EKOSISTEM PENYELENGGARAAN SERTIFIKAT ELEKTRONIK DALAM SISTEM PERDAGANGAN ELEKTRONIK

THE ECOSYSTEM OF ELECTRONIC CERTIFICATE IMPLEMENTATION IN ELECTRONIC COMMERCE SYSTEM

Ahmad Budi Setiawan

Puslitbang Aplikasi Informatika dan Informasi Komunikasi
Publik Jl. Medan Merdeka Barat No.9 Jakarta 10110
ahma003@kominfo.go.id

Naskah diterima 13 Oktober 2015, diedit 21 Oktober 2015, disetujui 29 Oktober 2015

Abstract

The Trend of e-commerce in Indonesia is growing and developing rapidly. It is driven from demographic trends that exist in Indonesia. If the electronic transaction business can be well managed business that will be a huge benefit to the economy. Currently e-commerce ecosystem in Indonesia is still unfavorable. One of the obstacles in electronic transactions, namely related payments. This problem arises because the consumer electronics business in Indonesia has yet to feel the ease and security in electronic transactions that affect their beliefs and attitudes. Related to this, online businesses have started offering payment solutions that enable customers. Therefore it takes an electronic transaction conducive ecosystem to support such solutions. In this case the Government is obliged to facilitate electronic transactions conducive ecosystem. In addition, the implementation of the strategy also needed institutional electronic certificate to encourage the growth Ecosystem transasksi Electronic System Operator reliability and performance as well as facilitate the Government in managing electronic certificate policy. This study aims to provide advice to the government in the form of an implementation strategy ecosystems electronic transactions. The study was conducted using Soft System. Results of this study provide advice to the Government related to the availability of infrastructure and institutional electronic certificates in electronic transaction systems ecosystem as well as focus on the enforcement of existing regulations.

Keywords*: Electronic Certificate, e-commerce, Soft System*

Abstrak

Tren perdagangan elektronis di Indonesia tumbuh dan berkembang cepat. Hal ini didorong dari tren demografis yang ada di Indonesia. Apabila bisnis transaksi elektronik dapat dikelola dengan baik akan menjadi bisnis yang memberikan keuntungan sangat besar bagi perekonomian. Saat ini ekosistem *e-commerce* di Indonesia masih kurang kondusif. Salah satu kendala dalam transaksi elektronik, yaitu terkait pembayaran. Permasalahan ini timbul karena para konsumen bisnis elektronik di Indonesia belum merasakan kemudahan dan keamanan dalam bertransaksi secara elektronik sehingga mempengaruhi kepercayaan dan sikap mereka. Terkait dengan hal tersebut, para pelaku bisnis online sudah mulai menawarkan solusi pembayaran yang memudahkan konsumen. Oleh karena itu dibutuhkan sebuah ekosistem transaksi elektronik yang kondusif untuk mendukung solusi tersebut. Dalam hal ini Pemerintah berkewajiban untuk memfasilitasi ekosistem transaksi elektronik yang kondusif. Di samping itu, dibutuhkan juga strategi implementasi kelembagaan sertifikat elektronik untuk mendorong tumbuh kembangnya Ekosistem Penyelenggara Sistem Transaksi Elektronik yang terpercaya dan handal serta memudahkan Pemerintah dalam mengelola kebijakan sertifikat elektronik. Kajian ini bertujuan untuk memberikan saran kepada pemerintah berupa strategi implementasi ekosistem transaksi elektronik. Kajian ini dilakukan dengan menggunakan metode *Soft System.* Hasil kajian ini memberikan saran kepada Pemerintah terkait ketersediaan infrastruktur dan kelembagaan sertifikat elektronik dalam ekosistem sistem transaksi elektronik serta fokus terhadap penegakkan hukum yang telah ada.

Kata-kata kunci: Sertifikat Elektronik, Perdagangan Elektronis, *Soft System*

PENDAHULUAN

Globalisasi teknologi komunikasi yang semakin terpadu membuat dunia menjadi seolah 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 bisnis secara elektronik. Transformasi proses bisnis yang semula dilakukan secara manual, saat ini sudah dilakukan secara elektronis dan *on-line* disebabkan oleh semakin pesatnya perkembangan teknologi informasi dan komunikasi. Bisnis dan transaksi elektronik (*e-Business, e-Government, e-Commerce, e-procurement*) adalah suatu trend yang sangat menjanjikan. Peluang tersebut disebabkan oleh kemudahan transaksi eketronik karena dapat dapat dilakukan kapanpun, dimanapun dan oleh siapapun secara *real time*. Berdasarkan terminologi UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), definisi Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya. Sementara itu, sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan elektronik. Adapun Penyelenggara sistem elektronik adalah setiap orang, penyelenggaraan negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/ atau keperluan pihak lain (Departemen Komunikasi dan Informatika, 2006).

Namun, semakin tingginya penggunaan teknologi informasi di era globalisasi komunikasi ini, semakin meningkat pula risiko yang dihadapi, terutama dari sisi kualitas dan keamanannya. Berbagai ancaman terhadap suatu data atau informasi yang dipertukarkan melalui jaringan internet menuntut suatu solusi keamanan yang salah satunya dengan menggunakan sertifikat elektronik yang dikeluarkan dan dikelola oleh pihak ketiga terpercaya (*Trusted Third Party*) atau lazim disebut CA (*Certification Authority*). CA atau dikenal juga dengan istilah sertifikat elektronik menjamin 4 (empat) aspek dalam transaksi elektronik, yaitu kerahasiaan (*confidentiality*), menyangkut kerahasiaan dari data atau informasi, dan perlindungan bagi informasi tersebut dari pihak yang tidak berwenang, Keotentikan (*authenticity*); menyangkut kemampuan seseorang, organisasi, atau komputer untuk membuktikan identitas dari pemilik yang sesungguhnya dari informasi tersebut, integritas (*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, dan Nir sangkal (*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. Ketidaknyamanan dalam transaksi elektronik menyebabkan berkembangnya isu-isu mengenai *trust* dalam transaksi elektronik baik dalam lingkup nasional, regional dan global.

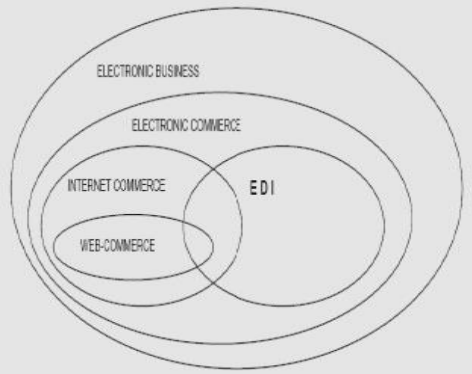
Keberhasilan sebuah transaksi bisnis secara elektronik dapat dinilai dari tiga kriteria, yaitu; dari sisi akses (*access*), keuntungan (*benefit*) dan komunitas (*community*). Sebuah transaksi elektronik dapat dikategorikan baik jika dapat diakses dengan cepat, aman, aplikasinya mudah digunakan dan cakupannya (*coverage*) luas. Selain itu, transaksi elektronik dapat memberikan keuntungan seperti: meningkatkan efisiensi, fleksibel, memperluas pasar (e*xpand market*) dan merespon customer secara *real time*. Dari sisi komunitas, transaksi elektronik dikategorikan baik jika dapat menjadikan masyarakat saling terhubung, mengubah budaya dan pola pikir (*mindset*), berhasil mengubah lingkngan ekosistem pasar. Ketiga kunci kesuksesan sebuah transaksi bisnis secara elektronik dijalankan dalam sebuah mekanisme bisnis (*enterprise*) dan berdasarkan aturan dan kebijakan yang berlaku. Transaksi elektronik harus aman dan andal, karena setiap penyelenggaraan transaksi elektronik wajib memiliki sertifikat keandalan dan sertifikat elektronik. Kajian ini ditujukan untuk menggali dan mempelajari strategi implementasi dan kelembagaan Penyelenggara Sertifikat Elektronik yang perlu dirancang oleh Kementerian Kominfo untuk memberikan arahan dan kebijakan dalam kegiatan transaksi elektronik yang andal dan terpercaya. Maka permasalahan yang dibahas dalam kajian ini adalah; Bagaimanakah ekosistem sertifikasi elektronik dalam penyelenggaraan sistem perdagangan elektronik di Indonesia guna mendukung tumbuh kembangnya industri Sertifikat Elektronik di Indonesia?

Hasil kajian ini diharapkan dapat memberikan manfaat, yaitu dapat dijadikan sebuah rekomendasi untuk Direktorat Keamanan Informasi, Ditjen APTIKA dalam membuat strategi dalam menerapkan regulasi/kebijakan dibidang sertifikat elektronik untuk transaksi elektronik. Di samping itu, dapat menjadi acuan bagi Direktorat Keamanan Informasi, Ditjen Aplikasi Informatika untuk menerapkan kebijakan lebih lanjut berdasarkan hasil kajian yang dilakukan. Adapun Tujuan penelitian ini adalah untuk memberikan rekomendasi penerapan kebijakan mengenai penyelenggaraan sertifikat elektronik yang digunakan dalam kegiatan transaksi elektronik agar mendukung tumbuh-kembangnya industri sertifikat elektronik di Indonesia. Selain itu diharapkan dapat memberikan masukan dalam pembuatan peta jalan implementasi ekosistem sertifikasi elektronik dan keandalan sebagai amanat PP No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Tinjauan Pustaka

Perdagangan melalui jaringan elektronik atau e-commerce didefinisikan sebagai aktivitas perdagangan melalui jaringan elektronik dengan menggunakan perangkat komputer untuk memudahkan semua operasi komputer. *E-commerce* melibatkan lebih dari satu

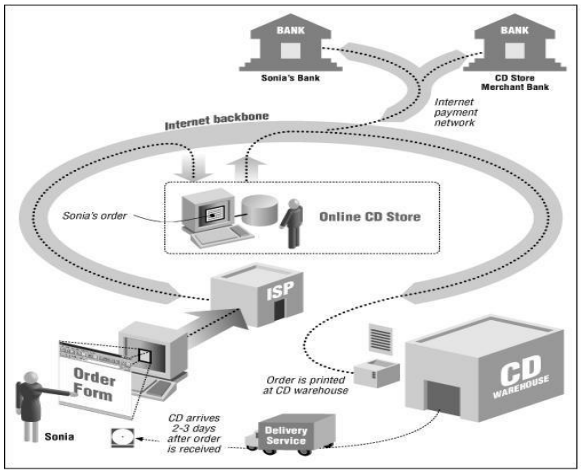
perusahaan, dan dapat diaplikasikan hampir di setiap jenis hubungan bisnis. *E-commerce* mengijinkan produsen untuk menjual produk-produk dan jasa secara *online*. Calon pelanggan atau konsumen dapat menemukan website produsen,membaca dan melihat produk-produk, memesan dan membayar produk-produk secara *online*. Pada website whatis.com terdapat pengertian *e-commerce* yaitu berhubungan dengan pembelian dan penjualan barang atau jasa melalui internet khususnya World Wide Web.



