijakan Pemerintah	Pemerintah mendukung berkembangnya CA sebagai Pihak Ketiga dalam setiap transaksi elektronik melalui UU ITE, UU penyelenggaraan CA dan RUU Pengawasan Badan CA	1
			37.50%

3.3.7. Ancaman Produk Pengganti

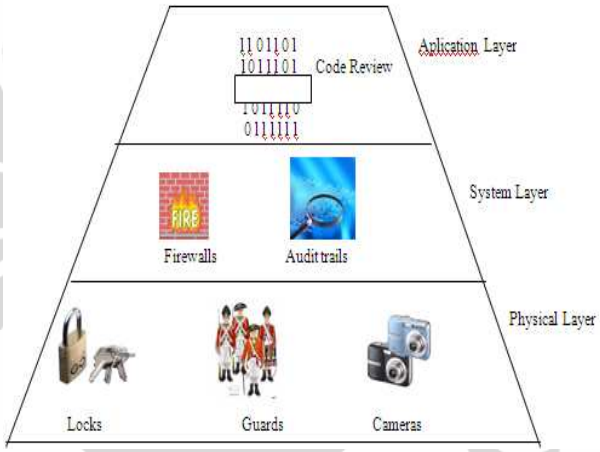
Produk atau jasa pengganti dapat memberikan batasan terhadap potensi keuntungan suatu industri. Ancaman dari produk pengganti akan dipengaruhi keberadaan variabel sumber tekanan sebagai berikut :

3.3.2.9. Produk Pengganti

Adanya produk pengganti yang akan membatasi jumlah laba potensial yang didapat dari suatu industri.

Kondisi :

Apabila ada produk pengganti bagi layanan CA yang akan disediakan oleh Lemsaneg, maka akan mengurangi laba/nilai. Keamanan didesain sesuai lapisan yang akan diamankan, seperti terlihat pada Gambar 3.6 berikut.

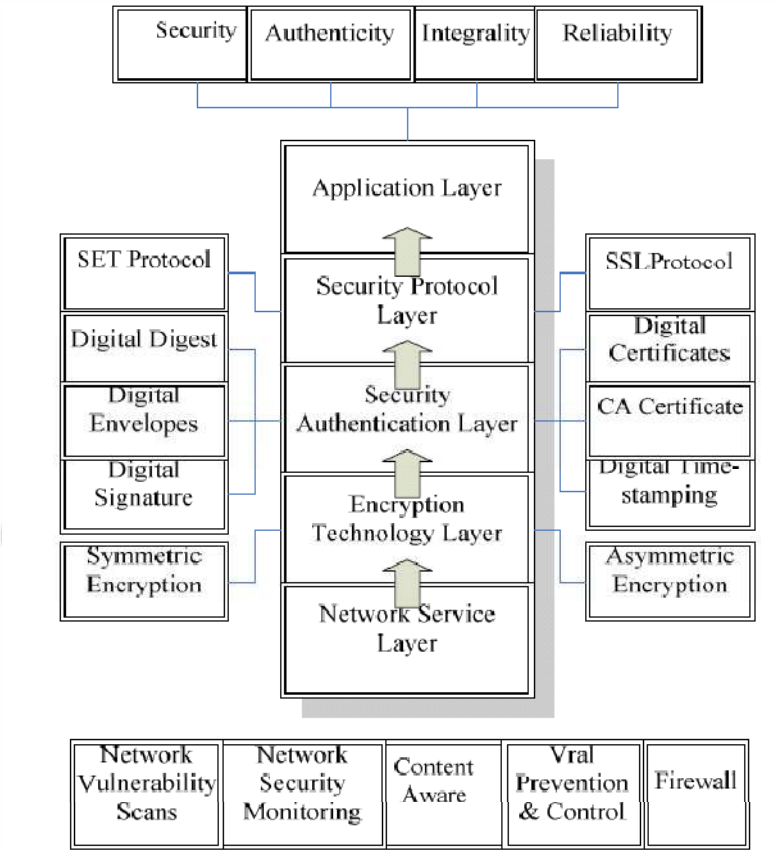


Gambar 3.6. Lapisan Keamanan [34]

Pengamanan pada era konvergensi akan diberikan pada layer Aplikasi, pada lapisan ini pengamanan yang dilakukan berupa kode-kode yang menyamarkan data yang dikirim. Menyamarkan data dengan menggunakan metode penyandian secara matematis atau kode dapat dilakukan menggunakan aplikasi software maupun dengan menggunakan perangkat khusus seperti alat penyandi data. Namun kebutuhan diera konvergensi tidak hanya bergantung pada sistem pengamanan tunggal tetapi membutuhan sebuah sistem untuk selalu mengupdate metode dan kunci yang dilakukan untuk menyamarkan data.

Saat ini tidak ada solusi yang sama tingkatnya dengan yang diberikan layanan keamanan CA. beberapa solusi yang serupa dapat berjalan dalam platform IP adalah *Virtual Private Network* (VPN) atau menggunakan alat penyandi berbasis IP (*encryptor devices*). Namun dalam

beberapa kondisi layanan keamanan ini hanya mampu menjadi solusi dalam sebuah *closed network*. Pada Gambar 3.7 Diperlihatkan lapisan-lapisan keamanan dalam sebuah teknologi pengamanan berbasis Internet Protokol, pada era konvergensi.



Gambar 3.7. Keamanan dalam Platform IP Network [35]

Dari informasi ini didapatkan nilai asumsi adalah 0 (nol) untuk parameter produk pengganti.

3.3.2.10. Layanan Produk Pengganti

Layanan yang ditawarkan perusahaan tidak memiliki benefit yang riil bagi pelanggan dibandingkan dengan produk pengganti yang ditawarkan pesaing.

Kondisi :

Apabila produk pengganti memiliki fitur layanan yang sama dengan fitur layanan CA lokal bahkan lebih lengkap, maka tekanan dari produk pengganti terrsebut akan kuat dalam industri Penyedia Jasa CA.

Produk pengganti seperti VPN atau alat penyandi memiliki fitur tampilan (*graphic user interface*) layanan yang hampir sama untuk pengamanan dengan menggunakan algoritma kriptografi dalam pengiriman data berbasis IP. Namun dalam layanan CA tidak hanya mengatur penyandian data yang dikirim tetapi juga mengatur dan memperbaharui seluruh dimensi keamanan yang diperlukan serta memberikan layanan interkoneksi yang diperlukan penggunanya. Dari informasi ini didapatkan nilai variabel tekanan dari produk pengganti tidak kuat atau bernilai 0 (nol).

3.3.2.11. Tarif Produk Pengganti

Makin menarik alternatif harga yang ditawarkan oleh produk pengganti, makin ketat pembatasan laba dari suatu industri.

Kondisi :

Jika produk pengganti bagi pengguna transaksi elektronik lebih murah dari apa yang ditawarkan maka variabel persaingan tarif dari ancaman produk pengganti akan memiliki tekanan yang kuat. Harga yang harus dibayar untuk produk pengganti layanan CA seperti perangkat penyandi berbasis IP lebih tinggi dibandingkan dengan menjadi pelanggan layanan CA. Dari informasi ini didapatkan nilai untuk parameter ini adalah 0 (nol).

3.3.2.12. Kualitas Produk Pengganti

Produk pengganti yang perlu mendapatkan perhatian besar adalah produk yang mempunyai kecenderungan untuk memiliki harga atau

kualitas yang lebih baik daripada produk industri atau dihasilkan oleh industri yang berlaba tinggi. Apabila kualitas produk pengganti ditawarkan lebih baik daripada produk industri akan menimbulkan tekanan yang kuat.

Kondisi :

Pada Tabel 3.5 berikut diberikan perbandingan antara layanan CA, VPN dan alat penyandi data.

Tabel 3.5. Perbandingan Kualitas Produk Pengganti

Variabel Pembanding	**Layanan CA**	**VPN solution**	**Alat Penyandi (IP Encryptor)**
Cakupan Dimensi Keamanan	✓ *Access Control* (Pengendali Akses) ✓ *Authetication* (Autentikasi) ✓ *Non Repudiation* (Nir-Sangkal) ✓ *Confidential* (Konfidensialitas) ✓ *Keamanan dalam berkomunikasi (Communication Security)* ✓ *Integrity* (Integritas) ✓ *Availability* (Ketersediaan) ✓ *Privacy*	✓ *Access Control* (Pengendali Akses) ✓ *Confidential* (Konfidensialitas) ✓ *Keamanan dalam berkomunikasi (Communication Security)* ✓ *Privacy*	✓ *Access Control* (Pengendali Akses) ✓ *Confidential* (Konfidensialitas) ✓ *Keamanan dalam berkomunikasi (Communication Security)* ✓ *Privacy*
Sifat Layanan	Memanage pertukaran kunci,	Memberikan semacam tunnel	Sebagai alat penyandi data

	penyandian informasi, update seluruh parameter keamanan sebelum data dikirimkan melalui media intranet atau internet.	yang aman pada platform internet atau intranet. Memiliki Paket Class of Services (CoS) berdasarkan media akses dan kecepatan data.	sebelum data dikirimkan melalui platform intranet atau internet.
Proses Aktifasi (bagi penyedia jasa)	Sangat Kompleks	Kompleks	Sederhana
Proses Aktifasi /Penggunaan (bagi pengguna)	Sederhana	Sederhana	Sederhana
Ketersediaan Produk	Mudah Didapat	Mudah Didapat	Lebih Sulit Didapat

Dari informasi ini didapatkan nilai variabel kualitas produk pengganti adalah 0 (nol).

3.3.2.13. Ketersediaan Produk Pengganti

Faktor ketersediaan yaitu apabila produk pengganti mudah didapat dalam industri, maka akan meningkatkan tekanan yang diakibatkan dari kekuatan ancaman produk pengganti terhadap layanan baru yang akan dibuat.

Kondisi :

Apabila produk pengganti mudah didapat dalam industri, maka akan meningkatkan tekanan yang diakibatkan dari kekuatan ancaman produk pengganti terhadap CA lokal milik Lemsaneg. Sebuah solusi VPN dan alat penyandian relatif mudah dan sederhana karena menggunakan pengamanan tunggal, meski solusi yang ditawarkan tidak lebih baik dari

sifat sistem layanan terintegrasi layanan CA. Dari informasi pada Tabel 3.5 didapatkan nilai variabel ketersediaan produk pengganti adalah 1 (satu).

3.3.2.14. Proses Aktifasi

Apabila proses aktifasi dari produk pengganti cepat, maka ancaman produk pengganti akan kuat memberi tekanan kepada industri.

Kondisi :

Karena pada alternatif produk pengganti seperti VPN dan alat penyandi data hanya menggunakan pengamanan tunggal (tidak berupa manajemen yang kontinu), cakupan keamanan yang lebih sedikit dan lebih sederhana, produk pengganti relatif lebih praktis dalam hal aktifasi. Sesuai informasi dari Tabel 3.5 didapatkan nilai variabel adalah 1 (satu).

3.3.2.15. Biaya Beralih Pemasok (ke Produk Pengganti)

Biaya beralih pemasok (*switching cost*) rendah, sehingga pembeli mudah beralih ke produk pengganti. Apabila proses aktifasi dari produk pengganti cepat, maka ancaman produk pengganti akan kuat memberi tekanan kepada industri.

Kondisi :

Apabila Biaya beralih Pemasok dari sisi pembeli untuk beralih dari produk CA lokal ke produk pengganti rendah, maka ancaman produk ataupun jasa pengganti akan semakin tinggi. Bagi pembeli, untuk berganti ke produk seperti alat penyandi data ataupun membangun sebuah solusi VPN dibutuhkan biaya yang tinggi. Dari informasi ini didapatkan nilai asumsi adalah 0 (nol).

3.3.2.16. Loyalitas Pelanggan

Apabila loyalitas pelanggan sangat relatif dimana royalitas tersebut dapat berubah karena faktor situasional dan tingkat kebutuhan

untuk suatu periode tertentu, maka tekanan produk pengganti akan tinggi kepada industri.

Kondisi :

Penyediaan jasa layanan keamanan CA didukung oleh pemerintah dan menjadi kebutuhan pengguna transaksi elektronik di era konvergensi untuk bisa berkomunikasi/transaksi mendunia. Akibatnya pembeli nantinya seperti di"wajib"kan dan membutuhkan layanan CA sehingga pelanggan dan pengguna layanan CA akan sangat loyal. Tingginya ancaman dan tingginya kejahatan digital terhadap pengiriman data berbasis IP diperlihatkan pada lampiran 5, Hasil Monitoring IDSIRTI. Dari infomasi ini didapatkan nilai variabel loyalitas pelanggan adalah 0 (nol).

Dari hasil perhitungan setiap variabel dalam Ancaman Produk Pengganti didapatkan hasil tekanan pada industri yang rendah (25%), seperti terlihat pada Tabel 3.6 berikut.

Tabel 3.6. Hasil Penilaian Variabel Ancaman Produk Pengganti

2. Ancaman Produk Pengganti (*Treat of Substitute*)			
No. Variabel	**Variabel**	**Indikator**	**Nilai**
2.1	Produk Pengganti	Saat ini tidak Ada produk pengganti setara dengan sistem keamanan layanan CA (dalam hal cakupan keamanan dan integrasi manajemen didalamnya), namun ada alternatif pengamanan berbasis IP	0
2.2	Layanan Produk Pengganti	Terdapat fitur layanan Produk Pengganti hampir sama (dalam hal *user interface*) tetapi tidak selengkap layanan CA	0
2.3	Tarif Produk Pengganti	Produk pengganti tidak lebih murah	0
2.4	Kualitas Produk Pengganti	Kualitas produk pengganti tidak lebih baik dari solusi keamann layanan CA	0
2.5	Ketersediaan Produk Pengganti	Meski tidak selengkap solusi keamanan CA, Produk Pengganti relatif lebih	1

		mudah didapat dari solusi CA	
2.6	Proses Aktifasi	Produk Pengganti relatif lebih praktis (dalam hal aktifasi)	1
2.7	Biaya Beralih Pemasok (ke Produk Pengganti)	Produk Pengganti Membutuhkan Switching Cost yang tinggi	0
2.8	Loyalitas Pelanggan	Pelanggan dapat "diwajibkan" menggunakan CA (sesuai UU ITE) dan tingginya kebutuhan di era konvergensi	0
			25.00%

3.3.8. Kekuatan Tawar Menawar Pembeli

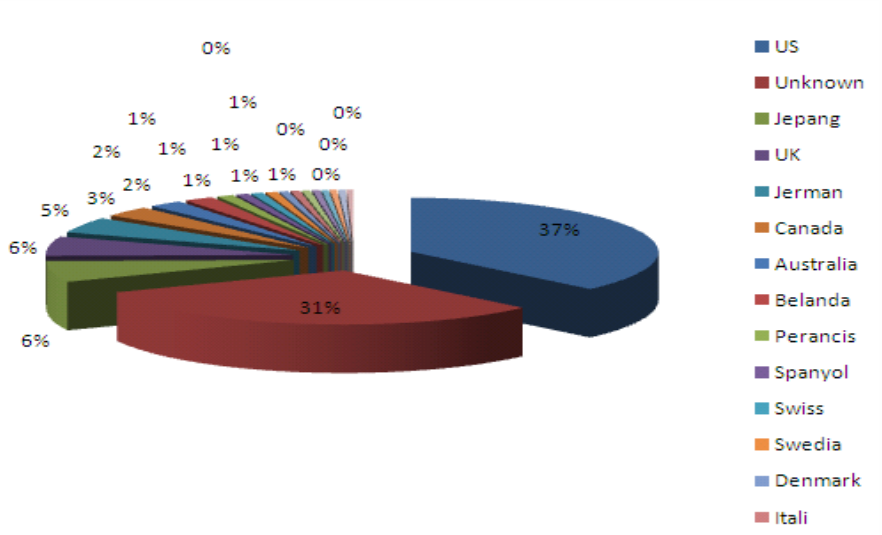
Analisis tekanan kekuatan tawar menawar pembeli menggambarkan pengaruh pembeli (pelanggan) terhadap keuntungan perusahaan. Daya tawar pembeli pada industri berperan dalam menekan harga untuk turun, serta memberikan penawaran dalam peningkatan kualitas ataupun layanan lebih dan memberikan kompetitor saling bersaing satu sama lain.

3.3.3.9. Pembeli Terpusat

Kelompok pembeli terpusat atau pembeli produk dalam jumlah besar sedangkan ada banyak pemasok yang mampu memenuhi produk yang diinginkan pembeli. Apabila industri didominasi oleh kelompok pembeli tertentu maka kekuatan tawar menawar dari pembeli akan mempunyai tekanan yang kuat kepada industri.

Kondisi :

Dalam industri penyediaan layanan CA, pembelian produk dilakukan oleh kelompok pembeli dalam area global (konvergen). Seperti terlihat pada Gambar 3.8 berikut, segmentasi pengguna layanan CA yang diambil dari salah satu survey penggunaan server yang terlindungi oleh aplikasi CA.



Gambar. 3.8 Segmentasi Pengguna Layanan CA

Pada gambar diatas grafik diambil dari 20 negara pengguna terbesar, dilihat dari jumlah server yang terlindungi oleh pengamanan. Penggunaan layanan keamanan untuk Indonesia berada pada peringkat ke 56 di dunia. Detail peringkat penggunaan layanan CA dapat dilihat pada Lampiran 4.

Pada industri layanan keamanan CA, pembelinya adalah pengguna transaksi elektronik individual, korporat, organisasi di seluruh dunia yang membutuhkan authentikasi ataupun identifikasi terhadap pihak-pihak bertransaksi yang ada didalam dan diluar negeri. Pada gambar Dari informasi ini didapatkan nilai asumsi parameter pembeli terpusat adalah 0 (nol).

3.3.3.10. Kapasitas Pembelian

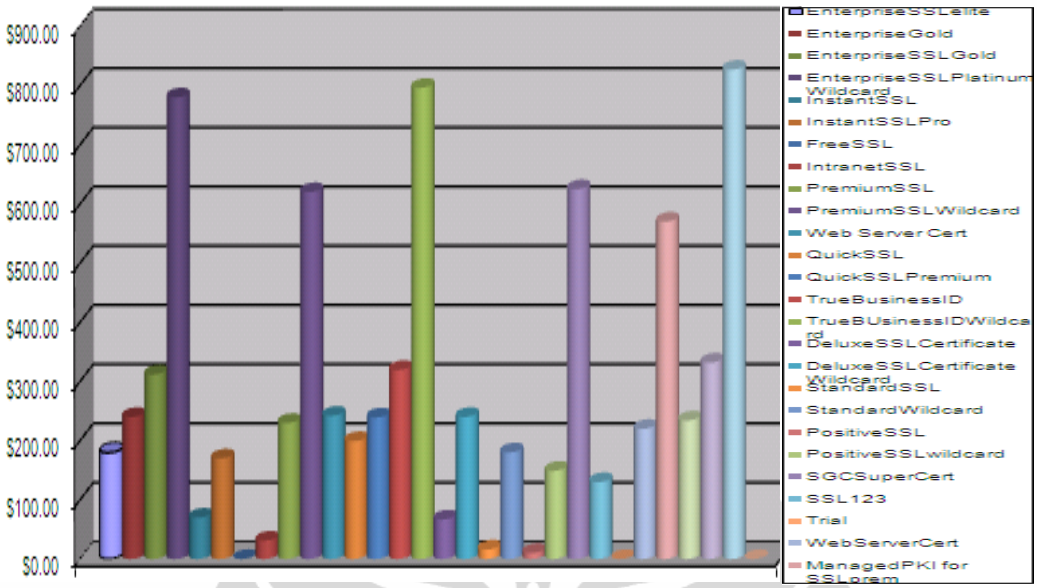
Produk yang dibeli dari suatu industri merupakan bagian yang signifikan dari biaya atau pembelian. Sehingga pembeli cenderung mencari harga yang menguntungkan dan menggunakan dananya untuk melakukan pembelian secara selektif. Apabila pembelian produk merupakan pengeluaran besar dari pembeli maka pembeli lebih selektif dalam menggunakan dananya, maka kekuatan tawar menawar dari pembeli akan mempunyai tekanan yang kuat kepada industri.

Kondisi :

Apabila pembelian produk merupakan pengeluaran besar dari pembeli maka pembeli lebih selektif dalam menggunakan dananya, akan didapatkan kekuatan tawar menawar dari pembeli akan mempunyai tekanan yag kuat kepada industri. Pada Tabel 3.7 dan Gambar 3.9 berikut diperlihatkan beberapa layanan dan biaya yang harus dikeluarkan oleh konsumen, biaya yang dikeluarkan relatif berkategori tinggi.

Tabel 3.7 Biaya Berlangganan Layanan Keamanan CA [36]

Provider	ProductName	Minimum Price (1 Year)	Browser Equity	Multi Year Option	Assurance (High/Low)
Codomo CA	EnterpriseSSLelite	$179.80	99%	5	High
	EnterpriseGold	$239.80	99%	5	High
	EnterpriseSSLGold	$311.80	99%	5	High
	EnterpriseSSLPlatinumWildcard	$779.80	99%	5	High
	InstantSSL	$69.80	99%	5	High
	InstantSSLPro	$169.80	99%	5	High
	FreeSSL	$0.00	99%	-	Low
	IntranetSSL	$31.00	99%	5	High
	PremiumSSL	$229.80	99%	5	High
	PremiumSSLWildcard	$619.80	99%	5	High
Entrust	Web Server Cert	$242.00	99%	4	High
Geotrust	QuickSSL	$199.20	99%	5	Low
	QuickSSLPremium	$239.20	99%	6	Low
	TrueBusinessID	$319.20	99%	5	High
	TrueBUsinessIDWildcard	$796.00	99%	5	High
GoDaddy	DeluxeSSLCertificate	$66.66	99%	3	High
	DeluxeSSLCertificateWildcard	$239.99	99%	3	High
	StandardSSL	$15.99	99%	10	Low
	StandardWildcard	$179.99	99%	10	Low
	PositiveSSL	$10.00	99%	10	Low
	PositiveSSLwildcard	$149.00	99%	10	Low
	SGCSuperCert	$624.75	99%	4	High
Thawte	SSL123	$129.80	99%	5	Low
	Trial	$0.00	99%	-	High
	WebServerCert	$219.80	99%	2	High
Verisign	ManagedPKI for SSLprem	$570.00	99%	2	High
	ManagedPKI for SSLstd	$234.00	99%	2	High
	Secure Site Cert	$331.67	99%	3	High
	Secure Site ProCert	$826.67	99%	3	High
	Trial	$0.00	99%	-	High



Gambar 3.9. Biaya Berlangganan Layanan CA [36]

Selain biaya tinggi, pembelian produk layanan CA merupakan pengeluaran yang relatif diperlukan/penting bagi pembeli. Dari informasi ini didapatkan nilai parameter kapasitas pembelian adalah 1 (satu), artinya pembeli akan semakin selektif menggunakan dana untuk pembelian layanan keamanan, sehingga memiliki tekanan yang kuat kepada industri layanan CA.

3.3.3.11. Differensiasi Produk (bagi Pembeli)

Apabila produk yang ditawarkan kepada pembeli tidak memiliki differensiasi, maka pembeli akan mudah mencari pemasok lain dalam industri dengan demikian menguatkan posisi tawar menawar pembeli.

Kondisi :

Contoh differensiasi produk dari sisi pembeli adalah dalam tingkat kemurahan harga, kompatibilitas dengan browser, instalasi yang relatif cepat dan sederhana, layanan pendukung yang cepat dan kualitas

layanan yang tinggi. Pada Gambar 3.10 berikut diperlihatkan macam-macam browser untuk interaksi transaksi elektronik.

Gambar 3.10. Browser Akses Layanan CA di Sisi Pengguna

Tidak hanya kompatibitas dengan browser pengguna, aspek lain untuk memberikan nilai tambah dan differensiasi produk pada layanan CA adalah kemampuan pelaksanaan pengelolaan keamanan yang handal, pada Lampiran 6 dan Lampiran 7 diperlihatkan contoh fitur differensiasi dan layanan-layanan CA. Dari informasi ini didapatkan nilai variabel adalah 1 (satu) karena pembeli dapat mencari layanan-layanan CA (yang terdifferensiasi dari sisi fitur layanan) sesuai kebutuhan.

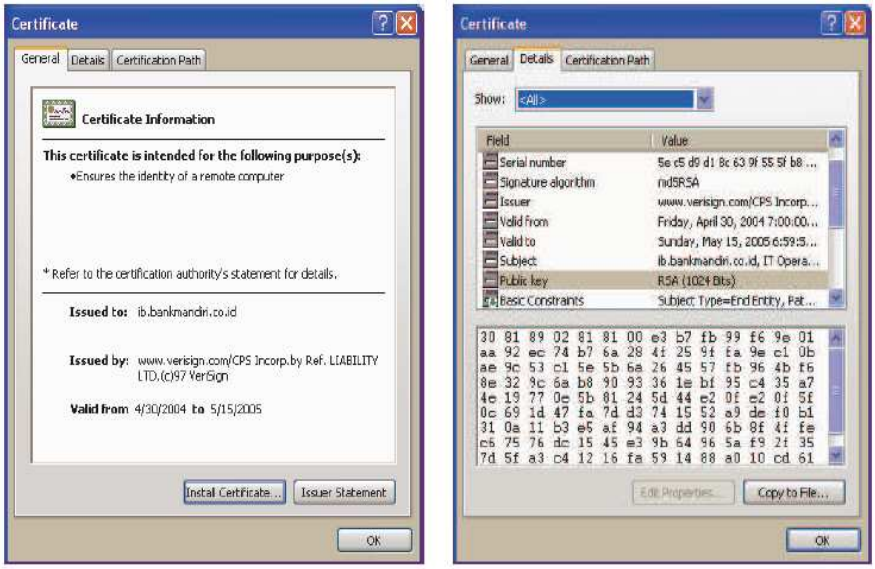
3.3.3.12. Biaya Beralih ke Pemasok (bagi Pembeli)

Pembeli menghadapi *switching cost* yang kecil, tidak ada biaya yang tertanam. Dengan biaya beralih pemasok yang rendah pembeli dapat berpindah operator jasa layanan keamanan dengan mudah, sehingga akan meningkatkan kekuatan penawaran pembeli.

Kondisi :

Dengan biaya beralih pemasok yang rendah pembeli dapat berpindah operator jasa layanan keamanan CA dengan mudah, sehingga akan meningkatkan kekuatan penawaran pembeli. Seperti diperlihatkan pada Gambar 3.9 Biaya Berlangganan Layanan CA, harga langganan sebuah layanan CA merupakan nilai yang cukup tinggi. Meski bernilai tinggi, jika pembeli akan berganti pemasok tidak diperlukan perangkat khusus untuk berganti pemasok layanan CA.

Biaya beralih ke Pemasok disisi pembeli relative rendah karena software *graphic user interface* layanan CA hanya berupa aplikasi software dan penggunaan browser seperti terlihat pada Gambar 3.11 berikut.



Gambar 3.11 Tampilan *Graphic User Interface* Aplikasi CA [37]

Dari informasi ini didapatkan nilai variabel Biaya beralih pemasok bagi pembeli adalah 1 (satu).

3.3.3.13. Orientasi Biaya

Pembeli yang berorientasi biaya, mendapatkan laba kecil. Laba yang rendah menimbulkan keinginan yang besar untuk menekan biaya. Apabila pembeli cenderung menekan biaya keamanan, maka kekuatan tawar menawar pembeli memiliki tekanan yang kuat kepada industri.

Kondisi :

Apabila pembeli cenderung menekan biaya layanan keamanan CA, maka kekuatan tawar menawar pembeli memiliki tekanan yang kuat kepada industri.

Di era konvergensi terdapat kebutuhan keamanan yang tinggi mengingat besarnya tingkat kejahatan pada layanan berbasis IP seperti

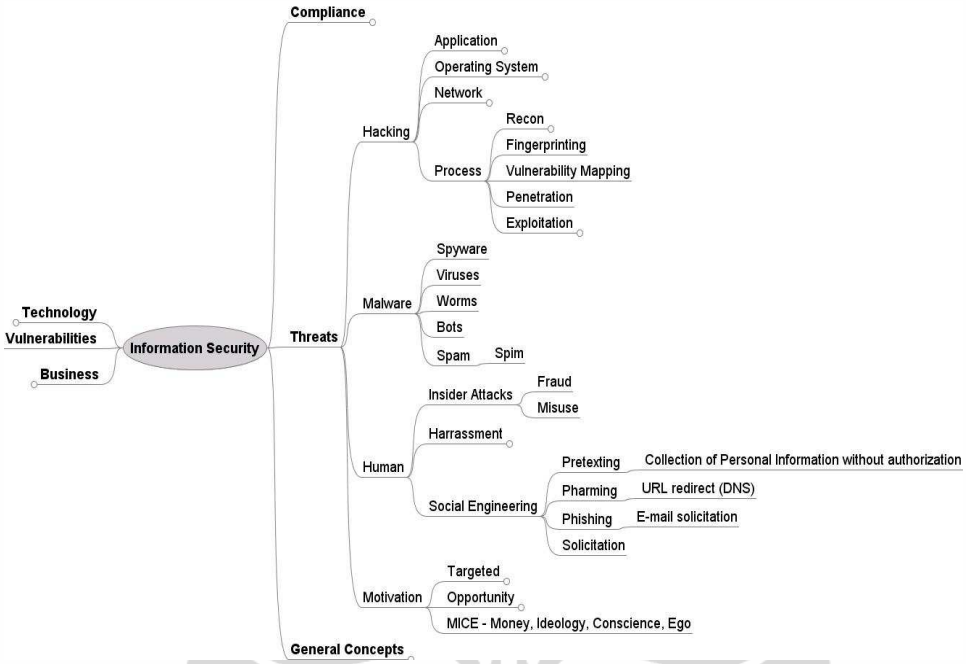
terlihat pada Gambar 3.8 berikut, saat ini terdapat layanan-layanan untuk melakukan *spoofing*, *modification* dan *interception* data elektronik.

Ketika berorientasi pada kualitas sebuah telekomunikasi, pembeli memiliki kecenderungan untuk tidak menekan biaya untuk sebuah keamanan. Dalam industri keamanan terkadang aplikasi yang bersifat gratis ataupun murah tidak berarti langsung mudah dijual atau digunakan oleh pembeli. Pembeli dalam hal ini pengguna transaksi elektronik diperhadapkan pada kondisi dimana kejahatan melalui internet sangat mungkin dilakukan. Seperti terlihat pada Tabel 3.8 berikut adalah tariff atau harga yang ditawarkan untuk pengambilan informasi.

Tabel 3.8 Harga untuk Pengambilan Informasi [38]

Item	Advertised Price (in US Dollars)
United States-based credit card with card verification value	$1–$6
United Kingdom-based credit card with card verification value	$2–$12
An identity (including US bank account, credit card, date of birth, and government issued identification number)	$14–$18
List of 29,000 emails	$5
Online banking account with a $9,900 balance	$300
Yahoo Mail cookie exploit—advertised to facilitate full access when successful	$3
Valid Yahoo and Hotmail email cookies	$3
Compromised computer	$6–$20
Phishing Web site hosting—per site	$3–5
Verified PayPal account with balance (balance varies)	$50–$500
Unverified PayPal account with balance (balance varies)	$10–$50
Skype account	$12
World of Warcraft account—one month duration	$10

Pembeli cenderung membutuhkan layanan-layanan keamanan termasuk layanan CA. Kebutuhan keamanan untuk transaksi elektronik dalam infrastruktur telekomunikasi dapat dipetakan pada Gambar 3.12 berikut :



Gambar 3.12 Pemetaan Kebutuhan Keamanan Infomasi Transaksi Elektronik [39]

Kebutuhan keamanan untuk transaksi elektronik dalam era konvergensi adalah layanan yang mutlak diperlukan. Layanan CA memberikan solusi untuk sebagian besar ancaman terhadap informasi, hal ini akan melemahkan posisi tawar menawar pembeli. Artinya pembeli tidak terlalu terpengaruh pada harga yang murah, tetapi cakupan layanan keamanan yang terpercaya sesuai kebutuhan pembeli. Dari informasi ini, didapatkan nilai variabel adalah 0 (nol).

3.3.3.14. Integrasi Balik

Integrasi Balik atau integrasi kebelakang adalah usaha untuk mengupayakan kepemilikan atau kendali yang lebih besar atas pemasok perusahaan [25]. Apabila pembeli cenderung melakukan integrasi balik (*Backward Integration*), maka tekanan dari kekuatan tawar menawar pembeli akan bertambah besar terhadap industri.

Kondisi :

Dalam industri layanan keamanan CA, hal ini mungkin terjadi bila pembeli dapat bernegosiasi dengan beberapa pemasok dari luar (ataupun mengadakan layanan sendiri) dan membeli beberapa komponen layanan dari pemasok luar tersebut.

Penggunaan layanan CA lokal untuk standar pengamanan dilindungi oleh undang-undang untuk terdaftar dan terstandarisasinya penyedia jasa layanan CA, oleh karena itu kecil kemungkinan pembeli melakukan hal tersebut. Penyebab lain pembeli melakukan integrasi balik adalah bila pembeli memiliki kemampuan IT yang kuat dan mampu membuat sistem pengamanan sendiri, terkadang hal ini tidak menjadi *core business* bagi pembeli. Dari informasi ini, didapatkan bahwa nilai variabel integrasi balik adalah 0 (nol).

3.3.3.15. Kualitas Produk (bagi Pembeli)

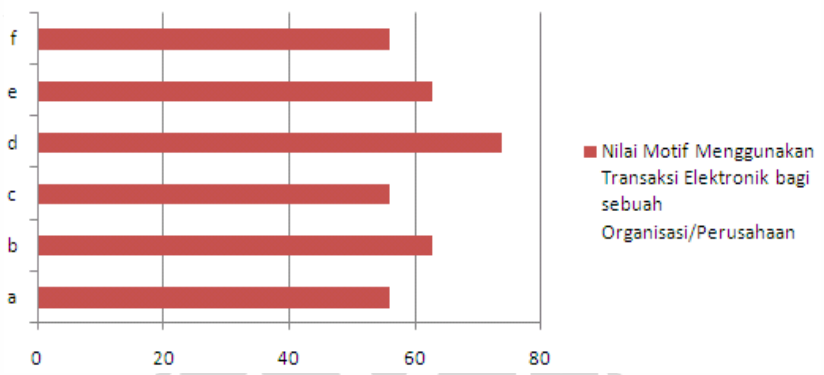
Apabila kualitas produk tidak terkait langsung dengan produk yang dihasilkan pembeli, maka kekuatan tekanan tawar menawar pembeli akan tinggi.