Gambar 1. Ruang Lingkup Perdagangan Elektronis

Mekanisme transaksi elektronik dengan *e-commerce* dimulai dengan adanya penawaran suatu produk tertentu oleh penjual (misalnya bertempat kedudukan di USA) di suatu website melalui server yang berada di Indonesia (misalnya detik.com). Apabila konsumen Indonesia melakukan pembelian, maka konsumen tersebut akan mengisi order mail yang telah disediakan oleh pihak penjual. Adapun cara transaksi pada *e-commerce,* permintaan pelanggan dikirim ke pedagang, kemudian setelah diterima oleh pedagang dan diverifikasi oleh pedagang, kemudian pelanggan yang melakukan pembayaran yang kemudian akan masuk ke server pembayaran. Pembayaran dapat dilakukan melalui kartu kredit, *smart cards,* rekening bank, dan sebagainya. Tahapan-tahapan dalam transaksi elektronik melalui *e-commerce* dapat diurutkan sebagai berikut:

1. *E-customer* dan *e-merchant* bertemu dalam dunia maya melalui server yang disewa dari Internet Server Provider (ISP) oleh *e-merchant.*
2. Transaksi melalui *e-commerce* disertai *term of use* dan *sales term condition* atau klausula standar, yang pada umumnya *e-merchant* telah meletakkan klausula kesepakatan pada *website*-nya, sedangkan *e-customer* jika berminat tinggal memilih tombol *accept* atau menerima.
3. Penerimaan *e-customer* melalui mekanisme "klik" tersebut sebagai perwujudan dari kesepakatan yang tentunya mengikat pihak *e-merchant.*
4. Pada saat kedua belah pihak mencapai kesepakatan, kemudian diikuti dengan proses pembayaran, yang melibatkan dua bank perantara dari masing-masing pihak, yaitu *acquiring merchant bank* dan *issuing e-customer bank.* Customer memerintahkan kepada *issuing customer bank* untuk dan atas nama *e-customer* melakukan sejumlah pembayaran atas harga barang kepada *acquiring merchant bank* yang ditujukan kepada *e-merchant.*
5. Setelah proses pembayaran selesai kemudian diikuti dengan proses pemenuhan prestasi oleh pihak *e-merchant* berupa pengiriman barang sesuai dengan kesepakatan mengenai saat penyerahan dan spesifikasi barang.



Gambar 2. Ilustrasi Mekanisme Transaksi Elektronik

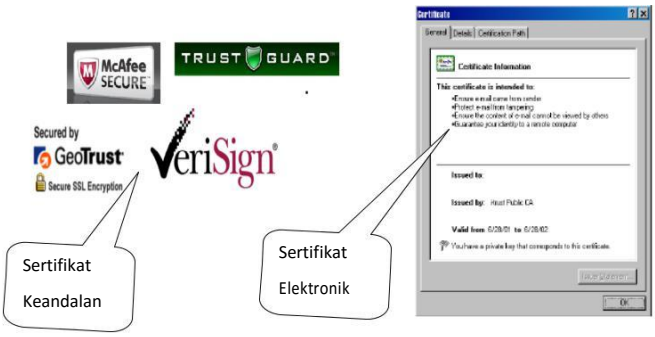
Pada transaksi elektronik, aplikasi menampilkan daftar barang yang tersedia. Lalu pengguna dapat memilih beberapa item yang ingin dibeli. Pada saat pengguna memilih suatu item barang, identitas barang tersebut dicatat, dan selanjutnya *user* dapat melanjutkan berbelanja atau memilih item yang lain. Server mengingat item apa saja yang telah dipesan. Pada saat pengguna melanjutkan *browsing*, server memelihara track pengguna tersebut dan pengguna tersebut dapat melakukan *check out* terhadap item-item yang telah dipesan.

Sertifikat Elektronik

Sertifikat Elektronik atau Sertifikat Digital adalah sertifikat yang bersifat elektronik dan memuat Tanda Tangan Elektronik serta identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik (PSrE). Adapun Kewenangan PSrE berdasarkan Pasal 60 PP PSTE, antara lain: (1). Pemeriksaan calon pemegang Sertifikat Elektronik. (2). Penerbitan Sertifikat Elektronik. (3). Perpanjangan masa berlaku Sertifikat Elektronik. (4). Pemblokiran dan pencabutan Sertifikat Elektronik. (5). Validasi Sertifikat Elektronik . (6). Pembuatan daftar Sertifikat Elektronik yang aktif dan yang dibekukan.

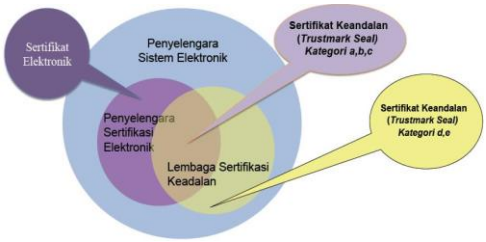
Sementara itu, Sertifikat Keandalan adalah dokumen yang menyatakan Pelaku Usaha yang menyelenggarakan Transaksi Elektronik telah lulus audit atau uji kesesuaian dari Lembaga Sertifikasi Keandalan. Lembaga Sertifikasi Keandalan (LSK) adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan Sertifikat Keandalan dalam Transaksi Elektronik. LSK, baik dalam Negeri maupun asing, harus

terdaftar dalam daftar Lembaga Sertifikasi Keandalan yang diterbitkan oleh Menteri (Pasal 62 PP PSTE).



Gambar 3. Contoh Sertifikat Keandalan dan Sertifikat Elektronik

Sertifikasi keandalan merupakan sebuah bukti bahwa pelaku usaha melakukan bisnis/perdagangan secara layak dan pada Sistem Elektronik Pelaku Usaha akan tertera logo sertifikasi (*trust mark*). Terdapat 5 (lima) kategori sertifikat keandalan, antara lain: (1). Pengamanan terhadap identitas, (2). Pengamanan terhadap pertukaran data, (3). Pengamanan terhadap kerawanan, (4). Pemeringkatan konsumen, dan (5). Pengamanan terhadap kerahasiaan data pribadi. Berdasarkan penjelasan tersebut, maka relasi antara Lembaga Sertifikasi Keandalan (LSK) dengan Penyelenggara Sertifikasi Elektronik (PSrE) adalah seperti digambarkan pada Gambar 4.



Gambar 4. Interelasi antara LSK dengan PSrE

Penyelenggaraan Transaksi Elektronik dalam lingkup publik atau privat yang menggunakan Sertifikat Elektronik untuk pelayanan publik wajib menggunakan sertifikat keandalan dan/atau sertifikat elektronik. Sertifikat keandalan tersebut wajib disertifikasi oleh LSK Indonesia yang telah terdaftar. Sertifikat Elektonik yang digunakan oleh Penyelenggara Transaksi Elektronik wajib memakai jasa penyelenggara Sertifikasi Elektronik (PSrE) yang telah tersertifikasi. Institusi Penyelenggara Sertifikasi Elektronik yang menyediakan sertifikat elektronik (*Certificate of Authority*) memfasilitasi sistem keamanan transaksi *online* (Internet) dengan Tanda Tangan Digital (*Digital Signature*) dan Infrastruktur Kunci Publik (*Public Key Encryption*). Sistem keamanan tersebut memiliki standar tertentu pada masing-masing proses. Standar spesifikasi teknis sertifikat elektronik umumnya menggunakan standar *X.509.v3*. Untuk proses enkripsi data untuk membentuk kunci publik pada sertifikat elektronik, pada umumnya digunakan standar enkripsi menggunakan salah satu algoritma kriptografi asimetris, yaitu algoritma RSA. Adapun untuk standar tanda tangan digital digunakan standar algoritma hashing, yaitu MD5, SHA dengan panjang kunci (key length) 1024 bit. (Choudhury, Bhatnagar, & Haque, 2002).

Konsep Soft Systems Methodology

Soft systems methodology (SSM) merupakan sebuah pendekatan untuk memecahkan masalah kompleks yang tidak terstruktur berdasarkan analisis holistik dan berpikir sistem. SSM juga merupakan sebuah metodologi partisipatori yang dapat membantu para *stakeholders* yang berbeda untuk mengerti perspektif masing-masing *stakeholders*. Fokus SSM adalah untuk menciptakan sistem aktivitas dan hubungan manusia dalam sebuah organisasi atau grup dalam rangka mencapai tujuan bersama. Pemikiran sistem selalu mencari keterpaduan antarbagian melalui pemahaman yang utuh, maka diperlukan suatu kerangka pikir baru yang dikenal sebagai pendekatan sistem (*system approach*). Pendekatan sistem ditandai dua hal: (1) mencari semua faktor penting yang ada untuk mendapat solusi terbaik dalam menyelesaikan masalah; dan (2) dibuat suatu unsur model kuantitatif untuk membantu keputusan secara rasional. Metodologi sistem dibagi dua: (1) *Hard system metodology* (HSM) seperti teknik operasional riset dan sistem dinamik; serta (2) *Soft System Metodology* (SSM). Untuk riset kebijakan sebaiknya digunakan teknik SSM, namun sering juga dimanfaatkan kehandalan sistem dinamik dari HSM untuk analisa sebab-akibat (Eriyatno dan Sofyan, 2007).