Kondisi :

Berdasarkan penelitian faktor yang melandasi perusahaan terdorong menggunakan *e-commerce* (transaksi elektronik) terdiri dari enam faktor yaitu [40] ;

a. Mengakses Pasar Global 56%
b. Mempromosikan Produk 63%
c. Membangun Merk 56%
d. Mendekatkan dengan pelanggan 74%
e. Membantu komunikasi lebih cepat dengan pelanggan 63%
f. Memuaskan pelanggan 56%

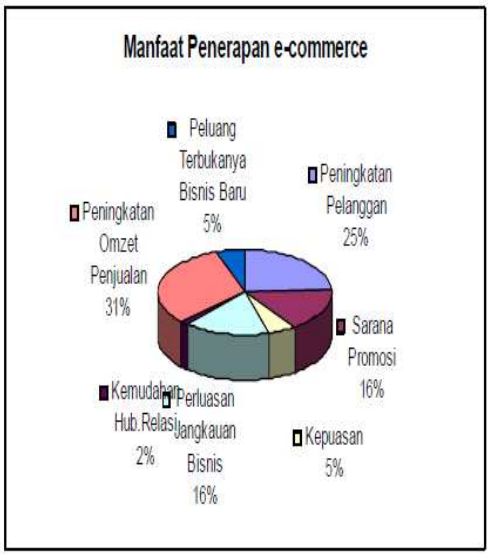
Gambar 4.13 memperlihatkan nilai prosentasi motif menggunakan *e-commerce* (transaksi elektronik).



Gambar 3.13 Motif Penggunaan *E-commerce* [40]

Dalam penelitian yang sama, didapatkan hasil pengaruh penerapan e-commerce seperti terlihat pada Gambar 3.14 berikut.

Jawaban	Jumlah	%
Omzet	18	31
Pelanggan	14	25
Perluasan Bisnis	9	16
Sarana Promosi	9	16
Terbukanya Bisnis	3	5
Kepuasan	3	5
Kemudahan Hub	1	2
Total	**57**	**100**

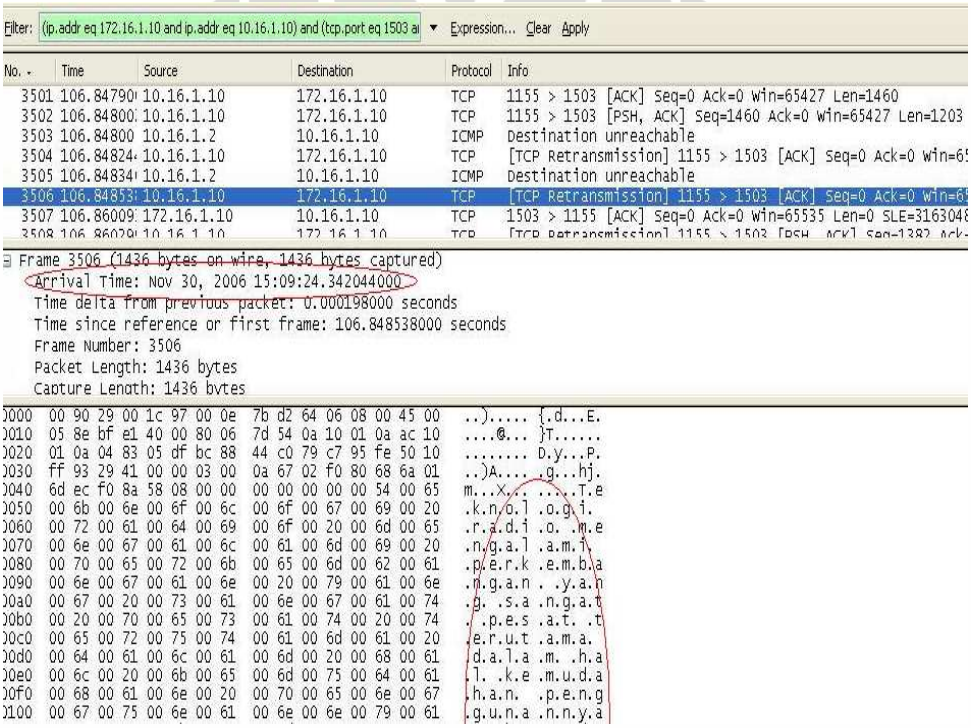


Gambar 3.14 Manfaat Penerapan *E-commerce* [40]

Dalam Penelitian tersebut didapatkan pula hasil adanya 2 (dua) faktor yang menjadi manfaat terbesar perusahaan setelah menerapkan e-commerce adalah kepuasan konsumen (74%) dan Keunggulan bersaing (81%). Dari deskripsi diatas diketahui bahwa penggunaan transaksi elektronik dan pengamanannya sangat berpengaruh bagi pembeli. Artinya kualitas produk

layanan CA terkait langsung dengan produk yang dihasilkan pembeli (perusahaan/individu yang menggunakan transaksi elektronik).

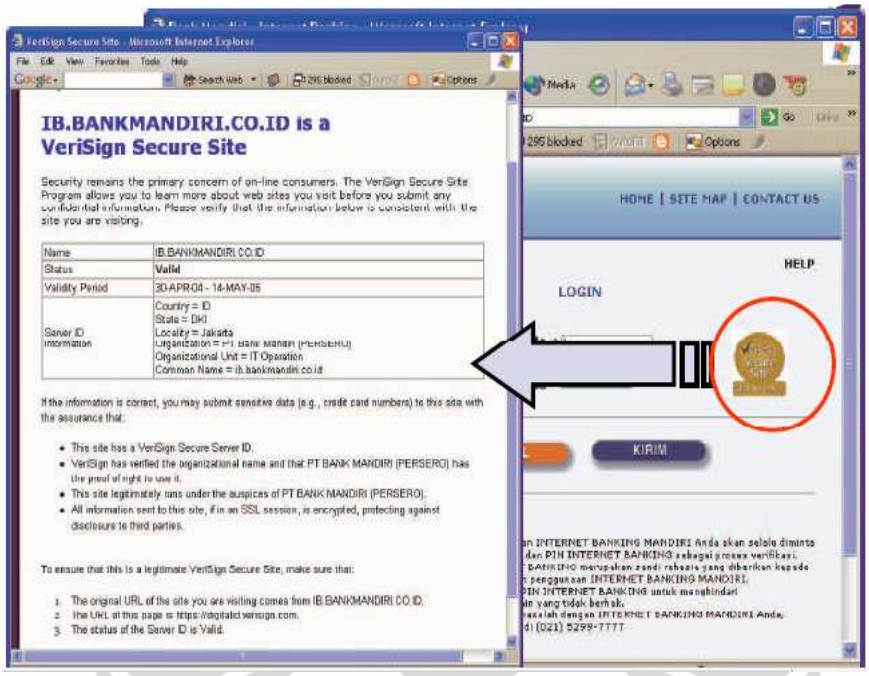
Pada saat bertransaksi, pembeli dalam hal ini pengguna transaksi elektronik tidak merasakan pengaruh secara langsung ada atau tidaknya pengamanan. Salah satu kondisi yang membuktikan pengaruh atau pentingnya layanan keamanan adalah bila terjadi pembobolan sistem keamanan tersebut. Meski tidak dirasakan secara langsung, dalam platform berbasis IP pembuktian pengamanan tetap dapat terlihat, seperti diperlihatkan pada Gambar 3.15 berikut.



Gambar 3.15 Aliran Data Elektronik

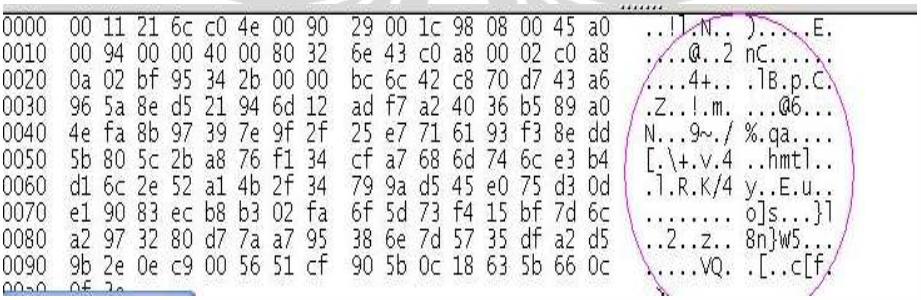
Pada Gambar 3.15 tersebut diperlihatkan salah satu transaksi yang berbasis IP, diambil dengan menggunakan *free software ethereal*. Dalam gambar tersebut data yang terkirim melalui platform protokol IP dapat dengan mudah dibaca dan diketahui oleh orang lain. Dalam kasus kejahatan melalui platform protokol IP, setelah diketahui data yang dikirim, data tersebut dapat di modifikasi atau diubah atau data digunakan untuk dipalsukan (misal rekening bank, jumlah rekening atau yang

lainnya). Pada Gambar 3.16 diperlihatkan sertifikat yang dimiliki oleh sebuah jasa perbankan yang menggunakan layanan CA.



Gambar 3.16 Sertifikat Layanan CA [41]

Pada transaksi yang menggunakan sistem pengamanan data tersebut tidak dapat dibaca atau diketahui orang lain, seperti terlihat pada Gambar 3.17 berikut.



Gambar 3.17. Data Elektronik dengan Layanan Keamanan

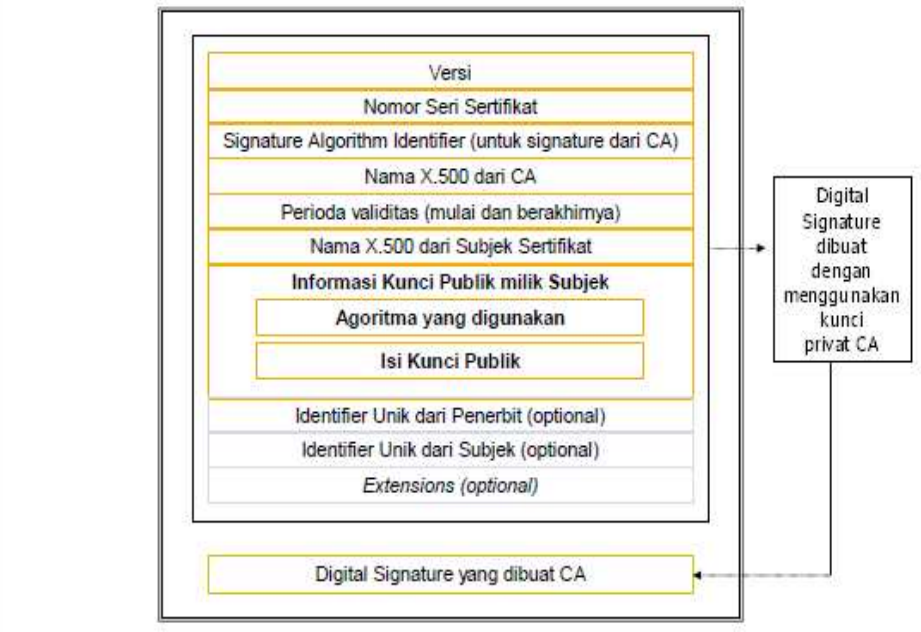
Dari informasi besarnya pengaruh dan kualitas layanan CA, sehingga pembeli tidak memiliki posisi tawar menawar yang kuat didapatkan nilai variabel kualitas produk adalah 0 (nol).

3.3.3.16. Informasi tentang Produk

Pembeli mempunyai informasi lengkap mengenai produk. Seperti informasi tentang permintaan, harga pasar yang aktual, dan bahkan biaya pemasok, biasanya posisi tawar-menawar menjadi lebih kuat.

Kondisi :

Bila pembeli dapat mendapatkan informasi mengenai pilihan produk dan penyedia jasanya, posisi tawar menawar pembeli menjai kuat. Pembeli dalam hal ini pengguna transaksi elektronik yang memiliki informasi yang lengkap tentang produk seperti harga, kemudahan koneksi, kualitas dan cakupan area layanan dari produk keamanan CA yang ditawarkan sehingga akan mudah untuk beralih ke penyedia jasa layanan keamanan CA lain, hal ini akan meningkatkan kekuatan penawaran pembeli. Pada Undang-undang penyelenggaraan CA, setiap penyedia jasa layanan keamanan CA diwajibkan menginformasikan metode yang digunakan dan cakupan yang jelas. Pada Gambar 3.18 diperlihatkan isi sebuah sertifikat layanan keamanan CA secara umum.



Gambar 3.18 Isi Sertifikat Layanan Keamanan CA [42]

Dalam era konvergensi, akses informasi terhadap informasi tersebut lebih mudah didapatkan. Pada pasal 13 Undang-undang ITE disebutkan bahwa layanan CA bisa berada di dalam negeri (lokal) dan di luar negeri (terdaftar di dalam negeri). Sesuai kondisi ini, didapatkan nilai variabel informasi tentang produk bagi pembeli adalah 1 (satu).

Dari hasil perhitungan setiap variabel dalam Kekuatan tawar menawar pembeli didapatkan hasil dalam skala medium (50%), seperti terlihat pada tabel 3.9 berikut.

Tabel 3.9. Hasil Penilaian Variabel Kekuatan Tawar menawar Pembeli

3. Kekuatan Tawar Menawar Pembeli *(Bargaining Power of Buyer)*			
No. Variabel	**Variabel**	**Indikator**	**Nilai**
3.1	Pembeli Terpusat	Pembelian produk dilakukan oleh kelompok pembeli dalam area global (konvergen)	0
3.2	Kapasitas Pembelian	Pembelian Produk layanan CA merupakan pengeluaran yang relatif diperlukan (penting bagi pembeli) dan besar sehingga pembeli akan lebih selektif	1
3.3	Differensiasi Produk (bagi Pembeli)	Produk yang dibeli adalah produk terdifferensiasi, sesuai kebutuhan dari sisi fitur, algoritma dan lain-lain.	1
3.4	Biaya Beralih ke Pemasok (bagi Pembeli)	Biaya beralih pemasok rendah	1
3.5	Orientasi Biaya	Pembeli cenderung tidak menekan biaya untuk kebutuhan keamanan	0
3.6	Integrasi Balik (Integrasi Kebelakang)	Pembeli tidak (kecil kemungkinan) melakukan integrasi balik	0
3.7	Kualitas Produk (bagi Pembeli)	Kualitas Produk industri keamanan layanan CA mempengaruhi kualitas produk atau jasa dari pembeli	0
3.8	Informasi tentang Produk	Pembeli memiliki informasi yang lengkap tentang produk yang akan dibeli	1
			50.00%

3.3.9. Kekuatan Tawar Menawar Pemasok

Pemasok dapat menggunakan kekuatan tawar-menawar terhadap pembeli dalam industri dengan cara menaikkan harga atau menurunkan kualitas produk atau jasa yang dibeli. Kondisi-kondisi yang membuat posisi pemasok kuat cenderung menyerupai kondisi yang membuat pembeli kuat.

3.3.4.7. Dominasi Pemasok

Apabila dalam industri layanan CA didominasi oleh pemasok yang terpusat biasanya pemasok dapat memberikan tekanan yang kuat kepada industri dalam harga, kualitas dan persyaratan penjualan produk pemasok maupun produk yag dihasilkan dari pembeli yang menggunakan produk pemasok.

Kondisi :

Pada industri layanan keamanan CA, untuk membentuk layanan ini dibutuhkan pemasok atau penyedia jasa seperti :

a. Penyedia Jasa Jaringan,Intranet, Internet (ISP, NAP, ITKP)
b. Aplikasi /Konten Browser
c. Sofftware Aplikasi CA atau VPN
d. Algoritma Penyandian, Algoritma Sistem, *Key Generator, Key Management System*
e. System Developer , Server, Database

Seperti pada transaksi elektronik seperti *e-commerce*, layanan keamanan CA di era konvergensi sangat berpengaruh pada jaringan intranet dan internet. Pemasok untuk industri layanan CA bersifat tidak didominasi oleh satu pemasok, kecuali untuk faktor (d). Pembuatan algoritma harus terkonsentrasi pada pihak-pihak yang benar-benar berkompetensi dan terpercaya, Hal ini harus dilakukan karena banyaknya pihak yang tidak berkepentingan yang ingin mengambil informasi. Salah

satu contoh pemecahan algoritma ataupun kunci yang digunakan diperlihatkan pada Tabel 3.10 berikut.

Tabel 3.10 Waktu yang diperlukan untuk Pemecahan Kunci [43]

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption per us	Time Required at 10^6 Decryption per us
32	2^32	35.8 mins	2.15 milliseconds
56	2^56	1142 years	10 hours
128	2^128	5.4*10^24 years	5.4*10^18 years
168	2^168	5.9*10^36 years	5.9*10^30 years

Pada Gambar 3.19 berikut digambarkan bahwa saat ini teknologi komputerisasi telah mampu melakukan pemecahan kunci ataupun sistem untuk dapat mengambil data pengguna transaksi elektronik meskipun data tersebut telah menggunakan metode penyandian.

Gambar 3.19 Komputer sebagai alat komputasi pemecahan Kunci dan Sistem Secure Socket Layer [44]

Dari informasi ini didapatkan nilai variabel Dominasi pemasok untuk algoritma adalah 1 (satu) dan pemasok jaringan dan komponen lain adalah 0 (nol).

3.3.4.8. Produk Pengganti

Apabila tidak terdapat produk pengganti dari pemasok lain maka akan meningkatkan kekuatan penawaran pemasok terhadap industri.

Kondisi :

Pada komponen jaringan (*intranet, internet, server, databases*) terdapat banyak perangkat lunak yang dikembangkan dengan lisensi seperti GPL (*General Public License*) atau *freeware*. Artinya perangkat lunak tersebut dapat digunakan secara gratis oleh pengguna. Contohnya snort sebagai *instrusion detection*, *antivirus*, *firewall*, *spammassin* sebagai *anti spam* dan lain sebagainya.

Beberapa aplikasi layanan CA dari beberapa perusahaan penyedia jasa CA di luar negeri diberikan secara gratis dalam tahap tertentu, meski untuk pengguna transaksi elektronik hal ini tidak sepenuhnya dapat digunakan.

Dengan demikian beberapa komponen layanan CA dapat tergantikan dengan pilihan-pilihan pemasok komponen produk pengganti. Dari informasi ini didapatkan nilai variabel produk pengganti adalah 0 (nol).

3.3.4.9. Pasar Pemasok

Apabila suatu industri bukan merupakan pelanggan utama dari pemasok maka kecenderungan pemasok dapat memaksakan kekuatannya pada industri tersebut.

Kondisi :

Apabila industri bukan pasar yang potensial maka akan meningkatkan kekuatan penawaran pemasok. Layanan keamanan CA merupakan pasar yang potensial bagi pemasok karena mendukung penggunaan telekomunikasi secara elektronik. Dari informasi ini didapatkan nilai variabel pasar pemasok adalah 0 (nol).

3.3.4.10. Kualitas Produk (dari Pemasok)

Apabila dalam suatu industri, kualitas produk pemasok sangat penting bagi industri maka akan meningkatkan kekuatan penawaran pemasok.

Kondisi :

Bagi industri layanan keamanan CA kualitas jaringan intranet, internet maupun *sistem developer* yang digunakan sangat penting. Akses yang cepat dan akurat sangat memerlukan sistem dan jaringan yang baik. Dari informasi ini didapatkan nilai variabel adalah 1 (satu).

3.3.4.11. Integrasi Maju

Integrasi Maju atau integrasi kedepan adalah usaha memperoleh kepemilikan atau kendali yang lebih besar atas distributor. Misalnya adalah mencari sistem distribusi yang lebih menguntungkan dengan memotong jalur distribusi. Apabila pemasok menunjukkan keinginan untuk melakukan integrasi maju maka akan meningkatkan kekuatan penawaran pemasok.

Kondisi :

Integrasi maju terjadi apabila pemasok adalah perusahaan yang berusaha untuk menjadi salah satu penyedia jasa layanan keamanan CA. Seperti penjelasan pada variabel Dominasi Pemasok, nilai untuk variabel Integrasi maju adalah 0 (nol).

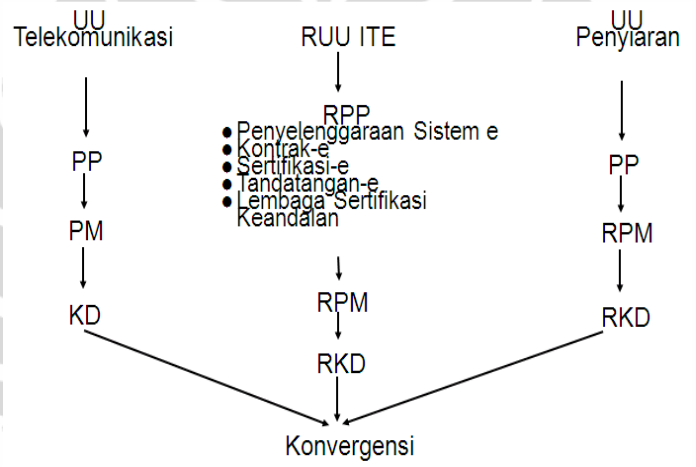
3.3.4.12. Kebijakan Pemerintah (bagi Pemasok)

Kebijakan pemerintah dalam membatasi perilaku pemasok juga mempengaruhi posisi industri dengan produk pengganti melalui regulasi, subsisi dan lain-lain. Kebijakan Pemerintah yang mendukung masuk dan berkembangnya pemasok akan meningkatkan kekuatan penawaran pemasok.

Kondisi :

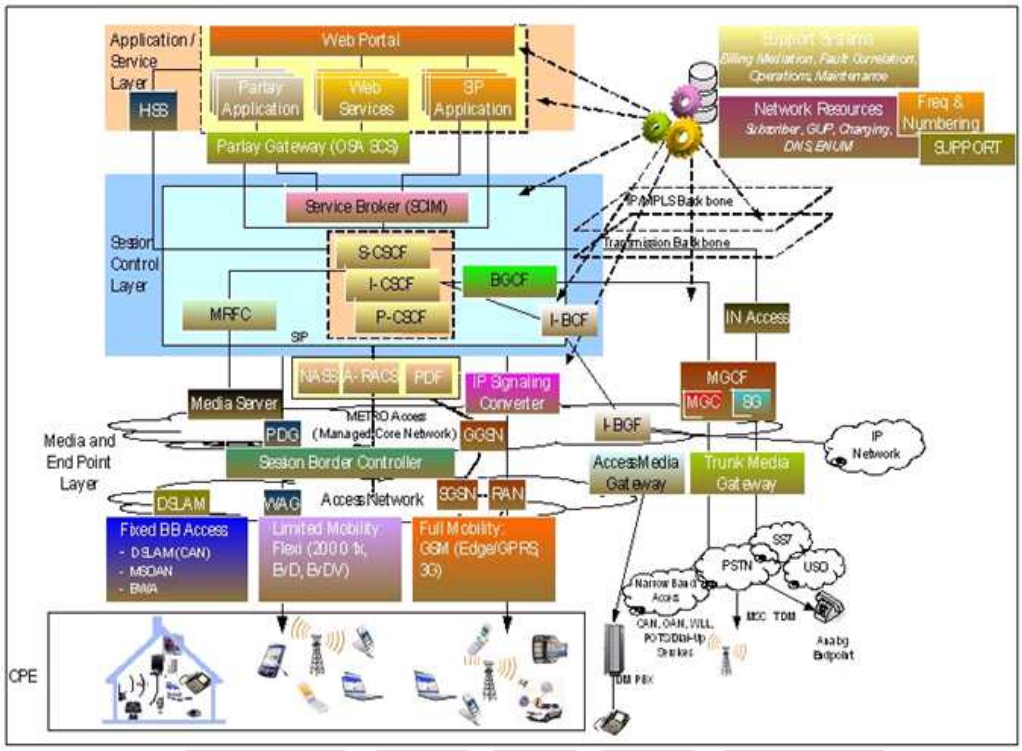
Kebijakan pemerintah yang mendukung masuk dan berkembangnya pemasok akan meningkatkan kekuatan penawaran pemasok.

Untuk mendukung telekomunikasi menuju konvergensi pemerintah membuat peraturan rancangan UU Konvergensi dan program-program untuk mendukung perkembangan perangkat hardware, software dan konten pendukung.



Gambar 3.20 Rancangan Undang-undang Konvergensi

Pada Gambar 3.20 diperlihatkan perubahan Undang-undang telekomunikasi kearah Undang-undang konvergensi. Selain mendukung melalui undang-undang kearah konvergensi, pemerintah membuat peraturan mengenai nilai minimal Tingkat Komponen Dalam Negeri (TKDN) yang harus ikuti oleh seluruh pemain industri telekomunikasi. Pada Gambar 3.21 berikut diperlihatkan perangkat pendukung layanan berbagai platform di era konvergensi.



Gambar 3.21. Perangkat Pendukung Layanan di Era Konvergensi

Dari informasi ini didapatkan nilai variabel dukungan Kebijakan Pemerintah dari sisi pemasok adalah 1 (satu).

Dari hasil perhitungan setiap variabel dalam Kekuatan tawar menawar pemasok didapatkan hasil tekanan pada industri yang medium (42,86%), seperti terlihat pada tabel 3.11 berikut.

Tabel 3.11. Hasil Penilaian Variabel Kekuatan Tawar menawar Pemasok

4.Kekuatan Tawar Menawar Pemasok (*Bargaining Power of Supplier*)			
No. Variabel	**Variabel**	**Indikator**	**Nilai**
4.1	Dominasi Pemasok	Pemasok perangkat layanan tidak didominasi oleh beberapa perusahaan terpusat,	1
		Penyedia algoritma dan sistem pengamanan didominasi terpusat	0
4.2	Produk Pengganti	Terdapat produk pemasok pengganti untuk beberapa komponen CA	0

4.3	Pasar Pemasok	Industri layanan keamanan berbasis IP merupakan pasar potensial yang penting bagi kelompok pemasok	0
4.4	Kualitas Produk (dari Pemasok)	Kualitas produk pemasok sangat penting bagi operator jasa layanan CA	1
4.5	Integrasi Maju (Integrasi Ke Depan)	Pemasok tidak (kecil kemungkinan) melakukan integrasi maju	0
4.6	Kebijakan Pemerintah (bagi Pemasok)	Pemerintah mendukung masuknya pemasok, misal dalam RUU konvergensi dan program yang disediakan untuk membangun pemasok di era konvergensi	1
			42.86%

3.3.10. Persaingan Diantara Perusahaan Eksisting

Kompetitor dalam hal ini adalah pemain yang menghasilkan serta menjual produk sejenis, yang akan bersaing dalam memperebutkan marketshare pasar. Intensitas persaingan akan tinggi apabila :

3.3.5.6. Jumlah & Ragam Pesaing

Banyaknya (jumlah) pemain dalam industri dengan kekuatan masing-masing tentu saja akan meningkatkan intensitas persaingan dalam kompetisi. Adanya pesaing yang beragam, mempunyai strategi beragam, asal-usul, karakteristik serta tujuan dan strategi bersaing yang berlainan akan meningkatkan persaingan industri.

Kondisi :

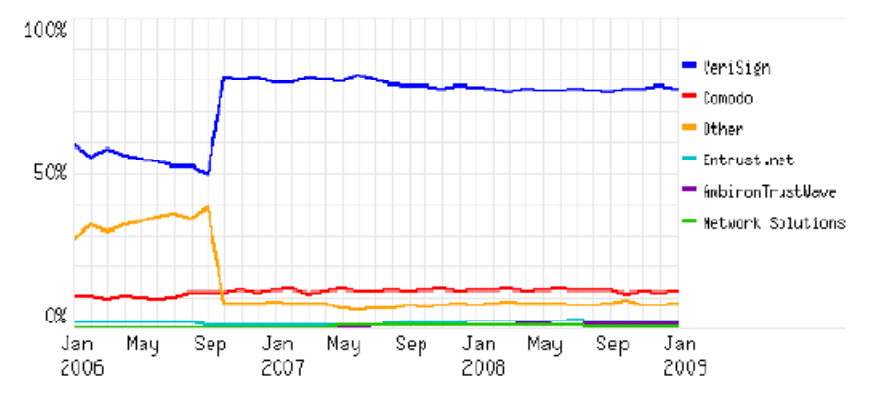
Apabila jumlah pesaing memiliki jumlah yang seimbang akan meningkatkan kompetisi diantara operator jasa layanan keamanan CA eksisting. Pesaingan penyedia jasa layanan CA diindonesia masih didominasi oleh penyedia jasa dari luar negeri. Pada Tabel 3.12 diperlihatkan penggunaan layanan keamanan CA pada jasa perbankan, 10 bank terbesar di Indonesia menggunakan layanan CA dari luar negeri.

Tabel 3.12. Layanan CA pada Jasa Perbankan di Indonesia [45]

No	Bank	Website	*Certificate Authority*
1	Bank Mandiri	www.bankmandiri.co.id	verisign
2	Bank Rakyat Indonesia	www.bri.co.id	-
3	Bank Central Asia	www.klikbca.com	cybertrust
4	Bank Negara Indonesia	www.bni.co.id	verisign
5	CIMB Niaga	www.cimbniaga.com	verisign
6	Bank Danamon	www.danamon.co.id	verisign
7	Pan Indonesia Bank	www.panin.co.id	verisign
8	Bank Permata	www.permatabank.com	verisign
9	Bank Internasional Indonesia	www.bii.co.id	verisign

10	Citibank NA	www.citibank.co.id	-

Dari sumber Lembaga Survey Netcraft didapatkan di Indonesia hanya menggunakan beberapa penyedia jasa layanan CA dan seluruhnya berasal dari Luar Negeri. Seperti diperlihatkan pada Gambar 3.22 berikut :



Gambar 3.22. Layanan CA di Indonesia

Dari informasi ini didapatkan nilai variabel adalah 1(satu) untuk jumlah pesaing yang seimbang dan nilai variaabel 0 (nol) untuk pesaing yang beragam.

3.3.5.7. Pertumbuhan Industri

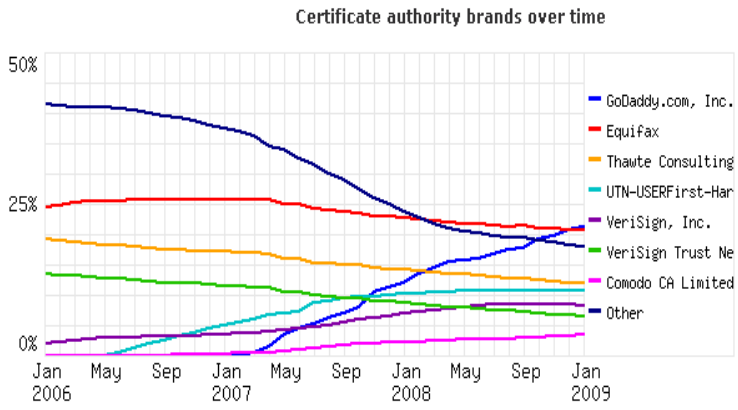
Pertumbuhan industri yang lamban akan membuat tingkat persaingan jadi tinggi. Apabila pertumbuhan industri layanan keamanan lamban bahkan cenderung menurun akan mengubah persaingan menjadi ajang perebutan pangsa pasar untuk perusahaan yang ingin melakukan ekspansi.

Kondisi :

Apabila pertumbuhan industri penyedia jasa layanan CA lamban bahkan cenderung menurun akan mengubah persaingan menjadi ajang perebutan pasar untuk perusahaan-perusahaan yang ingin melakukan

ekspansi. Setiap perusahaan akan melakukan diversifikasi produk aliansi, dan pengembangan model bisnis baru agar dapat bertahan dan tidak tersingkirkan dari peta persaingan industri.

Saat ini pertumbuhan industri layanan CA naik mengingat kebutuhan keamanan data di era konvergensi. Dari hasil penelitian lembaga survey SSL didapatkan bahwa merk layanan CA mengalami penurunan akibat mulai banyaknya pesaing industri layanan keamanan CA dari perusahaan swasta maupun pemerintah disetiap negara [56]. Seperti diperlihatkan pada Gambar 3.23 berikut.



Gambar 3.23 Penurunan Merk CA [56]

Dari informasi ini didapatkan nilai variabel untuk pertumbuhan industri layanan CA adalah 1 (satu).

3.3.5.8. Differensiasi Produk

Apabila dalam suatu industri tidak terdapat differensiasi produk maka akan meningkatkan persaingan antar pemain yang ada.

Kondisi :

Dalam layanan keamanan CA lokal differensiasi produk akan tinggi, dari sisi algoritma yang digunakan, fitur yang menyesuaikan pada kebiasaan dan karakteristik pengguna layanan ini. Dari informasi ini didapatkan nilai variabel Differensiasi Produk adalah 0 (nol).

3.3.5.9. Penambahan Kapasitas

Peningkatan kapasitas layanan akan berpengaruh pada tingkat persaingan dimana semakin tinggi kapasitas maka semakin tinggi pula tingkat persaingan dalam industri.

Kondisi :

Layanan CA didesain untuk memenuhi kebutuhan masyarakat pengguna transaksi elektronik dengan meningkatnya kebutuhan di era konvergensi memaksa setiap penyedia jasa layanan ini memperbesar kapasitas , maka nilai untuk variabel ini adalah 1 (satu).

3.3.5.10. Hambatan Pengunduran Diri

Hambatan pengunduran diri adalah faktor ekonomi, strategi, dan emosional yang membuat perusahaan tetap bersaing dalam bisnis meskipun mereka mungkin memperoleh laba atas investasi yang rendah atau bahkan negatif. Hambatan pengunduran diri yang tinggi akan mempertinggi intensitas persaingan pada industri.

Kondisi :

Pada bagian sebelumnya dijelaskan bahwa untuk mendukung atau membangun layanan keamanan CA dibutuhkan Penyedia Jasa Jaringan, Intranet, Internet (ISP, NAP, ITKP), Aplikasi /Konten Browser, Software Aplikasi CA atau VPN, Algoritma Penyandian, Algoritma Sistem, *Key Generator, Key Management System, System Developer , Server, Database.*

Ketika kompenen produksi tersebut memerlukan investasi yang besar, proses perijinan, standarisasi yang kompleks serta melibatkan sumber daya yang banyak maka akan memperbesar hambatan pengunduran diri yang tinggi. Maka nilai variabel adalah 1 (satu).

Dari hasil perhitungan setiap variabel dalam Persaingan Diantara Perusahaan Eksisting didapatkan hasil tekanan pada industri yang medium (66.67%), seperti terlihat pada Tabel 3.13 berikut.