Implementasi konsep SSM menurut Checkland (Checklan & Poulter, 2006) yang dikembangkan lebih lanjut oleh Eriyatno dan Sofyan (Eriyanto & Sofyan, 2007) dilakukan dalam tujuh siklus: (1) situasi permasalahan tidak terstruktur (*problem situation*); (2) situasi permasalahan yang ditemu kenali, dalam bentuk *rich picture*, belum dalam pola kesisteman; (3) pendefinisian sistem yang relevan, dilakukan pertimbangan terhadap enam hal: *customers*, *actors*, *tranformation process*, *world view, owner*, dan *environmental constraints* (CATWOE); (4) model konseptual, CATWOE sebagai basis untuk menghasilkan model inovatif dari model yang ada; (5) perbandingan antara model konseptual dan situasi permasalahan yang ditemu-kenali; (6) identifikasi hal yang diinginkan secara sistematis dan perubahan yang layak secara efektif; dan (7) tindakan untuk memperbaiki keadaan.

Pemodelan Sistem

Pemodelan adalah terjemahan bebas dari istilah *modelling* untuk menghindari berbagai pengertian atau penafsiran yang berbeda-beda, pemodelan dapat diartikan sebagai suatu gugus aktivitas pembuatan model. Model didefinisikan sebagai perwakilan atau abstraksi dari sebuah objek atau situasi aktual. Pemodelan sistem yang bertujuan menghasilkan model kebijakan (*policy model*) adalah kombinasi dari dua referensi utama (Eriyatno, 2012), yaitu: (1) *Logical Thinking Process* (Dettmer, 2007); dan (2) SSM (Checkland, 1990). Validasi model merupakan

usaha untuk menyimpulkan bahwa model sistem yang dibangun merupakan representasi yang sah dari realitas yang dikaji sehingga dapat dihasilkan kesimpulan yang meyakinkan dan valid (Eriyatno, 2012). Validasi yang digunakan dalam penelitian ini adalah *face validity*. *Face validity*, yaitu pengukuran validitas dengan meminta pendapat para pakar yang berpengetahuan tentang sistem, apakah model yang diajukan telah berperilaku yang wajar. Teknik ini dapat digunakan dalam menentukan apakah logika dalam model konseptual dianggap benar dan hubungan *input-output* model beroperasi secara wajar. Proses validasi dilakukan menggunakan pendapat pakar, untuk mengetahui kesesuaian dan kelayakan model serta kebenaran logika dan teori dalam model konseptual, yang menjelaskan hubungan *input-output* model secara masuk akal. Pemodelan sistem yang bertujuan menghasilkan model kebijakan *(policy model)* adalah konvergensi dari *logical thinking process* (Dettmer, 2007) dan *soft system methodology-SSM* (Checkland dan Poulter, 2006). Melalui SSM *learning models* dirancang suatu model aktivitas yang berorientasi tujuan *(Purposeful Activity Models, PAM).* Model aktivitas tersebut dapat diwujudkan ke dalam bentuk model kelembagaan, model manajerial, atau model finansial. Input pemodelan system dapat diperoleh dari berbagai analisis, seperti *Analytical Network Process (ANP), Analytical Heirarchy Process (AHP),* atau *Interpretative Structural Modeling (ISM)* serta matriks kebijakan lainnya.

Penelitian yang Pernah Dilakukan

Penelitian yang pernah dilakukan dan relevan sebagai pembanding dalam penelitian ini, yaitu:

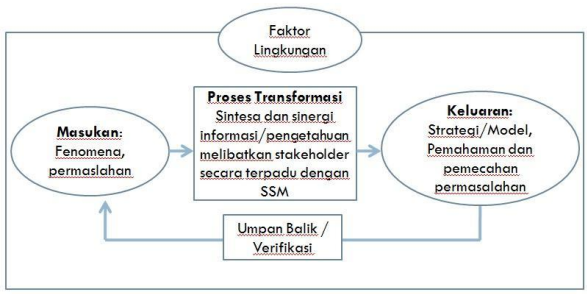
Pertama, penelitian yang dilakukan oleh Agus Riyanto, Eriyatno, Bomer Pasaribu, Agus Maulana dengan judul penelitian "Perancangan Model Integrasi Manajemen Kebijakan *Outsourcing* dalam Perspektif Hubungan Industrial", Tahun 2014 (Riyanto, Eriyatno, Pasaribu, Maulana, 2014). Penelitian tersebut bertujuan untuk merancang model integrasi manajemen kebijakan *outsourcing* dalam perspektif hubungan industrial untuk menciptakan harmonisasi aspek sosial budaya, ekonomi, dan hukum. Penelitian tersebut dilakukan dengan Metode Soft System Methodology (SSM). Data dikumpulkan melalui *Focus Group Discussion* (FGD), *In Depth Interview* (IDI) dan survei pakar. Teknik analisis menggunakan analisis CATWOE (*Customer, Actor, Transformation, World view, Owner, Environment Constraint*),Business Process Management (BPM), Analytical Network Process (ANP), *Strategic Assumption Surfacing and Testing* (SAST). Model dirancang melalui SSM Learning Model yang bertujuan untuk merancang *Purposeful Activity Models* (PAM).

Kedua, penelitian berikutnya adalah yang dilakukan oleh Willy Susilo, Eriyatno, M. Joko Affandi dan D. Agus Goenawan (Susilo, Eriyatno, Affandi, Goenawan, 2011). Judul penelitian tesebut adalah "Rancang Bangun Model Audit Manajemen Sumber Daya Manusia, Menggunakan Pendekatan Sistem". Penelitian ini menggunakan metodologi sistem lunak (*Soft System Methodology*). Tujuan dari penelitian tersebut adalah untuk merancang model audit Manajemen Sumber Daya Manusia (SDM), dengan menggunakan metodologi sistem lunak (SSM). Penelitian dilakukan dalam dua tahap. Tahap pertama adalah merancang model audit, menggunakan *Strategic Assumption Surfacing and Testing* (SAST), dan *Interpretatif Structural Modeling* (ISM), melalui *Focus Group Discussion* (FGD).

Ketiga, terkait dengan Sertifikat Elektronik, penelitian yang pernah dilakukan oleh Ahmad Budi Setiawan sebelumnya adalah Studi Standardisasi Sertifikat elektronik dan Keandalan Dalam Penyelenggaraan Sistem Transaksi Elektronik (Setiawan, 2014). Dalam penelitian tersebut juga menggunakan pendekatan *Soft System Methodology* dengan *tools Strategic Assumption Surfacing and Testing* (SAST) sebagai alat analisa untuk menentukan standar berikut kebijakan yang diambil oleh para pemangku-kepentingan (*stakeholder*) dalam system transaksi elektronik.

Kerangka Kerja Penelitian

Dalam konteks *Soft System Methodology*, menurut Jackson (2003), sistem adalah suatu keutuhan yang komplek di mana kefungsiannya tergantung pada bagian-bagian dan interaksi antar bagian tersebut. Pemikiran sistematis dalam konteks penyelesaian permasalahan yang kompleks adalah pemikiran mengenai hubungan keterkaitan, konteks/ lingkungan dengan memberikan penekanan yang lebih pada hubungan interaksi dari masing-masing unsur atau bagian-bagian secara utuh daripada masing-masing unsur dan bagian-bagian tersebut namun secara terpisah dan lebih fokus pada pendekatan proses sebagai pendekatan dalam pemecahan permasalahan yang kompleks. Konsep pemecahan masalah kompleks dengan pendekatan sistem lunak dapat diilustrasikan dalam Gambar 5 berikut ini.



Gambar 5. Skema Kerangka Kerja Penelitian

1) Fase Masukan

Fase ini dilakukan inventarisasi permasalahan yang muncul dalam kaitan implementasi sebuah standarisasi. Adanya kebijakan yang akan dikeluarkan dan disertai dengan permaslahan yang akan muncul jika kebijakan tersebut diimplementasikan akan dianalisis lebih lanjut. Analisis yang dilakukan melibatkan seluruh faktor yang ada pada lingkungan dimana kebijakan tersebut akan diimplementasikan. Dalam rangka inventarisasi permasalahan dapat juga dilakukan studi perbandingan dan juga studi terhadap literature yang terkait.

2) Proses Transformasi

Merupakan proses sintesis dan sinergi data/ informasi/pengetahuan untuk memahami permasalahan secara komprehensif. Pemahaman permasalahan secara komprehensif dapat melibatkan berbagai *stakeholder* atau yang mewakilkan yang terlibat dalam lingkungan implementasi kebijakan secara terpadu. Proses tersebut dilakunan dengan *Soft System Methodology* (SSM).

3) Fase Keluaran

Fase tersebut adalah pemahaman terhadap permasalahan dan tersedianya keputusan terhadap pemecahan sebuah permasalahan. Hasil dalam fase ini dapat berupa rekomendasi, strategi ataupun model yang dijadikan kerangka berpikir dalam penyelesaian permasalahan. Terhadap hasil fase tersebut dilakukan umpan balik/verifikasi berupa penilaian dari ahli/pakar yang berkompeten.