Tabel 3.13. Hasil Penilaian Variabel Persaingan Diantara Perusahaan Eksisting

5.Persaingan Antara Perusahaan Eksisting (*Rivalry Among Competitor*)			
No. Variabel	**Variabel**	**Indikator**	**Nilai**
5.1	Jumlah dan Ragam Pesaing	Jumlah Pesaing yang seimbang	1
		Pesaing dalam indutri keamanan yang beragam	0
5.2	Pertumbuhan Industri	Pertumbuhan industri yang pesat	1
5.3	Diferensiasi Produk	Kurangnya Differensiasi produk (dalam hal algoritma), Layanan CA yang ada saat ini menggunakan algoritma standar.	0
5.4	Penambahan Kapasitas	Penambahan kapasitas dalam jumlah besar dan selalu dibutuhkan proses pembaruan (update) untuk komponen layanan keamanan CA	1
5.6	Hambatan Pengunduran Diri	Hambatan pengunduran diri dari industri tinggi, akibat tingginya investasi dan permintaan yang tinggi	1
			66.67%

3.2.4. Potensi Kompetitif Layanan CA di Era Konvergensi

Dari hasil identifikasi dan pembobotan tekanan setiap variabel dalam Porter 5 Forces, dilakukan penggambaran secara visual setiap tekanan yang ada dalam industri penyediaan layanan keamanan CA di era konvergensi. Potensi keuntungan kompetitif (peluang) akan tinggi bila akumulasi dari setiap tekanan tersebut pada masing-masing faktor adalah rendah [25].

Daya tarik suatu industri terjadi apabila semua tekanan dalam Porter 5 Force adalah rendah. Semakin rendah tekanan, maka semakin tinggi keunggulan kompetitif yang dimiliki oleh produk/layanan yang akan dipasarkan dalam industri tersebut. Berdasarkan hasil analisis yang telah dilakukan terhadap kelima

tekanan dalam porter 5 forces yang berperan dalam penentuan keunggulan kompetitif penyediaan layanan CA kepada publik di era konvergensi diperoleh kondisi seperti diperlihatkan pada Tabel 3.14 berikut :

Tabel 3.14 Hasil Analisa Pemodelan Porter 5 Forces terhadap Penyediaan Layanan Keamanan CA di Era Konvergensi

No	Faktor Kekuatan	Jumlah Nilai Kekuatan	Jumlah Penilaian Parameter	Nilai Porter	Skala
1	Ancaman Pendatang Baru	3	8	0.375	MEDIUM
2	Ancaman Produk Pengganti	2	8	0.250	LOW
3	Kekuatan Tawar Menawar Pembeli	4	8	0.500	MEDIUM
4	Kekuatan Tawar Menawar Pemasok	3	7	0.429	MEDIUM
5	Persaingan Diantara Perusahaan Eksisting	4	6	0.667	MEDIUM
Tekanan Kompetitif Rata-rata				0.444	MEDIUM

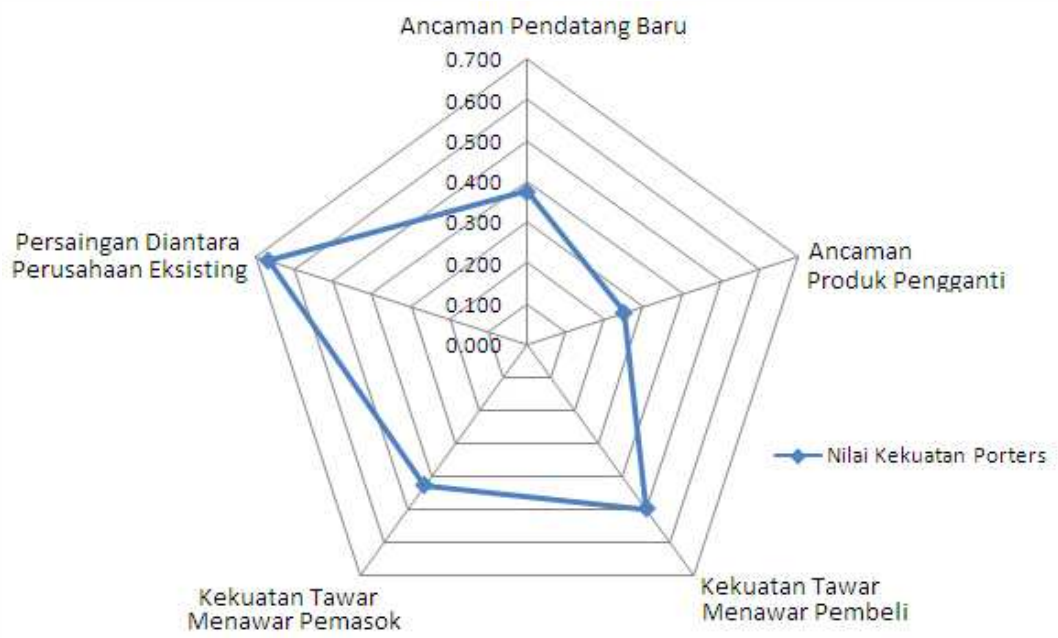
Tekanan dari kelima kekuatan tersebut memberikan tekanan Medium sebagai situasi tekanan rata-rata terhadap layanan CA di era konvergensi. Dalam hal ini Lembaga Sandi Negara dapat saja dengan mudah masuk ke dalam industri karena industri tidak memiliki faktor hambatan masuk yang kuat untuk menghadang (37,5% tekanan bagi Pendatang Baru). Lembaga Sandi Negara memiliki kompetensi (mampu melakukan differensiasi) dalam hal pengamanan. Aplikasinya layanan CA belum ada pengganti yang dapat dikatakan setara dengan nilai tekanan produk pengganti pada skala rendah (25%).

Potensi kompetitif penyediaan layanan CA sangat dipengaruhi oleh tekanan persaingan didalam industri sebagai reaksi yang kuat merespon kedatangan Lembaga Sandi Negara dalam melayani kebutuhan keamanan CA. Persaingan Diantara perusahaan eksisting bernilai tertinggi yaitu 66,7 % diantara seluruh tekanan porter pada industry penyediaan layanan CA. Setiap pemain eksisting merupakan pemain yang telah memiliki identitas dan memiliki kehadiran mendunia.

Tekanan dari sisi pemasok dan pembeli berkategori medium dengan nilai tekanan tidak lebih dari 50% menekan industry. Hal ini terjadi akibat besarnya

kebutuhan di era konvergensi dan kuatnya pengaruh layanan CA bagi pemasok dan pembeli (pengguna transaksi elektronik).

Penggambaran Matrik dari kelima faktor kekuatan yang berpengaruh terhadap peyediaan layanan keamanan CA di era konvergensi diperlihatkan pada Gambar 3.24 berikut :



Gambar 3.24 Porter 5 Force Layanan CA di Era Konvergensi

Pada Gambar 3.24 terlihat bahwa faktor yang mendominasi tekanan kompetitif terhadap penyediaan layanan CA di era konvergensi adalah Persaingan di antara Perusahaan Eksisting dan Kekuatan Tawar menawar Pembeli. Dari kedua kekuatan dominan tersebut, kekuatan Persaingan diantara Perusahaan Eksisting merupakan kekuatan yang harus diantisipasi oleh perusahan atau organisasi yang akan melakukan penyediaan layanan CA di era konvergensi.

BAB IV
STRATEGI PENYEDIAAN LAYANAN KEAMANAN CA

Pada Bab III telah dilakukan analisi potensi kompetitif penyediaan layanan CA di era konvergensi, didapatkan faktor paling dominan yang harus diantisipasi adalah persaingan diantara perusahaan atau organisasi penyedia jasa layanan CA yang saat ini ada (Persaingan Eksisting).

Setelah kekuatan-kekuatan yang mempengaruhi persaingan didiagnosis, suatu organisasi/perusahaan berada dalam posisi mengenali kekuatan dan kelemahannya relatif terhadap industri [25]. Beberapa industri yang berubah dengan cepat dapat dikatakan sebagai pasar yang bergolak dan memiliki laju cepat (*turbulent, high velocity markets*), termasuk didalamnya industri telekomunikasi, bioteknologi, *hardware/software* komputer [26]. Untuk menyusun strategi dalam hal penyediaan layanan CA di era konvergensi akan dilakukan penyusunan perencanaan strategi dengan pendekatan manajemen strategis.

Proses perencanaan strategi merupakan senjata kompetitif bagi kesuksesan sebuah organisasi atau perusahaan. Strategi merupakan respon secara terus menerus maupun adaptif terhadap peluang dan ancaman eksternal serta kekuatan dan kelemahan internal yang dapat mempengaruhi organisasi [27]. Strategi adalah alat yang sangat penting untuk mencapai keunggulan bersaing atau *Competitive Advantage*, yaitu kegiatan spesifik yang dikembangkan oleh suatu organisasi atau perusahaan agar lebih unggul dibandingkan dengan pesaingnya. Beberapa jenis strategi adalah sebagai berikut [27]:

i. Strategi Tingkat Korporat

   Strategi tingkat korporat merupakan analisa portofolio organisasi/perusahaan secara keseluruhan dalam kaitannya dengan kekuatan dan daya tarik industri. Strategi dalam tingkatan ini berkaitan dengan bagaimana mengubah kemampuan spesifik (*Distinctive Competitif*) ke Keunggulan Bersaing (*Competitif Advantage)*. Strategi korporat

menjadi landasan bagi penyusunan strategi dalam tingkat yang lebih rendah.

ii. Strategi Unit Bisnis

Strategi unit bisnis menganalisis hubungan antara posis strategis bisnis saat ini dengan kemungkinan strategi berikut ancamannya dengan periode waktu perencanaan.

iii. Strategi Fungsional

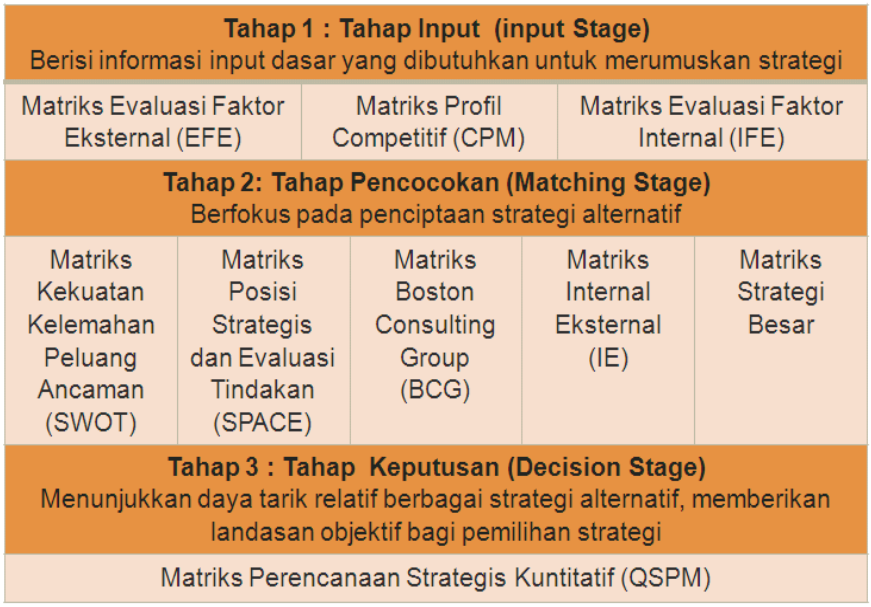
Strategi fungsional atau strategi operasional merupakan strategi yang langsung diimplementasi oleh setiap fungsi-fungsi yang ada di organisasi.

Formulasi strategi dilakukan dalam tingkat penentuan Strategi Korporat yaitu untuk menyusun strategi agar organisasi dapat merumuskan arah strategi yang akan dijalankan, dengan cara mengubah *distinctive competence* menjadi *competitive advantage*. Perencanaan Strategi merupakan proses penyusunan perencanaan jangka panjang, dalam prosesnya lebih banyak menggunakan analisis [26][27]. Tujuan perencanaan strategi adalah [26][27] :

1). Menyusun strategi sehingga sesuai dengan misi, sasaran serta kebijakan organisasi.
2). Analisis situasi menentukan strategi yang sesuai dengan peluang eksternal dan kekuatan internal agar dapat menghasilkan kompetensi organisasi/perusahaan.

Untuk menyusun strategi bagi organisasi (dalam hal ini Lembaga Sandi Negara) Penyediaan layanan keamanan CA kepada publik di era konvergensi pada bagian ini akan dilakukan formulasi strategi dengan menggunakan pendekatan manajemen strategis.

Tehnik-tehnik formulasi strategi dalam manajemen strategis dilakukan dalam 3 tahapan kerangka pengambilan keputusan, seperti ditunjukkan pada Gambar 4.1. Alat yang ditampilkan dalam kerangka ini dapat diterapkan untuk semua ukuran dan jenis organisasi serta dapat membantu para penyusun strategi mengidentifikasi, mengevaluasi dan memilih strategi [26].



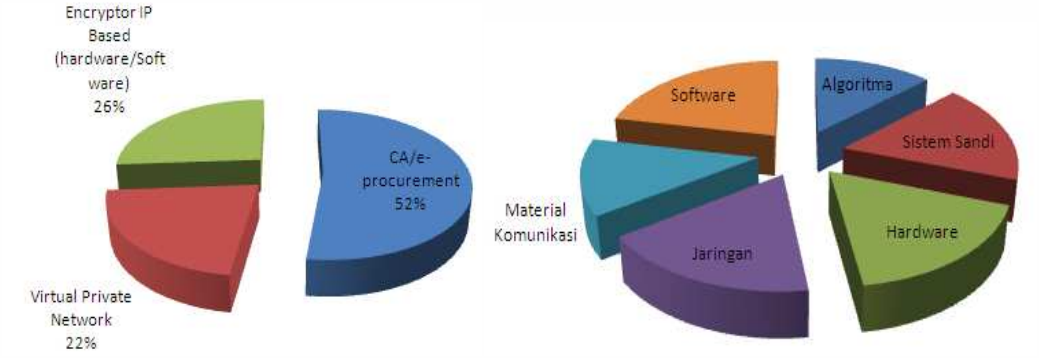
Gambar 4.1 Tahapan Perencanaan Strategi dalam Manajemen Strategis [26]

Tehnik-tehnik perencanaan strategi dalam manajemen strategis dilakukan dalam 3 tahapan kerangka pengambilan keputusan, yaitu tahap input, tahap pencocokan dan tahap keputusan. Dari hasil analisis yang dilakukan terhadap faktor-faktor kunci untuk menentukan strategi dalam penyediaan layanan CA, dihasilkan alternatif strategi yang dapat diambil oleh Lembaga Sandi Negara untuk menyediakan layanan keamanan CA kepada publik di era konvergensi telekomunikasi.

1.7. Tahap Input

Tahap ini bertujuan mengetahui berbagai faktor eksternal dan internal organisasi yang mempengaruhi penyediaan layanan keamanan CA ke publik kemudian mengidentifikasi ke dalam matrik EFE (Evaluasi faktor Eksternal) dan IFE (Evaluasi Faktor Internal).

Dari hasil identifikasi faktor internal dan eksternal penyediaan layanan CA, dilakukan konfirmasi kepada pihak-pihak yang berkaitan dengan penelitian, pengembangan dan manajemen pengamanan telekomunikasi berbasis IP di Lembaga Sandi Negara.



Gambar 4.2 Bidang Pekerjaan Responden

Pada Gambar 4.2 diperlihatkan bidang pekerjaan 22 orang responden survey kuisioner, seluruh responden pernah melakukan penelitian dan pengembangan pengamanan berbasis IP di Lembaga Sandi Negara.

Model jawaban kuisioner yang digunakan untuk menghitung nilai bobot (tingkat pengaruh) adalah sebagai berikut :

Tabel 4.1 Model Jawaban Kuisioner Penyediaan Layanan CA untuk menetapkan Tingkat Pengaruh (Bobot)

STS	Sangat tidak setuju jika isu tidak relevan dengan kondisi saat ini
TS	Tidak setuju jika isu tidak relevan dengan kondisi saat ini
RR	Ragu-ragu jika isu tidak dapat dijustifikasi
KS	Kurang Setuju mengenai relevansi isu dengan kondisi saat ini
SS	Sangat Setuju jika isu relevan dengan kondisi saat ini

Karena jumlah rating harus sama dengan 1.00 untuk setiap matriks evaluasi, maka rating untuk setiap responden tidak selalu sama, tergantung dari banyak jumlah model jawaban yang dipilih, atau dapat diformulasikan sebagai berikut :

A (SS) + B (KS) + C (RR) + D (TS) + E (STS) = 1.00 (Persamaan 4.1)

Dimana :

A = Jumlah banyaknya jawaban SS dalam satu matrik evaluasi peresponden

B = Jumlah banyaknya jawaban KS dalam satu matrik evaluasi peresponden

C = Jumlah banyaknya RR dalam satu matrik evaluasi peresponden

D = Jumlah banyaknya TS dalam satu matrik evaluasi peresponden

E = Jumlah banyaknya STS dalam satu matrik evaluasi peresponden

SS = Bobot nilai Sangat Setuju

KS = Bobot nilai Setuju

R R= Bobot nilai Ragu-ragu

TS = Bobot nilai Tidak Setuju

STS = Bobot nilai Sangat Tidak Setuju

Agar lebih mudah maka nilai rasio perbandingan antara SS hingga STS, dibuat sama dengan 2, sehingga :

SS : KS : RR : TS : STS = 1 : 2 : 4 : 8 : 16 (Persamaan 4.2)

Jika nilai SS = X, maka :

KS = 1/2 X (Persamaan 4.3)

RR = 1/4 X (Persamaan 4.4)

TS = 1/8 X (Persamaan 4.5)

STS = 1/16 X (Persamaan 4.6)

Dari persamaan 4.1, 4.3, 4.4, 4.5 dan 4.6 didapat cara menentukan nilai X adalah dengan persamaan sebagai berikut :

$$A(1X) + B\left(\frac{1}{2}X\right) + C\left(\frac{1}{4}X\right) + D\left(\frac{1}{8}X\right) + E\left(\frac{1}{16}X\right) = 1 \qquad \text{(Persamaan 4.7)}$$

$$X = \frac{16}{16A+8B+4C+2D+1E} \qquad \text{(Persamaan 4.8)}$$

Dimana X adalah nilai tingkat pengaruh bagi jawaban Sangat Setuju responden, selanjutnya nilai jawaban KS, RR , TS dan STS per responden dapat diperhitungkan dengan menggunakan persamaan 4.3, 4.4, 4.5 dan 4.6.

Sementara untuk mendapatkan tingkat kepentingan (rating), digunakan model pada Tabel 4.2 berikut :

Tabel 4.2 Model Jawaban Kuisioner Penyediaan Layanan CA untuk menetapkan Tingkat Kepentingan (Rating)

1	Isu yang disampaikan sangat tidak penting
2	Isu yang disampaikan tidak penting
3	Isu yang disampaikan penting
4	Isu yang disampaikan sangat penting

Masing-masing responden bebas untuk memasukkan nilai rating sesuai dengan pendapatnya untuk setiap variabel internal eksternal yang disampaikan.

Perhitungan nilai bobot dan rating untuk rekapitulasi tabel IFE, EFE dilakukan dengan menjumlahkan nilai (rating/bobot) yang didapat dari responden dalam variabel yang sama, kemudian dibagi dengan jumlah responden.

Pada bagian selanjutnya dalam matriks IFE dan EFE diberikan nilai akhir perhitungan. Detail contoh perhitungan dan hasil perhitungan survey untuk skor bobot faktor internal dan eksternal diberikan pada Lampiran 8, 9 dan 10.

4.1.1. Evaluasi Faktor Internal

Penilaian internal berupaya mengidentifikasi dan evaluasi kekuatan serta kelemahan suatu organisasi dalam area fungsional yang dicakup termasuk didalamnya adalah manajemen, pemasaran, keuangan/akuntansi, produksi/operasi, penelitian dan pengembangan serta sistim informasi [25]. Langkah-langkah dalam membuat evaluasi dengan matriks IFE adalah sebagai berikut [26]:

i. Membuat daftar faktor-faktor internal utama yang mempengaruhi.

ii. Memberikan bobot pada setiap faktor yang berkisar dari 0,0 (tidak penting) sampai 1,0 (penting). Jumlah total seluruh bobot yang diberikan pada faktor-faktor yang teridentifikasi harus sama dengan satu.

iii. Memberi peringkat antara 1 sampai 4 pada setiap faktor eksternal utama untuk menunjukkan seberapa efektif strategi dalam suatu organisasi dalam merespon faktor tersebut. Dimana sangat lemah (peringkat=1), lemah (peringkat 2), kuat (peringkat 3) dan sangat kuat (peringkat 4). Pemberian bilai peringkat untuk faktor kekuatan bersifat positif (kekuatan yang semakin besar diberi rating +4, tetapi bila kekuatan kecil diberi rating +1), Pemberian nilai rating kelemahan adalah kebalikannya [27].

iv. Mengalikan bobot setiap faktor dengan peringkatnya untuk menemukan skor bobot.

v. Menjumlahkan skor bobot untuk setiap variabel untuk mendapatkan Total Skor Bobot EFE untuk organisasi.

4.1.1.1.Analisa Faktor Internal

Internal Factor Evaluation (IFE) pada penelitian ini mencakup faktor-faktor kemampuan internal organisasi dalam penyediaan layanan keamanan CA kepada publik. Berikut adalah faktor kekuatan (*strength*) dan kelemahan (*weakness*) yang diidentifikasi :

4.1.1.1.1. Kekuatan (Strength)

S1. Visi Misi Lemsaneg

Visi Misi Lemsaneg yang tertuang dalam Peraturan Kepala Lembaga Sandi Negara nomor 7 tahun 2009, mendukung untuk menjadi sebuah

LPND yang terpercaya, professional dan mandiri dalam persandian. Selain menyelenggarakan operasional pengamanan informasi, salah satu misinya adalah menyusun kebijakan dalam bidang persandian tidak hanya disektor pemerintahan tetapi juga sektor publik. Dalam Perka yang sama, Lemsaneg juga memiliki misi untuk memfasilitasi dan mengembangkan persandian sektor pemerintahan dan publik serta menyelenggarakan operasional pengamanan informasi sebagai unsur pelayanan tugas pokok.

S2. Kompetensi Dalam Pengamanan

Kompetensi yang menjadi faktor kekuatan dalam hal penyediaan layanan CA adalah kemampuan untuk melaksanakan pengamanan informasi dan telekomunikasi. Faktor ini diidentifikasi sebagai faktor kekuatan bagi karena sampai saat ini Lemsaneg dapat melakukan tugas pengamanan informasi sesuai teknologi atau perangkat yang digunakan oleh instansi pemerintah.

S3. Kemampuan Mengatur Aspek Keamanan

Salah satu kompetensi yang dimiliki adalah kemampuan memproduksi algoritma dan sistem sandi serta pengaturan, pembaharuan setiap parameter yang digunakan dalam sebuah proses penyandian. Pengaturan dan pembaharuan aspek keamanan dapat dilakukan secara *online* atau *offline* sesuai kebutuhan.

S4. Penelitian dalam Pengamanan Berbasis IP

Lemsaneg secara mandiri memiliki dan telah melaksanakan fungsi pengkajian melalui Pusat penelitian dan pengembangan Persandian. Didalamnya dilakukan pengkajian tidak hanya pada sisi algoritma/sistem sandi tetapi juga mengenai material komunikasi peralatan/perangkat hardware dan software serta bidang jaringan.

S5. Kemampuan Operasional Layanan CA

Meski belum menyediakan layanan CA, lemsaneg telah memiliki pengalaman dan operasional penyediaan layanan keamanan seperti CA, e-procurement meskipun dalam lingkup pemerintahan.

S6. Kemampuan Differensiasi

Kemampuan differensiasi dalam hal kemampuan membangun layanan CA menggunakan sistem atau algoritma mandiri (*proprietary algorithm*) menjadi faktor kekuatan dalam penyediaan layanan CA.

S7. Adanya Jaringan Unit Tehnis Persandian

Saat ini Lemsaneg dapat melakukan komunikasi dan berkoordinasi dalam hal pengamanan informasi dengan jaringan (Unit Tehnis Persandian) yang ada di daerah dan di luar negeri. Unit Tehnis Persandian dapat dijadikan sebagai asset dalam membentuk jaringan kerja Lemsaneg di daerah dan di luar negeri.

4.1.1.1.2. Kelemahan (Weakness)

W1. Struktur Organisasi

Dalam Struktur Organisasi Tata Kerja (SOTK) Lemsaneg belum ada struktur (fungsi divisi) yang memiliki tugas untuk melayani kebutuhan publik dalam hal penyediaan layanan keamanan.

W2. Koordinasi Penyediaan Layanan CA

Penyediaan layanan CA bagi keperluan publik bagi Lemsaneg adalah hal baru yang membutuhkan koordinasi yang kompleks karena belum pernah diadakan sebelumnya. Termasuk dalam hal ini adalah tuntutan layanan CA harus diterima dalam lingkup nasional dan internasional.

W3. Identifikasi Peluang

Meski terdapat peluang bagi Lemsaneg untuk tampil sebagai pendatang baru dalam hal penyedia jasa layanan keamanan CA untuk publik secara

langsung, faktor ini menjadi unsur kelemahan mengingat belum terdeteksinya peluang tersebut disisi internal. Termasuk diantaranya bahwa Lemsaneg adalah organisasi pemerintahan (non profit). Dengan adanya penyedia Layanan CA nasional tidak hanya mengamankan data-data penting yang di olah perangkat CA luar negeri tetapi akan memudahkan identifikasi pengguna transaksi elektronik di Indonesia.

W4. Sumber Daya bidang Penyediaan Layanan CA

Jumlah dan kualitas Sumber Daya yang harus dipersiapkan untuk melakukan penyediaan layanan CA kepada publik perlu dialokasikan dan ditambah mengingat kebutuhan mempelajari, mengatur dan melakukan fungsi pembaharuan (*update*) untuk kebutuhan secara global.

W5. Kompleksitas Layanan CA

Pembangunan layanan CA memiliki tingkat kompleksitas yang tinggi dari sisi tehnis dan pengaturan setiap aspeknya. Beberapa komponen layanan keamanan yang harus di bentuk adalah :

i. Sistem dan Metodologi Pengendalian Akses (*Access Control Systems and Methodology*).
ii. Keamanan Telekomunikasi dan Jaringan (*Telecommunications and Network Security*).
iii. Kriptografi (*Cryptography*).
iv. Model dan Arsitektur Keamanan (*Security Architecture & Models*).
v. Keamanan Pengoperasian (*Operations Security*).
vi. Keamanan Aplikasi dan Pengembangan Sistem (*Application and Systems Development Security*).
vii. Rencana Kesinambungan Usaha dan Pemulihan Bencana (*Disaster Recovery and Business Continuity Plan - DRP/BCP*).
viii. Hukum, Investigasi, dan Etika (*Laws,Investigations and Ethics*).
ix. Keamanan Fisik (*Physical Security*).
x. Audit (*Auditing*).

W6. Produk Hukum Internal

Belum adanya produk hukum internal untuk tugas pengamanan (ataupun persandian) bagi kebutuhan pelayanan kepada publik menjadi faktor kelemahan bagi Lemsaneg dalam hal penyediaan layanan CA kepada publik di era konvergensi.

W7. Sumber Dana & Pengambilan Keputusan

Faktor sumber dana dan pusat pengambilan keputusan yang memerlukan persetujuan pemerintah pusat dapat menjadi kendala dalam hal keputusan setiap strategi termasuk diantaranya dalam penyediaan layanan CA di era konvergensi bagi keperluan publik.

4.1.1.2. Skor Bobot Faktor Internal

Hasil identifikasi faktor internal organisasi (*Internal Factor Evaluation*-IFE) dan penilaiannya diperlihatkan pada Tabel 4.3 berikut.

Tabel 4.3. Matrik IFE Penyediaan Layanan CA

Faktor Internal Utama		**Peringkat**	**Bobot**	**Skor Bobot**
kekuatan (*Strength*):				
S1	Sesuai Visi Misinya Lemsaneg dapat penyelenggarakan layanan-layanan keamanan untuk kepentingan publik	3.409	0.077	0.261
S2	Kompetensi/kemampuan untuk pengamanan informasi dan telekomunikasi	3.455	0.063	0.217
S3	Kemampuan untuk mengatur setiap aspek keamanan (misal kunci penyandian, sistem sandi, algoritma dan parameter lain yang diperlukan)	3.591	0.079	0.282
S4	Lemsaneg telah melakukan penelitian dan penyediaan layanan keamanan berbasis *Internet Protokol* (IP)	3.682	0.071	0.260
S5	Kemampuan penelitian, pembangunan & operasional layanan sejenis (*Certificate Authority*)	3.727	0.069	0.259
S6	kemampuan membangun layanan *Certificate Authority* (CA) dengan differensiasi	3.682	0.074	0.271
S7	Adanya komunikasi atau berhubungan dalam hal koordinasi pengamanan informasi dengan Unit Tehnis Persandian	3.591	0.076	0.274
		Nilai Strength :	**0.508**	**1.825**

kelemahan (*weakness*):				
W1	Perlu struktur organisasi (dalam Lemsaneg) yang melayani penyediaan layanan keamanan bagi publik	1.318	0.082	0.108
W2	Penyediaan layanan CA kepada publik adalah hal baru dan membutuhkan koordinasi yang kompleks	1.318	0.080	0.106
W3	Lemsaneg berpeluang sebagai pendatang baru dalam penyedia jasa layanan keamanan CA (*publik service*)	1.636	0.056	0.092
W4	Alokasi Jumlah dan Kualitas Sumber Daya yang perlu dipersiapkan	1.273	0.086	0.110
W5	Tingkat kompleksitas yang tinggi (rumit)	1.909	0.051	0.098
W6	Belum adanya produk hukum internal untuk tugas pengamanan (ataupun persandian) bagi kepentingan publik	1.545	0.063	0.098
W7	Lemsaneg adalah salah satu lembaga pemerintahan non departemen dimana pengambilan keputusan dan sumber dana sangat bergantung pada pemerintah pusat	1.864	0.065	0.121
		Nilai Weakness :	**0.992**	**0.731**
			Total Skor Bobot Faktor Internal :	**2.556**

Dari hasil perhitungan pada Tabel 4.3 didapatkan nilai Total Skor Bobot Faktor Internal adalah sebesar 2,556.

4.1.2. Evaluasi Faktor Eksternal

Dalam matriks Evaluasi Faktor Eksternal (*External Factor Evaluation*-EFE) akan diidentifikasi peluang dan ancaman yang akan mempengaruhi penyediaan layanan keamanan CA di industri telekomunikasi. Dalam pendekatan manajemen strategis, matriks ini digunakan untuk mengevaluasi informasi ekonomi, sosial, budaya, demografis, lingkungan, politik, pemerintahan, hukum, teknologi dan kompetitif [26].

Langkah-langkah dalam membuat evaluasi dengan matriks EFE adalah sebagai berikut [26]:

i. Membuat daftar faktor-faktor eksternal utama yang mempengaruhi.

ii. Memberikan bobot pada setiap faktor yang berkisar dari 0,0 (tidak penting) sampai 1,0 (penting). Jumlah total seluruh bobot yang diberikan pada faktor-faktor yang teridentifikasi harus sama dengan satu.

iii. Memberi peringkat antara 1 sampai 4 pada setiap faktor eksternal utama untuk menunjukkan seberapa efektif strategi dalam suatu organisasi dalam merespon faktor tersebut. Dimana 4=responnya sangat bagus, 3=responnya diatas rata-rata, 2=responnya rata-rata, 1=responnya dibawah rata-rata. Pemberian bilai peringkat untuk faktor peluang bersifat positif (peluang yang semakin besar diberi rating +4, tetapi bila peluang kecil diberi rating +1), Pemberian nilai rating ancaman adalah kebalikannya [27].

iv. Mengalikan bobot setiap faktor dengan peringkatnya untuk menemukan skor bobot.

v. Menjumlahkan skor bobot untuk setiap variabel untuk mendapatkan Total Skor Bobot EFE untuk organisasi.

4.1.2.1.Analisa Faktor Eksternal

External Factor Evaluation (EFE) pada penelitian ini mencakup faktor-faktor kemampuan eksternal yang mempengaruhi organisasi dalam hal penyediaan layanan keamanan CA kepada publik. Berikut adalah faktor peluang (*opportunities*) dan ancaman (*treath*) yang diidentifikasi :

4.1.2.1.1. Peluang (Opportunities)

O1. Kebutuhan Layanan Keamanan di Era Konvergensi

Layanan keamanan CA dalam komunikasi berbasis IP di era konvergensi merupakan kebutuhan yang sangat penting. Salah satu indikatornya adalah besarnya ancaman keamanan terhadap pengambilan informasi data digital dalam transaksi elektronik serta belum adanya CA di Indonesia yang memiliki jangkauan nasional ataupun internasional di era konvergensi.

O2. Dukungan Undang-Undang

Penyelenggaraan layanan keamanan CA didukung dengan adanya undang-undang transaksi elektronik (UU ITE) yang mewajibkan penggunaan layanan CA lokal dalam setiap transaksi elektronik. Meski dalam Undang Undang penyelenggaraan CA disebutkan pula bahwa penyedia Layanan

CA dapat menggunakan layanan CA luar negeri, layanan CA luar negeri wajib tersertifikasi sesuai standar, berbadan hukum Indonesia dan berdomisili di Indonesia serta terikat pada fungsi pengawasan (audit).

O3. Belum adanya Organisasi CA Global Indonesia

Saat ini belum ada organisasi/perusahaan layanan CA di Indonesia, yang dapat melayani dalam cakupan nasional atau internasional. Beberapa perusahan telekomunikasi seperti PT.Telkom menyediakan layanan i-trust sebagai cyber notary dalam lingkup internal, atau Ina sign untuk aplikasi e-procurement pemerintah daerah Surabaya.

O4. Produk Pengganti Layanan CA

Tidak adanya produk pengganti yang setara ataupun lebih baik dari sistem pengamanan yang ditawarkan oleh layanan CA untuk komunikasi berbasis IP di era konvergensi menjadi sebuah peluang bagi organisasi yang akan menyediakan layanan CA.

O5. Remunerasi

Dalam membentuk *good governance* yang dicanangkan oleh pemerintah, setiap Lembaga Negara harus dapat terukur dapat melayani publik. Penyediaan layanan CA bagi keperluan publik merupakan peluang bagi Lemsaneg untuk memenuhi kewajiban dalam melayani kebutuhan publik dan mencapai posisi strategis dalam pemerintahan.

O6. Kesiapan Infrastruktur Data

Penyediaan layanan CA didukung oleh infrastruktur telekomunikasi yang telah mampu mengirimkan informasi dalam bentuk data sampai dengan *streaming* data. Kesiapan infrastruktur data dan besarnya pengguna layanan data juga menjadi peluang penyediaan layanan berbasis data seperti layanan keamanan CA.

O7. Keamanan dan Tingkat Kepuasan Pengguna

Adanya pengamanan pada setiap transaksi elektronik akan meningkatkan keamanan, efisiensi transaksi dan tingkat kepuasan pelanggan, artinya CA merupakan hal yang dibutuhkan oleh publik pengguna transaksi digital di era konvergensi. Hal ini dapat dikategorikan sebagai peluang untuk menyediakan layanan keamanan CA bagi keperluan publik.

4.1.2.1.2. Ancaman (Treath)

T1. Investasi Besar

Dibutuhkan investasi yang besar untuk membuat layanan CA dengan jangkauan global. Hal ini juga terkait dengan kemampuan financial negara, karena sumber dana Lembaga Sandi Negara berasal dari Negara.

T2. Kualitas Jaringan Data

Salah satu faktor yang harus dipenuhi dalam pengamanan informasi adalah kualitas media pengirim. Kualitas harus baik karena setiap informasi yang diamankan menggunakan metode penyandian tidak boleh rusak atau hilang, karena rentan tidak bisa dikembalikan sesuai informasi aslinya.

T3. Security Awareness

Dibutuhkan tingkat pengetahuan dan kesadaran mengenai keamanan (security awareness) yang pengguna (dalam hal ini publik) untuk dapat mendukung dan mengoptimalkan penggunaan layanan-layanan keamanan termasuk layanan CA.

T4. Persaingan Global dalam Penyediaan Layanan Keamanan CA

Saat ini tingkat persaingan yang dihadapi untuk menjadi penyedia jasa layanan CA dalam tingkat global akibat sifat *borderless* (tanpa batas) dari era konvergensi.

T5. Jangkauan layanan Pesaing

Penyedia jasa layanan CA yang ada di Indonesia adalah operator luar negeri baik perusahaan swasta, organisasi atau akademisi yang kehadirannya telah mendunia.

T6. Kebutuhan Hadir Mendunia (*Global Presence*)

Karena dalam era konvergensi terbuka batas dunia maka layanan CA lokal harus hadir dan diterima tidak hanya nasional tetapi juga internasional. Oleh karena itu diperlukan pemenuhan standar-standar keamanan minimal seperti jaminan stabilitas financial, kompetensi tehnis nasional seperti SNI 19-7125-2005 dan kompetensi standar internasional ISO/IEC 27000:2005.

4.1.2.2.Skor Bobot Faktor Eksternal

Matriks EFE yang mencakup faktor peluang dan ancaman Penyediaan layanan CA diberikan pada Tabel 4.4.

Tabel 4.4 Matrik EFE Penyediaan Layanan CA

Faktor Eksternal Utama		**Bobot**	**Peringkat**	**Skor Bobot**
kekuatan (*Strength*):				
O1	Kebutuhan Layanan Keamanan CA di Era Konvergensi	3.682	0.094	0.347
O2	Dukungan Undang-undang	3.773	0.083	0.315
O3	Belum ada organisasi/perusahaan layanan CA di Indonesia.	3.273	0.060	0.197
O4	Belum ada Solusi yang setara dengan layanan CA	2.864	0.035	0.099
O5	Adanya Tuntutan Remunerasi bagi LPND	3.591	0.076	0.272
O6	Kesiapan Infrastruktur Data	3.682	0.062	0.230
O7	Layanan CA meningkatkan keamanan, efisiensi dan tingkat kepuasan pengguna transaksi elektronik	3.773	0.095	0.358
Nilai Opportunities :			**0.506**	**1.818**

kelemahan (*weakness*):				
T1	Investasi Besar untuk membangun Layanan CA	1.500	0.090	0.134
T2	Kualitas jaringan telekomunikasi (data)	1.273	0.098	0.125
T3	Dibutuhkan pengetahuan dan kesadaran mengenai keamanan (*security awareness*)	1.636	0.101	0.128
T4	Persaingan Global	3.000	0.076	0.124
T5	Kompetensi Persaingan Lemsaneg terhadap jangkauan layanan pesaing	3.000	0.047	0.141
T6	Kebutuhan hadir mendunia	1.409	0.084	0.119
		Nilai Treath :	**1.0**	**0.772**
			Total Skor Bobot Faktor Eksternal :	**2.590**

Dari hasil perhitungan pada Tabel 4.3 didapatkan nilai Total Skor Bobot Faktor Eksternal adalah sebesar 2,590.

1.8. Tahap Pencocokan

Pada tahap pencocokan akan dilakukan perumusan awal alternatif strategi yang mungkin dilakukan dalam penyediaan layanan CA. Pada tahap pencocokan dalam penelitian ini hanya akan dibahas mengenai alternatif strategi dari matriks IE (Internal Eksternal) dan SWOT (*Strength Weakness Opportunities Threat*).

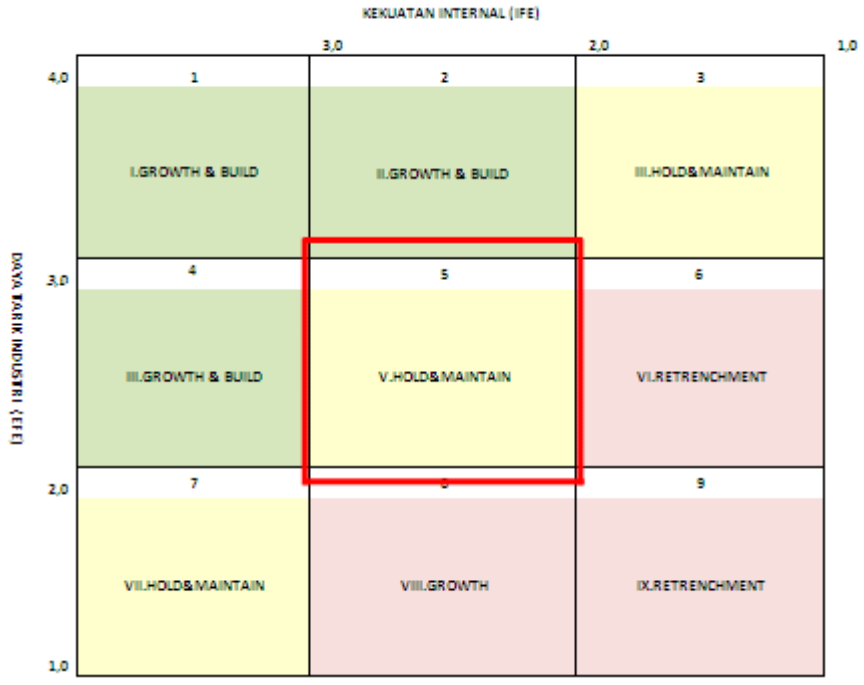
4.2.1. Matriks Internal Eksternal

Matrik internal eksternal ini dikembangkan dari model *General Electric* (GE Model), matriks internal eksternal diperlihatkan pada Gambar 4.3. Pemodelan strategi internal eksternal tersebut digunakan untuk mengidentifikasikan 9 (sembilan) sel yang digunakan untuk penentuan strategi organisasi, namun pada prinsipnya kesembilan sel strategi tersebut mengelompokkan hasil analisis data menjadi tiga strategi utama yaitu [26][27]:

1. *Growth Strategy* yang merupakan pertumbuhan perusahaan itu sendiri atau upaya diversifikasi.
2. *Stability Strategy* adalah strategi yang diterapkan tanpa mengubah arah strategi yang telah diterapkan.

3. *Retrenchment Strategy* adalah usaha memperkecil atau mengurangi usaha yang dilakukan organisasi atau perusahaan.

Matriks IE didasarkan pada dua dimensi kunci yaitu skor bobot IFE total pada sumbu x dan skor bobot EFE total pada sumbu y. Berdasarkan perhitungan dalam identifikasi faktor eksternal dan internal organisasi [25]. Pada tahap input dalam Tabel 4.1 dan Tabel 4.2, diperoleh rasio internal : eksternal untuk penyediaan layanan CA di era konvergensi adalah 2.556 : 2.590. Dari hasil perbandingan ini menunjukan bahwa layanan CA masuk dalam sel *hold and maintain* seperti diperlihatkan pada Gambar 4.3 berikut.



Gambar 4.3 Matriks IE Penyediaan Layanan CA

Strategi yang direkomendasi dalam sel *hold and maintain* adalah strategi menjaga dan mempertahankan seperti penetrasi pasar dan pengembangan produk [25]. Strategi yang dapat diterapkan pada sel ini adalah *stability strategy* dan *growth strategy* melalui integrasi horizontal [27]. Definisi dan contoh strategi sesuai matriks IE diperlihatkan pada Tabel 4.5 berikut.

Tabel 4.5 Strategi Alternatif Penyediaan Layanan CA Sesuai Matriks IE

Jenis Strategi		Definisi
Stability (Intensif)	Penetrasi Pasar	Mencari pangsa pasar yang lebih besar untuk produk atau jasa melalui upaya pemasaran yang baik
	Pengembangan Produk	Mengupayakan peningkatan penjualan melalui perbaikan produk saat ini maupun hasil pengembangan
Growth	Integrasi Horizontal	Mengupayakan Kepemilikan atau kendali yang lebih besar atas pesaing

4.2.2. Matriks SWOT

Dalam Manajemen Strategis dikatakan bahwa, strategi sering kali di definisikan sebagai pencocokan yang dibuat suatu organisasi antara sumber daya dan keterampilan eksternalnya serta peluang dan resiko yang diciptakan oleh faktor eksternalnya [26]. Selain matriks IE, alat yang dapat digunakan untuk menyusun strategi adalah matriks *Strength Weakness Opportunities Threath* (SWOT). Dalam analisis SWOT digambarkan kuadran posisi organisasi dan merumuskan 4 (empat) jenis alternatif strategi terkait dengan optimalisasi kombinasi faktor internal dan eksternal.

Pada tahap ini penulisan mengidentifikasi faktor kekuatan, kelemahan, peluang dan ancaman dari organisasi sesuai hasil tahap input. Pengidentifikasian faktor kekuatan dan kelemahan digunakan untuk menyusun strategi mencapai peluang yang ada serta mengurangi potensi ancaman yang mungkin bisa mengganggu organisasi.

4.2.2.1. Kuadran SWOT

Analisis SWOT membandingkan antara faktor eksternal dengan faktor internal. Dengan menggunakan perumusan :

Faktor internal :

$Nilai_{(kekuatan\text{-}kelemahan)} = \Sigma$ (rating (S_n) x bobot (S_n)) - Σ (rating (W_n) x bobot (W_n)) (pers 4.9)

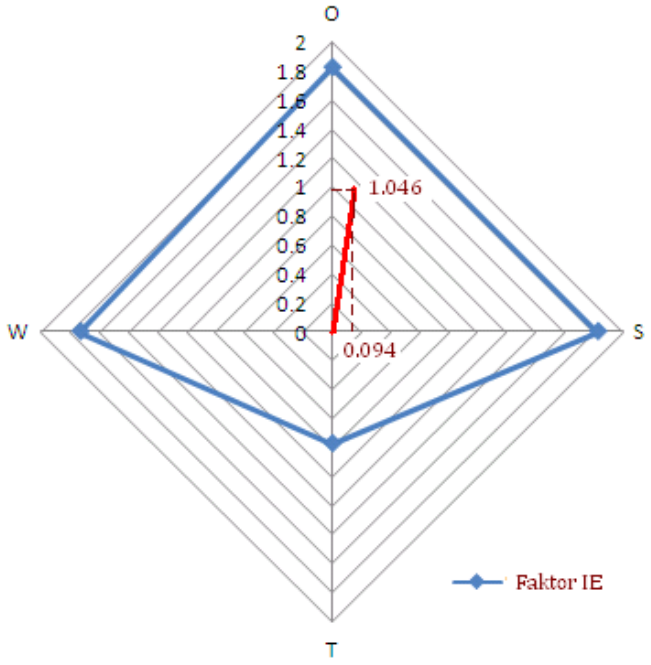
$Nilai_{(kekuatan\text{-}kelemahan)} = 1{,}825\text{-}1{,}731=0{,}094$

Faktor eksternal :

$Nilai_{(peluang\text{-}tantangan)} = \Sigma$ (rating (O_n) x bobot (O_n)) - Σ (rating (P_n) x bobot (P_n)) (pers 4.2)

$Nilai_{(peluang\text{-}tantangan)} = 1{,}818\text{-}0{,}772=1{,}046$

Dari hasil perhitungan selisih setiap faktor adalah internal sebesar 0,094 dan eksternal 1,046. Pada Gambar 4.4 berikut diperlihatkan kuadran SWOT internal dan eksternal sesuai perhitungan identifikasi internal eksternal tersebut.



Gambar 4.4 Kuadran SWOT Penyediaan Layanan CA

Kuadran I merupakan situasi yang sangat menguntungkan dimana sebuah organisasi atau perusahaan memiliki peluang dan kekuatan sehingga dapat memanfaatkan peluang yang ada [27]. Strategi yang harus diterapkan dalam kondisi ini adalah mendukung kebijakan pertumbuhan yang agresif (Growth Oriented Strategy) [25][27].

Strategi pertumbuhan (Growth Strategy) didesain untuk mencapai pertumbuhan yang dapat dicapai dengan memberikan strategi biaya terbaik/termurah, mengembangkan produk baru, menambah kualitas produk atau jasa atau meningkatkan akses ke pasar yang lebih luas.

4.2.2.2. Analisis SWOT

Dari hasil identifikasi faktor eksternal dan internal, posisi organisasi dalam kuadran SWOT. Dengan mempertimbangkan arah dan rekomendasi strategi matriks IE serta kuadran SWOT, didapatkan 4 jenis strategi yaitu :

[1]. Strategi SO

Strategi *Strength-Opportunity* (*SO Strategy*), yaitu strategi yang memanfaatkan kekuatan internal untuk menarik keuntungan. Strategi dibuat berdasarkan visi misi organisasi dengan menggunakan kekuatan untuk memanfaatkan peluang. Strategi SO dan referensi faktor kekuatan dan peluangnya adalah sebagai berikut :

SO 1. Menetapkan cakupan layanan CA yang akan diberikan untuk keperluan publik di era konvergensi, memastikan *core competencies* sesuai hasil analisa kebutuhan. (S1, S2, S3, S4, S5,O1, O2, O3, O7)

SO 2. Membentuk dan membangun Layanan CA dengan sistem persandian dan algoritma proprietary. (S1, S2, S3, S4, S5,O1, O2, O3, O4, O5, O7,O8)

SO 3. Menguatkan strategi sosialisasi (marketing) untuk membentuk identitas dan merk layanan kepada publik secara global (S1, S2,S3,O1,O2,O3,O6,O7).

SO 4. Mengatur seluruh aspek keamanan informasi dalam era konvergensi sesuai kebutuhan sistem pengamanan. (S1, S2,S3,O1,O2,O3,O6,O7).

[2]. Strategi WO

Strategi *Weakness-Opportunity* (*WO Strategy*), yaitu strategi untuk memperbaiki kelemahan internal dengan mengambil keuntungan dari peluang eksternal. Strategi WO dan referensi faktor kelemahan dan peluangnya adalah sebagai berikut :

WO 1. Menguatkan kemampuan untuk "melayani publik", juga termasuk kaitan remunerasi (W1,W2,W3,W4,O1,O2,O3).

WO 2. Membentuk Struktur (dalam Lemsaneg) untuk melayani kebutuhan publik (W1,W2,W3,W4,W5,W6,O1,O2,O3,O4,O5).

WO 3. Lebih melakukan sosialisasi & marketing mengenai adanya CA lokal (Indonesia) (W2, W3, W7,O1,O2,O3,O6,O7).

WO 4. Aktif Berkontribusi dalam hal pengaturan perundang-undangan terkait Layanan CA di era konvergensi (W2, W3, W7,O1,O2,O3,O6,O7).

[3]. Strategi ST

Strategi *Strength-Threat* (*ST Strategy*), yaitu strategi dengan menggunakan kekuatan untuk menghindari atau mengurangi dampak peluang eksternal. Strategi ST dan referensi faktor kekuatan dan ancamannya adalah sebagai berikut :

ST 1. Mengajukan investasi/Kerjasama dalam hal pembangunan CA dengan pemerintah ataupun lembaga/departemen terkait (S1,S2, S3,S4,S5,S6,T1,T4,T5,T6).

ST 2. Aktif mendukung upaya pemerataan telekomunikasi dan memberikan solusi-solusi pengamanan kepada publik (S1,S2,S3,S4,T2,T3,T5,T6).

ST 3. Melakukan kerjasama dengan antar pemerintah, organisasi, perusahaan penyedia layanan CA yang telah bersifat global (S1,S2,S3,S4,T2,T3,T5,T6).

[4]. Strategi WT

Strategi *Weakness-Threat* (*WT Strategy*), yaitu strategi taktik defensif untuk mengurangi kelemahan internal. Strategi WT dan referensi faktor kelemahan dan ancamannya adalah sebagai berikut :

WT 1. Aktif berkontribusi dalam hal pengaturan perundang-undangan terkait Layanan CA di era konvergensi (W1,W3,W7,T3,T5,T6).

1.9. Tahap Keputusan

Dalam pendekatan manajemen strategis, selain perumusan strategi-strategi pemeringkatan, digunakan pula tehnik analisis yang dirancang untuk menentukan daya tarik relatif dari berbagai strategi yang telah dirumuskan [26]. Tehnik tersebut adalah Matriks Perencanaan Strategi Kuantitatif (*Quantitatif Strategic Planning Matrix* - QSPM). Tehnik ini secara obyektif menunjukkan strategi yang relatif terbaik dengan kondisi yang telah dianalisa untuk dijalankan oleh organisasi. QSPM menggunakan analisis input dari tahap 1 dan hasil pencocokan dari analisis tahap 2 untuk secara obyektif menentukan strategi yang dapat dijalankan.

Jumlah Skor Keseluruhan Daya Tarik Total menunjukan strategi yang paling menarik disetiap rangkaian strategi alternative, dengan faktor internal eksternal yang dapat mempengaruhi keputusan strategi. Pembobotan dilakukan dengan melakukan wawancara dan kuisioner kepada pihak manajemen.

4.3.1. Strategi Alternatif Penyediaan Layanan CA

Dalam teori pemodelan Porter 5 Forces, menurut Porter strategi yang memungkinkan organisasi untuk memperoleh keunggulan kompetitif terdiri dari 3 (tiga) landasan berbeda yaitu Strategi Kepemimpinan Biaya, Strategi Differensiasi dan Strategi Fokus. Ketiga jenis strategi ini disebut sebagai strategi generik (*generic strategic*) yang dapat diterapkan dalam mencapai keunggulan kompetitif sebuah organisasi atau perusahaan.

Pada hasil analisa matriks IE (pada bagian 4.2.1) didapatkan posisi dalam sel *hold and maintain,* strategi yang direkomendasi adalah strategi menjaga dan mempertahankan seperti penetrasi pasar dan pengembangan produk [25]. Strategi yang dapat diterapkan pada sel ini adalah *stability strategy* dan *growth strategy* melalui integrasi horizontal [27]. Dalam analisa SWOT (pada bagian 4.2.2) didapatkan kuadran posisi organisasi berada pada kuadran I. Strategi yang harus diterapkan dalam kondisi ini adalah mendukung kebijakan pertumbuhan yang agresif (*Growth Oriented Strategy*). Pada Tabel 4.6 berikut diidentifikasi rekomendasi strategi sesuai hasil analisa Porter 5 Forces, IE Matriks dan Analisis SWOT.

Tabel 4.6 Pilihan Strategi Alternatif Penyediaan Layanan CA

Sumber	Jenis & Definisi Strategi Alternatif		
Porter 5 Forces (Strategy Generic)	Keunggulan/ kepemimpinan biaya	Menekankan pemroduksian produk/layanan yang distandarisasi dengan biaya per unit yang sangat rendah untuk para konsumen yang peka terhadap harga	
		1. Strategi Biaya Rendah	Strategi menawarkan produk/jasa kepada konsumen pada harga terendah di industri
		2. Strategi Biaya Terbaik	Strategi menawarkan produk/jasa kepada konsumen pada harga terbaik di industri
	Differensiasi	Strategi yang bertujuan menghasilkan produk dan jasa yang dianggap unik di Industri dan diarahkan kepada konsumen yang relatif peka terhadap harga.	
	Fokus	Strategi memproduksi produk dan jasa yang memenuhi kebutuhan sekelompok kecil konsumen.	
		1. Fokus Biaya Rendah	Strategi menawarkan produk atau jasa kepada sekelompok kecil konsumen dengan nilai terbaik yang tersedia dipasar
		2. Fokus Nilai Terbaik	Strategi menawarkan produk atau jasa kepada sekelompok kecil konsumen pada harga terendah yang tersedia di industri
Matriks IE	*Stability* (Intensif)	Penetrasi Pasar	Mencari pangsa pasar yang lebih besar untuk produk atau jasa melalui upaya pemasaran yang baik
		Pengembangan Produk	Mengupayakan peningkatan penjualan melalui perbaikan produk saat ini maupun hasil pengembangan
	Growth	Integrasi Horizontal	Mengupayakan Kepemilikan atau kendali yang lebih besar atas pesaing
SWOT	*Growth Oriented Strategy*	Strategi Kepemimpinan Biaya	Menekankan pemroduksian produk/layanan yang distandarisasi dengan harga rendah atau harga terbaik
		Pengembangan/ Penambahan kualitas Produk	Mengupayakan peningkatan penjualan melalui perbaikan produk saat ini maupun hasil pengembangan.
		Pengembangan Pasar	Mencari pangsa pasar yang lebih besar untuk produk atau jasa melakui upaya pemasaran yang baik.
		Penetrasi Pasar	Memperkenalkan produk atau jasa ke wilayah geografis baru.

4.3.2. Identifikasi Strategi untuk QSPM

Secara konseptual, QSPM menentukan daya tarik relatif dari berbagai strategi yang dibangun berdasarkan faktor-faktor keberhasilan penting eksternal dan internal [26]. Kemudian faktor-faktor tersebut dibandingkan terhadap strategi alternatif yang mungkin dilakukan oleh sebuah organisasi atau persahaan. Daya tarik relatif dari setiap serangkaian strategi alternatif dihitung dengan menentukan dampak kumulatif dari setiap faktor penting eksternal dan internal [26].

Pada Tabel 4.4 telah diidentifikasi Strategi Alternatif yang dapat diterapkan dalam penyediaan layanan CA. Untuk memudahkan proses justifikasi manajemen untuk menentukan alternatif strategi paling menarik (terbaik) maka strategi yang telah diidentifikasi tersebut dikelompokan menjadi 3 alternatif Stratetegi untuk dimasukkan dalam matriks QSPM. Pada Tabel 4.5 diberikan 3 alternatif strategi yang akan dimasukkan sebagai pilihan strategi dalam penyediaan layanan CA.

4.3.2.1.Fokus Nilai Terbaik

Strategi fokus nilai terbaik (*best value focus*) menawarkan jasa atau produk dengan harga yang lebih rendah, kualitas layanan, fitur layanan dan lain-lain. Organisasi dapat secara efektif menjalankan strategi berfokus dalam hubungannya dengan strategi differensiasi atau kepeminpinan biaya [26].

Strategi differensiasi dapat dilakukan dengan pengembangan produk (*produk development*) yang mengupayakan peningkatan penjualan dengan cara memperbaiki atau memodifikasi produk atau jasa yang ada saat ini. Melalui pengembangan produk memungkinkan dilakukan penambahan kualitas produk yang akan diberikan.

4.3.2.2.Pengembangan Pasar

Pengembangan pasar (*market development*) meliputi pengenalan produk atau jasa yang ada saat ini kewilayah-wilayah baru. Penetrasi Pasar adalah strategi

yang mengupayakan peningkatan pangsa pasar untuk produk atau jasa yang ada di pasar saat ini melalui upaya-upaya pemasaran yang lebih luas. Strategi pengembangan dan penetrasi pasar dapat dilakukan dengan menerapkan strategi-strategi marketing serta memperluas akses distribusi.

4.3.2.3.Integrasi Horizontal

Integrasi horizontal mengacu pada strategi yang mengupayakan kepemilikan atau kendali yang lebih besar terhadap pesaing. Salah satu contoh strategi horizontal adalah merger, akuisisi, pengambilalihan.

Tabel 4.7 Alternatif Strategi dalam QSPM

Alternatif	Strategi	Cakupan Strategi
1	Fokus	Pengembangan Produk
		Penambahan kualitas Produk
		Differensiasi
		Fokus Nilai Terbaik
		Kepemimpinan Biaya
2	Pengembangan Pasar	Pengembangan Pasar
		Penetrasi Pasar
		Memperluas Akses Distribusi
3	Integrasi	Integrasi Horizontal

Tabel 4.7 diatas memperlihatkan 3 alternatif strategi yang dirumuskan sesuai hasil analisa tahap sebelumnya (Tabel 4.6). Justifikasi manajemen tahap ke 2 akan membuat keputusan strategi mana yang paling menarik untuk dijalankan organisasi dengan menggunakan metode QSPM.

4.3.3. Perhitungan Matriks QSPM

Setelah dilakukan identifikasi terhadap strategi yang paling mungkin dilakukan dalam hal penyediaan layanan CA, dilakukan survey melalui wawancara dan kuisioner terhadap pihak manajemen terkait daya tarik relative terhadap strategi yang telah dirumuskan.

Langkah-langkah dalam membuat matriks QSPM adalah sebagai berikut [26]:

i. Membuat daftar berbagai peluang/ancaman eksternal dan kekuatan/kelemahan internal utama dikolom kiri QSPM.

ii. Memberikan bobot pada setiap faktor yang berkisar dari 0,0 (tidak penting) sampai 1,0 (penting). Jumlah total seluruh bobot yang diberikan pada faktor-faktor yang teridentifikasi (baik internal maupun eksternal) harus sama dengan 1 (satu).

iii. Mengidentifikasi berbagai strategi alternatif (telah dirumuskan pada tahap sebelumnya) yang harus dipertimbangkan dan diterapkan oleh organisasi. Mencatat strategi-strategi dalam baris teratas QSPM.

iv. Menentukan Skor Daya Tarik (*Attractiveness Score*-AS), didefinisikan sebagai nilai numerik yang mengindikasi daya tarik relatif dari setiap strategi. Skor daya tarik ditentukan dengan mengamati setiap faktor eksternal dan internal utama, dengan pertanyaan "apakah faktor ini mempengaruhi pilihan strategi yang dibuat?". Jika jawabannya adalah "ya" maka strategi kemudian perlu diperbandingkan relatif terhadap faktor utama tersebut. Secara khusus, skor daya tarik harus diberikan pada setiap strategi untuk menunjukan daya tarik relatif satu strategi atas strategi yang lain. Kisaran Skor Daya Tarik adalah 1=tidak memiliki daya tarik, 2=daya tariknya rendah, 3=daya tariknya sedang dan 4=daya tariknya tinggi. Jika jawabannya "tidak" maka strategi tidak perlu diperbandingkan relatif terhadap faktor utama tersebut.

v. Menghitung Skor Daya Tarik Total, *Total Attractiveness Score* (TAS). Didefinisikan sebagai hasil kali antara bobot dan Skor Daya Tarik disetiap baris. Semakin tinggi Skor Data Tarik Totalnya semakin menarik pula strategi alternative tersebut (hanya dengan mempertimbangkan faktor keberhasilan penting yang berdekatan).

vi. Menghitung Jumlah Keseluruhan Daya Tarik Total, *Sum Total Attractiveness Score* –STAS) disetiap kolom strategi.

Tabel 4.8 adalah hasil perhitungan QSPM untuk strategi penyediaan layanan CA di era konvergensi.

Tabel 4.8 Matriks QSPM

No.	Faktor Utama	Bobot	Fokus Nilai Terbaik		Pengembangan / Penetrasi Pasar		Integrasi Horizontal	
			AS	TAS	AS	TAS	AS	TAS
Internal								
I1	Visi Misi Lemsaneg	0.100	3.333	0.333	3.333	0.333	2.333	0.233
I2	Kompetensi/kemampuan pengamanan Lemsaneg	0.070	2.000	0.139	2.667	0.186	3.667	0.255
I3	Kemampuan manajemen aspek security	0.089	2.000	0.178	3.333	0.297	2.333	0.208
I4	Ketersediaan sarana pendukung CA (penelitian&operasional)	0.058	3.333	0.195	3.333	0.195	3.000	0.175
I5	Penelitian, pembangunan & operasional layanan *CA*	0.070	2.667	0.186	3.667	0.255	2.667	0.186
I6	kemampuan menjadi *CA* bagi publik (propietary algoritma).	0.070	2.667	0.186	3.667	0.255	2.667	0.186
I7	Pengaruh Dukungan Unit Tehnis Persandian	0.037	3.667	0.136	2.667	0.099	3.000	0.112
I8	Kemampuan struktur organisasi melayani publik	0.047	3.667	0.172	3.000	0.141	2.667	0.125
I9	Kompleksitas Koordinasi	0.078	3.667	0.286	2.667	0.208	3.333	0.260
I10	Peluang sebagai pendatang baru dalam penyedia jasa layanan keamanan CA (*publik service*)	0.070	2.667	0.186	3.667	0.255	3.000	0.209

I11	Jumlah dan Kualitas SDM	0.070	2.333	0.162	3.667	0.255	3.000	0.209
I12	Kompleksitas layanan CA	0.070	2.333	0.162	3.667	0.255	3.000	0.209
I13	Dukungan produk hukum internal untuk tugas pengamanan (ataupun persandian) bagi kepentingan publik	0.100	3.667	0.366	2.667	0.266	2.333	0.233
I14	Sumber Dana & Pengambilan Keputusan	0.111	3.000	0.334	3.667	0.409	3.000	0.334
		1.0						
Eksternal								
E1	Kebutuhan Tinggi di Era Konvergensi	0.111	2.333	0.258	3.333	0.369	3.333	0.369
E2	Dukungan Undang-undang & Hukum	0.101	3.000	0.304	3.667	0.371	2.667	0.270
E3	Tidak adanya CA lokal di Indonesia	0.080	2.333	0.186	3.667	0.292	3.000	0.239
E4	Pengganti Layanan CA	0.053	-	-	-	-	-	-
E5	Pengaruh Remunerasi	0.051	-	-	-	-	-	-
E6	Kesiapan Infratruktur Telekomunikasi (Data)	0.080	3.333	0.266	2.667	0.212	2.667	0.212
E7	Keamanan,efisiensi dan kepuasan yang dicapai oleh publik	0.101	3.333	0.337	3.000	0.304	3.333	0.337
E8	Investasi	0.080	3.000	0.239	2.667	0.212	3.000	0.239
E9	Kualitas jaringan data, sarana prasarana	0.080	2.333	0.186	4.000	0.319	3.333	0.266
E10	Security Awareness Publik	0.067	3.000	0.201	3.333	0.223	4.000	0.267
E11	Persaingan penyediaan layanan CA	0.051	2.333	0.118	4.000	0.202	3.000	0.152
E12	Kemampuan kehadiran mendunia	0.042	3.333	0.142	2.000	0.085	2.000	0.085
E13	Kesiapan Ekonomi & Teknologi di Indonesia untuk berorientasi keamanan	0.105	2.667	0.281	4.000	0.421	3.667	0.386
		1.0						
STAS				**5.539**		**6.421**		**5.756**

Setelah dilakukan penghitungan (detail hasil perhitungan diberikan di lampiran 11) nilai daya tarik total dan bobot setiap faktor eksternal internal terhadap setiap strategi yang mungkin dilakukan organisasi, didapat nilai tertinggi adalah 6,421 untuk strategi pengembangan dan penetrasi pasar.

4.3.4. Analisa Strategi Penyediaan Layanan CA bagi Lemsaneg

Dari hasil analisa potensi kompetitif penyediaan layanan CA di era konvergensi didapatkan bahwa tekanan dari kelima kekuatan dalam porter 5 force tersebut memberikan tekanan Medium (44%), artinya penyedia jasa layanan keamanan CA baru (dalam hal ini lemsaneg) dapat masuk kedalam industri dengan peluang untuk berhasil yang tinggi. Ditambah lagi dengan adanya dukungan undang-undang melalui UU ITE agar penyedia jasa layanan CA adalah pemain lokal (di Indonesia).

Dari hasil identifikasi dan analisis tahap sebelumnya di dapatkan nilai positif yang dimiliki Lembaga Sandi Negara salah satunya adalah kemampuan tehnis dalam hal penyediaan informasi dan sumber daya organisasi yang cukup dalam bidang pengamanan informasi. Meskipun tantangan yang harus dihadapi adalah saat ini penyedia jasa layanan CA di Indonesia adalah pemain perusahaan asing.

Nilai lebih lain yang dapat dilakukan oleh Lemsaneg adalah dari sisi differensiasi algoritma, mengingat panyedia jasa CA dari luar negeri tidak terdifferensiasi atau masih menggunakan algoritma standar.

Dari hasil formulasi strategi dengan pendekatan manajemen strategis, untuk menjadi sebuah penyedia jasa layanan CA bagi keperluan publik, lemsaneg harus memiliki strategi kearah pengembangan dan penetrasi pasar, dalam hal ini kepada publik secara langsung. Terlebih saat ini *security awareness* yang dimiliki publik belum tinggi serta menghadapi ancaman keamanan transaksi elektronik dalam jaringan berbasis IP. Juga tantangan global bahwa penyedia jasa layanan CA yang harus hadir mendunia.

Industri layanan CA merupakan peluang bagi Lemsaneg dalam mencapai posisi strategis di Indonesia. Pada Gambar 4.5 diperlihatkan strategi penyediaan

layanan CA kepada publik yang dapat dilakukan oleh Lemsaneg untuk mencapai posisi strategis.