Metode Penelitian

a. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan *Soft System Methodology* (SSM), yaitu sebuah pendekatan holistik di dalam melihat aspek-aspek riil dan konseptual di masyarakat. SSM melihat setiap yang terjadi sebagai *Human Activity System*, karena serangkaian aktivitas manusia dapat disebut sebagai sebuah sistem, yaitu setiap aktivitas-aktivitas tersebut saling berhubungan dan membentuk suatu ikatan. Untuk memperoleh data dan informasi dilakukan penelitian langsung di lapangan dengan metode wawancara melalui wawancara mendalam (*deep interview*) dan survei pakar.

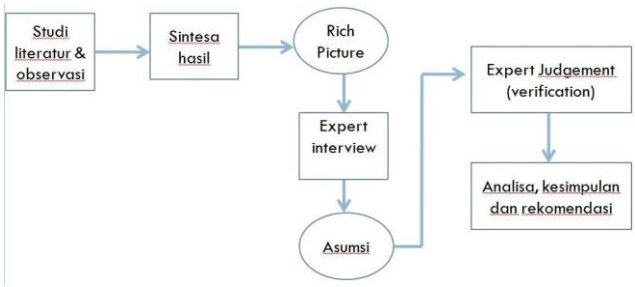
Berdasarkan kepakaran yang dimiliki, dapat digali asumsi yang paling signifikan berpengaruh terhadap hal-hal yang penting dan kritikal dalam proses penyusunan maupun perumusan program, kegiatan dan inisiatif. Pemeringkatan asumsi dilakukan berdasarkan:

1) Seberapa penting pengaruh asumsi tersebut terhadap keberhasilan atau kegagalan penerapan kebijakan standardisasi sertifikasi elektronik dan sertifikasi keandalan
2) Seberapa jauh keyakinan bahwa asumsi tersebut dapat dibenarkan

b. Tahapan Penelitian

Metode SSM yang digunakan dalam merancang bangun model adalah SSM *Learning Models* yang bertujuan mendesain *Purposeful Activity Models* (PAM) dengan menerapkan *logical thinking process* (Dettmer, 2007). Penelitian ini dilaksanakan dalam beberapa tahapan, yaitu (1) studi pustaka (studi literatur) untuk menentukan ruang lingkup penelitian, (2) survei pengumpulan data di beberapa lokasi yang ditentukan serta survei pakar untuk mengakuisisi pengetahuan *thinking respondent* secara purposive sampling (Cooper dan Schindler, 2008).

Tahap survei pakar yang dilakukan melalui wawancara mendalam dan diskusi terfokus (FGD). Gambar berikut ini adalah skema motode penelitian yang dilakukan:

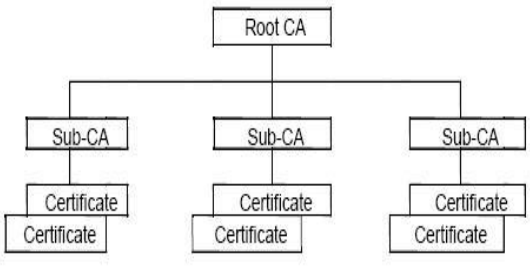


Gambar 6. Alur Kerangka Kerja Penelitian

HASIL PENELITIAN DAN PEMBAHASAN

Model Penyelenggara Sertifikat Elektronik

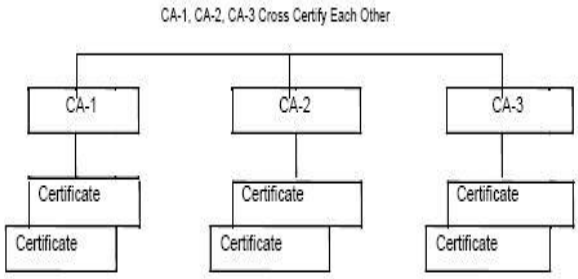
Penyelenggara Sertifikat Elektronik atau *Certification Authority* (CA) dapat dihubungkan dengan menggunakan dua arsitektur dasar atau hibrida (gabungan dari dua model dasar). Kedua model dasar tersebut antara lain: (1) hirarkis dan (2) *cross-certified* atau lintas-sertifikat (*shared trust*). Dalam model hirarkis, tingkat tertinggi (atau "Root") PSrE atau dikenal dengan PSrE induk dikerahkan dan bawahan PSrE dapat diatur untuk berbagai bisnis unit, domain atau komunitas minat. Root CA memvalidasi bawahan PSrE, yang pada gilirannya masalah sertifikat untuk menurunkan tingkat CA atau langsung ke pelanggan. PSrE induk memiliki persyaratan keamanan yang lebih ketat daripada PSrE bawahan. Meskipun sulit bagi penyerang untuk mengakses PSrE induk (yang dalam beberapa implementasi hanya secara online dalam peristiwa langka bahwa ia harus mengeluarkan, memperbarui, atau mencabut sertifikat PSrE CA bawahan), salah satu kelemahan model ini adalah bahwa PSrE induk merupakan titik tunggal kegagalan. Kepatuhan terhadap kebijakan yang ditetapkan dapat diuji melalui audit dari bawahan PSrE dan, dalam beberapa kasus, Otoritas Pendaftaran (*Registartion Authority*). Gambar berikut menggambarkan struktur dan hubungan antar otoritas sertifikasi dan pelanggan yang beroperasi di model hirarkis.



Gambar 7. CA Model Hirarkis

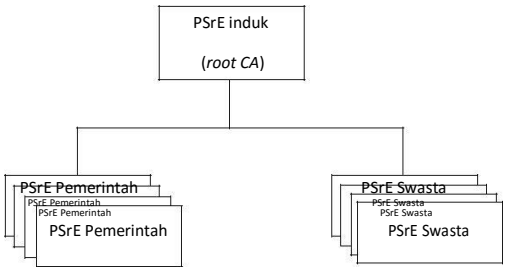
Dalam model alternatif, PSrE model *cross-*bersertifikat yang dibangun di atas model "peer-to-peer". Daripada menyebarkan PSrE induk (Root CA) secara umum, kepercayaan lintas sertifikasi saham Model antara CA diketahui satu sama lain. *Cross-certification* adalah proses di mana dua CA menyatakan kepercayaan sertifikat yang lain. Jika dua PSrE, PSrE 1 dan PSrE 2, dalam

model *cross*-sertifikasi, PSrE 1 menciptakan dan digital menandatangani sertifikat yang berisi kunci publik dari PSrE 2 (dan sebaliknya). Akibatnya, pengguna baik domain PSrE yakin bahwa setiap PSrE mempercayai pelanggan lain dan oleh karena itu dalam setiap domain dapat memercayai satu sama lain. PSrE model *Cross*-bersertifikat tidak tunduk pada titik tunggal kegagalan dalam model hirarkis. Namun, jaringan hanya sekuat terlemah CA, dan membutuhkan kebijakan yang terus-menerus. Pada model *cross*-bersertifikat, untuk membangun dan mempertahankan sebuah komunitas kepercayaan, audit dapat dilakukan untuk memastikan bahwa setiap PSrE cross-bersertifikat sesuai dengan satu set minimal praktek yang disepakati oleh para anggota komunitas kepercayaan. Diagram berikut menggambarkan struktur dan hubungan antar otoritas sertifikasi dan pelanggan yang beroperasi pada model *cross*-bersertifikat.



Gambar 8. CA Model *cross-certified*

Dalam model hibrida, implementasi baik struktur hierarkis dan lintas-sertifikasi (*cross-certified*) digabungkan secara bersamaan. Misalnya, dua komunitas dengan model hierarkis yang saling *trust*, sangat memungkinkan jika ingin melakukan *cross*-sertifikasi antara satu sama lain, sehingga anggota masing-masing komunitas dapat mengandalkan sertifikat yang dikeluarkan oleh yang lain untuk melakukan *e-commerce*. Dalam model hierarki (*hierarchical model*), PSrE induk dibagi menjadi Sub-sub PSrE yang lebih kecil. Pembagian PSrE menjadi sub-PSrE didasarkan pada model bisnis yang ditangani. Sehingga tiap sub-PSrE akan menangani pelanggan/pengguna yang berbeda bisnisnya. Karena pembagian CA menjadi sub- CA yang spesifik pada model bisnis tertentu maka model ini cocok digunakan untuk negara yang memiliki banyak variasi tipe model bisnis yang spesifik dan masing-masing bisnis telah berkembang. Sementara itu dalam PSrE model *cross certification model*, peran PSrE induk (*root CA*) dilakukan oleh masing-masing PSrE. Sehingga posisi *root* CA dapat dihilangkan. Proses di PSrE induk dapat digantikan dengan saling memvalidasi sertifikat dari PSrE yang lain (*shared trust*). Struktur ini cocok digunakan untuk negara yang mempunyai banyak variasi tipe bisnis namun tidak spesifik dengan *load* yang tinggi. Berdasarkan ketiga model yang telah dijelaskan tersebut dan hasil dalam penelitian ini, maka model PSrE yang tepat untuk diimplementasikan di Indonesia adalah model "hirarkis" atau disebut juga dengan model PSrE berinduk. Hal ini disesuaikan dengan regulasi yang telah berlaku sebelumnya, yaitu UU ITE dan PP PSTE. Selain itu, Indonesia juga memiliki beberapa variasi tipe model bisnis yang spesifik dan masing-masing bisnis telah berkembang. Usulan model bisnis PSrE di Indonesia adalah tampak seperti Gambar 9.



Gambar 9. Usulan model PSrE di Indonesia

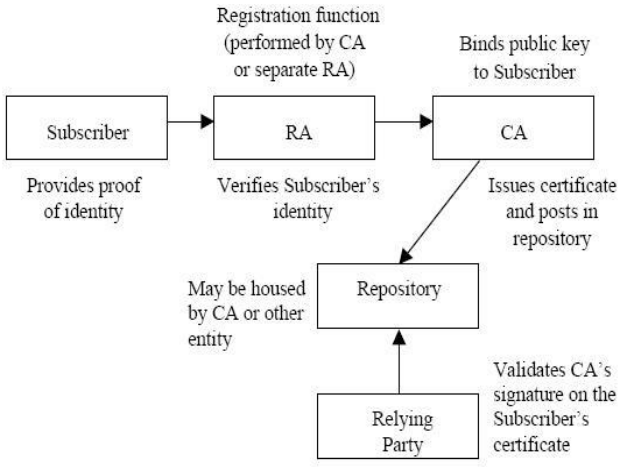
Model PSrE di Indonesia membedakan 2 (dua) model bisnis PSrE, yaitu Pemerintah dan Swasta (*Private*) termasuk individu masyarakat, namun demikian, Pemerintah tetap dapat memegang kendali PSrE. Posisi PSrE induk di Indonesia adalah Pemeritah melalui Kementerian Kominfo sebagai regulator di sektor TIK. Baik pada PSrE pemerintah maupun PSrE swasta memiliki spesifikasi bisnis yang berbeda-beda pula. Sebagai contoh, pada PSrE Pemerintah, didalamnya juga dapat dibedakan ke dalam beberapa jenis PSrE, seperti PSrE Pemerintahan Daerah, PSrE kependudukan, PSrE perdagangan, PSrE keuangan dan perpajakan, dan lain sebagainya sesuai dengan tugas dan fungsi masing-masing instansi. Pada tiap instansi memiliki PSrE yang mempunyai spesifikasi khusus sebagaimana tugas dan fungsi instansi tersebut dan instansi tersebut menjadi sub-PSrE di bawah PSrE induk. Dalam contoh lain, PSrE swasta terdiri dari PSrE yang berasal dari organisasi bisnis yang berbeda, seperti PSrE perbankan, PSrE industri, dan lain sebagainya. Masing-masing jenis PSrE memiliki spesifikasi yang berbeda sesuai dengan model bisnis organisasi PSrE.

Otoritas Pendaftaran

Sebuah Otoritas Pendaftaran atau *Registration Authority* (RA) adalah sebuah entitas yang bertanggung jawab untuk identifikasi dan otentikasi pelanggan, tetapi tidak menandatangani atau masalah sertifikat. Dalam beberapa kasus, PSrE melakukan fungsi pendaftaran pelanggan internal. Dalam kasus lain, PSrE mungkin mendelegasikan fungsi RA kepada otoritas pendaftaran eksternal yang biasanya disebut Otoritas Pendaftaran sebagai *repository* atau *Local Registration Authorities* (LRAs). Hal ini dapat mungkin atau tidak mungkin menjadi bagian dari badan *repository* yang sama dengan PSrE. Dalam kasus lain lagi, seorang pelanggan dari PSrE (misalnya, perusahaan) dapat mengatur dengan PSrE bahwa untuk menjalankan fungsi RA sendiri atau menggunakan agennya. Proses pendaftaran awal untuk pelanggan adalah sebagai berikdapat berbeda. Hal ini dikarenakan langkah-langkah yang dapat bervariasi dari PSrE ke PSrE dan juga akan tergantung pada Kebijakan Sertifikat (*Certificate Policy*) di mana sertifikat tersebut akan dikeluarkan. Pelanggan pertama menghasilkan sendiri *repository* sepasang kunci publik/*private* (pribadi). Dalam beberapa implementasi, PSrE mungkin menghasilkan pasangan kunci pelanggan dan mengirimkannya dengan aman ke pelanggan, tapi ini biasanya dilakukan hanya untuk enkripsi pasangan kunci,

bukan tanda tangan pasangan kunci. Kemudian pelanggan menghasilkan bukti identitas sesuai dengan yang berlaku sertifikat persyaratan kebijakan dan menunjukkan bahwa ia memegang kunci pribadi yang sesuai dengan kunci repository tanpa mengungkapkan kunci pribadi. Hal ini biasanya dilakukan dengan menandatangani data secara digital menggunakan kunci pribadi, dengan tanda tangan digital milik pelanggan kemudian diverifikasi oleh PSrE. Setelah hubungan antara orang dan sebuah kunci repository diverifikasi, PSrE mengeluarkan sertifikat. PSrE secara digital menandatangani setiap sertifikat yang mengeluarkan dengan kunci pribadi untuk menyediakan sarana untuk menetapkan keaslian dan integritas sertifikat.

Selanjutnya PSrE memberitahukan pelanggan dari penerbitan sertifikat dan memberikan pelanggan kesempatan untuk meninjau isi sertifikat sebelum dipublikasikan. Dengan asumsi pelanggan setujui keakuratan sertifikat, pelanggan akan menerbitkan sertifikat dan/atau memiliki PSrE yang menerbitkannya dan membuatnya tersedia untuk pengguna lain. Repositori adalah database sertifikat elektronik yang tersedia secara online. Repositori dapat dipertahankan oleh PSrE atau pihak ketiga yang dikontrak untuk tujuan itu, atau oleh pelanggan, atau oleh pihak lain. Pelanggan dapat memperoleh sertifikat dari pelanggan lain dan informasi status sertifikat dari *repository*. Sebagai contoh, jika sertifikat pelanggan yang dicabut, *repository* akan menunjukkan bahwa sertifikat pelanggan telah dicabut dan tidak boleh diandalkan. Kemampuan untuk memperbarui *repository* biasanya disimpan oleh PSrE. Pelanggan dan pihak lain akan mengakses secara *read-only access* ke *repository*. Karena sertifikat yang tersimpan dalam *repository* digital ditandatangani oleh CA, maka mereka tidak dapat melakukan tindakan kejahatan dengan cara mengubah tanpa deteksi, bahkan jika ada orang yang hack ke dalam *repository*. Gambar berikut menggambarkan hubungan antara pelanggan dan fungsi RA dan CA.



Gambar 10. Relasi antara CA dengan RA

Penyelenggara Sertifikat Elektronik untuk Meningkatkan Keamanan Transaksi Elektronik

Penyelenggara Sertifikasi Elektronis (PSrE), menurut UU ITE, adalah subjek hukum yang berfungsi sebagai pihak ketiga yang layak dipercaya untuk menyelenggarakan tanda tangan elektronik untuk memastikan identitas dan status subjek hukum pemilik tanda tangan tersebut selama keberlakuan tanda tangan elektronik. Tujuan utama yang diperankan PSrE yaitu menerbitkan sertifikat elektronik atas tanda tangan elektronik. Dengan demikian, identitas dan status subjek hukum pemilik tanda tangan dipastikan ketika diterbitkannya sertifikat elektronik. Secara umum bentuk organisasi PSrE harus memiliki elemen-elemen, antara lain:

1. Berbentuk badan hukum Indonesia dan beroperasi di Indonesia, serta memiliki izin operasi PSrE dari Menteri Komunikasi dan Informatika berdasarkan pertimbangan dan usulan dari TPPSE;
2. Memiliki peran *cross border*, berarti hukum nasional mengatur keberadaan PSrE yang ada sebagai subjek hukum di Indonesia dan hukum nasional mengakui eksistensi keberadaan PSrE internasional yang eksis sesuai hukum tempat domisili PSrE tersebut;
3. Sebagai subjek hukum, PSrE sebagai pihak ketiga terpercaya yang memberikan kepastian/ pengesahan identitas pelanggan dan pengesahan pasangan kunci publik dan kunci pribadi;
4. Layanan PSrE terbuka dan dapat diakses oleh seluruh aplikan (pemohon) yang membutuhkan PSrE;
5. Independen dan tidak memihak;
6. Memiliki fungsi manajemen dalam sistem operasinya sesuai kriteria sertifikasi SNI yang dipersyaratkan dan memenuhi persyaratan/ kesesuaian standar manajemen (ISO/IEC 27001: 2005, *Information Technology - Security Technique Information Security Management System Requirement*), yaitu:
   a. *Policy Authority* yang bertanggung jawab menetapkan kebijakan tertulis *Certificate Policy* (CP) dan *Certification Practice Statement* (CPS), serta melakukan *management review* untuk mengevaluasi dan melakukan perbaikan terhadap pelaksanaan CPS;
   b. *Registration Authority* yang bertanggung jawab memverifikasi data identitas pemegang sertifikat dan memvalidasi kebenarannya;
   c. *Certificate Issuer* bertanggung jawab menerbitkan kunci kriptografi atau memvalidasi kunci kriptografi apabila kunci tersebut diterbitkan oleh pihak lain, serta melaksanakan pembuatan, pembubuhan tanda tangan PSrE dan publikasi serta pemeliharaan Sertifikat Digital (SD);
   d. *Repository Service* yang bertanggung jawab mempublikasikan CP, CPS, SD dan *revocation status bulletin,* baik melalui *repository* yang dimiliki oleh PSrE maupun oleh pihak lain;
   e. *Revocation Management* yang bertanggung jawab mengawasi penyalahgunaan SD, menyelidiki kebenaran pengaduan yang diterima, menentukan langkah-langkah yang harus dilakukan sehubungan dengan pembekuan atau pembatalan SD, serta menyusun *revocation status bulletin.*

7. Status personal badan hukum PSrE tunduk sepenuhnya kepada hukum Indonesia;
8. Personal CA harus orang yang kompeten, memenuhi kualifikasi dan terlatih, bersertifikat/lisensi untuk kriteria teknis tertentu, menguasai teknis SNI terkait, komunikatif lisan dan tertulis, bebas dari konflik kepentingan.