Gambar 4.5. Strategi Penyediaan Layanan CA

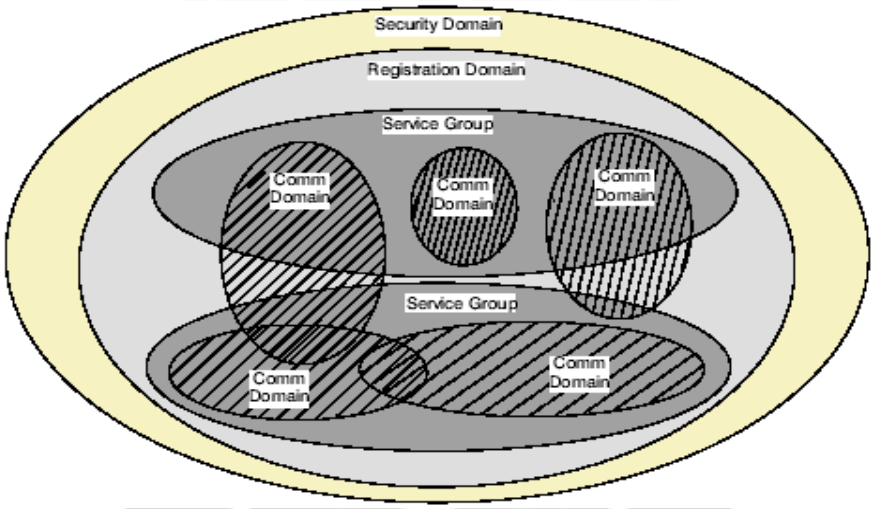
Untuk menyediakan layanan keamanan CA untuk keperluan publik, Lembaga Sandi Negara perlu melakukan langkah strategi sebagai berikut :

4.3.4.1. Peningkatan Kompetensi Kompetitif Pelayanan Publik

Untuk menyediakan layanan CA, Lemsaneg dapat melakukan strategi peningkatan kekuatan kompetitif internal organisasi dalam hal pelayanan kepada publik, sehingga dapat menjadi modal sebelum melakukan pelayanan CA kepada publik pengguna transaksi elektronik di era konvergensi. Langkah yang dapat diambil adalah menentukan struktur (divisi fungsional) yang dapat melakukan dan mengatur pelayanan kepada publik, meningkatkan kompetensi pegawai untuk pelayanan publik.

4.3.4.2. Membentuk Identitas & Merk Layanan CA

Strategi membentuk identitas kepada publik menjadi strategi yang penting diterapkan bagi Lemsaneg mengingat saat ini Lemsaneg masih berada dalam ruang lingkup pemerintahan dan belum memiliki identitas yang dikenal oleh publik. Sebelum membentuk identitas kepada publik, Lemsaneg harus menetapkan posisi dalam penyediaan layanan CA. Dalam hal ini Lemsaneg sebagai *policy authority*, *registration authority*, *certification authority, cyber notary* dan lain-lain. Pada Gambar 4.6 diperlihatkan visualisasi cakupan layanan keamanan yang dapat dibentuk.



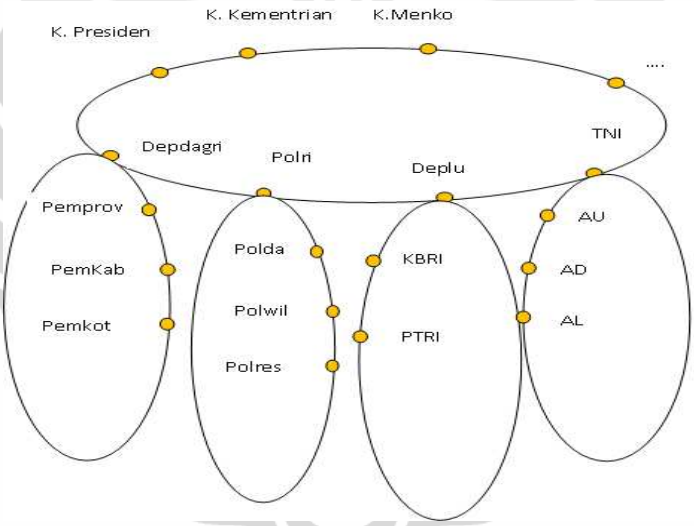
Gambar 4.6 Visualisasi Cakupan Layanan

Penetapan merk atau nama layanan kepada publik diperlukan untuk memudahkan publik mengenali Lemsaneg sebagai penyedia layanan keamanan. Merk ini juga digunakan untuk setiap layanan yang akan ditawarkan misalnya layanan manajemen kunci, layanan manajemen sertifikat, layanan *time stamping* transaksi elektronik dan lain-lain.

4.3.4.3. Menciptakan Strategic Partner

Menciptakan Strategic partner dalam hal ini penyedia layanan keamanan CA lain dilakukan untuk membentuk layanan baru, layanan bernilai tambah (*Value Added Service*) dan memperluas akses distribusi.

Industri layanan keamanan dalam teknologi berbasis IP seperti layanan CA merupakan industri yang memiliki kebersamaan pasar dengan pesaing (penyedia jasa layanan CA lain). Dalam industri ini konsumen dapat berada diluar negeri, yang menggunakan standar penyedia layanan keamanan CA di negara lain. Strategi yang dapat diterapkan Lemsaneg dalam menyediakan layanan CA bagi keperluan publik adalah melakukan kerjasama dengan *strategic partner*, dalam hal ini adalah penyedia jasa layanan CA lain yang telah memiliki jangkuan yang global dan standar internasional. Kerjasama dengan *strategic partner* dapat menguatkan posisi strategis Lemsaneg sebagai penyedia layanan-layanan keamanan secara global.



Gambar 4.6 Jaring Komunikasi Sandi

Strategic partner juga dapat dibentuk melalui optimalisasi Unit Tehnis Persandian (UTP) yang saat ini telah ada. Pada Gambar 4.5 diperlihatkan Jaring Komunikasi Sandi, Optimalisasi UTP dilakukan untuk membuat jalur *marketing* atau sosialisasi kepada publik. Jaring Komunikasi Sandi seperti JKS VVIP, JKS Antar instansi, JKS Intern Instansi, JKS VIP Internal Instansi dan JKS Khusus dapat dioptimalkan sebagai *strategic partner* untuk memperluas akses Lemsaneg dalam hal penyediaan layanan CA di era konvergensi.

4.3.4.4. Penguatan Strategi Marketing (Sosialisasi)

Menguatkan strategi-strategi pemasaran layanan dilakukan selain untuk membentuk identitas juga untuk meningkatkan *security awareness* publik. Penguatan disisi marketing dapat dilakukan melalui tindakan membentuk kelompok konsumen sesuai karakteristik (Strategi Segmentasi Pasar), memilih segmen pasar yang akan dimasuki (Strategi *Targeting*) dan menetapkan posisi untuk membangun atau mengkomunikasikan *core competencies* yang telah dimiliki Lemsaneg (Strategi *Positioning*).

Salah satu sukses faktor yang harus dimiliki Lemsaneg dalam hal penyediaan layanan CA kepada publik adalah melakukan Differensiasi sistem dan algoritma sendiri (*Fully National Algorithm*). Differensiasi dilakukan dalam sistem dan pengaturan Penyandian (encryption), *Key Exchange, Digital Signature, Authentication Protocol, Key Management, Web Security* dan lain sebagainya.

Alternatif langkah lain dalam penguatan strategi marketing adalah dengan berkontribusi aktif dalam pemerataan telekomunikasi dan mengajukan solusi-solusi pengamanan yang diperlukan didalamnya. Hal ini dilakukan sebagai upaya untuk membentuk dan membangun kepercayaan publik dalam pelayanan kebutuhan keamanan di era konvergensi. Serta mendapatkan nilai loyalitas publik terhadap merk untuk meningkatkan keunggulan bersaing

Penyediaan Layanan keamanan CA dari Lembaga Sandi Negara dapat dilakukan sebagai proses untuk meningkatkan kualitas pelayanan pemerintah terhadap publik. Publik dapat merasakan layanan-layanan keamanan dan membentuk “rasa tanggung jawab” pemerintah terhadap kebutuhan publik. Hingga akhirnya dapat mewujudkan ketahanan dalam hal keamanan informasi, yang akan mendukung majunya perekonomian dan telekomunikasi di Indonesia.

BAB V
KESIMPULAN

1. Hasil analisa potensi kompetitif penyediaan layanan keamanan CA di era konvergensi menggunakan pemodelan Porter 5 Forces didapatkan :
   i. Penyediaan layanan keamanan CA di era konvergensi memiliki potensi kompetitif Medium (44%).
   ii. Lemsaneg relatif mudah masuk ke dalam industri penyediaan layanan keamanan CA karena industri penyediaan layanan CA tidak memiliki faktor hambatan masuk yang kuat untuk menghadang (37.5%).
   iii. Potensi kompetitif penyediaan layanan CA sangat dipengaruhi oleh faktor persaingan didalam industri penyedia layanan CA (66.7%), persaingan diidentifikasi sebagai faktor yang paling kuat merespon setiap pendatang baru yang akan menyediakan layanan CA.
2. Hasil analisa strategi penyediaan layanan CA bagi keperluan publik di era konvergensi dengan menggunakan pendekatan manajemen strategis didapatkan bahwa :
   i. Posisi Organisasi berada pada Kuadran 1 (pada analisa SWOT) dan kuadran 5 (pada Matrik IE), sehingga arah strategi yang dapat diambil adalah strategi pertumbuhan (*growth strategy*).
   ii. Alternatif strategi penyediaan layanan CA di era konvergensi diantaranya fokus nilai terbaik, pengembangan & penetrasi pasar serta integrasi horizontal.
   iii. Untuk membuat penyediaan layanan CA bernilai strategis bagi Lemsaneg, maka organisasi dapat melakukan strategi diantaranya adalah Meningkatkan Kompetensi Kompetitif Pelayanan Publik, Membentuk Identitas & Merk Layanan CA, Melakukan Kerjasama dengan *Strategic Partner* dan Penguatan Strategi Marketing (Sosialisasi).

DAFTAR REFERENSI

[1]. "_____", *Telecommunication*, Presentasi Badan Regulasi Telekomunikasi Indonesia (BRTI), 2009.

[2]. Indonesia Security Incident Response Team On Internet Infrastructure (ID-SIRTII), *Tren Keamanan Internet Indonesia* 2010. http://www.idsirtii.or.id/index.php/news/2010/1/21/82/tren-keamanan-internet-indonesia-2010.html, tanggal akses terakhir 22 September 2010.

[3]. Internet Users & Population Statistics. *Internet Usage in Asia*. http://www.internetworldstats.com/stats3.htm diakses tanggal 29 September 2010.

[4]. Assosiasi Penyelenggara Jasa Internet. *Data pengguna internet APJII*, www.APJII.org tanggal akses terakhir 22 September 2010.

[5]. Direktorat Telekomunikasi, Sub Direktorat Akses Protokol Internet. *Rekapitulasi Jasa Multimedia*, 2009.

[6]. Departemen komunikasi dan Informatika, *Tren keamanan Internet*, 2010.

[7]. Direktorat Jenderal Pos & Telekomunikasi, Depkominfo, *Roadmap Infrastruktur Teknologi Informasi dan Komunikasi Indonesia*, 2007.

[8]. Budi Rahardjo,*e-Commerce di Indonesia Peluang dan Tantangan*, 2003.

[9]. Onno W.Purbo. *Kebijakan e-commerce di APEC 2001*. http://kambing.ui.ac.id/bebas/v09/onno-ind-1/application/e-commerce/kebijakan-e-commerce-di-apec-02-2001.rtf tanggal akses terakhir 29 September 2010.

[10]. "_____" , *Sosialisasi Jaring Komunikasi Sandi Nasional*, Presentasi Lembaga Sandi Negara, 2010.

[11]. Business Value Analysis, "*Global Entertainment and Media Outlook:2006-2010*. PricewaterhouseCooper. 2006.

[12]. Celtic Initiative (Cooperaation for a European Sustained Leadership in Telecommunication), *Techno economics of integrated communication system and services*, 2004.

[13]. ClearCommerce Corporation Research. *Fraud Prevention Guide*. 2009.

[14]. Herbert Bertine, Telecommunication Security ITU-T Study Group 17, 2007.

[15]. "_____", *Cara Kerja Sertifikat Digital (Public Key Infrastructure)*, http://tiptopku.blogspot.com/2010/05/cara-kerja-sertifikat-digital-pki.html diakses tanggal 24 Oktober 2010.

[16]. Man Young Ree, *Internet Security, Cryptographic Principles Algorithm and Protoco*l, wiley, 2003.

[17]. Menezes, Alfred J.Van Ooschot, Paul C. & Vanstone, *Handbook of Aplied Cryptography*. Boca Raton CRC Pres LCC, 2003.

[18]. "_____", Service Design Certificate Authority, http://www.ca.com/Images/InlineImage/ tanggal akses terakhir 13 November 2010.

[19]. Undang-undang Nomor 29/PERM/M.KOMINFO/011/2006 Tentang Pedoman Penyelenggaraan Certificate Authority (CA) di Indonesia.

[20]. Saiful Hidayat, *Penyelenggaraan CA sebagai Trust Third Parties dalam Transaksi Elektronis Telkom Presentation*. November 2009.

[21]. Website Resmi Bank Mandiri, Login Internet Banking, diakses tanggal 22 September 2010.

[22]. Peraturan Kepala Lembaga Sandi Negara No.7 Tahun 2009 Tentang Visi dan Misi Lembaga sandi Negara.

[23]. "_____" , *Sosialisasi Jaring Komunikasi Sandi Nasional*, Presentasi Lembaga Sandi Negara, 2010.

[24]. Peraturan Presiden Republik Indonesia Nomor 5 Tahun 2010 Tentang Rencana Pembangunan Jangka Menengah Nasional.

[25]. Michael E.Porter, "*Strategi Bersaing*". Karisma Publishing Group, 2007.

[26]. Fred R, David. *Manajemen Strategis Konsep*. Pearson Eduction, 2009.

[27]. Freddy Rangkuti, *Analisis SWOT Tehnik Membedah Kasus Bisnis, Reorientasi Konsep Perencanaan Strategis untuk menghadapi Abad 21*, 2008.

[28]. Which SSL, *SSL Market Share*, http://www.whichssl.com/ssl-market-share, tanggal akses terakhir 1 Desember 2010.

[29]. Peter J.Butziger, *Managing Your Return on Investment (ROI) for Publik Key Infrsatruktur (PKI) security in the Digital Future*, 22nd NISSC Conference, 1999.

[30]. Rahmat M Samik Ibrahim, *Serba Serbi Keamanan Sistem Informasi*, 2005.

[31]. Dokumen S 7799, British Standard Institute 7799, *Information Technology - Code of practice for information security management*.

[32]. Dokumen ISO/IEC 17799 *Information Technology - Code of practice for information security management*, 2000.

[33]. Undang-undang Republik Indonesia nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

[34]. Kapil Raina, *PKI Security Solution For The Enterprise*, Wiley Publishing 2005.

[35]. Ge Qingping, Feng Li, Yang Li, *Probe into E-commerce Security Technology,* International Forum on Computer Science Technology and Aplication, IEEE 2009.

[36]. WhichSSL Website, *Vendor Compare on SSL Product*, http://www.whichssl.com/comparisons/ tanggal akses terakhir 2 Desember 2010.

[37]. "_____", certificate authority, http://www.codeproject.com tanggal akses terakhir 1 Oktober 2010.

[38]. Richardus Eko Indrajit, Enam Aspek Menjaga dan Melindungi Dunia Maya, 2008.

[39]. Sarwono Sutikno, Mindmap Keamanan Informasi, Presentasi Internal Sekolah Tinggi Sandi Negara, 2010.

[40]. Luciana Spica Almilia, Lidia Robahi, *Penerapan E-commerce sebagai Upaya Meningkatkan Persaingan Bisnis Perusahaan*, Surabaya,2005.

[41]. Website resmi Bank Mandiri (Verisign Secure Site), https://www.bankmandiri.co.id , tanggal akses terakhir 22 November 2010.

[42]. Undang-undang Republik Indonesia nomor 29 tahun 2008 tentang Penyelenggaraan Certificate Authority.

[43]. Istiyanto ,Jazi Eko, Ph.D., *Information security & e-government*, http://jazi.staff.ugm.ac.id/ . 2010. tanggal akses 22 September 2010.

[44]. Istiyanto ,Jazi Eko, Ph.D., *Information security & e-government*, http://jazi.staff.ugm.ac.id/ . 2010. tanggal akses 22 September 2010.

[45]. KompasOnline, 10 bank terbesar , http://bisniskeuangan.kompas.com/read/2009/10/13/14250554/ini.dia.10.bank.terbesar.di.indonesia tanggal akses terakhir 22 November 2010.

[46]. Website resmi Bank Mandiri, www.bankmandiri.co.id , login internet banking tanggal akses terakhir 22 November 2010.

[47]. Website resmi Bank Rakyat Indonesia, www.bri.co.id , login internet banking tanggal akses terakhir 22 November 2010.

[48]. Website resmi Bank Central Asia, www.klikbca.com, login internet banking tanggal akses terakhir 22 November 2010.

[49]. Website resmi Bank Negara Indonesia, www.bni.co.id, login internet banking tanggal akses terakhir 22 November 2010.

[50]. Website resmi CIMB Niaga, www.cimbniaga.com, login internet banking tanggal akses terakhir 22 November 2010.

[51]. Website resmi Bank Danamon, www.danamon.co.id , login internet banking tanggal akses terakhir 22 November 2010.

[52]. Website resmi Panin Indonesia, www.panin.co.id , login internet banking tanggal akses terakhir 22 November 2010.

[53]. Website resmi Bank Permata, www.permatabank.com , login internet banking tanggal akses terakhir 22 November 2010.

[54]. Website resmi Bank Internasional Indonesia, www.bii.co.id , login internet banking tanggal akses terakhir 22 November 2010.

[55]. Website resmi Citibank NA, www.citibank.co.id , login internet banking tanggal akses terakhir 22 November 2010.

[56]. Netcraft Certification Services. MarketShare of Certification Authority.https://ssl.netcraft.com/ssl-sample-report/Cmatch/sert tanggal akses 1 Desember 2010.

Authority	Group	Current %	2006	2007	2008												2009
			Jan	Jan	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
GoDaddy.com, Inc.	Go Daddy	21.17	0	0	94077	107835	120416	131172	135793	140976	150875	160287	164184	182037	192818	204246	214735
Equifax Secure Inc.	VeriSign	12.79	97510	110015	110703	111634	112988	114424	116226	118255	119858	120980	123338	124676	126490	128321	129779
Thawte Consulting cc	VeriSign	11.19	77418	88394	105413	106158	106939	107848	108612	109291	109947	110286	111196	111841	112497	113067	113469
UTN-USERFirst-Hardware	Comodo	10.58	0	27542	79670	83388	85743	89468	92170	93837	96502	97998	99705	101376	103717	105612	107355
VeriSign, Inc.	VeriSign	8.23	8564	19382	54202	57518	61517	65600	69294	72088	75157	76710	78261	79799	81038	82260	83470
Equifax	VeriSign	7.80	15102	35607	69762	70305	71147	71873	72506	73220	73977	73759	75055	76138	77118	78279	79121
VeriSign Trust Network	VeriSign	6.38	61792	64896	68459	68510	68363	68282	67502	67370	67136	66901	66598	65978	65589	65119	64711
Comodo CA Limited	Comodo	3.37	0	1109	16498	18039	18858	20432	21827	22906	24386	25126	26863	28290	30109	32093	34190
Network Solutions L.L.C.	Network Solutions	2.55	1768	7356	18448	19181	20042	20781	21490	22334	23086	23626	24440	24877	25260	25585	25844
Starfield Technologies, Inc.	Go Daddy	2.25	29209	58623	37418	33799	32305	31519	30497	29620	28705	27986	26530	25710	24988	23962	22784
DigiCert Inc		1.57	2067	3636	9123	9636	10159	10840	11059	11828	12569	12779	14173	15041	15282	15498	15916
Entrust.net	Entrust.net	1.33	10613	10444	11684	11812	11992	12152	12306	12445	12606	12790	12944	13198	13312	13396	13493
GlobalSign nv-sa	GlobalSign	1.24	1836	2348	6268	6852	7565	8278	8983	9689	10476	11029	11505	11767	12056	12275	12619
Cybertrust		0.67	0	609	3709	3927	4203	4450	4758	4979	5257	5434	5640	5921	6263	6504	6795
SecureTrust Corporation	AmbironTrustWave	0.63	0	0	4098	4517	4990	5318	5529	5728	5976	6197	6393	6262	6067	6186	6392
Thawte Consulting (Pty) Ltd.	VeriSign	0.60	10723	8281	6940	6902	6819	6711	6635	6566	6516	6454	6378	6287	6207	6178	6096

Authority	Group	Current %	2006	2007	2008												2009
			Jan	Jan	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
Root CA		0.56	3218	4272	5277	5359	5353	5466	5610	5628	5742	5720	5818	5872	5880	5785	5631
IPS Certification Authority s.l.		0.55	1499	2287	4375	4509	4705	4880	5118	5343	5438	5524	5512	5633	5692	5536	5606
Secure Business Services, Inc.	Comodo	0.47	42	1064	4407	4516	4547	4516	4504	4551	4616	4599	4596	4512	4540	4647	4782
RSA Data Security, Inc.	VeriSign	0.42	63511	53634	27206	24431	20957	17988	15026	12781	9994	8824	7741	6724	5955	5167	4304
Betrusted Japan Co., Ltd.		0.34	0	193	2381	2437	2544	2713	2788	2848	2959	3009	3118	3209	3292	3396	3468
StartCom Ltd.		0.33	1074	2124	2324	2313	2307	2333	2285	2532	2627	2719	2796	2952	3159	3278	3325
SECOM Trust.net		0.30	0	1897	4217	4325	4387	4393	4335	4238	4115	3915	3776	3595	3444	3269	3041
Alpha	GlobalSign	0.27	0	0	448	534	752	881	1099	1267	1466	1596	1757	1898	2154	2450	2709
GlobalSign	GlobalSign	0.25	0	0	581	695	839	1038	1267	1453	1681	1825	2018	2169	2297	2419	2569
TC TrustCenter for Security in Data Networks GmbH		0.24	2841	3166	3424	3420	3407	3363	3350	3313	3287	3242	3187	3076	2892	2698	2470
CAcert Inc.		0.23	16	825	1772	1815	1859	1909	1986	2059	2112	2139	2189	2223	2240	2308	2337
Comodo Limited	Comodo	0.20	48515	23088	10657	9692	8573	7434	6391	5501	4463	3960	3432	2925	2576	2309	2037
T-Systems Enterprise Services GmbH		0.19	0	1277	1764	1777	1784	1784	1808	1816	1831	1834	1866	1891	1915	1925	1936
U.S. Government		0.19	1665	1897	2068	2056	2051	2039	2027	2038	2004	2012	2005	1996	1983	1947	1928
SECOM Trust Systems CO.,LTD.		0.17	0	0	0	5	6	58	175	335	505	659	891	1095	1301	1487	1740
Servision Inc.		0.14	0	0	0	23	110	219	347	458	593	748	916	1042	1151	1297	1439
Trusted Secure Certificate Authority	Comodo	0.14	192	420	1111	1152	1180	1213	1237	1252	1288	1327	1360	1379	1414	1454	1461
Akamai Technologies Inc		0.14	0	200	881	914	946	961	992	1023	1071	1074	1123	1168	1185	1280	1371

Authority	Group	Current %	2006	2007	2008												2009
			Jan	Jan	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
XRamp Security Services Inc	AmbironTrustWave	0.12	2830	4792	2755	2465	2157	1912	1827	1752	1661	1600	1500	1407	1340	1274	1170
AddTrust AB	Comodo	0.12	4678	12650	5767	4966	3980	2985	2309	2118	2023	1981	1936	1847	1688	1479	1169
Digi-Sign Limited	Comodo	0.10	49	518	941	952	952	957	966	1002	1002	990	1030	1033	1027	1031	1031
UTN - DATACorp SGC	Comodo	0.09	0	15	355	403	423	471	498	548	605	650	703	753	811	853	906
Trustwave Holdings, Inc.		0.08	0	0	0	0	0	0	0	0	0	0	7	354	693	801	804
TBS INTERNET	Comodo	0.07	0	296	674	705	703	724	721	730	746	676	775	802	811	768	751
Unizeto Sp. z o.o.		0.07	0	263	415	432	437	477	496	521	551	569	582	618	651	680	709
thawte, Inc.	VeriSign	0.06	0	0	240	255	282	303	326	353	390	416	455	509	566	607	656
RegisterFly.com, inc.	Comodo	0.06	0	305	953	902	855	838	780	752	722	721	741	737	706	637	565
Firstserver, Inc.		0.06	532	870	323	347	372	1317	1331	1346	1291	1166	1042	944	831	735	616
Cybertrust Inc		0.06	0	0	235	267	308	362	420	478	483	477	500	523	546	570	624
TDC		0.05	429	514	509	384	468	474	484	490	491	493	499	500	496	500	487
FNMT		0.05	158	215	412	418	421	429	432	435	446	451	458	463	465	467	469
Entrust, Inc.	Entrust.net	0.05	0	0	88	93	103	118	121	132	147	155	167	184	192	207	473
Microsoft Secure Server Authority		0.05	421	364	364	335	340	363	371	383	431	454	451	440	485	486	530
NetLock Halozatbiztonsagi Kft.		0.05	177	216	355	360	371	385	392	387	410	413	434	449	464	491	498
WebSpace-Forum, Thomas Wendt	Comodo	0.05	0	59	377	386	398	423	434	442	465	474	481	504	513	523	541
Sonera		0.04	70	141	279	291	310	318	334	345	347	354	366	389	403	420	427
UniCERT Brasil Certificadora		0.04	189	212	304	311	315	325	331	332	325	325	328	326	329	319	363

Authority	Group	Current %	2006	2007	2008												2009
			Jan	Jan	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
Register.com	Comodo	0.04	0	0	0	0	0	0	0	0	0	0	1	46	100	227	384
Webtizen Inc.		0.04	0	0	94	118	130	152	172	199	262	317	358	333	363	418	442
TC TrustCenter GmbH		0.04	0	0	1	8	27	48	68	94	126	157	185	219	259	315	368
QuoVadis Limited		0.03	52	57	79	79	91	108	116	128	138	164	178	201	212	240	257
GlobalSign Inc		0.03	207	309	313	303	295	275	262	263	259	269	270	268	271	276	270
GeoTrust Inc	VeriSign	0.03	0	0	68	81	89	105	112	126	134	147	165	184	213	240	263
Nestle		0.03	43	139	213	214	217	222	227	236	247	249	253	248	248	256	263
ICP-Brasil		0.03	98	133	209	206	209	220	221	226	233	252	264	269	276	281	279
OptimumSSL CA	Comodo	0.03	0	0	309	333	351	365	372	368	375	373	368	346	345	349	351
Ford Motor Company - Enterprise Issuing CA01		0.03	0	0	0	5	47	62	88	108	152	184	206	240	259	278	305
TAIWAN-CA.COM Inc.		0.03	36	59	192	199	206	205	208	212	218	236	267	273	275	279	290
Accenture		0.02	114	141	179	181	183	187	188	185	190	193	198	194	197	197	197
MULTICERT-CA		0.02	111	122	199	198	202	204	202	206	211	218	218	218	216	208	217
Certicamara S.A. Entidad de Certificacion		0.02	0	89	134	140	149	153	165	168	176	183	187	196	202	204	201
DigiNotar B.V.		0.02	0	0	137	141	148	159	161	161	166	167	168	166	165	168	169

Authority	Group	Current %	2006	2007	2008												2009
			Jan	Jan	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
Universitaet Karlsruhe		0.02	0	0	140	145	150	158	189	199	205	210	212	213	219	222	223
America Online Inc.		0.02	0	0	0	0	0	0	0	76	96	102	125	160	180	214	225
A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH		0.02	0	0	193	199	210	210	212	207	210	211	211	216	217	219	217
National Institute of Informatics		0.02	0	0	56	77	88	106	116	130	138	147	159	175	190	201	206
Positive Software Corporation	Comodo	0.02	469	2596	757	707	659	600	564	507	444	392	291	234	227	218	212
GlobalTrust	Comodo	0.02	0	61	153	159	165	174	180	184	189	184	192	184	175	171	162
Sun Microsystems Inc		0.02	155	163	196	195	196	198	198	202	205	204	198	187	190	188	196
Getronics PinkRoccade Nederland B.V.		0.02	0	0	76	80	92	105	107	109	115	123	127	137	139	143	154
The USERTRUST Network	VeriSign	0.02	6142	1393	571	547	523	486	520	496	494	496	505	497	450	174	168
Etisalat		0.02	113	135	193	193	181	189	193	201	206	215	220	219	221	218	220
CENTRAL SECURITY PATROLS CO., LTD.	Comodo	0.01	0	1	111	112	114	110	111	117	115	116	116	114	110	107	105
I.T. Telecom		0.01	69	74	105	108	110	118	121	120	125	130	130	132	134	137	140
Digicert Sdn. Bhd.		0.01	0	0	7	8	14	17	25	25	30	39	39	43	45	46	52
WoSign, Inc.	Comodo	0.01	0	0	35	42	41	48	51	54	63	66	77	77	80	85	99
Regionales Hochschulrechenzentrum Kaiserslautern		0.01	0	0	11	10	12	12	12	25	28	28	30	31	32	32	81
Agencia Catalana de Certificacio (NIF Q-0801176-I)		0.01	0	0	48	50	51	52	54	56	57	58	59	58	59	60	60

Authority	Group	Current %	2006	2007	2008												2009
			Jan	Jan	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
Government of Korea		0.01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	128
Digital Signature Trust		0.01	36	64	122	120	122	125	127	130	136	140	140	147	144	98	77
AS Sertifitseerimiskeskus		0.01	0	76	101	103	105	103	104	106	109	109	111	112	111	106	108
Serasa		0.01	38	48	52	51	54	53	56	58	60	64	68	71	71	74	73
SAIC		0.01	22	54	83	85	87	83	81	80	91	88	90	94	90	92	92
\\xE8\\xA1\\x8C\\xE6\\x94\\xBF\\xE9\\x99\\xA2		0.01	0	0	107	108	109	113	115	117	121	126	127	125	134	135	138
Wells Fargo		0.01	52	63	82	86	86	87	86	83	83	86	87	88	88	87	86
DigiNotar		0.01	31	33	45	48	49	49	51	53	55	54	57	59	61	62	67
Anthem Inc		0.01	26	73	76	69	70	74	76	77	81	82	80	80	94	92	91
AddTrust Sweden AB	Comodo	0.01	13	49	81	85	84	84	80	84	88	87	90	92	91	92	94
LGPKI		0.01	0	0	0	0	0	64	70	73	76	78	79	78	80	82	85
Generalitat Valenciana		0.01	0	0	56	57	59	56	52	52	54	54	52	56	55	51	52
Louisiana State University Issuing CA 1		0.01	0	9	51	54	57	59	62	64	65	65	62	64	66	64	64
KICA		0.01	14	0	0	0	0	0	0	0	0	0	0	0	0	0	91
PinkRoccade Infrastructure Services BV		0.01	0	0	78	80	80	78	79	79	78	77	77	76	72	71	66
Saphety		0.01	0	48	95	95	95	101	107	108	110	112	109	113	115	115	117
Bayer Group		0.01	0	0	9	15	26	32	41	44	55	60	65	69	72	70	71
Actalis S.p.A.		0.01	16	25	38	51	53	54	56	60	60	61	63	68	76	83	89

Authority	Group	Current %	2006	2007	2008												2009
			Jan	Jan	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
KEYNECTIS		0.01	0	0	0	8	15	16	24	36	38	42	45	54	58	67	79
Wachovia Corporation		0.01	34	32	51	52	55	56	59	62	63	64	71	75	78	82	82
OVH SAS	Comodo	0.01	0	0	48	60	83	128	154	172	191	37	230	255	292	139	96
Prvni certifikacni autorita a.s.		0.01	0	105	100	101	97	98	96	96	92	92	90	83	75	70	56
RSA Security Inc.		0.01	19	20	57	59	61	66	68	71	77	84	86	89	96	97	97
Hongkong Post		0.01	0	105	110	110	114	118	117	120	118	119	119	123	121	124	130
CERTINOMIS		0.01	0	3	32	35	37	35	36	39	44	46	51	52	54	51	56
CFC		0.01	82	85	126	130	131	134	133	132	133	131	131	133	130	128	127
INTEC Communications Inc.		0.01	46	60	96	96	97	107	107	109	111	112	115	116	119	122	125
Network Associates		0.01	35	54	67	69	68	69	70	70	74	75	77	78	78	80	56
Earthlink Inc		0.01	5	71	81	81	82	80	81	81	82	83	86	84	75	73	72
Dell Inc.		0.01	76	91	97	98	96	99	95	103	100	100	101	103	102	104	103
InfoCert SpA		0.01	0	0	0	4	13	20	23	33	37	40	43	56	63	69	70
mikroBIT Sp. z o.o.		0.01	101	94	89	89	89	59	59	58	58	58	59	60	60	59	57
LuxTrust s.a		0.01	0	0	50	51	54	58	61	65	65	66	66	63	63	62	59
MasterCard Worldwide		0.01	0	0	52	70	75	74	74	75	79	79	76	78	79	81	84
RBC Hosting Center	Comodo	0.01	0	0	0	1	9	14	23	27	32	39	51	64	71	86	101
Mortgage and Settlement Service Trust CA		0.01	37	46	57	57	59	60	60	61	59	43	45	61	52	54	54

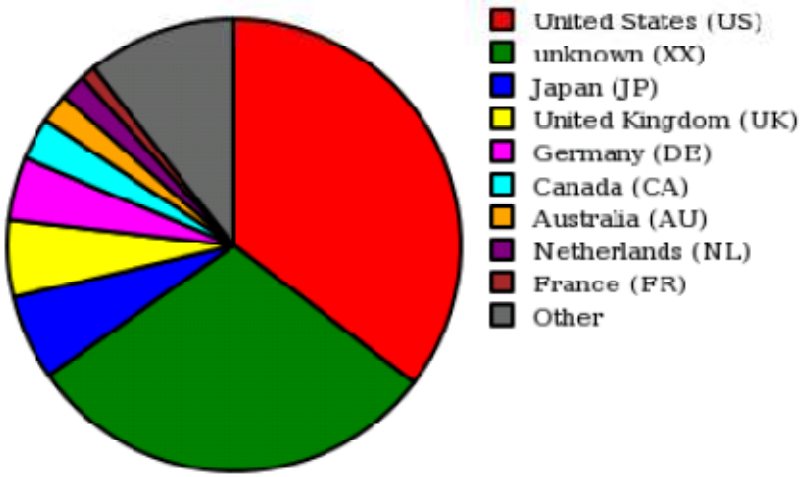
Authority	Group	Current %	2006	2007	2008												2009
			Jan	Jan	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
Japan Certification Services, Inc.		0.01	109	110	127	124	122	114	116	113	112	113	109	108	108	108	106
Postecom S.p.A.		0.01	72	94	137	130	132	133	133	134	142	143	142	146	145	146	142
AC Camerfirma SA		0.01	0	66	106	110	113	118	125	127	133	132	143	144	144	151	150
EUNETIC GmbH	Comodo	0.01	0	0	0	0	0	0	0	0	0	0	13	44	60	84	107
Deutsche Post World Net		0.01	0	0	39	38	38	37	37	38	39	41	49	55	61	65	65
Intesa Sanpaolo S.p.A. CA Servizi Esterni		0.01	0	0	0	0	0	0	0	0	0	0	0	0	5	52	81
Kas Bank NV		0.00	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
BAH		0.00	13	14	19	19	18	19	17	17	19	21	20	21	20	19	22
Hochschule fuer Technik, Wirtschaft und Kultur Leipzig		0.00	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
Universitaet Augsburg		0.00	0	0	0	0	0	0	0	0	0	2	2	2	2	2	2
Martin-Luther-Universitaet Halle-Wittenberg		0.00	0	0	2	2	2	2	2	2	2	2	2	2	2	2	2
USERTRUST - Server Authentication		0.00	0	2	4	4	5	4	3	4	4	4	4	4	4	4	4
Fachhochschule Oldenburg/Ostfriesland/Wilhelmshaven		0.00	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Universitaet Erfurt		0.00	0	0	1	1	1	2	2	2	2	2	2	2	2	2	2
agentschap Centraal Informatiepunt Beroepen Gezondheidszorg		0.00	0	0	1	1	1	1	2	3	3	3	3	3	3	5	6
Coventry City Council		0.00	0	0	1	1	1	1	1	1	2	2	2	1	1	1	1
Otto-Friedrich-Universitaet Bamberg		0.00	0	0	1	1	1	1	1	1	1	1	1	2	3	4	4