PSrE merupakan institusi yang menyediakan sertifikat digital (Penyelengara Sertfikasi Elektronik/ *Certification Authority*) untuk memfasilitasi sistem keamanan transaksi online (Internet) dengan *Digital Signature* dan *Public Key Encryption*. Selain tujuan utama tersebut, PSrE dapat menyediakan pelayanan-pelayanan lainnya yang bertujuan untuk menunjang penyelenggaraan tanda tangan elektronik agar mampu mengikuti evolusi teknologi, misalnya dengan menyediakan jasa *time stamping*, jasa pembuatan kunci publik, pengarsipan elektronis dan lain-lainnya. Sebagai pihak ketiga terpercaya, PSrE dapat memberikan jaminan keamanan meliputi:

1. Memiliki kebijakan keamanan (*Security Policy*) yang memadai;
2. Memiliki prosedur dan mekanisme yang dapat mendeteksi jika terjadi masalah keamanan dan mengatasinya dengan menyempurnakan prosedur dan mekanisme tersebut;
3. Memiliki peraturan-peraturan dan tanggung jawab yang dapat menjadi acuan bahwa operasional PSrE telah dijalankan dengan benar;
4. Memiliki prosedur dan media untuk berkomunikasi dengan para pengguna;
5. Menjalankan peraturan dan prosedur secara konstan sesuai dengan level kepercayaan yang telah ditetapkan;
6. Kualitas dari prosedur operasional dan layanan yang diberikan telah di sertifikasi oleh Lembaga Sertifikasi – PSrE (LS-PSrE);
7. Menuangkan dengan jelas hak dan tanggung jawab PSrE dan penggunaannya dalam kontrak berlangganan;
8. Memiliki pemahaman yang jelas antara PSrE dengan penggunanya atas tanggung jawab masing-masing pihak;
9. Sesuai dengan peraturan perundangan yang berlaku;
10. Telah mengidentifikasikan dengan jelas kemung-kinan adanya ancaman keamanan dan cara mengatasinya;
11. Melakukan penilaian risiko (*Risk Assesment*) secara berkala;
12. Memiliki organisasi dan sumber daya manusia (SDM) yang sesuai dengan layanan PSrE dan level kepercayaan yang telah ditetapkan;
13. Level kepercayaan dari PSrE dapat diturunkan kepada sebuah Sub PSrE namun tetap dapat dilakukan proses pengecekan dan klarifikasi;
14. Kondisi bahwa PSrE selalu dimonitor dan diawasi oleh Tim Pengawas Penyelenggara Sertifikat Elektronik-TPPSE agar tetap sesuai dengan peraturan yang telah ditetapkan.

Keberadaan PSrE harus diawasi secara intensif karena produk-produk PSrE memiliki nilai *evidence.* Pengawasan PSrE diperlukan untuk mendapat kepastian hukum dan melindungi kepentingan masyarakat dari risiko kerugian akibat perbuatan PSrE yang tidak bertanggung jawab. Dalam implementasinya, pengawasan PSrE dilakukan oleh sebuah Tim ad-hoc yang dibentuk oleh Kementerian Komunikasi dan Informatika. Tim Pengawas Penyelenggara Sertifikat Elektronik (TPPSE), secara umum bertugas mengawasi, mengendalikan, berfungsi sebagai PSrE induk (*Root* CA) dan memberikan pertimbangan serta mengusulkan penerbitan atau pencabutan izin operasi PSrE kepada Menteri Komunikasi dan Informatika.

PSrE induk adalah sebuah lembaga/unit yang berfungsi menandatangani kunci publik (*digital certificate*) CA, mengatur dan menjalankan proses *cross* PSrE. Berdasarkan PP PSTE Pasal 61, dijelaskan bahwa Penyelenggara sertifikasi elektronik yang beroperasi di Indonesia wajib memperoleh pengakuan dari Menteri. Pengakuan sebagaimana dimaksud, terdiri atas tingkatan, yaitu; (a). terdaftar, (b). tersertifikasi; atau (c). berinduk. Adapun yang dimaksud dengan "penyelenggara sertifikasi elektronik yang memperoleh pengakuan status berinduk" adalah penyelenggara sertifikasi elektronik yang menerbitkan Sertifikat Elektronik dengan menggunakan Tanda Tangan Elektronik *Root Certification Authority* yang dikeluarkan oleh Menteri. Terdapat 2 (dua) jenis pengawasan yang harus dilakukan terhadap PSrE yaitu pengawasan teknis dan pengawasan operasional. Agar pengawasan PSrE efektif, pengawasan teknis dan pengawasan operasional harus merupakan suatu kesatuan pengawasan yang menyeluruh.

A. Pengawasan Teknis

Pengawasan Teknis bersifat preventif, yaitu pelaksanaan penilaian kesesuaian oleh LS- PSrE untuk membuktikan bahwa suatu PSrE telah memenuhi persyaratan yang ditetapkan. Penilaian kesesuaian yang dilakukan LS- PSrE merupakan suatu kombinasi fungsi pengujian dan audit serta evaluasi dan pengambilan keputusan yang diterapkan bagi kategori PSrE. Produk penilaian kesesuaian ini adalah *Certificate of Conformity* (sertifikat kesesuaian) dan *Mark of Conformity* (tanda kesesuaian). Penilaian kesesuaian mempunyai fungsi seleksi, determinasi, peninjauan dan pengesahan serta pengawasan.

1. Fungsi seleksi dalam penilaian kesesuaian akan digunakan untuk:
   a. Membuktikan kemampuan PSrE memenuhi persyaratan, antara lain PSrE sesuai dengan kriteria penilaian CP, CPS, *PKI-Key Management Life Cycle*, *SD Management Life Cycle*, manajemen operasi PSrE, dan tanggung jawab organisasi;
   b. Penentuan metode audit serta pengujian fasilitas dan proses pembuatan SD;
   c. Pengumpulan informasi yang relevan untuk pelaksanaan fungsi *determination*.
2. Fungsi determinasi dalam penentuan kesesuaian dapat berupa kombinasi sejumlah kegiatan yaitu:

a. Audit serta pengujian fasilitas dan proses pembuatan SD serta teknologi *appraisal* teknologi yang dipergunakan;
b. Pengujian sampel SD;
c. Audit teknik keamanan teknologi informasi (TI) dan sistem manajemen;
d. Audit sistem manajemen mutu yang diterapkan pada semua lingkup jasa PSrE.

3. Fungsi peninjauan dan pengesahan, yaitu:
   a. Evaluasi semua informasi dan data yang dihasilkan oleh fungsi determinasi;
   b. Pengambilan keputusan;
   c Penerbitan SD atau tanda kesesuaian;
4. Fungsi pengawasan diperlukan untuk memastikan bahwa PSrE mampu memelihara dan mengendalikan produk agar tetap sesuai dengan persyaratan serta dapat berupa kombinasi sejumlah kegiatan, tergantung pada skema yang diterapkan, seperti:
   a. Pengujian atau inspeksi sampel SD;
   b. Inspeksi sampel SD yang telah beredar;
   c. Audit dan pengujian ulang fasilitas dan proses pembuatan SD;
   d. Audit Keamanan TI dan Sistem Manajemen Mutu yang diterapkan.

Dalam hal ini fungsi pengawasan tidak perlu dilakukan secara komprehensif sebagaimana saat penilaian awal.

B. Pengawasan Operasional

Pengawasan Operasional (bersifat korektif), yaitu suatu kegiatan pemeriksaan mengenai persyaratan operasional PSrE. Pengawasan operasional sangat diperlukan untuk mengkoreksi dan menindak PSrE yang tidak memenuhi persyaratan.

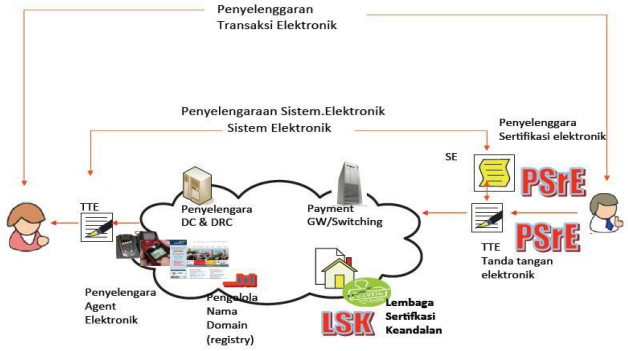
1. Pengawasan Operasional dilakukan oleh TPPSE.
2. Tujuan pengawasan TPPSE untuk keperluan:
   a. Mencegah operasi PSrE yang belum mendapatkan izin operasi dari TPPSE;
   b. Mengawasi penerbitan dan penggunaan SD dari PSrE yang dinilai oleh LS-PSrE tidak dapat memelihara kesesuaiannya terhadap ketentuan SNI yang dipersyaratkan atau ternyata digunakan untuk keperluan yang tidak sesuai peruntukannya. TPPSE berwenang meneliti seluruh PSrE yang terindikasi menyimpang sesuai dengan penilaian LS-PSrE, untuk kemudian memutuskan sanksi dan menghentikan aktivitas PSrE.
   c. Pengawasan Operasional yang dilakukan TPPSE sangat penting untuk menegakkan regulasi pasar dan melindungi pengguna PSrE.

Analisa Implementasi Ekosistem Sertifikat Elektronik

Metode SSM berfokus untuk menciptakan sistem aktivitas dan hubungan manusia dalam sebuah organisasi atau kelompok dalam rangka mencapai tujuan bersama. Berpikir dengan sistem merupakan suatu bidang transdisiplin yang muncul sebagai respon terhadap keterbatasan dari pendekatan teknikal dalam proses reduksi untuk memecahkan masalah. Pemikiran sistem dalam konteks pemecahan masalah yang kompleks adalah pemikiran mengenai keterkaitan, konteks/ lingkungan dengan memberikan penekanan lebih pada hubungan interaksi dari unsur-unsur/bagian-bagian secara utuh daripada unsur-unsur/bagian-bagian secara terpisah dan lebih fokus pada proses sebagai pendekatan dalam pemecahan permasalahan yang kompleks.

Dalam langkah pengembangan model, dapat diawali dengan menggunakan pendekatan *rich picture* untuk menstrukturkan situasi permasalahan atau suatu kondisi berkaitan dengan standarisasi sertifikat elektronik dan sertifikat keandalan dalam penyelenggaraan system transaksi elektronik, baik dari aspek standarisasi, peran kelembagaan, hubungan lintas pemangku kepentingan, proses transformasi, cara pandang dan ekosistem.

Kompleksitas perihal tujuan, fungsi dan peran para pemangku kepentingan (*stakeholder*) dalam implementasi standarisasi sertifikat elektronik dan keandalan dapat dirancang *rich picture* seperti ditunjukan pada Gambar 11. berikut ini.



Gambar 11. *Rich Picture* Sistem Transaksi Elektronik

Keterikatan, keterlibatan lembaga atau institusi serta peran dan fungsinya terkait implementasi kebijakan di dalam standarisasi sistem transasksi elektronik mempengaruhi terciptanya ekosistem bisnis transaksi elektronik yang harmonis dan iklim bisnis yang kondusif. Oleh karenanya, dibutuhkan pengkayaan di dalam menempatkan lembaga-lembaga yang berpengaruh secara langsung dan tidak langsung dalam sebuah *rich picture* sebelum dibangun sebuah model sistem hubungan antara lembaga yang mempengaruhi sistem transasksi elektronik. Dengan proses CATWOE digunakan untuk menganalisis kebijakan implementasi standarisasi system elektronik dan keandalan seperti yang dijelaskan dalam UU ITE dan PP PSTE. Hal ini agar diperoleh gambaran yang lebih spesifik,

terstruktur, dan komprehensif implementasinya dalam perspektif sistem transaksi elektronik. Mengacu pada kajian yang telah dilakukan sebelumnya (Setiawan, 2014), hasil analisis teridentifikasi pihak yang berkepentingan, kebutuhan para pihak, aktivitas untuk pencapaian tujuan serta kendala yang dapat diantisipasi dalam model, seperti ditunjukkan pada Tabel berikut ini.

Tabel 1.
Hasil Analisis Proses CATWOE pada Sistem Transaksi Elektronik

Cutomer	
1.	Industi keuangan dan Perbankan
2.	Perusahaan penyedia jasa telekomunikasi/ISP/ Operator
3.	Pelaku bisnis yang menggunakan transaksi elektronik
Actor - Owner	
1.	Pelaku bisnis yang menggunakan transaksi elektronik (PSE)
2.	Industi keuangan dan Perbankan
3.	Perusahaan penyedia jasa telekomunikasi/ISP/ Operator
4.	Pemerintah, selaku Regulator
Transformation	
1.	pemerintah melaksanakan UU yang terkait, dan komitmen pada perlindungan keamanan informasi dalam transaksi elektronik serta melakukan audit kepatuhan
2.	menyediakan infrastruktur dan kelembagaan: Lembaga Penyelenggara Sertifikat Elektronik (PSrE) atau *certificate of authority* (CA)
3.	membangun iklim kesadaran pada masyarakat mengenai pentingnya keamanan informasi dalam transaksi elektronik
4.	membangun pusat data dan DRP *(Disaster Recovery Plan)*
5.	melibatkan komunitas dan profesional
6.	mengembangkan inkubator industri CA di Indonesia yang menggunakan standarisasi milik bangsa
World View	
1.	Penerapan standar dan kebijakan yang tepat
2.	Kesejahteraan, keamanan dan keberlanjutan bisnis PSE
3.	Iklim usaha kondusif
4.	Terciptanya Kelembagaan PSrE sebagai penyelenggara CA
Environment Constraint	
1.	Kurangnya komunitas dan asosiasi di bidang TI
2.	Masih tingginya *e-literacy* di masyarakat
3.	Rendahnya kesadaran masyarakat akan transaksi elektronik yang aman
4.	Kebijakan/regulasi dan standarisasi yang sudah ada tidak didukung dengan tumbuhnya ekosistem bisnsis PSrE yang kondusif

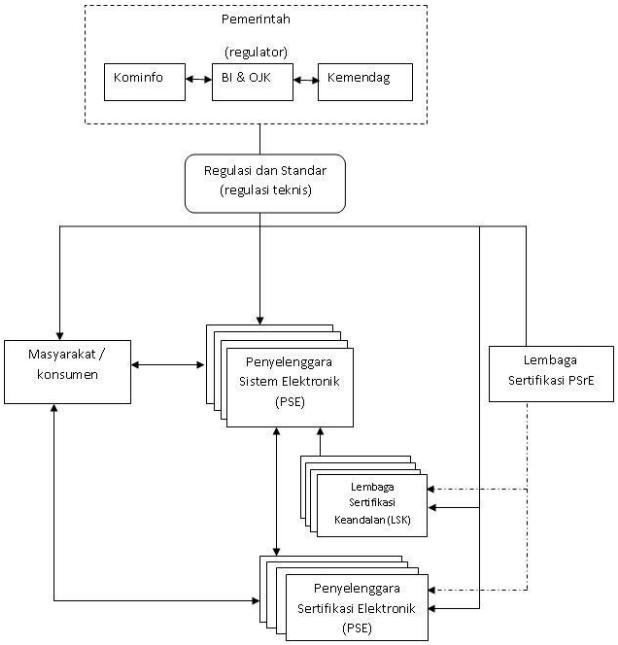
Berdasarkan *rich picture* dan analisis dengan proses CATWOE, dihasilkan rumusan *root definition* (RD) sebagai berikut: "*Sistem transaksi elektronik terpadu melibatkan peran pihak yang terkait, dalam merencanakan implementasi standarisasi transaksi elektronik yang efektif pada masing-masing pihak, dan melakukan pengelolaan aktivitas secara tepat dan efesien, serta melakukan pengendalian yang baik dan terintegrasi dengan membangun komunikasi dan melaksanakan kebijakan UU dan regulasi terkait serta standarisasi untuk membangun sistem transaksi elektronis yang terpercaya agar tercipta iklim bisnis yang harmonis dan kondusif".* Untuk menemukan solusi dirancang model aktivitas dalam *purposefull activity model* (PAM) yang strukturnya telah didiskusikan dengan pakar dan para pemangku kepentingan. Aktivitas yang dibangun dalam model untuk resolusi konflik dengan integrasi kelembagaan dalam sistem transasksi eektronik serta optimalisasi fungsi pengendaliannya. Pemahaman terhadap regulasi dan standarisasi terkait lainnya dalam implementasi kebijakan standarisasi sertifikasi sistem elektronik dapat meningkatkan keamanan dan harmonisasi iklim bisnis dengan transaksi elektronik.

Integrasi Ekosistem Sertifikasi Elektronik

Model manajemen terintegrasi melibatkan beberapa sektor pemerintah yang terkait dan mengintegrasikan setiap pihak pemangku kepentingan (*stakeholder*), yang terdiri dari unsur pemerintah, Penyelenggara Sistem Elektronik, komunitas yang menaungi Penyelenggara Sistem Elektronik, Lembaga Audit dan Akreditasi serta Lembaga Sertifikasi Penyelenggara Sistem Elektronik, serta masyarakat. Pemangku kepentingan dari unsur pemerintah, setidaknya terdapat 3 (tiga) instansi yang terlibat, yaitu: Kementerian Kominfo, BI dan OJK serta Kementerian Perdagangan. Unsur pemerintah mengeluarkan berbagai regulasi yang terkait dengan penyelenggaraan ekosistem perdagangan sistem elektronik dengan memanfaatakan sertifikat elektronik. Regulasi yang dikeluarkan bersifat mengikat kepada setiap entitas yang terlibat dalam ekosistem setiap entitas yang terlibat dalam ekosistem perdagangan elektronik. Mengingat adanya keterkaikan dalam hal regulasi yang dikeluarkan, maka harus ada koordinasi antar masing-masing instansi terkait.

Regulasi yang dikeluarkan dapat berupa Undang-Undang, Peraturan Pemerintah dan juga Regulasi Teknis (standard). Standard teknis Penyelenggaraan Sistem Transaksi Elektronik, Sertifikat Elektronik dan Sertifikat Keandalan dapat merujuk pada standardisasi yang sudah ada dan berlaku secara umum. Namun demikian, harus dilakukan penyesuaian terhadap kondisi yang ada. Lembaga audit dan akreditasi berperan dalam mengaudit untuk memberikan penilaian (*assess*) terhadap Penyelenggara Sertifikasi Elektronik. Tujuan dilakukannya audit dan penilaian adalah untuk menilai kepatuhan setiap entitas yang terlibat dalam ekosistem perdagangan elektronik terhadap regulasi dan standar yang berlaku. Lembaga Audit dan Akreditasi melakukan kegiatan audit berdasarkan regulasi dan standar yang dikeluarkan oleh Pemerintah. Setelah dilakukan proses audit dan penilaian, maka dikeluarkan akreditasi terhadap institusi Penyelenggara Sertifikasi Elektronik. Akreditasi tersebut dapat membuktikan bahwa Penyelenggara Sertifikasi

Elektronik (PSrE) layak untuk memberikan layanan kepada Penyelenggara Sistem Elektronik. Penyelenggara Sistem Transaksi Elektronik (PSTE) memberikan layanan secara langsung kepada masyarakat dan konsumen yang ingin melakukan transaksi secara elektronik atau *on-line*. Dalam penelitian sebelumnya (Setiawan, 2014), telah diusulkan integrasi Ekosistem Sertifikat Elektronik seperti pada gambar berikut ini.



Gambar 12. Bagan Usulan Ekosistem Manajemen dan Regulasi Sertifikat Elektronik

Adanya model ekosistem sertifikat elektronik dalam transaksi elektronik dapat memperjelas tata hubungan dan kewajiban serta tanggung jawab dari masing-masing *stakeholder*. Lebih lanjut, berdasarkan hasil analisis menggunakan dalam kajian yang telah dilakukan, maka dapat diusulkan langkah-langkah yang dapat ditempuh oleh para *stakeholder* secara hierarkis tabel di bawah ini menunjukkan saran dan usulan langkah-langkah untuk stakeholder berdasarkan resume hasil analisis penelitian.