Total Market Share - as per June 23, 2010				High Assurance Certificates (With Business Validation)							SSL Without Any Business Validation		% High Assurance vs. Non-Validated SSL
SSL PROVIDER	Total SSL Certificates Found	Total Market Share	Rank	OV	OV %	EV	EV %	Total High Assurance	% High Assurance	Rank	NV	NV %	
GoDaddy	421,854	20.52%	1	14,318	1.43%	1,553	4.61%	15,871	1.53%	8	405,983	39.82%	4% / 96%
GeoTrust	334,668	16.28%	2	27,758	2.77%	1,094	3.25%	28,852	2.78%	7	305,816	29.99%	9% / 91%
COMODO	301,308	14.66%	3	225,046	22.45%	2,779	8.25%	227,825	21.99%	1	73,483	7.21%	76% / 24%
VeriSign	220,117	10.71%	4	198,649	19.82%	21,449	63.64%	220,098	21.24%	2	19	0.00%	100% / 0%
Thawte	176,078	8.57%	5	101,044	10.08%	2,278	6.76%	103,322	9.97%	3	72,756	7.14%	59% / 41%
Network Solutions	38,332	1.86%	6	37,184	3.71%	1,131	3.36%	38,315	3.70%	4	17	0.00%	100% / 0%
GlobalSign	37,794	1.84%	7	9,082	0.91%	606	1.80%	9,688	0.94%	11	28,106	2.76%	26% / 74%
Entrust	34,333	1.67%	8	33,138	3.31%	1,195	3.55%	34,333	3.31%	5	0	0.00%	100% / 0%
DigiCert	33,145	1.61%	9	32,531	3.25%	613	1.82%	33,144	3.20%	6	1	0.00%	100% / 0%
Firstserver	31,235	1.52%	10	1,553	0.15%	0	0.00%	1,553	0.15%	13	29,682	2.91%	5% / 95%
All Other Providers	*118,120*	5.75%	-	*81,282*	*8.54%*	*1,006*	*1.77%*	*82,288*	*7.94%*	-	*35,832*	*3.51%*	*70% / 30%*
Unknown	*308,715*	15.02%	-	*240,794*	*24.02%*	*0*	*0.00%*	*240,794*	*23.24%*	-	*67,921*	*6.66%*	*78% / 22%*
TOTAL	2,055,699			1,002,379		33,704		1,036,083			1,019,616		50% / 50%

ID	TASK NAME	DURATION	START	FINISH	PREDECESSORS
1	**PKI Trust Solution Project-Project start**	**19.5 days**	**Mon 3/24/03**	**Fri 4/18/03**	
2	**Preparation**	**15 days**	**Mon 3/24/03**	**Fri 4/11/03**	
3	Order and ship software and hardware	5 days	Mon 3/24/03	Fri 3/28/03	
4	kick-off meeting	1 day	Mon 3/31/03	Mon 3/31/03	3
5	Review/agreement statement to work	5 days	Mon 4/7/03	Fri 4/11/03	4FS+4 days
6	Request and install secure server ID to enable SSL	1 day	Mon 3/24/03	Mon 3/24/03	
7	Config server for certificate	1 day	Tue 3/25/03	Tue 3/25/03	6
8	Complete pre-engagement checklist	1 day	Wed 3/26/03	Wed 3/26/03	7
9	**CA generation**	**5 days**	**Tue 4/1/03**	**Mon 4/7/03**	
10	Identify hierarchy and naming	4 days	Tue 4/1/03	Fri 4/4/03	4
11	CA generation	1 day	Mon 4/7/03	Mon 4/7/03	10
12	**Setup for production system**	**4.5 days**	**Tue 4/8/03**	**Mon 4/14/03**	
13	enroll for administrator certificate	1 day	Tue 4/8/03	Tue 4/8/03	11
14	authenticate order	3 days	Wed 4/9/03	Fri 4/11/03	13
15	CA loaded on production machines	3 days	Wed 4/9/03	Fri 4/11/03	13
16	Approve/pick up administration certificate	0.5 days	Mon 4/14/03	Mon 4/14/03	15
17	**Setup and deployment for test/staging system**	**3.5days**	**Tue 3/8/03**	**Fri 4/11/03**	
18	enroll for administrator certificate	1 day	Tue 4/8/03	Tue 4/8/03	11
19	CA set up on test machine	2 days	Wed 4/9/03	Wed 4/10/03	18
20	Approve/pick up administration certificate	0.5 days	Fri 4/11/03	Fri 4/11/03	19
21	**setup and configuration of registration modules**	**8.5 days**	**Mon 3/24/03**	**Thu 4/3/03**	
22	install and costumize software	0.5 days	Mon 3/24/03	Mon 3/24/03	
23	develop registration verification function (including automated verification)	5 days	Mon 3/24/03	Mon 3/31/03	22
24	test registration	1 day	Mon 3/31/03	Tue 4/1/03	23
25	run script against policy to configure web pages for modules used	1 day	Tue 4/1/03	Wed 4/2/03	24
26	download and install policy file	1 day	Wed 4/2/03	Thu 4/3/03	25
27	**installation of optional modules**	**2.5 days**	**Fri 4/11/03**	**Tue 4/15/03**	**20**
28	**email server integration**	**2.5 days**	**Fri 4/11/03**	**Tue 4/15/03**	
29	verify configuration of needed servers	0.5 days	Fri 4/11/03	Tue 4/11/03	
30	make a necessary changes to the mail server configuration	0.5 days	Mon 4/14/03	Mon 4/14/03	29
31	**testing-PKI intgration with Microsoft Email Platform**	**1.5 days**	**Mon 4/14/03**	**Tue 4/15/03**	
32	create outlook profile on two end-user machines	0.5 days	Mon 4/14/03	Mon 4/14/03	30
33	enroll and issue certificates to each end user	0.25 days	Tue 4/15/03	Tue 4/15/03	32
34	set up outlook (email client) security profile to use the new	0.25 days	Tue 4/15/03	Tue 4/15/03	33

	certificate for signing/encryption				
35	exchange encrypted email between the two end users	0.25 days	Tue 4/15/03	Tue 4/15/03	34
36	verify thet dcryption is succesful for both end users	0.25 days	Tue 4/15/03	Tue 4/15/03	35
37	**key escrow service (depending on PKI vendor)**	**2.5 days**	**Fri 4/11/03**	**Tue 4/15/03**	
38	verify the database schemas	1 day	Fri 4/11/03	Mon 4/14/03	
39	set up configuration files	1 day	Mon 4/14/03	Tue 4/15/03	38
40	install optional hardware for crypto function (key generation)	0.5 days	Tue 4/15/03	Tue 4/15/03	39
41	configure the certificate renewal process	0.5 days	Fri 4/11/03	Fri 4/11/03	
42	create and configure the key escrow data source (on database system)	0.5 days	Fri 4/11/03	Fri 4/11/03	
43	**testing-key manger**	**1.5 days**	**Fri 4/11/03**	**Mon 4/14/03**	
44	enroll, delete, and recover a certificate and key pair	1.5 days	Fri 4/11/03	Mon 4/14/03	
45	**(move) activate system for production**	**4 days**	**Fri 4/11/03**	**Thu 4/17/03**	
46	configure web pages to point to production system	1 day	Fri 4/11/03	Mon 4/14/03	20
47	enrollment/approval for production RA certificate	1 day	Mon 4/14/03	Tue 4/15/03	46
48	install RA (administrator) certificate	1 day	Tue 4/15/03	Wed 4/16/03	47
49	test certificate enrollment/revocation/renewal	1 day	Wed 4/16/03	Thu 4/17/03	48
50	**training and knowledge transfer**	**1 day**	**Thu 4/17/03**	**Fri 4/18/03**	
51	documentation	1 day	Thu 4/17/03	Fri 4/18/03	49
52	administrator and end-user training	1 day	Thu 4/17/03	Fri 4/18/03	49
53					
54	general availability	0 days	Wed 4/16/03	Wed 4/16/03	48

Sites by Geographical Location



Location	Sites	Percentage
United States (US) - by server | by OS | by CA	358840	35.38
unknown (XX) - by server | by OS | by CA	302071	29.78
Japan (JP) - by server | by OS | by CA	61294	6.04
United Kingdom (UK) - by server | by OS | by CA	56323	5.55
Germany (DE) - by server | by OS | by CA	45843	4.52
Canada (CA) - by server | by OS | by CA	30401	3.00
Australia (AU) - by server | by OS | by CA	21611	2.13
Netherlands (NL) - by server | by OS | by CA	18706	1.84
France (FR) - by server | by OS | by CA	10692	1.05
Spain (ES) - by server | by OS | by CA	7846	0.77
Switzerland (CH) - by server | by OS | by CA	7607	0.75

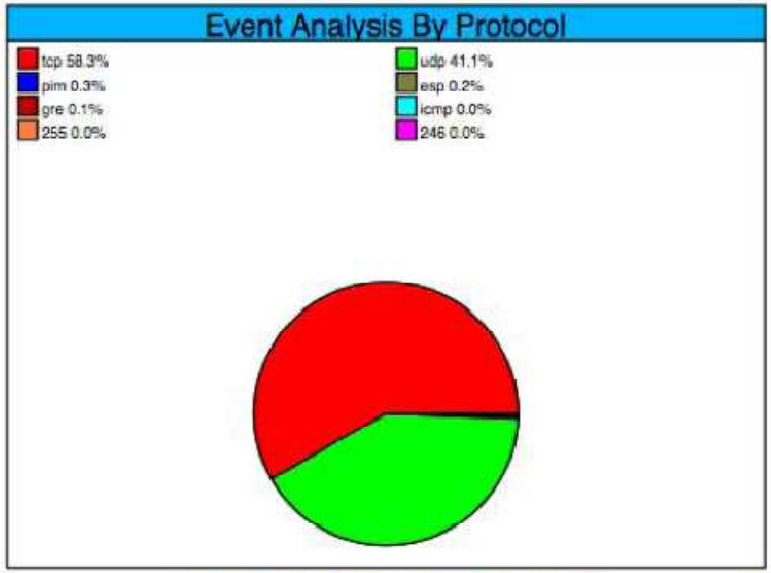
Location	Sites	Percentage
Sweden (SE) - by server | by OS | by CA	7241	0.71
Denmark (DK) - by server | by OS | by CA	5770	0.57
Italy (IT) - by server | by OS | by CA	5648	0.56
Korea (South) (KR) - by server | by OS | by CA	5348	0.53
Brazil (BR) - by server | by OS | by CA	4672	0.46
Turkey (TR) - by server | by OS | by CA	4305	0.42
New Zealand (Aotearoa (NZ) - by server | by OS | by CA	4215	0.42
Norway (NO) - by server | by OS | by CA	4136	0.41
Austria (AT) - by server | by OS | by CA	4092	0.40
Finland (FI) - by server | by OS | by CA	3689	0.36
Poland (PL) - by server | by OS | by CA	3333	0.33
Ireland (IE) - by server | by OS | by CA	3052	0.30
Belgium (BE) - by server | by OS | by CA	2736	0.27
Hong Kong (HK) - by server | by OS | by CA	2050	0.20
Israel (IL) - by server | by OS | by CA	2021	0.20
Taiwan (TW) - by server | by OS | by CA	1976	0.19
Singapore (SG) - by server | by OS | by CA	1900	0.19
South Africa (ZA) - by server | by OS | by CA	1803	0.18
Mexico (MX) - by server | by OS | by CA	1684	0.17
Czech Republic (CZ) - by server | by OS | by CA	1593	0.16
India (IN) - by server | by OS | by CA	1493	0.15
China (CN) - by server | by OS | by CA	1278	0.13
Portugal (PT) - by server | by OS | by CA	1244	0.12
Russian Federation (RU) - by server | by OS | by CA	1097	0.11
Hungary (HU) - by server | by OS | by CA	877	0.09
Malaysia (MY) - by server | by OS | by CA	759	0.07
Argentina (AR) - by server | by OS | by CA	723	0.07

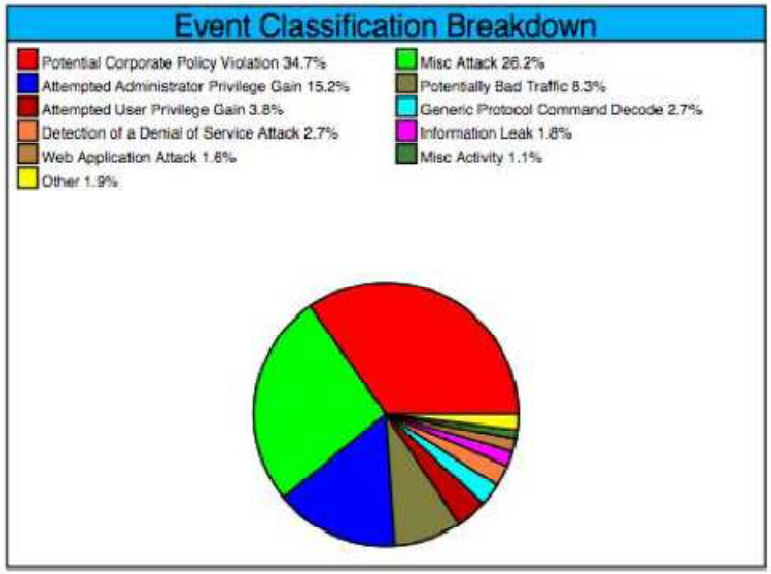
Location	Sites	Percentage
Greece (GR) - by server | by OS | by CA	696	0.07
Thailand (TH) - by server | by OS | by CA	613	0.06
Chile (CL) - by server | by OS | by CA	600	0.06
United Arab Emirates (AE) - by server | by OS | by CA	571	0.06
Iceland (IS) - by server | by OS | by CA	507	0.05
Colombia (CO) - by server | by OS | by CA	469	0.05
Costa Rica (CR) - by server | by OS | by CA	455	0.04
Luxembourg (LU) - by server | by OS | by CA	444	0.04
Philippines (PH) - by server | by OS | by CA	428	0.04
Croatia (Hrvatska) (HR) - by server | by OS | by CA	426	0.04
Malta (MT) - by server | by OS | by CA	398	0.04
Estonia (EE) - by server | by OS | by CA	388	0.04
Cyprus (CY) - by server | by OS | by CA	369	0.04
Slovenia (SI) - by server | by OS | by CA	363	0.04
Romania (RO) - by server | by OS | by CA	346	0.03
Slovakia (Slovak Repu (SK) - by server | by OS | by CA	321	0.03
Gibraltar (GI) - by server | by OS | by CA	295	0.03
Panama (PA) - by server | by OS | by CA	293	0.03
Lithuania (LT) - by server | by OS | by CA	288	0.03
Peru (PE) - by server | by OS | by CA	274	0.03
Indonesia (ID) - by server | by OS | by CA	245	0.02
Latvia (LV) - by server | by OS | by CA	217	0.02
Puerto Rico (PR) - by server | by OS | by CA	216	0.02
Saudi Arabia (SA) - by server | by OS | by CA	209	0.02
Bulgaria (BG) - by server | by OS | by CA	204	0.02
Ukraine (UA) - by server | by OS | by CA	201	0.02
Venezuela (VE) - by server | by OS | by CA	191	0.02

Location	Sites	Percentage
Kuwait (KW) - by server | by OS | by CA	179	0.02
Netherlands Antilles (AN) - by server | by OS | by CA	177	0.02
Bermuda (BM) - by server | by OS | by CA	164	0.02
Virgin Islands (Briti (VG) - by server | by OS | by CA	138	0.01
Uruguay (UY) - by server | by OS | by CA	137	0.01
Ecuador (EC) - by server | by OS | by CA	134	0.01
Dominican Republic (DO) - by server | by OS | by CA	131	0.01
Nigeria (NG) - by server | by OS | by CA	115	0.01
Guatemala (GT) - by server | by OS | by CA	109	0.01
Liechtenstein (LI) - by server | by OS | by CA	108	0.01
Viet Nam (VN) - by server | by OS | by CA	101	0.01
Belize (BZ) - by server | by OS | by CA	92	0.01
Pakistan (PK) - by server | by OS | by CA	85	0.01
Jamaica (JM) - by server | by OS | by CA	83	0.01
Egypt (EG) - by server | by OS | by CA	81	0.01
Bahamas (BS) - by server | by OS | by CA	79	0.01
Mauritius (MU) - by server | by OS | by CA	76	0.01
Cayman Islands (KY) - by server | by OS | by CA	75	0.01
El Salvador (SV) - by server | by OS | by CA	68	0.01
Barbados (BB) - by server | by OS | by CA	67	0.01
Qatar (QA) - by server | by OS | by CA	67	0.01
Sri Lanka (LK) - by server | by OS | by CA	66	0.01
Bahrain (BH) - by server | by OS | by CA	62	0.01
Seychelles (SC) - by server | by OS | by CA	60	0.01
Trinidad and Tobago (TT) - by server | by OS | by CA	58	0.01
Saint Kitts and Nevis (KN) - by server | by OS | by CA	56	0.01
Lebanon (LB) - by server | by OS | by CA	54	0.01

Location	Sites	Percentage
Andorra (AD) - by server | by OS | by CA	54	0.01
Jordan (JO) - by server | by OS | by CA	53	0.01
Macau (MO) - by server | by OS | by CA	52	0.01
Antigua and Barbuda (AG) - by server | by OS | by CA	50	0.00
Honduras (HN) - by server | by OS | by CA	46	0.00
Guernsey (GG) - by server | by OS | by CA	45	0.00
Morocco (MA) - by server | by OS | by CA	44	0.00
Aruba (AW) - by server | by OS | by CA	44	0.00
Vanuatu (VU) - by server | by OS | by CA	40	0.00
Kenya (KE) - by server | by OS | by CA	39	0.00
Nicaragua (NI) - by server | by OS | by CA	38	0.00
Monaco (MC) - by server | by OS | by CA	38	0.00
Paraguay (PY) - by server | by OS | by CA	38	0.00
Virgin Islands (Ameri (VI) - by server | by OS | by CA	36	0.00
Bolivia (BO) - by server | by OS | by CA	34	0.00
Anguilla (AI) - by server | by OS | by CA	34	0.00
Kazakhstan (KZ) - by server | by OS | by CA	33	0.00
Georgia (GE) - by server | by OS | by CA	31	0.00
Oman (OM) - by server | by OS | by CA	31	0.00
Bosnia and Herzegovin (BA) - by server | by OS | by CA	31	0.00
Angola (AO) - by server | by OS | by CA	30	0.00
Moldova (MD) - by server | by OS | by CA	29	0.00
San Marino (SM) - by server | by OS | by CA	25	0.00
Macedonia (MK) - by server | by OS | by CA	25	0.00
Nepal (NP) - by server | by OS | by CA	24	0.00
New Caledonia (NC) - by server | by OS | by CA	24	0.00
Guam (GU) - by server | by OS | by CA	23	0.00

Location	Sites	Percentage
Mongolia (MN) - by server | by OS | by CA	23	0.00
Jersey (JE) - by server | by OS | by CA	21	0.00
Belarus (BY) - by server | by OS | by CA	21	0.00
Fiji (FJ) - by server | by OS | by CA	21	0.00
Iran (IR) - by server | by OS | by CA	20	0.00
Greenland (GL) - by server | by OS | by CA	19	0.00
Namibia (NA) - by server | by OS | by CA	19	0.00
Yugoslavia (YU) - by server | by OS | by CA	18	0.00
Isle of Man (IM) - by server | by OS | by CA	18	0.00
French Polynesia (PF) - by server | by OS | by CA	17	0.00
Saint Lucia (LC) - by server | by OS | by CA	17	0.00
Algeria (DZ) - by server | by OS | by CA	17	0.00
Faroe Islands (FO) - by server | by OS | by CA	17	0.00
Dominica (DM) - by server | by OS | by CA	17	0.00
Armenia (AM) - by server | by OS | by CA	16	0.00
Ghana (GH) - by server | by OS | by CA	16	0.00
Bangladesh (BD) - by server | by OS | by CA	15	0.00
Albania (AL) - by server | by OS | by CA	15	0.00
US Minor Outlying Isl (UM) - by server | by OS | by CA	14	0.00
Brunei Darussalam (BN) - by server | by OS | by CA	14	0.00
Saint Vincent and the (VC) - by server | by OS | by CA	14	0.00
Senegal (SN) - by server | by OS | by CA	13	0.00
Azerbaijan (AZ) - by server | by OS | by CA	13	0.00
Turks and Caicos Isla (TC) - by server | by OS | by CA	11	0.00
Cambodia (KH) - by server | by OS | by CA	11	0.00
Cote D'Ivoire (Ivory (CI) - by server | by OS | by CA	11	0.00
Maldives (MV) - by server | by OS | by CA	10	0.00



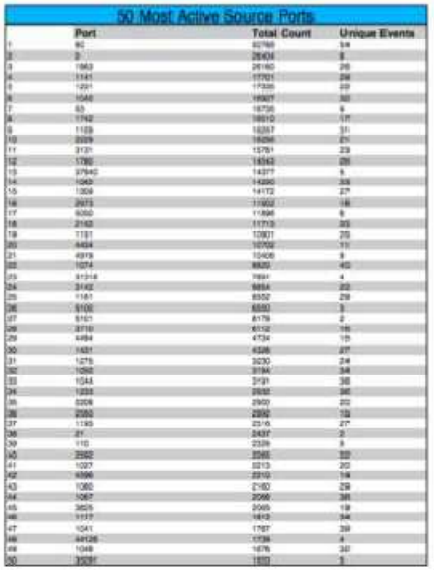


50 Most Active Events

	Event	Count
1	SQL heap-based overflow attempt (1:4966)	143174
2	SQL Worm propagation attempt OUTBOUND (1:2004)	143021
3	SQL Worm propagation attempt (1:2003)	142978
4	CHAT IRC message (1:1463)	99637
5	http_inspect: NON-RFC DEFINED CHAR (119:14)	58276
6	P2P BitTorrent transfer (1:2181)	51364
7	CHAT MSN message (1:540)	38472
8	http_inspect: OVERSIZE REQUEST-URI DIRECTORY (119:19)	31441
9	frag3: Fragmentation overlap (123:8)	29356
10	CHAT Yahoo Messenger Message (1:3891)	26918
11	P2P GNUTella client request (1:1402)	23227
12	P2P Outbound GNUTella client request (1:3466)	22892
13	CHAT IRC nick change (1:542)	18525
14	SPYWARE-PUT Trackware fulwebproducts myweb search toolbar functi...	17330
15	WEB-MISC Apache http server mod_proxy http request crafted date hand...	17027
16	SQL generic sql update injection attempt (1:13614)	16773
17	WEB-CLIENT GIF image width descriptor buffer overflow attempt (1:8418)	14687
18	WEB-CLIENT Malformed PNG detected ICCP overflow attempt (1:6060)	14277
19	CHAT IRC channel notice (1:618)	12219
20	CHAT Yahoo IM message (1:3457)	11847
21	CHAT IRC channel join (1:1729)	11716
22	CHAT Yahoo IM ping (1:2452)	11204
23	WEB-MISC Apache http server mod_proxy http response crafted date ha...	10045
24	DNS zone response containing RDATA address detected (1:10249)	9549
25	CHAT MSN user search (1:1366)	7283
26	CHAT Yahoo IM successful chat join (1:2456)	7096
27	http_inspect: OVERSIZE CHUNK ENCODING (119:18)	6852
28	CHAT Yahoo IM conference watch (1:2461)	6548
29	CHAT IRC dns request (1:1709)	5618
30	BAD-TRAFFIC bad frag bits (1:1322)	5206
31	SMTP Novell GroupWise client IMG SRC buffer overflow (1:13564)	5038
32	SHELLCODE base64 x86 NOOP (1:12798)	4818
33	smtp: Attempted command buffer overflow (124:1)	4354
34	WEB-CLIENT Malformed PNG detected IDAT overflow attempt (1:9758)	3627
35	BAD-TRAFFIC IP Proto 103 PIM (1:2189)	3024
36	CHAT Yahoo IM successful logon (1:2455)	2951
37	CHAT MSN outbound file transfer request (1:1366)	2837
38	WEB-MISC PCT Client_Hello overflow attempt (1:2018)	2491
39	CHAT MSN outbound file transfer accept (1:1368)	2282
40	smtp: Attempted specific command buffer overflow (128:4)	2186
41	smtp: Attempted header name buffer overflow (124:7)	2143
42	WEB-MISC Apache http server mod_proxy http response crafted date ha...	2017
43	SHELLCODE base64 x86 NOOP (1:12801)	1808
44	CHAT Yahoo Messenger File Transfer Receive Request (1:2458)	1676
45	POLICY failed FTP login attempt (1:13360)	1602
46	SPYWARE-PUT Hijacker marketscore runtime detection (1:5760)	1581
47	WEB-CLIENT xmlHttp arbitrary code execution attempt (1:8316)	1539
48	BAD-TRAFFIC data in TCP SYN packet (1:526)	1519
49	SPYWARE-PUT Trackware casalemedia runtime detection (1:5913)	1480
50	WEB-MISC SSLv3 Invalid Client Hello attempt (1:2022)	1457

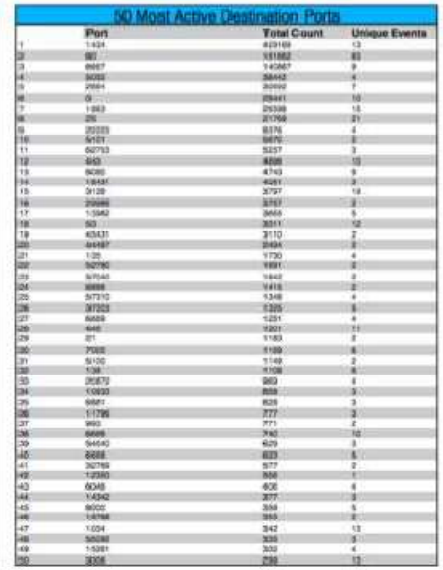
50 Least Active Events

	Event	Count
1	WEB-CLIENT ShockwaveFlash ShockwaveFlash 9 ActiveX function call ...	1
2	SPYWARE-PUT Trackware pornyscan runtime detection - self update (1...	1
3	NETBIOS SMB-DS Isass DsRolerUpgradeDownlevelServer WriteAndX (1...	1
4	DOS Cisco IMA DOS event data length) denial of service attempt (1:8325)	1
5	BACKDOOR absinmote pro 3.1 runtime detection - init connection (1:11317)	1
6	DNS UDP inverse query overflow (1:3584)	1
7	WEB-CLIENT Microsoft Media Player .asf markers detected (1:12972)	1
8	BACKDOOR hornet 1.0 runtime detection - fetch processes list (1:7536)	1
9	WEB-CLIENT Windows Metafile invalid header size integer overflow (1...	1
10	WEB-CLIENT 3ivx MP4 file parsing mem buffer overflow attempt (1:15317)	1
11	BACKDOOR exception 1.0 runtime detection - initial connection server-to-...	1
12	SPYWARE-PUT Trackware myway speedbar / mywebsearch toolbar runt...	1
13	SPECIFIC-THREATS Microsoft SPNEGO ASN.1 library heap corruption ...	1
14	WEB-FRONTPAGE /_vti_bin/owssvr.dll access (1:1248)	1
15	WEB-CLIENT 3ivx MP4 file parsing dcs buffer overflow attempt (1:13019)	1
16	MYSQL client overflow attempt (1:3670)	1
17	SPYWARE-PUT Trackware myway speedbar / mywebsearch toolbar runt...	1
18	WEB-CLIENT excel style handling overflow attempt (1:7024)	1
19	BACKDOOR ftn remote client runtime detection - server-to-client (1:7642)	1
20	WEB-CLIENT Dlink IEACtlent ActiveX clsid access (1:9829)	1
21	WEB-CLIENT Java Virtual Machine malformed GIF buffer overflow attem...	1
22	WEB-CLIENT Malformed PNG detected pHYs overflow attempt (1:8696)	1
23	WEB-CLIENT 3ivx MP4 file parsing cmt buffer overflow attempt (1:13018)	1
24	SPYWARE-PUT Trackware smartadhome user agent detected (1:7497)	1
25	POP3 PCT Client_Hello overflow attempt (1:2518)	1
26	IMAP list overflow attempt (1:2118)	1
27	IMAP Novell NetMail APPEND command buffer overflow attempt (1:10311)	1
28	SMTP SSLv2 openssl get shared ciphers overflow attempt (1:9437)	1
29	SPYWARE-PUT Adware gamespy_arcade runtime detection (1:3835)	1
30	WEB-CLIENT winreg clsid attempt (1:3146)	2
31	MYSQL yaSSL SSLv2 Client Hello Message Challenge Buffer Overflow a...	2
32	SMTP HELO overflow attempt (1:1943)	2
33	EXPLOIT Microsoft Exchange calendar malformed property (1:12619)	2
34	SQL heap-based overflow attempt (1:4966)	2
35	MYSQL yaSSL SSLv2 Client Hello Message Session ID Buffer Overflow ...	2
36	NETBIOS SMB-DS ShellemRuntimor RemoteCreateInstance WriteAndX (...	2
37	DOS Cisco attempt (1:1340)	2
38	WEB-MISC SSLv3 invalid data version attempt (1:3486)	2
39	SPYWARE-PUT Hijacker coolwebsearch cantsoup runtime detection (1:6...	2
40	WEB-MISC NetGear router default password login attempt admin:password	2
41	WEB-IIS Malformed Hit-Highlighting Argument File Access Attempt (1:1013)	2
42	NETBIOS SMB-DS unsupmsg PNP_QueryResConfList little endian atte...	2
43	WEB-CLIENT Adodb Stream ActiveX Object Access CreateObject Funct...	2
44	DOS MSDTC attempt (1:1438)	2
45	NETBIOS SMB-DS unsupmsg PNP_QueryResConfList WriteAndX little ...	2
46	MYSQL yaSSL SSLv2 Client Hello Message Cipher Length Buffer Overf...	2
47	NETBIOS SMB-DS srvsvc NetPathCanonicalize little endian overflow a...	2
48	SPYWARE-PUT Adware download accelerator plus runtime detection	3
49	WEB-CGI /cgi-sys/scancgi.cgi access (1:2022)	3
50	WEB-MISC HP Openview NNM ovalPasswd.exec Unix command execut...	3



50 Most Active Source Ports

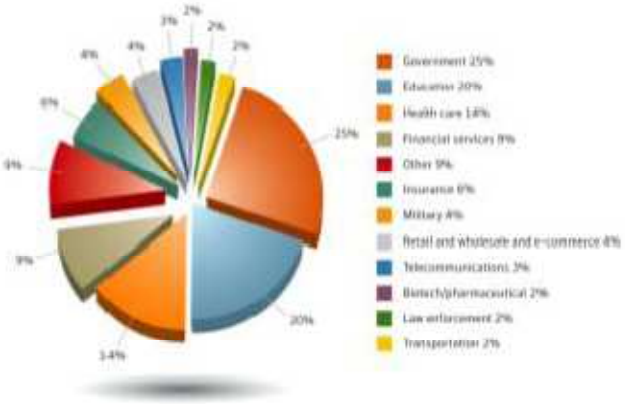
	Port	Total Count	Unique Events
1	80	82788	54
2	0	28404	9
3	1863	26160	26
4	1141	17701	28
5	1201	17335	23
6	1046	16907	30
7	53	16726	6
8	1742	16010	17
9	1129	15257	31
10	2029	15054	21
11	3121	13781	23
12	1785	13343	28
13	37640	11477	5
14	1049	11400	33
15	1309	11172	27
16	2973	11002	18
17	6000	11896	6
18	2142	11713	33
19	1151	10801	29
20	4434	10702	11
21	4919	10408	9
22	1074	9820	40
23	61318	9591	4
24	3142	9464	22
25	1161	9302	29
26	5100	8993	3
27	5101	8178	2
28	3710	8112	16
29	4484	4734	15
30	1431	4246	27
31	1275	3230	24
32	1026	3194	34
33	1044	3131	38
34	1228	2930	36
35	3356	2902	22
36	2355	2892	13
37	1195	2516	27
38	21	2437	3
39	110	2339	9
40	2552	2265	22
41	1027	2213	20
42	4096	2210	14
43	1060	2182	29
44	1067	2066	38
45	3825	2065	19
46	1117	1913	34
47	1041	1797	39
48	64128	1739	4
49	1048	1676	32
50	3597	1653	5

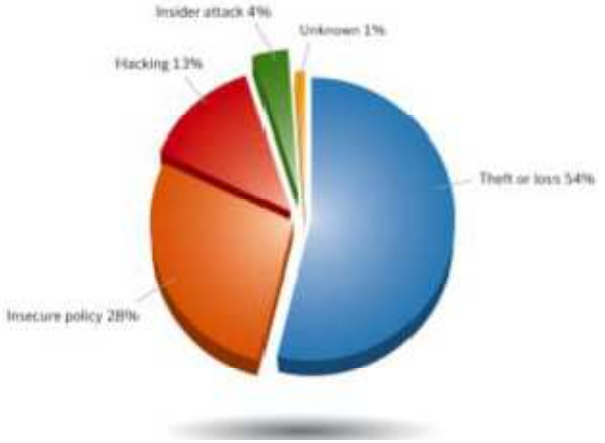


50 Most Active Destination Ports

	Port	Total Count	Unique Events
1	1434	429169	13
2	80	151882	83
3	8867	143867	9
4	9088	58442	4
5	2564	30992	7
6	0	29441	10
7	1863	26388	18
8	25	21768	21
9	20222	8376	4
10	5101	5870	3
11	50753	5257	3
12	993	4698	10
13	9080	4743	9
14	19681	4261	3
15	3128	3797	19
16	20988	3767	3
17	13562	3455	5
18	53	3311	12
19	63431	3110	2
20	44487	2484	2
21	135	1730	4
22	52795	1691	3
23	57640	1442	3
24	8888	1418	2
25	57310	1348	4
26	37223	1225	3
27	6699	1201	4
28	446	1201	11
29	81	1183	2
30	7000	1169	6
31	5150	1149	2
32	139	1108	5
33	35870	993	6
34	10933	858	3
35	9897	829	3
36	11795	777	3
37	993	771	2
38	6699	740	12
39	54640	629	3
40	8888	623	5
41	39789	577	2
42	12380	558	1
43	9045	406	4
44	14342	377	3
45	9002	359	5
46	14788	345	2
47	1034	342	13
48	56286	335	3
49	13281	302	4
50	3306	299	13

Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Host Rank	Command and Control Server Rank	Phishing Host Rank	Bot Rank	Attack Rank
1	United States	31%	1	1	1	1	2	1
2	China	10%	3	2	4	8	1	2
3	Germany	7%	7	3	3	2	4	3
4	France	4%	9	4	14	4	3	4
5	United Kingdom	4%	4	13	9	3	6	6
6	South Korea	4%	12	9	2	9	11	9
7	Canada	3%	5	23	5	7	10	5
8	Spain	3%	13	5	15	16	5	7
9	Taiwan	3%	8	11	6	6	7	11
10	Italy	3%	2	8	10	14	12	10





SSL Provider	Product Name	Minimum Price per Year ($)*	Browser ubiquity	Accepted Browsers	Validation Level	Multi Year Options	Free and functional SSL Trial?	High/Low Assurance
COMODO CA	EnterpriseSSL Elite	$179.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	EnterpriseSSL Gold	$239.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	EnterpriseSSL Platinum	$311.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	EnterpriseSSL Platinum Wildcard	$779.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	InstantSSL	$69.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	InstantSSL Pro	$169.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	FreeSSL	$0.00	99%		Domain Only	n/a	Yes	Low
COMODO CA	Intranet SSL	$31.00	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	PremiumSSL	$229.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	PremiumSSL Wildcard	$619.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High

Entrust	Web server cert	$242.00	99%		Domain ownership and Company Legitimacy	Up to 4 years	n/a	High
GeoTrust	QuickSSL	$199.20	99%		Domain only	Up to 5 years	n/a	Low
GeoTrust	QuickSSL Premium	$239.20	99%		Domain only	Up to 6 years	n/a	Low
GeoTrust	True BusinessID	$319.20	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
GeoTrust	True BusinessID Wildcard	$796.00	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
Go Daddy ®	Deluxe SSL Certificate	$66.66	99%		Domain ownership and Company Legitimacy	Up to 3 years	n/a	High
Go Daddy ®	Deluxe SSL Certificate Wildcard	$239.99	99%		Domain ownership and Company Legitimacy	Up to 3 years	n/a	High
Go Daddy ®	Standard SSL	$15.99	99%		Domain only	Up to 10 years	n/a	Low
Go Daddy ®	Standard Wildcard	$179.99	99%		Domain only	Up to 10 years	n/a	Low
Comodo CA	PositiveSSL	$10.00	99%		Domain only	Up to 10 years	n/a	Low
Comodo CA	PositiveSSL Wildcard	$149.00	99%		Domain only	Up to 10 years	n/a	Low
Thawte	SGC Super cert	$624.75	99%		Domain only	Up to 4 years	n/a	High

Thawte	SSL 123	$129.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	Low
Thawte	Trial	$0.00	0%	-	Domain ownership and Company Legitimacy	n/a	No	High
Thawte	Web server cert	$219.80	99%		Domain only	Up to 2 years	n/a	High
Verisign	Managed PKI for SSL prem	$570.00	99%		Domain ownership and Company Legitimacy	Up to 2 years	n/a	High
Verisign	Managed PKI for SSL Std	$234.00	99%		Domain ownership and Company Legitimacy	Up to 2 years	n/a	High
Verisign	Secure Site Cert	$331.67	99%		Domain ownership and Company Legitimacy	Up to 3 years	n/a	High
Verisign	Secure Site Pro Cert	$826.67	99%		Domain ownership and Company Legitimacy	Up to 3 years	n/a	High
Verisign	Trial	$0.00	0%	-	Domain ownership and Company Legitimacy	n/a	No	High

Hosted Certification Authority (CA)	VeriSign hosts and operates a Certification Authority that enables enterprises to achieve lower total cost of ownership than stand-alone in-house PKI implementations, and has the following functionality: • Generate Certification Authority key pairs. • Activate and deactivate Certification Authority certificates. • Maintain Certificate Revocation Lists (CRLs). • Certificate issuance to internal and external users, Web servers and devices. • Supports validation of a certificate's status using Online Certificate Status Protocol (OCSP) standards.
Registration Authority (RA)	Allow administrators to: • Authenticate, approve, or reject certificate requests from subscribers, and revoke certificates. • Generate reports on certificate activity
Mission-Critical Reliability	• VeriSign Managed PKI Service employs the same PKI technology that is used throughout its military-grade public key infrastructure and Network Operations Center: • Supports 24x7x365 monitoring, management, and escalation across the globe with full disaster recovery. • Certified annually by KPMG as part of a SAS-70 security audit. A regular WebTrust audit of VeriSign's PKI infrastructure is also conducted.
Complete Certificate Lifecycle Management	Managed PKI Service Control Center gives enterprise administrators full control over enrolling, approving, revoking, and renewing digital certificates.
Flexible Deployment	**Fully-Hosted by VeriSign:** Solution is completely hosted by VeriSign at secure facilities. **Partially-Hosted by the Enterprise:** Enterprise may localize, brand, and host end-user enrollment pages.
Automated Administration	Interfaces with widely used directory services, such as Microsoft Active Directory, and automatically approves requests to issue or renew digital certificates.
Scalable	• Delivers carrier-class scalability and is architected to support the highest volume and peak load requirements in the industry. • Overall system architecture is designed to support the issuance and management of over 100 million certificates per year. • VeriSign's diagnostic procedures, security practices, operational policies, and infrastructure have been tested and proven over time and designed with scalability in mind.
World-class Service and Support	• VeriSign's Professional and Support Services alleviate the burden of planning, implementing, and maintaining an in-house, full-scale support infrastructure. • VeriSign Support Services can devote more resources to state-of-the-art technology, security, and training than is feasible for most enterprises.
Rapid Deployment	• In compliance with Public Certificate Authority specifications and VeriSign's existing infrastructure, the PKI platform, policies, and procedures are already in place and ready to be leveraged by customers. • VeriSign Professional Services can implement an installation of VeriSign Managed PKI Service that is partially-hosted by the enterprise in less than one-third the time of a typical in-house, software-based PKI solution. With fully-hosted implementations, VeriSign manages the entire PKI environment on behalf of the customer.
Standards-based	VeriSign has a strong commitment to open standards, innovative technology and strategic collaborations to enable the flexibility and ease-of-use that enterprises require. • Supports standard certificate types, including S/MIME, SSL, and IPSec, as well as PKI industry standards such as X.509 v3, LDAP, PKCS #7, PKCS #10, and PKCS #12. • VeriSign's open approach to security enables organizations to operate freely in diverse environments, and maximize return on, and preservation of, existing investments.
Key Management Service	Allows administrators to backup and recover user private keys with minimal risk and minimal security costs. This solution has three main functions: • Generate and distribute end user keys and digital certificates • Backup of private encryption keys • Recovery of keys and digital certificates The Key Management Service works with leading messaging solutions.
Support for Third-party Hardware Security Modules	Provides an added layer of security for solutions employing Local Hosting and Automated Administration.

Yth. Bapak/Ibu,

Perkenalkan saya Rini Wisnu Wardhani, bekerja di Lembaga Sandi Negara. Saat ini sedang melakukan penelitian dalam rangka penyelesaian tesis, sebagai salah satu syarat untuk kelulusan Pasca Sarjana di Universitas Indonesia, Jurusan Tehnik Elektro, Bidang Kekhususan Manajemen Telekomunikasi.

Saya memerlukan bantuan Bapak/Ibu dalam mengisi kuisioner yang saya lampirkan berikut ini. Kuisioner ini akan sangat membantu saya dalam melakukan penelitian thesis dengan tema "Potensi kompetitif dan formulasi strategi penyediaan layanan CA (*Certificate Authority*) di era konvergensi telekomunikasi".

Jika terdapat pertanyaan dalam pengisian kuisioner ini, mohon untuk dituliskan dalam lembar kuisioner yang kosong. Terima Kasih atas bantuan dan kerjasamanya.

A. Petunjuk Pengisian

a) Tingkat Kepentingan
Pada bagian ini, Bapak/Ibu diminta untuk mengisi tingkat kepentingan dengan pilihan "4" apabila isu yang disampaikan sangat penting dan terkait erat dengan penyediaan layanan CA. Pilihan "1" apabila isu yang disampaikan sangat tidak penting terhadap penyediaan layanan CA di era konvergensi.

b) Tingkat Pengaruh
Pada bagian ini, Bapak/Ibu diminta untuk mengisi tingkat pengaruh dengan pilihan "sangat setuju" apabila isu yang disampaikan sangat relevan terhadap penyediaan layanan CA di era konvergensi dan "sangat tidak setuju" apabila isu yang disampaikan sangat tidak relevan dengan kondisi saat ini.

Keterangan :	
Tingkat Kepentingan	**Tingkat Pengaruh**
1 = Sangat Tidak Penting	SS=Sangat Setuju
2 = Tidak Penting	KS=Kurang Setuju
3 = Penting	RR=Ragu-ragu
4 = Sangat Penting	TS = Tidak Setuju
	STS = Sangat Tidak Setuju

Contoh Pengisian :

kode	Faktor	TINGKAT KEPENTINGAN				TINGKAT PENGARUH				
		Sangat Tidak Penting	Tidak Penting	Penting	Sangat Penting	Sangat Tidak Setuju	Tidak Setuju	Ragu-ragu	Kurang Setuju	Sangat Setuju
		1	2	3	4	STS	TS	RR	KS	SS
s1	Sesuai Visi Misinya Lemsaneg dapat penyelenggarakan layanan-layanan keamanan untuk kepentingan publik			√						√
s2	Lemsaneg telah memiliki kompetensi/kemampuan untuk pengamanan informasi dan telekomunikasi		√						√	

B. Layanan CA dalam Konvergensi Telekomunikasi

Saat ini teknologi telekomunikasi bergerak kearah era konvergensi. Konvergensi merupakan integrasi yang progresif dari beberapa platform jaringan yang berbeda untuk menyalurkan layanan yang serupa dan atau layanan-layanan yang berbeda yang disalurkan pada platform jaringan yang sama. Pada era konvergensi seluruh teknologi dan layanan dapat saling terhubung menggunakan teknologi berbasis *internet protokol* (IP).

Layanan CA-PKI (*Certificate Authority – Publik Key Infrastruktur*) adalah salah satu solusi pengamanan yang dapat diterapkan untuk memenuhi kebutuhan keamanan di era konvergensi tersebut. *Certificate Authority* (CA) secara umum didefinisikan sebagai pihak ketiga yang terpercaya dalam setiap transaksi elektronik berbasis IP. Secara sederhana, CA berperan sebagai pengatur (manajemen) kunci, update setiap parameter sampai dengan penghancuran kunci.

Besarnya kebutuhan publik (dalam hal ini pengguna transaksi dalam platform IP) dalam era konvergensi nantinya memberikan peluang untuk meyediakan layanan ini untuk menjamin dimensi keamanan sesuai standar organisasi telekomunikasi di Dunia (ITU-T). Cakupan dimensi keamanan dalam layanan CA di era konvergensi diantaranya adalah aspek *confidential, privacy, non-repudiation, Authentication dan Integrity.*

C. Data Responden

Lama bekerja di Lembaga Sandi Negara :

- ☐ 0 - 5 tahun
- ☐ 6 - 10 tahun
- ☐ 11 - 20 tahun
- ☐ 21 - 30 tahun
- ☐ >30 tahun

Bidang Pekerjaan :

- ☐ Algoritma dan Sistem Sandi
- ☐ Hardware
- ☐ Jaringan
- ☐ Material Komunikasi
- ☐ Software
- ☐ Lainnya ……

D. Kuisioner Penyediaan Layanan CA di Era Konvergensi

kode	Faktor	TINGKAT KEPENTINGAN				TINGKAT PENGARUH				
		Sangat Tidak Penting	Tidak Penting	Penting	Sangat Penting	Sangat Tidak Setuju	Tidak Setuju	Ragu-ragu	Kurang Setuju	Sangat Setuju
		1	2	3	4	STS	TS	RR	KS	SS
kekuatan (*Strength*):										
S1	Sesuai Visi Misinya Lemsaneg dapat penyelenggarakan layanan-layanan keamanan untuk kepentingan publik									
S2	Lemsaneg telah memiliki kompetensi/kemampuan untuk pengamanan informasi dan telekomunikasi									
S3	Lemsaneg telah memiliki kemampuan untuk mengatur setiap aspek keamanan (misal kunci penyandian, sistem sandi, algoritma dan parameter lain yang diperlukan)									
S4	Lemsaneg telah melakukan penelitian dan penyediaan layanan keamanan berbasis *Internet Protokol* (IP)									
S5	Lemsaneg telah melakukan penelitian, pembangunan & operasional layanan *Certificate Authority* (CA)									

S6	Lemsaneg memiliki kemampuan membuat layanan *Certificate Authority* (CA) bagi keperluan publik dengan menggunakan propietary algoritma.									
S7	Lemsaneg dapat melakukan komunikasi atau berhubungan dalam hal koordinasi pengamanan informasi dengan Unit Tehnis Persandian									

Kode	Faktor	1	2	3	4	STS	TS	RR	KS	SS
kelemahan (*weakness*):										
W1	Sangat perlu adanya struktur organisasi (dalam Lemsaneg) yang melayani penyediaan layanan keamanan publik									
W2	Penyediaan layanan *Certificate Authority* (CA) bagi keperluan publik bagi Lemsaneg adalah hal baru yang membutuhkan koordinasi yang kompleks karena belum pernah diadakan sebelumnya									
W3	Lemsaneg berpeluang sebagai pendatang baru dalam penyedia jasa layanan keamanan CA (*publik service*)									
W4	Jumlah dan Kualitas Sumber Daya yang dipersiapkan untuk melakukan Penyediaan Layanan CA kepada publik perlu ditambah									
W5	Salah satu kelemahan Layanan CA adalah tingkat kompleksitas yang tinggi (rumit)									
W6	Belum adanya payung hukum untuk tugas pengamanan (ataupun persandian) bagi kepentingan publik									

W7	Lemsaneg adalah salah satu lembaga pemerintahan non departemen dimana pengambilan keputusan dan sumber dana sangat bergantung pada pemerintah pusat									
Peluang (Opportunities):										
O1	Layanan Keamanan dalam komunikasi (berbasis IP di Era konvergensi) merupakan kebutuhan yang sangat penting									
O2	penyelenggaraan layanan keamanan CA didukung dengan undang-undang (seperti UU ITE, UU Penyelenggaraan CA dan UU Pengawasan CA)									
O3	Saat ini belum ada organisasi/perusahaan layanan CA di Indonesia, yang dapat melayani dalam cakupan nasional ataupun internasional									
O4	Saat ini tidak ada solusi yang lebih baik dari penggunaan CA untuk pengamanan komunikasi data berbasis IP									
Kode	Faktor	1	2	3	4	STS	TS	RR	KS	SS
O5	Salah satu tuntutan Remunerasi adalah setiap lembaga pemerintahan harus dapat "terukur" melayani publik									
O6	Saat ini Kesiapan Infratruktur telekomunikasi (Data) telah cukup untuk mengaplikasikan layanan CA									
O7	Adanya pengamanan (dengan layanan CA) pada setiap Transaksi Elektronik akan meningkatkan keamanan, efisiensi dan tingkat kepuasan pengguna transaksi elektronik									
Ancaman (Treath) :										
T1	Dibutuhkan investasi yang besar untuk membuat layanan CA baru untuk keperluan publik sampai dengan jangkauan global									
T2	Dibutuhkan jaringan telekomunikasi (data) yang baik untuk mengaplikasikan layanan CA bagi keperluan publik									

T3	Dibutuhkan pengetahuan dan kesadaran mengenai keamanan (security awareness) dari publik untuk menerapkan keamanan secara optimal									
T4	Saat ini penyedia jasa layanan CA yang ada di indonesia adalah operator luar negeri yang kehadirannya telah mendunia (misal verisign, geotrust, thawte)									
T5	Sulit bagi Lemsaneg untuk bersaing dengan layanan-layanan CA dari Luar Negeri karena merk sudah terkenal dan jangkauan pelayanan yang luas									
T6	Karena dalam era konvergensi terbukanya batas dunia, maka layanan CA harus hadir tidak hanya nasional tetapi juga secara mendunia									

E. Pertanyaan dan Saran

1). Apakah Bapak/ibu pernah ikut serta dalam pengkajian teknologi atau pengamanan terhadap perangkat (*hardware/software*) berbasis *internet protokol* (IP) berikut ?

- ☐ E-mail / Pengamanan Email
- ☐ VoIP / Pengamanan VoIP
- ☐ Jaringan Komputer / Pengamanan Jaringan Komputer
- ☐ Virtual Private Network/Client Server
- ☐ Aplikasi /Software/konten berbasis jaringan komputer (IP)
- ☐ e-ktp/e-transaction/e-procurement/e-numbering

Lainnya :

……
……

……
……

2). Bagaimana pendapat atau saran Bapak/Ibu mengenai Lembaga Sandi Negara sebagai penyelenggara CA untuk kebutuhan publik ?

……

……

……

-Terima Kasih-

SSL Provider	Product Name	Minimum Price per Year ($)*	Browser ubiquity	Accepted Browsers	Validation Level	Multi Year Options	Free and functional SSL Trial?	High/Low Assurance
COMODO CA	EnterpriseSSL Elite	$179.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	EnterpriseSSL Gold	$239.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	EnterpriseSSL Platinum	$311.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	EnterpriseSSL Platinum Wildcard	$779.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	InstantSSL	$69.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	InstantSSL Pro	$169.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	FreeSSL	$0.00	99%		Domain Only	n/a	Yes	Low
COMODO CA	Intranet SSL	$31.00	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	PremiumSSL	$229.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
COMODO CA	PremiumSSL Wildcard	$619.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High

Entrust	Web server cert	$242.00	99%		Domain ownership and Company Legitimacy	Up to 4 years	n/a	High
GeoTrust	QuickSSL	$199.20	99%		Domain only	Up to 5 years	n/a	Low
GeoTrust	QuickSSL Premium	$239.20	99%		Domain only	Up to 6 years	n/a	Low
GeoTrust	True BusinessID	$319.20	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
GeoTrust	True BusinessID Wildcard	$796.00	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	High
Go Daddy ®	Deluxe SSL Certificate	$66.66	99%		Domain ownership and Company Legitimacy	Up to 3 years	n/a	High
Go Daddy ®	Deluxe SSL Certificate Wildcard	$239.99	99%		Domain ownership and Company Legitimacy	Up to 3 years	n/a	High
Go Daddy ®	Standard SSL	$15.99	99%		Domain only	Up to 10 years	n/a	Low
Go Daddy ®	Standard Wildcard	$179.99	99%		Domain only	Up to 10 years	n/a	Low
Comodo CA	PositiveSSL	$10.00	99%		Domain only	Up to 10 years	n/a	Low
Comodo CA	PositiveSSL Wildcard	$149.00	99%		Domain only	Up to 10 years	n/a	Low
Thawte	SGC Super cert	$624.75	99%		Domain only	Up to 4 years	n/a	High

Thawte	SSL 123	$129.80	99%		Domain ownership and Company Legitimacy	Up to 5 years	n/a	Low
Thawte	Trial	$0.00	0%	-	Domain ownership and Company Legitimacy	n/a	No	High
Thawte	Web server cert	$219.80	99%		Domain only	Up to 2 years	n/a	High
Verisign	Managed PKI for SSL prem	$570.00	99%		Domain ownership and Company Legitimacy	Up to 2 years	n/a	High
Verisign	Managed PKI for SSL Std	$234.00	99%		Domain ownership and Company Legitimacy	Up to 2 years	n/a	High
Verisign	Secure Site Cert	$331.67	99%		Domain ownership and Company Legitimacy	Up to 3 years	n/a	High
Verisign	Secure Site Pro Cert	$826.67	99%		Domain ownership and Company Legitimacy	Up to 3 years	n/a	High
Verisign	Trial	$0.00	0%	-	Domain ownership and Company Legitimacy	n/a	No	High

Hosted Certification Authority (CA)	VeriSign hosts and operates a Certification Authority that enables enterprises to achieve lower total cost of ownership than stand-alone in-house PKI implementations, and has the following functionality: • Generate Certification Authority key pairs. • Activate and deactivate Certification Authority certificates. • Maintain Certificate Revocation Lists (CRLs). • Certificate issuance to internal and external users, Web servers and devices. • Supports validation of a certificate's status using Online Certificate Status Protocol (OCSP) standards.
Registration Authority (RA)	Allow administrators to: • Authenticate, approve, or reject certificate requests from subscribers, and revoke certificates. • Generate reports on certificate activity.
Mission-Critical Reliability	• VeriSign Managed PKI Service employs the same PKI technology that is used throughout its military-grade public key infrastructure and Network Operations Centers. • Supports 24x7x365 monitoring, management, and escalation across the globe with full disaster recovery. • Certified annually by KPMG as part of a SAS-70 security audit. A regular WebTrust audit of VeriSign's PKI infrastructure is also conducted.
Complete Certificate Lifecycle Management	Managed PKI Service Control Center gives enterprise administrators full control over enrolling, approving, revoking, and renewing digital certificates.
Flexible Deployment	**Fully-Hosted by VeriSign:** Solution is completely hosted by VeriSign at secure facilities. **Partially-Hosted by the Enterprise:** Enterprise may localize, brand, and host end-user enrollment pages.
Automated Administration	Interfaces with widely used directory services, such as Microsoft Active Directory, and automatically approves requests to issue or renew digital certificates.
Scalable	• Delivers carrier-class scalability, and is architected to support the highest volume and peak load requirements in the industry. • Overall system architecture is designed to support the issuance and management of over 100 million certificates per year. • VeriSign's diagnostic procedures, security practices, operational policies, and infrastructure have been tested and proven over time and designed with scalability in mind.
World-class Service and Support	• VeriSign's Professional and Support Services alleviate the burden of planning, implementing, and maintaining an in-house, full-scale support infrastructure. • VeriSign Support Services can devote more resources to state-of-the-art technology, security, and training than is feasible for most enterprises.
Rapid Deployment	• In compliance with Public Certificate Authority specifications and VeriSign's existing infrastructure, the PKI platform, policies, and procedures are already in place and ready to be leveraged by customers. • VeriSign Professional Services can implement an installation of VeriSign Managed PKI Service that is partially-hosted by the enterprise in less than one-third the time of a typical in-house, software-based PKI solution. With fully-hosted implementations, VeriSign manages the entire PKI environment on behalf of the customer.
Standards-based	VeriSign has a strong commitment to open standards, innovative technology and strategic collaborations to enable the flexibility and ease-of-use that enterprises require. • Supports standard certificate types, including S/MIME, SSL, and IPSec, as well as PKI industry standards such as X.509 v3, LDAP, PKCS #7, PKCS #10, and PKCS #12. • VeriSign's open approach to security enables organizations to operate freely in diverse environments, and maximize return on, and preservation of, existing investments.
Key Management Service	Allows administrators to backup and recover user private keys with minimal risk and minimal security costs. This solution has three main functions: • Generate and distribute end user keys and digital certificates • Backup of private encryption keys • Recovery of keys and digital certificates The Key Management Service works with leading messaging solutions.
Support for Third-party Hardware Security Modules	Provides an added layer of security for solutions employing Local Hosting and Automated Administration.

Yth. Bapak/Ibu,

Perkenalkan saya Rini Wisnu Wardhani, bekerja di Lembaga Sandi Negara. Saat ini sedang melakukan penelitian dalam rangka penyelesaian tesis, sebagai salah satu syarat untuk kelulusan Pasca Sarjana di Universitas Indonesia, Jurusan Tehnik Elektro, Bidang Kekhususan Manajemen Telekomunikasi.

Saya memerlukan bantuan Bapak/Ibu dalam mengisi kuisioner yang saya lampirkan berikut ini. Kuisioner ini akan sangat membantu saya dalam melakukan penelitian thesis dengan tema "Potensi kompetitif dan formulasi strategi penyediaan layanan CA (*Certificate Authority*) di era konvergensi telekomunikasi".

Jika terdapat pertanyaan dalam pengisian kuisioner ini, mohon untuk dituliskan dalam lembar kuisioner yang kosong. Terima Kasih atas bantuan dan kerjasamanya.

F. Petunjuk Pengisian

c) Tingkat Kepentingan
Pada bagian ini, Bapak/Ibu diminta untuk mengisi tingkat kepentingan dengan pilihan "4" apabila isu yang disampaikan sangat penting dan terkait erat dengan penyediaan layanan CA. Pilihan "1" apabila isu yang disampaikan sangat tidak penting terhadap penyediaan layanan CA di era konvergensi.

d) Tingkat Pengaruh
Pada bagian ini, Bapak/Ibu diminta untuk mengisi tingkat pengaruh dengan pilihan "sangat setuju" apabila isu yang disampaikan sangat relevan terhadap penyediaan layanan CA di era konvergensi dan "sangat tidak setuju" apabila isu yang disampaikan sangat tidak relevan dengan kondisi saat ini.

Keterangan :	
Tingkat Kepentingan	**Tingkat Pengaruh**
1 = Sangat Tidak Penting	SS=Sangat Setuju
2 = Tidak Penting	KS=Kurang Setuju
3 = Penting	RR=Ragu-ragu
4 = Sangat Penting	TS = Tidak Setuju
	STS = Sangat Tidak Setuju

Contoh Pengisian :

kode	Faktor	TINGKAT KEPENTINGAN				TINGKAT PENGARUH				
		Sangat Tidak Penting	Tidak Penting	Penting	Sangat Penting	Sangat Tidak Setuju	Tidak Setuju	Ragu-ragu	Kurang Setuju	Sangat Setuju
		1	2	3	4	STS	TS	RR	KS	SS
s1	Sesuai Visi Misinya Lemsaneg dapat penyelenggarakan layanan-layanan keamanan untuk kepentingan publik			√						√
s2	Lemsaneg telah memiliki kompetensi/kemampuan untuk pengamanan informasi dan telekomunikasi		√						√	

G. Layanan CA dalam Konvergensi Telekomunikasi

Saat ini teknologi telekomunikasi bergerak kearah era konvergensi. Konvergensi merupakan integrasi yang progresif dari beberapa platform jaringan yang berbeda untuk menyalurkan layanan yang serupa dan atau layanan-layanan yang berbeda yang disalurkan pada platform jaringan yang sama. Pada era konvergensi seluruh teknologi dan layanan dapat saling terhubung menggunakan teknologi berbasis *internet protokol* (IP).

Layanan CA-PKI (*Certificate Authority – Publik Key Infrastruktur*) adalah salah satu solusi pengamanan yang dapat diterapkan untuk memenuhi kebutuhan keamanan di era konvergensi tersebut. *Certificate Authority* (CA) secara umum didefinisikan sebagai pihak ketiga yang terpercaya dalam setiap transaksi elektronik berbasis IP. Secara sederhana, CA berperan sebagai pengatur (manajemen) kunci, update setiap parameter sampai dengan penghancuran kunci.

Besarnya kebutuhan publik (dalam hal ini pengguna transaksi dalam platform IP) dalam era konvergensi nantinya memberikan peluang untuk meyediakan layanan ini untuk menjamin dimensi keamanan sesuai standar organisasi telekomunikasi di Dunia (ITU-T). Cakupan dimensi keamanan dalam layanan CA di era konvergensi diantaranya adalah aspek *confidential, privacy, non-repudiation, Authentication dan Integrity.*

H. Data Responden

Lama bekerja di Lembaga Sandi Negara :

- ☐ 0 - 5 tahun
- ☐ 6 - 10 tahun
- ☐ 11 - 20 tahun
- ☐ 21 - 30 tahun
- ☐ >30 tahun

Bidang Pekerjaan :

- ☐ Algoritma dan Sistem Sandi
- ☐ Hardware
- ☐ Jaringan
- ☐ Material Komunikasi
- ☐ Software
- ☐ Lainnya ……

I. Kuisioner Penyediaan Layanan CA di Era Konvergensi

kode	Faktor	TINGKAT KEPENTINGAN				TINGKAT PENGARUH				
		Sangat Tidak Penting	Tidak Penting	Penting	Sangat Penting	Sangat Tidak Setuju	Tidak Setuju	Ragu-ragu	Kurang Setuju	Sangat Setuju
		1	2	3	4	STS	TS	RR	KS	SS
kekuatan (*Strength*):										
S1	Sesuai Visi Misinya Lemsaneg dapat penyelenggarakan layanan-layanan keamanan untuk kepentingan publik									
S2	Lemsaneg telah memiliki kompetensi/kemampuan untuk pengamanan informasi dan telekomunikasi									
S3	Lemsaneg telah memiliki kemampuan untuk mengatur setiap aspek keamanan (misal kunci penyandian, sistem sandi, algoritma dan parameter lain yang diperlukan)									
S4	Lemsaneg telah melakukan penelitian dan penyediaan layanan keamanan berbasis *Internet Protokol* (IP)									
S5	Lemsaneg telah melakukan penelitian, pembangunan & operasional layanan *Certificate Authority* (CA)									
S6	Lemsaneg memiliki kemampuan membuat layanan *Certificate Authority* (CA) bagi keperluan publik dengan menggunakan propietary algoritma.									
S7	Lemsaneg dapat melakukan komunikasi atau berhubungan dalam hal koordinasi pengamanan informasi dengan Unit Tehnis Persandian									

Kode	Faktor	1	2	3	4	STS	TS	RR	KS	SS
kelemahan (*weakness*):										
W1	Sangat perlu adanya struktur organisasi (dalam Lemsaneg) yang melayani penyediaan layanan keamanan publik									
W2	Penyediaan layanan *Certificate Authority* (CA) bagi keperluan publik bagi Lemsaneg adalah hal baru yang membutuhkan koordinasi yang kompleks karena belum pernah diadakan sebelumnya									
W3	Lemsaneg berpeluang sebagai pendatang baru dalam penyedia jasa layanan keamanan CA (*publik service*)									
W4	Jumlah dan Kualitas Sumber Daya yang dipersiapkan untuk melakukan Penyediaan Layanan CA kepada publik perlu ditambah									
W5	Salah satu kelemahan Layanan CA adalah tingkat kompleksitas yang tinggi (rumit)									
W6	Belum adanya payung hukum untuk tugas pengamanan (ataupun persandian) bagi kepentingan publik									
W7	Lemsaneg adalah salah satu lembaga pemerintahan non departemen dimana pengambilan keputusan dan sumber dana sangat bergantung pada pemerintah pusat									
Peluang (Opportunities):										
O1	Layanan Keamanan dalam komunikasi (berbasis IP di Era konvergensi) merupakan kebutuhan yang sangat penting									
O2	penyelenggaraan layanan keamanan CA didukung dengan undang-undang (seperti UU ITE, UU Penyelenggaraan CA dan UU Pengawasan CA)									

O3	Saat ini belum ada organisasi/perusahaan layanan CA di Indonesia, yang dapat melayani dalam cakupan nasional ataupun internasional									
O4	Saat ini tidak ada solusi yang lebih baik dari penggunaan CA untuk pengamanan komunikasi data berbasis IP									
Kode	Faktor	1	2	3	4	STS	TS	RR	KS	SS
O5	Salah satu tuntutan Remunerasi adalah setiap lembaga pemerintahan harus dapat "terukur" melayani publik									
O6	Saat ini Kesiapan Infratruktur telekomunikasi (Data) telah cukup untuk mengaplikasikan layanan CA									
O7	Adanya pengamanan (dengan layanan CA) pada setiap Transaksi Elektronik akan meningkatkan keamanan, efisiensi dan tingkat kepuasan pengguna transaksi elektronik									
Ancaman (Treath) :										
T1	Dibutuhkan investasi yang besar untuk membuat layanan CA baru untuk keperluan publik sampai dengan jangkauan global									
T2	Dibutuhkan jaringan telekomunikasi (data) yang baik untuk mengaplikasikan layanan CA bagi keperluan publik									
T3	Dibutuhkan pengetahuan dan kesadaran mengenai keamanan (security awareness) dari publik untuk menerapkan keamanan secara optimal									
T4	Saat ini penyedia jasa layanan CA yang ada di indonesia adalah operator luar negeri yang kehadirannya telah mendunia (misal verisign, geotrust, thawte)									
T5	Sulit bagi Lemsaneg untuk bersaing dengan layanan-layanan CA dari Luar Negeri karena merk sudah terkenal dan jangkauan pelayanan yang luas									

T6	Karena dalam era konvergensi terbukanya batas dunia, maka layanan CA harus hadir tidak hanya nasional tetapi juga secara mendunia									

J. Pertanyaan dan Saran

3). Apakah Bapak/ibu pernah ikut serta dalam pengkajian teknologi atau pengamanan terhadap perangkat (*hardware/software*) berbasis *internet protokol* (IP) berikut ?

- ☐ E-mail / Pengamanan Email
- ☐ VoIP / Pengamanan VoIP
- ☐ Jaringan Komputer / Pengamanan Jaringan Komputer
- ☐ Virtual Private Network/Client Server
- ☐ Aplikasi /Software/konten berbasis jaringan komputer (IP)
- ☐ e-ktp/e-transaction/e-procurement/e-numbering

Lainnya :

……

……

4). Bagaimana pendapat atau saran Bapak/Ibu mengenai Lembaga Sandi Negara sebagai penyelenggara CA untuk kebutuhan publik ?