Hasil analisis penelitian menunjukkan bahwa terdapat 4 (empat) langkah usulan direktif dalam tata kelola sistem transaksi elektronik yang dikaitkan dengan isu strategis pada masing-masing tingkatan. Regulasi yang harus diacu dalam pengembangan ekosistem antara lain seperti: UU 11/2008 tentang ITE, PP PSTE, UU 36/1999 tentang Telekomunikasi dan PP 52/2000, ISO/SNI 19-7125-2005. Sementara itu pada tingkatan strategik, terkait dengan penyediaan kebijakan teknis untuk sertifikasi elektronik dan ekosistem bisnis yang kondusif. Adapun pada tingkatan taktikal mengatur hal-hal koordinasi tingkat kebijakan dan operasional pada tingkatan lebih dasar dan pada tingkatan teknis dan operasional lebih fokus mengatur pada hal-hal ketersediaan infrastruktur dan dukungan teknis operasional.

Tabel 2.
***Resume* Penelitian Untuk Usulan Direktif Bagi Pemangku Kebijakan**

No	Teknik / Hirarki	Usulan Direktif	
		Langkah	**Fokus Isu**
1	Acuan	Kebijakan terkait Sertifikat elektronik pada Sistem Transaksi elektronik mengacu pada: UU 11/2008 tentang ITE, PP PSTE, UU 36/1999 tentang Telekomunikasi dan PP 52/2000, ISO/SNI 19-7125-2005, ISO/SNI 27001 dan standard teknis lainnya yang terkait dengan sistem pengamanan dan tata kelola sistem transaksi elektronik.	
2	Strategis	1. Membuat regulasi teknis untuk sertifikasi elektronik 2. Membuat kebijakan yang mengatur keterlibatan pihak ketiga multinasional 3. Melaksanakan prosedur audit dan evaluasi melalui Lembaga Sertifikasi Keandalan 4. Proteksi pemerintah (regulator) terhadap munculnya sertifikat elektronik palsu 5. Memberlakukan standar yang mengatur layanan dasar Penyelenggara Sertifikasi Elektronik (PSrE)	Kebijakan Teknis Sertifikasi Elektronik dan ekosistem bisnis yang kondusif

No	Teknik / Hirarki	Usulan Direktif	
		Langkah	**Fokus Isu**
4	Teknis dan Operasional	1. Menjamin ketersediaan infrastruktur pendukung transaksi elektronik sesuai dengan regulasi yang berlaku, seperti UU ITE, PP PSTE dan sebagainya. 2. Tersedianya Pusat data (*data center*) berikut DRC dan *collocation* Dalam Negeri; terkait dengan kedaulatan dan keamanan data. 3. Penyediaan inkubator bisnis industri sertifikasi elektronik nasional; untuk mendukung tumbuh-kembangnya industri sertifikat elektronik dan aplikasi lainnya yang terkait dengan perdaganagn elektronik 4. Tersedianya SDM yang siap dan handal dalam operasionalisasi system transaksi elektronik 5. Sosialisasi kepada masyarakat terkait dengan kesadaran akan keamanan transaksi elektronik	Ketersediaan infrastruktur dan dukungan teknis operasional

PENUTUP

Kesimpulan

Berdasarkan hasil pembahasan dalam penelitian ini, dapat disimpulkan bahwa, Untuk membangun sebuah ekosistem transaksi elektronik, pemangku kebijakan perlu menekankan pada aspek ketersediaan (*availability*) baik infrastruktur maupun sistem. Setiap entitas yang terkait dalam ekosistem perlu diaudit secara berkala oleh Lembaga Sertifikasi yang ditunjuk oleh pemangku kebijakan. Dalam melakukan audit, perlu mengacu pada regulasi dan kebijakan yang terkait.Sedangkan model bisnis dalam ekosistem Transaksi Elektronik bergantung pada kepercayaan kepercayaan (*trust*). Oleh karena itu, setiap pelaku industri yang melakukan transaksi harus membangun dan mendapatkan kepercayaan dari masyarakat, pelaku dan konsumen dalam transaksi elektronik.

Saran

Berdasarkan hasil penelitian dan kesimpulan penelitian yang telah diuraikan, disampaikan beberapa saran sebagai berikut:

Pemerintah terkait selaku pemangku kepentingan dan kebijakan harus fokus pada ketersediaan infrastruktur, yaitu dengan membentuk Lembaga *certificate of authority* (CA) atau PSrE Nasional, infrastruktur teknis pendukung dan mengimplementasikan standar teknis dan standard operasional yang dapat diacu oleh para pelaku tansaksi elektronik. Perlu adanya komitmen dan penegakan hukum yang dapat menjamin keamanan masyarakat dalam bertransaksi elektronik. Memfasilitasi dan mendorong tumbuh kembang industri pembuat PSrE dan lain sebagainya serta terbentuknya inkubator untuk industri tersebut. Pemerintah perlu memperkuat koordinasi antar pemangku kepentingan dan membuat kebijakan yang dapat memayungi koordinasi lintas sektoral untuk menjamin ekosistem yang kondusif. Perlu dibangun iklim kesadaran pada masyarakat mengenai pentingnya keamanan informasi dalam transaksi elektronik melalui sosialisasi, edukasi dan bimbingan teknis mengenai keamanan informasi dan transaksi elektronik.

Ucapan Terima Kasih

Bersama ini saya mengucapkan terima kasih kepada Badan Litbang SDM Kominfo, dan reviewer maupun Mitra Bestari yang telah berperan aktif memberikan dorongan dan semua pihak yang men-*support* terwujudnya karya tulis saya ini.

DAFTAR PUSTAKA

Calder, Alan and Steve Watkins. (2003). *IT Governance, Data Security & BS 7799/ISO 17799 A Manager's Guide to Effective Information Security.* London: Kogan Page.

Checkland, P., & Poulter, J. (2006). *Learning for Action.* England (GB): John Wiley & Sons Ltd.

Checkland, P.B. (1981). *System Thinking, System Practice.* John Wiley & Sons, Chichester.

Checkland, P., Scholes, J. (1990). *Soft Systems Methodology in Action,* Chichester, UK: Wiley.

Choudhury, Suranjan., Bhatnagar, Kartik., and Haque, Wasim. (2002). *Public Key Infrastructure: Implementation and Design*. New York (US). M&T Books. ISBN: 0−7645−4879−4

CSPP. (1998). The Computer Systems Policy Project. www. cspp.org

Cooper, D. R., & Schindler, P. S. (2008). B*usiness Resarch Methods.* New York: McGraw-Hill Companies,. Inc.

Dettmer, H. W. (2007). *The Logical Thinking Process: a Systems Approach to Complex Problem Solving.* Milwaukee, Wisconsin (US): ASQ Quality Press.

Eriyatno. (2013). *Ilmu Sistem: Meningkatkan Integrasi dan Koordinasi Manajemen*. Jilid Dua, Edisi pertama. Larasati L, editor. Surabaya (ID): Penerbit Guna Widya.

Eriyatno, & Sofyar, F. (2007). *Riset Kebijakan:Metode Penelitian untuk Pascasarjana.* Bogor (ID): IPB Press.

Fleischmann, Amy. (1995). Personal Data Security: Divergent Standards in the European Union and the United States. Fordham International Law Journal. Volume 19, Issue 1. Article 7.

Flood Jackson. (1991). *Creative Problem Solving:Total Systems Interventions*. Wiley & Sons, Chichester,UK.

GIAC Security Essentials Certification (GSEC). (2004). *Information security management system (BS7799-2:2002) implementation overview*. GSEC Practical Requirements (v.1.4). SANS Institute.

Jackson, M. C. (2003). *System Thinking: Creative Holism for Managers".* John Wiley & Sons, New York.

JTC 1 TAG. (2002). Frequently Asked Questions: International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management. US. http://www.jtc1tag.org/

Mason, M. (1981). *Challenging Strategic Planning Assumptions*. Chichester (GB): John Wiley & Son.

Susilo, Willy., Eriyatno, Affandi, M. Joko., Goenawan, Agus. (2011). *Rancang Bangun Model Audit Manajemen Sumber Daya Manusia, Menggunakan Pendekatan Sistem*. Jurnal Manajemen IKM, vol. 6. No. 2, pp. 133-142.

Ramakrishnan, Prasanna, CISSP. (2004). "*Information Security Management Systems*." The CISSP and SSCP Open Study Guides Website. CISSP and SSCP.

Riyanto, Agus., Eriyatno., Pasaribu, Bomer., Maulana, Agus. (2014). *Perancangan Model Integrasi Manajemen Kebijakan Outsourcing dalam Perspektif Hubungan Industrial*. Jurnal Manajemen Teknologi. Vol.13, No.1, pp. 79-93. Unit Research and Knowledge, School of Business and Management - Institut Teknologi Bandung (SBM-ITB).

Setiawan, Ahmad Budi., *Studi Standardisasi Sertifikat Elektronik dan Keandalan dalam Penyelenggaraan Sistem Transaksi Elektronik*. (2014). Buletin Pos dan Telekomunikasi Vol. 12 No. 2, pp. 119-134.

Sumber Lain

Departemen Komunikasi dan Informatika. (2006). Naskah Akademik Rancanan Undang-Undang Informasi dan Transaksi Elektronik. Jakarta: Indonesia.

International Organization for Standardization/ International Electrotechnical Commission. (2000). International Standard ISO/IEC 17799: Information technology - Code of practice for information security management. Geneva: ISO.

International Organization for Standardization/ International Electrotechnical Commission. (1996) International Standard ISO/IEC TR 13335-1:1996 Guidelines for the management of IT security - Part 1: Concepts and models for IT Security. Geneva: ISO.