……

……

……

-Terima Kasih-

CONTOH PERHITUNGAN KUISIONER

Berikut contoh perhitungan Jawaban Kuisioner untuk Responden 1 untuk kuisioner IE dan Responden 1 untuk justifkasi manajemen melalui matriks QSPM:

I. Tingkat Pengaruh (Bobot) Faktor Internal

	Hal 1	Hal 2	Hal 3	Jumlah jawaban	ket
A= jumlah jawaban SS	5	2	0	7	A
B= jumlah jawaban KS	2	4	0	6	B
C= jumlah jawaban RR		1		1	C
D= jumlah jawaban TS		0		0	D
E= jumlah jawaban STS				0	E
Jumlah jawaban :	7	7	0		
Jumlah default :	7	7	0	X=	0.097560976

Maka nilai tingkat pengaruh (bobot) untuk responden 1 adalah :	
nilai bobot jawaban SS faktor internal :	0.098
nilai bobot jawaban KS faktor internal :	0.049
nilai bobot jawaban RR faktor internal :	0.024
nilai bobot jawaban TS faktor internal :	0.012
nilai bobot jawaban STS faktor internal :	0.006

II. Tingkat Pengaruh (Bobot) Faktor Eksternal

	Hal 1	Hal 2	Hal 3	Jumlah jawaban	ket
A= jumlah jawaban SS	0	1	8	9	A
B= jumlah jawaban KS	0	2	1	3	B
C= jumlah jawaban RR		0		0	C
D= jumlah jawaban TS		1		1	D
E= jumlah jawaban STS				0	E
Jumlah jawaban :	0	4	9		
Jumlah default	0	4	9	X=	0.094117647

Maka nilai tingkat pengaruh (bobot) untuk responden 1 adalah :	
nilai bobot jawaban SS faktor eksternal :	0.094
nilai bobot jawaban KS faktor eksternal :	0.047
nilai bobot jawaban RR faktor eksternal:	0.024
nilai bobot jawaban TS faktor eksternal :	0.012
nilai bobot jawaban STS faktor eksternal:	0.006

III. Jumlah Tingkat Kepentingan (Rating)

Jawaban		Nilai Rating Faktor Internal		Nilai Rating Faktor Eksternal	
		Strength	Weakness	Opportunities	Treath
		(S1,S2,S3,S4,S5,S6,S7)	(W1,W2,W3,W4,W5,W6,W7)	(O1,O2,O3,O4,O5,O6,O7)	(T1,T2,T3,T4,T5,T6)
1	Isu yang disampaikan sangat tidak penting	1.00	4.00	1.00	4.00
2	Isu yang disampaikan tidak penting	2.00	3.00	2.00	3.00
3	Isu yang disampaikan penting	3.00	2.00	3.00	2.00
4	Isu yang disampaikan sangat penting	4.00	1.00	4.00	1.00

Nilai rating tiap responden mengikuti tabel diatas, untuk statement kuisioner yang sudah bernilai negative (seperti pada T5) perhitungan dilakukan tetap mengikuti nilai opportunities tabel diatas (tidak dibalik).

IV. Menghitung Variabel Faktor Internal/Eksternal seluruh Responden :

a) Pada contoh diatas dilakukan perhitungan untuk responden 1, selanjutnya dilakukan perhitungan nilai bobot dan rating masing-masing responden (sampai dengan responden ke-22) .
b) Hasil Jawaban setiap variabel faktor Strength (S1,S2,S3,S4,S5,S6,S7), W (W1,W2,W3,W4,W5,W6,W7), O(O1,O2,O3,O4,O5,O6,O7) dan T (T1,T2,T3,T4,T5,T6) direkap kemudian di cari rata-rata per faktor. Rata-rata dilakukan dengan cara menjumlahkan nilai total jawaban 22 responden dibagi dengan jumlah responden. Dilakukan per variabel.
c) Untuk mendapatkan skor bobot faktor dimensi internal/eksternal dalam tabel IFE dan EFE nilai rata-rata tersebut diolah dengan cara mengikuti aturan pembuatan tabel IFE dan EFE (dengan menjumlahkan hasil perkalian setiap faktor tingkat pengaruh dan tingkat kepentingan internel/eksternal).

V. Menghitung Matriks QSPM (Responden 1 QSPM)

a) Perhitungan kuisioner QSPM dilakukan dengan menggunakan model jawaban:

Bobot : Tingkat Kepentingan	AS (Attractive Score) : Skor Daya Tarik
Apakah isu ini sangat penting&berkaitan erat dengan penyediaan layanan CA kepada publik ?	**Apakah Faktor Ini mempengaruhi pilihan strategi yang dibuat?**
4: Sangat Penting	4: Daya tariknya tinggi
3: Penting	3: Daya tariknya sedang
2: Tidak Penting	2: Daya tariknya rendah
1: Sangat Tidak Penting	1: Tidak memiliki daya tarik

b) Konversi nilai bobot dan nilai attractive score dilakukan dengan metode yang sama dengan perhitungan faktor IE.

VI. Hasil Perhitungan Responden 1 QSPM

Sebagai contoh, berikut diberikan hasil perhitungan untuk responden 1 (justifikasi manajemen) untuk input matriks QSPM.

Perhitungan Bobot Internal QSPM

	hal 1	Jumlah jawaban	ket
A= jumlah jawaban 4	10	10	A
B= jumlah jawaban 3	4	4	B
C= jumlah jawaban 2	0	0	C
D= jumlah jawaban 1	0	0	D
jumlah jawaban :	14		
jumlah default	14	X=	0.083333333

maka nilai rating internal responden 1 QSPM	adalah :
nilai rating 4	0.083333333
nilai rating 3	0.041666667
nilai rating 2	0.020833333
nilai rating 1	0.010416667
Jumlah	1

Perhitungan Bobot Eksternal QSPM

	hal 2	Jumlah jawaban	ket
A= jumlah jawaban 4	8	8	A
B= jumlah jawaban 3	4	4	B
C= jumlah jawaban 2	1	1	C
D= jumlah jawaban 1	0	0	D
jumlah jawaban :	13		
jumlah default	13	X=	0.097560976

maka nilai rating eksternal responden 1 QSPM	adalah :
nilai rating 4	0.09756
nilai rating 3	0.04878
nilai rating 2	0.02439
nilai rating 1	0.0122
Jumlah	1

VII. Menghitung nilai daya tarik strategi seluruh responden QSPM

a) Total attractive score didapatkan dengan mengalikan nilai bobot rata-rata dari 3 responden dan nilai attractive score perfaktor yang dipertanyakan.

b) Sum Total Attractive Score didapat dengan menjumlahkan setiap nilai attractive score setiap strategi alternative.

c) Pemilihan strategi dilakukan dengan melihat nilai STAS tertinggi.

HASIL PERHITUNGAN FAKTOR STRENGTH

	S1			S2			S3			S4			S5			S6			S7		
Responden	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total
R1	3.000	0.098	0.293	3.000	0.098	0.293	3.000	0.098	0.293	4.000	0.098	0.390	4.000	0.098	0.390	4.000	0.098	0.390	3.000	0.049	0.146
R2	3.000	0.104	0.312	3.000	0.013	0.039	4.000	0.104	0.416	3.000	0.026	0.078	3.000	0.104	0.312	4.000	0.104	0.416	4.000	0.104	0.416
R3	4.000	0.071	0.286	4.000	0.071	0.286	4.000	0.071	0.286	4.000	0.071	0.286	4.000	0.071	0.286	4.000	0.071	0.286	4.000	0.071	0.286
R4	4.000	0.077	0.308	4.000	0.077	0.308	4.000	0.077	0.308	4.000	0.077	0.308	4.000	0.077	0.308	4.000	0.077	0.308	4.000	0.038	0.154
R5	3.000	0.029	0.086	3.000	0.029	0.086	4.000	0.114	0.457	4.000	0.029	0.114	4.000	0.029	0.114	3.000	0.114	0.343	3.000	0.114	0.343
R6	4.000	0.104	0.416	3.000	0.052	0.156	4.000	0.052	0.208	3.000	0.104	0.312	4.000	0.052	0.208	4.000	0.052	0.208	2.000	0.052	0.104
R7	4.000	0.095	0.381	3.000	0.095	0.286	3.000	0.095	0.286	3.000	0.095	0.286	4.000	0.095	0.381	4.000	0.048	0.190	4.000	0.048	0.190
R8	4.000	0.118	0.471	3.000	0.118	0.353	3.000	0.059	0.176	3.000	0.059	0.176	3.000	0.029	0.088	3.000	0.059	0.176	4.000	0.118	0.471
R9	3.000	0.040	0.120	3.000	0.080	0.240	3.000	0.080	0.240	4.000	0.080	0.320	4.000	0.080	0.320	3.000	0.040	0.120	3.000	0.080	0.240
R10	3.000	0.078	0.235	4.000	0.020	0.078	3.000	0.078	0.235	4.000	0.078	0.314	4.000	0.078	0.314	3.000	0.039	0.118	4.000	0.078	0.314
R11	3.000	0.038	0.115	3.000	0.038	0.115	4.000	0.077	0.308	4.000	0.077	0.308	4.000	0.077	0.308	4.000	0.077	0.308	4.000	0.077	0.308
R12	4.000	0.078	0.314	4.000	0.078	0.314	4.000	0.078	0.314	4.000	0.078	0.314	3.000	0.078	0.235	4.000	0.078	0.314	4.000	0.078	0.314
R13	3.000	0.074	0.222	3.000	0.074	0.222	3.000	0.074	0.222	4.000	0.074	0.296	3.000	0.074	0.222	4.000	0.074	0.296	3.000	0.074	0.222
R14	4.000	0.092	0.368	4.000	0.092	0.368	4.000	0.092	0.368	4.000	0.092	0.368	4.000	0.092	0.368	4.000	0.092	0.368	4.000	0.092	0.368
R15	3.000	0.066	0.197	3.000	0.016	0.049	3.000	0.016	0.049	3.000	0.033	0.098	3.000	0.033	0.098	3.000	0.033	0.098	3.000	0.066	0.197
R16	4.000	0.092	0.368	4.000	0.092	0.368	4.000	0.092	0.368	4.000	0.092	0.368	4.000	0.092	0.368	4.000	0.092	0.368	4.000	0.092	0.368
R17	3.000	0.074	0.222	3.000	0.074	0.222	4.000	0.074	0.296	3.000	0.074	0.222	3.000	0.074	0.222	3.000	0.074	0.222	4.000	0.074	0.296
R18	4.000	0.111	0.444	4.000	0.028	0.111	3.000	0.111	0.333	4.000	0.028	0.111	4.000	0.028	0.111	4.000	0.111	0.444	4.000	0.111	0.444
R19	3.000	0.095	0.286	4.000	0.095	0.381	4.000	0.095	0.381	3.000	0.048	0.143	4.000	0.095	0.381	4.000	0.048	0.190	3.000	0.095	0.286
R20	4.000	0.100	0.400	3.000	0.025	0.075	4.000	0.050	0.200	4.000	0.050	0.200	4.000	0.050	0.200	3.000	0.050	0.150	3.000	0.025	0.075
R21	2.000	0.006	0.012	4.000	0.096	0.386	3.000	0.048	0.145	4.000	0.096	0.386	4.000	0.096	0.386	4.000	0.096	0.386	4.000	0.096	0.386
R22	3.000	0.047	0.140	4.000	0.023	0.093	4.000	0.093	0.372	4.000	0.093	0.372	4.000	0.023	0.093	4.000	0.093	0.372	4.000	0.047	0.186
Hasil S	3.409	0.077	0.272	3.455	0.063	0.219	3.591	0.079	0.285	3.682	0.071	0.262	3.727	0.069	0.260	3.682	0.074	0.276	3.591	0.076	0.278

HASIL PERHITUNGAN FAKTOR WEAKNESS

	W1			W2			W3			W4			W5			W6			W7		
Responden	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total
R1	1.000	0.049	0.049	1.000	0.049	0.049	1.000	0.049	0.049	2.000	0.098	0.195	2.000	0.049	0.098	1.000	0.098	0.098	3.000	0.024	0.073
R2	2.000	0.026	0.052	2.000	0.104	0.208	2.000	0.026	0.052	2.000	0.104	0.208	2.000	0.052	0.104	1.000	0.104	0.104	2.000	0.026	0.052
R3	1.000	0.071	0.071	1.000	0.071	0.071	1.000	0.071	0.071	1.000	0.071	0.071	1.000	0.071	0.071	1.000	0.071	0.071	1.000	0.071	0.071
R4	1.000	0.077	0.077	1.000	0.077	0.077	1.000	0.077	0.077	1.000	0.077	0.077	1.000	0.077	0.077	1.000	0.077	0.077	1.000	0.038	0.038
R5	1.000	0.114	0.114	2.000	0.057	0.114	2.000	0.057	0.114	1.000	0.114	0.114	2.000	0.029	0.057	1.000	0.114	0.114	1.000	0.057	0.057
R6	1.000	0.104	0.104	1.000	0.104	0.104	1.000	0.104	0.104	1.000	0.104	0.104	2.000	0.052	0.104	1.000	0.052	0.052	3.000	0.013	0.039
R7	1.000	0.095	0.095	1.000	0.095	0.095	3.000	0.012	0.036	1.000	0.095	0.095	3.000	0.012	0.036	2.000	0.024	0.048	1.000	0.095	0.095
R8	1.000	0.118	0.118	2.000	0.059	0.118	2.000	0.029	0.059	2.000	0.118	0.235	3.000	0.029	0.088	3.000	0.029	0.088	2.000	0.059	0.118
R9	2.000	0.080	0.160	2.000	0.040	0.080	2.000	0.080	0.160	1.000	0.080	0.080	2.000	0.080	0.160	2.000	0.080	0.160	2.000	0.080	0.160
R10	2.000	0.078	0.157	1.000	0.078	0.078	2.000	0.078	0.157	1.000	0.078	0.078	1.000	0.078	0.078	1.000	0.078	0.078	1.000	0.078	0.078
R11	1.000	0.077	0.077	1.000	0.077	0.077	1.000	0.077	0.077	1.000	0.077	0.077	1.000	0.077	0.077	1.000	0.077	0.077	1.000	0.077	0.077
R12	2.000	0.078	0.157	2.000	0.078	0.157	2.000	0.020	0.039	1.000	0.078	0.078	3.000	0.078	0.235	1.000	0.039	0.039	2.000	0.078	0.157
R13	1.000	0.074	0.074	2.000	0.074	0.148	3.000	0.074	0.222	1.000	0.074	0.074	1.000	0.019	0.019	2.000	0.074	0.148	2.000	0.074	0.148
R14	1.000	0.092	0.092	1.000	0.011	0.011	1.000	0.046	0.046	1.000	0.092	0.092	1.000	0.011	0.011	1.000	0.011	0.011	1.000	0.092	0.092
R15	2.000	0.066	0.131	2.000	0.131	0.262	2.000	0.033	0.066	3.000	0.066	0.197	2.000	0.131	0.262	2.000	0.016	0.033	3.000	0.033	0.098
R16	1.000	0.092	0.092	1.000	0.092	0.092	1.000	0.092	0.092	1.000	0.046	0.046	4.000	0.006	0.023	4.000	0.006	0.023	4.000	0.006	0.023
R17	1.000	0.074	0.074	1.000	0.074	0.074	1.000	0.037	0.037	1.000	0.074	0.074	1.000	0.074	0.074	2.000	0.074	0.148	2.000	0.074	0.148
R18	3.000	0.056	0.167	1.000	0.111	0.111	2.000	0.028	0.056	1.000	0.111	0.111	2.000	0.028	0.056	1.000	0.028	0.028	3.000	0.111	0.333
R19	1.000	0.095	0.095	1.000	0.095	0.095	2.000	0.024	0.048	2.000	0.048	0.095	1.000	0.024	0.024	2.000	0.095	0.190	2.000	0.095	0.190
R20	1.000	0.100	0.100	1.000	0.100	0.100	1.000	0.100	0.100	1.000	0.100	0.100	1.000	0.100	0.100	1.000	0.100	0.100	2.000	0.050	0.100
R21	1.000	0.096	0.096	1.000	0.096	0.096	2.000	0.024	0.048	1.000	0.096	0.096	4.000	0.006	0.024	2.000	0.048	0.096	1.000	0.096	0.096
R22	1.000	0.093	0.093	1.000	0.093	0.093	1.000	0.093	0.093	1.000	0.093	0.093	2.000	0.047	0.093	1.000	0.093	0.093	1.000	0.093	0.093
Hasil W	1.318	0.082	0.102	1.318	0.080	0.105	1.636	0.056	0.082	1.273	0.086	0.109	1.909	0.051	0.085	1.545	0.063	0.085	1.864	0.065	0.106

HASIL PERHITUNGAN FAKTOR OPPORTUNITIES

	O1			O2			O3			O4			O5			O6			O7		
Responden	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total
R1	4.000	0.094	0.376	4.000	0.047	0.188	3.000	0.047	0.141	3.000	0.012	0.035	4.000	0.094	0.376	4.000	0.094	0.376	4.000	0.094	0.376
R2	3.000	0.101	0.304	4.000	0.101	0.405	2.000	0.006	0.013	3.000	0.025	0.076	3.000	0.051	0.152	3.000	0.006	0.019	3.000	0.101	0.304
R3	4.000	0.106	0.424	4.000	0.106	0.424	2.000	0.013	0.026	2.000	0.013	0.026	4.000	0.106	0.424	4.000	0.106	0.424	4.000	0.106	0.424
R4	4.000	0.110	0.441	4.000	0.110	0.441	2.000	0.028	0.055	2.000	0.014	0.028	4.000	0.110	0.441	4.000	0.055	0.221	4.000	0.110	0.441
R5	3.000	0.105	0.316	4.000	0.105	0.421	4.000	0.105	0.421	3.000	0.026	0.079	3.000	0.053	0.158	3.000	0.026	0.079	4.000	0.105	0.421
R6	3.000	0.094	0.281	4.000	0.094	0.374	4.000	0.094	0.374	3.000	0.094	0.281	4.000	0.094	0.374	3.000	0.047	0.140	3.000	0.094	0.281
R7	4.000	0.096	0.386	4.000	0.096	0.386	3.000	0.048	0.145	3.000	0.012	0.036	4.000	0.096	0.386	4.000	0.096	0.386	4.000	0.096	0.386
R8	3.000	0.129	0.387	3.000	0.065	0.194	3.000	0.032	0.097	2.000	0.016	0.032	2.000	0.016	0.032	3.000	0.065	0.194	3.000	0.129	0.387
R9	4.000	0.083	0.333	3.000	0.083	0.250	4.000	0.083	0.333	4.000	0.083	0.333	4.000	0.083	0.333	4.000	0.042	0.167	3.000	0.083	0.250
R10	4.000	0.083	0.333	4.000	0.083	0.333	4.000	0.083	0.333	3.000	0.042	0.125	4.000	0.083	0.333	4.000	0.083	0.333	4.000	0.083	0.333
R11	4.000	0.090	0.360	4.000	0.090	0.360	4.000	0.090	0.360	3.000	0.045	0.135	3.000	0.045	0.135	4.000	0.090	0.360	4.000	0.090	0.360
R12	3.000	0.090	0.270	4.000	0.090	0.360	4.000	0.090	0.360	4.000	0.011	0.045	4.000	0.022	0.090	4.000	0.090	0.360	4.000	0.090	0.360
R13	4.000	0.085	0.340	4.000	0.085	0.340	3.000	0.085	0.255	3.000	0.085	0.255	3.000	0.085	0.255	4.000	0.085	0.340	4.000	0.085	0.340
R14	4.000	0.082	0.330	4.000	0.082	0.330	4.000	0.082	0.330	4.000	0.082	0.330	4.000	0.082	0.330	4.000	0.082	0.330	4.000	0.082	0.330
R15	3.000	0.085	0.255	3.000	0.043	0.128	3.000	0.043	0.128	3.000	0.021	0.064	3.000	0.021	0.064	4.000	0.021	0.085	3.000	0.043	0.128
R16	4.000	0.090	0.360	4.000	0.090	0.360	4.000	0.090	0.360	1.000	0.006	0.006	4.000	0.090	0.360	4.000	0.090	0.360	4.000	0.090	0.360
R17	3.000	0.056	0.169	3.000	0.056	0.169	2.000	0.014	0.028	2.000	0.014	0.028	4.000	0.113	0.451	2.000	0.014	0.028	4.000	0.113	0.451
R18	4.000	0.099	0.395	4.000	0.099	0.395	3.000	0.025	0.074	2.000	0.012	0.025	3.000	0.025	0.074	4.000	0.099	0.395	4.000	0.099	0.395
R19	4.000	0.096	0.386	4.000	0.096	0.386	4.000	0.096	0.386	3.000	0.024	0.072	4.000	0.096	0.386	3.000	0.048	0.145	4.000	0.096	0.386
R20	4.000	0.098	0.390	3.000	0.012	0.037	4.000	0.098	0.390	3.000	0.049	0.146	3.000	0.098	0.293	4.000	0.012	0.049	4.000	0.098	0.390
R21	4.000	0.095	0.381	4.000	0.095	0.381	3.000	0.048	0.143	3.000	0.048	0.143	4.000	0.095	0.381	4.000	0.095	0.381	4.000	0.095	0.381
R22	4.000	0.105	0.421	4.000	0.105	0.421	3.000	0.026	0.079	4.000	0.026	0.105	4.000	0.105	0.421	4.000	0.026	0.105	4.000	0.105	0.421
Hasil O	3.682	0.094	0.347	3.773	0.083	0.322	3.273	0.060	0.220	2.864	0.035	0.109	3.591	0.076	0.284	3.682	0.062	0.240	3.773	0.095	0.359

HASIL PERHITUNGAN FAKTOR TREATH

	T1			T2			T3			T4			T5*			T6		
Responden	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total	Rating	Bobot	Total
R1	2.000	0.047	0.094	2.000	0.094	0.188	1.000	0.094	0.094	1.000	0.094	0.094	3.000	0.094	0.282	2.000	0.094	0.188
R2	1.000	0.101	0.101	1.000	0.101	0.101	2.000	0.101	0.203	2.000	0.101	0.203	3.000	0.101	0.304	2.000	0.101	0.203
R3	1.000	0.106	0.106	1.000	0.106	0.106	1.000	0.106	0.106	3.000	0.013	0.040	2.000	0.007	0.013	1.000	0.106	0.106
R4	1.000	0.110	0.110	1.000	0.110	0.110	1.000	0.110	0.110	3.000	0.014	0.041	2.000	0.007	0.014	1.000	0.110	0.110
R5	2.000	0.053	0.105	2.000	0.053	0.105	2.000	0.105	0.211	2.000	0.105	0.211	4.000	0.105	0.421	2.000	0.053	0.105
R6	1.000	0.094	0.094	1.000	0.094	0.094	2.000	0.094	0.187	2.000	0.012	0.023	3.000	0.006	0.018	1.000	0.094	0.094
R7	1.000	0.096	0.096	1.000	0.096	0.096	1.000	0.096	0.096	1.000	0.048	0.048	3.000	0.024	0.072	1.000	0.096	0.096
R8	1.000	0.129	0.129	2.000	0.129	0.258	2.000	0.129	0.258	2.000	0.032	0.065	3.000	0.065	0.194	2.000	0.065	0.129
R9	2.000	0.083	0.167	2.000	0.083	0.167	1.000	0.083	0.083	1.000	0.083	0.083	3.000	0.042	0.125	1.000	0.083	0.083
R10	2.000	0.083	0.167	2.000	0.083	0.167	2.000	0.083	0.167	2.000	0.083	0.167	3.000	0.042	0.125	2.000	0.083	0.167
R11	1.000	0.090	0.090	1.000	0.090	0.090	1.000	0.090	0.090	1.000	0.090	0.090	2.000	0.011	0.022	2.000	0.045	0.090
R12	1.000	0.090	0.090	2.000	0.090	0.180	1.000	0.090	0.090	1.000	0.090	0.090	4.000	0.045	0.180	1.000	0.090	0.090
R13	1.000	0.085	0.085	1.000	0.085	0.085	1.000	0.085	0.085	2.000	0.085	0.170	3.000	0.085	0.255	2.000	0.085	0.170
R14	1.000	0.082	0.082	1.000	0.082	0.082	1.000	0.082	0.082	1.000	0.082	0.082	4.000	0.010	0.041	1.000	0.082	0.082
R15	2.000	0.170	0.340	1.000	0.170	0.170	2.000	0.170	0.340	3.000	0.170	0.511	3.000	0.021	0.064	2.000	0.021	0.043
R16	4.000	0.090	0.360	1.000	0.090	0.090	1.000	0.090	0.090	1.000	0.090	0.090	1.000	0.006	0.006	1.000	0.090	0.090
R17	1.000	0.113	0.113	1.000	0.113	0.113	1.000	0.113	0.113	1.000	0.113	0.113	4.000	0.056	0.225	1.000	0.113	0.113
R18	2.000	0.049	0.099	1.000	0.099	0.099	1.000	0.099	0.099	2.000	0.099	0.198	3.000	0.099	0.296	1.000	0.099	0.099
R19	2.000	0.048	0.096	1.000	0.096	0.096	1.000	0.096	0.096	1.000	0.096	0.096	3.000	0.012	0.036	1.000	0.096	0.096
R20	1.000	0.098	0.098	1.000	0.098	0.098	1.000	0.098	0.098	1.000	0.098	0.098	4.000	0.098	0.390	2.000	0.049	0.098
R21	2.000	0.048	0.095	1.000	0.095	0.095	1.000	0.095	0.095	2.000	0.048	0.095	3.000	0.048	0.143	1.000	0.095	0.095
R22	1.000	0.105	0.105	1.000	0.105	0.105	1.000	0.105	0.105	1.000	0.026	0.026	3.000	0.053	0.158	1.000	0.105	0.105
Hasil T	1.500	0.090	0.128	1.273	0.098	0.123	1.273	0.101	0.132	1.636	0.076	0.120	3.000	0.047	0.154	1.409	0.084	0.111

PERHITUNGAN RATING ATTRACTIVE SCORE QSPM

PENYEDIAAN LAYANAN CA

No.	Faktor Utama	Rating Responden 1			Rating Responden 2			Rating Responden 3			Rata-rata Rating		
Internal		Fokus Nilai Terbaik	Pengembangan Pasar	Integrasi	Fokus Nilai Terbaik	Pengembangan Pasar	Integrasi	Fokus Nilai Terbaik	Pengembangan Pasar	Integrasi	Fokus Nilai Terbaik	Pengembangan Pasar	Integrasi
I1	Visi Misi Lemsaneg	4.00	3.00	2.00	2.00	4.00	3.00	4.00	3.00	2.00	3.33	3.33	2.33
I2	Kompetensi/kemampuan pengamanan Lemsaneg	3.00	3.00	3.00	1.00	2.00	4.00	2.00	3.00	4.00	2.00	2.67	3.67
I3	Kemampuan manajemen aspek security	3.00	3.00	2.00	1.00	4.00	3.00	2.00	3.00	2.00	2.00	3.33	2.33
I4	Ketersediaan sarana pendukung CA (penelitian&operasional)	3.00	4.00	3.00	4.00	2.00	3.00	3.00	4.00	3.00	3.33	3.33	3.00
I5	Penelitian, pembangunan & operasional layanan *CA*	4.00	4.00	3.00	1.00	4.00	2.00	3.00	3.00	3.00	2.67	3.67	2.67
I6	kemampuan menjadi *CA* bagi publik (propietary algoritma).	4.00	4.00	3.00	1.00	4.00	3.00	3.00	3.00	2.00	2.67	3.67	2.67
I7	Pengaruh Dukungan Unit Tehnis Persandian	3.00	3.00	3.00	4.00	2.00	3.00	4.00	3.00	3.00	3.67	2.67	3.00
I8	Kemampuan struktur organisasi melayani publik	3.00	4.00	3.00	4.00	1.00	2.00	4.00	4.00	3.00	3.67	3.00	2.67

I9	Kompleksitas Koordinasi	4.00	4.00	3.00	4.00	1.00	3.00	3.00	3.00	4.00	3.67	2.67	3.33
I10	Peluang sebagai pendatang baru dalam penyedia jasa layanan keamanan CA (*publik service*)	3.00	3.00	3.00	2.00	4.00	3.00	3.00	4.00	3.00	2.67	3.67	3.00
I11	Jumlah dan Kualitas SDM	4.00	4.00	4.00	1.00	4.00	3.00	2.00	3.00	2.00	2.33	3.67	3.00
I12	Kompleksitas layanan CA	3.00	3.00	3.00	1.00	4.00	3.00	3.00	4.00	3.00	2.33	3.67	3.00
I13	Dukungan produk hukum internal untuk tugas pengamanan (ataupun persandian) bagi kepentingan publik	3.00	3.00	2.00	4.00	2.00	3.00	4.00	3.00	2.00	3.67	2.67	2.33
I14	Sumber Dana & Pengambilan Keputusan	4.00	4.00	3.00	2.00	4.00	3.00	3.00	3.00	3.00	3.00	3.67	3.00

No.	Faktor Utama	Rating Responden 1			Rating Responden 2			Rating Responden 3			Rata-rata Rating		
Eksternal		Fokus Nilai Terbaik	Pengembangan Pasar	Integrasi	Fokus Nilai Terbaik	Pengembangan Pasar	Integrasi	Fokus Nilai Terbaik	Pengembangan Pasar	Integrasi	Fokus Nilai Terbaik	Pengembangan Pasar	Integrasi
E1	Kebutuhan Tinggi di Era Konvergensi	3	3	3	1	3	4	3	4	3	2.33	3.33	3.33
E2	Dukungan Undang-undang & Hukum	4	4	3	1	4	2	4	3	3	3.00	3.67	2.67
E3	Tidak adanya CA lokal di Indonesia	3	4	3	2	4	3	2	3	3	2.33	3.67	3.00

E4	Pengganti Layanan CA	3	3	3	-	-	-	2	3	3	-	-	-
E5	Pengaruh Remunerasi	-	-	-	4	1	2	-	-	-	-	-	-
E6	Kesiapan Infratruktur Telekomunikasi (Data)	4	4	3	4	2	3	2	2	2	3.33	2.67	2.67
E7	Keamanan,efisiensi dan kepuasan yang dicapai oleh publik	4	4	4	4	1	2	2	4	4	3.33	3.00	3.33
E8	Investasi	3	4	3	4	2	3	2	2	3	3.00	2.67	3.00
E9	Kualitas jaringan data, sarana prasarana	3	4	3	2	4	3	2	4	4	2.33	4.00	3.33
E10	Security Awareness Publik	4	4	4	2	3	4	3	3	4	3.00	3.33	4.00
E11	Persaingan penyediaan layanan CA	3	4	3	2	4	3	2	4	3	2.33	4.00	3.00
E12	Kemampuan kehadiran mendunia	3	3	2	4	1	2	3	2	2	3.33	2.00	2.00
E13	Kesiapan Ekonomi & Teknologi di Indonesia untuk berorientasi keamanan	**3**	4	4	**1**	4	3	**4**	4	4	2.67	4.00	3.67

Quantitative Strategic Planning Matrix

PENYEDIAAN LAYANAN CA

No.	Faktor Utama	Bobot	Fokus		Pengembangan Pasar		Integrasi	
			AS	TAS	AS	TAS	AS	TAS
Internal								
I1	Visi Misi Lemsaneg	0.100	3.333	0.333	3.333	0.333	2.333	0.233
I2	Kompetensi/kemampuan pengamanan Lemsaneg	0.070	2.000	0.139	2.667	0.186	3.667	0.255
I3	Kemampuan manajemen aspek security	0.089	2.000	0.178	3.333	0.297	2.333	0.208
I4	Ketersediaan sarana pendukung CA (penelitian&operasional)	0.058	3.333	0.195	3.333	0.195	3.000	0.175
I5	Penelitian, pembangunan & operasional layanan *CA*	0.070	2.667	0.186	3.667	0.255	2.667	0.186
I6	kemampuan menjadi *CA* bagi publik (propietary algoritma).	0.070	2.667	0.186	3.667	0.255	2.667	0.186
I7	Pengaruh Dukungan Unit Tehnis Persandian	0.037	3.667	0.136	2.667	0.099	3.000	0.112
I8	Kemampuan struktur organisasi melayani publik	0.047	3.667	0.172	3.000	0.141	2.667	0.125
I9	Kompleksitas Koordinasi	0.078	3.667	0.286	2.667	0.208	3.333	0.260
I10	Peluang sebagai pendatang baru dalam penyedia jasa layanan keamanan CA (*publik service*)	0.070	2.667	0.186	3.667	0.255	3.000	0.209
I11	Jumlah dan Kualitas SDM	0.070	2.333	0.162	3.667	0.255	3.000	0.209
I12	Kompleksitas layanan CA	0.070	2.333	0.162	3.667	0.255	3.000	0.209

I13	Dukungan produk hukum internal untuk tugas pengamanan (ataupun persandian) bagi kepentingan publik	0.100	3.667	0.366	2.667	0.266	2.333	0.233
I14	Sumber Dana & Pengambilan Keputusan	0.111	3.000	0.334	3.667	0.409	3.000	0.334
		1.039						
Eksternal								
E1	Kebutuhan Tinggi di Era Konvergensi	0.111	2.333	0.258	3.333	0.369	3.333	0.369
E2	Dukungan Undang-undang & Hukum	0.101	3.000	0.304	3.667	0.371	2.667	0.270
E3	Tidak adanya CA lokal di Indonesia	0.080	2.333	0.186	3.667	0.292	3.000	0.239
E4	Pengganti Layanan CA	0.053	-	-	-	-	-	-
E5	Pengaruh Remunerasi	0.051	-	-	-	-	-	-
E6	Kesiapan Infratruktur Telekomunikasi (Data)	0.080	3.333	0.266	2.667	0.212	2.667	0.212
E7	Keamanan,efisiensi dan kepuasan yang dicapai oleh publik	0.101	3.333	0.337	3.000	0.304	3.333	0.337
E8	Investasi	0.080	3.000	0.239	2.667	0.212	3.000	0.239
E9	Kualitas jaringan data, sarana prasarana	0.080	2.333	0.186	4.000	0.319	3.333	0.266
E10	Security Awareness Publik	0.067	3.000	0.201	3.333	0.223	4.000	0.267
E11	Persaingan penyediaan layanan CA	0.051	2.333	0.118	4.000	0.202	3.000	0.152
E12	Kemampuan kehadiran mendunia	0.042	3.333	0.142	2.000	0.085	2.000	0.085
E13	Kesiapan Ekonomi & Teknologi di Indonesia untuk berorientasi keamanan	0.105	2.667	0.281	4.000	0.421	3.667	0.386
		1.000						
STAS				**5.539**		**6.421**		**5.756**