Studi Standardisasi Sertifikat Elektronik dan Keandalan dalam Penyelenggaraan Sistem Transaksi Elektronik

The Study of Electronics Certificate and Certificate of Reliability Standarization in The Implementation of Electronic Transaction 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: 7 Mei 2014; Direvisi: 10 Juni 2014; Disetujui: 20 Juni 2014

***Abstract*— Business and electronic transactions have become a trend today because of the ease of the transaction. The issue of trust (confidence) in electronic transactions nationally, regionally and globally has increased along with the problems in terms of information security in electronic transactions. The Indonesian government has provided a legal guarantee to the public in electronic transactions. This was stated in Law No. 11 of 2008 on Information and Electronic Transactions (ITE Law) as well as the issuance of government regulation No. 82 Year 2012 on the Implementation of Electronic Transaction System (PP PSTE). In these regulations mandated to any Electronic Transaction System Operator must have Electronic Certificate and Certificate of Reliability. Based on this, the necessary technical regulations in the implementation of these regulations. In general, there have Standard issued by various international and national organizations. Thus, implementation of the strategy needed standardization and reliability of electronic certificates to encourage the growth of Human Operator System Electronic security be a trusted and reliable as well as facilitate the Government in regulating the standards. This study aims to provide advice to the government in the form of an electronic certificate standardization strategy implementation and reliability certificates. The study was conducted by using Soft System with SAST technique. The results of this study provide advice to the Government related to the availability of infrastructure and institutional electronic certificates and certificate ecosystem reliability in electronic transaction system and focus on the enforcement of existing regulations.**

***Keywords*— Electronic Certificate, Information Security, Soft System**

***Abstrak*— Bisnis dan transaksi elektronik telah menjadi trend saat ini oleh karena kemudahan dalam transaksi. Isu trust (kepercayaan) pada transaksi elektronik dalam lingkup nasional, regional dan global telah meningkat seiring dengan adanya permasalahan dalam hal keamanan informasi dalam transaksi elektronik. Pemerintah Indonesia telah memberikan jaminan hukum kepada masyarakat dalam bertransaksi elektronik. Hal ini tertuang dalam Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) dan juga dikeluarkannya peraturan Pemerintah No. 82 Tahun 2012 Tentang Penyelenggaraan Sistem Transaksi Elektronik (PP PSTE). Dalam regulasi tersebut diamanatkan kepada setiap Penyelenggara Sistem Transaksi Elektronik harus memiliki Sertifikat Elektronik dan Sertifikat Keandalan. Berdasarkan hal tersebut, diperlukan regulasi teknis dalam implementasi regulasi tersebut. Secara umum, telah ada Standard yang dikeluarkan oleh berbagai Organisasi Internasional dan Nasional. Dengan demikian, dibutuhkan strategi implementasi standardisasi sertifikat elektronik dan keandalan untuk mendorong tumbuh kembangnya Ekosistem Penyelenggara Sistem Transasksi Elektronik yang terpercaya dan handal serta memudahkan Pemerintah dalam meregulasi standard tersebut. Kajian ini bertujuan untuk memberikan saran kepada pemerintah berupa strategi implementasi standardisasi sertifikat elektronik dan sertifikat keandalan. Kajian ini dilakukan dengan menggunakan metode Soft System dengan teknik SAST. Hasil kajian ini memberikan saran kepada Pemerintah terkait ketersediaan infrastruktur dan kelembagaan sertifikat elektronik dan sertifikat keandalan dalam ekosistem sistem transaksi elektronik serta fokus terhadap penegakkan hukum yang telah ada.**

Kata kunci*— Sertifikat Elektronik, Keamanan Informasi, *Soft System

I. PENDAHULUAN

Teknologi informasi dan komunikasi telah sangat maju dan menembus pada hampir semua aspek. Dalam aspek bisnis, transaksi bisnis yang dilakukan secara manual, saat ini sudah dilakukan secara elektronis dan *on-line* menggunakan teknologi informasi dan komunikasi. Bisnis dan transaksi elektronik (*e-Business, e-Government, e-Commerce, e-procurement*) adalah suatu tren yang menjanjikan. Hal ini disebabkan oleh mudahnya pemanfaatan transaksi eketronik karena dapat dapat dilakukan kapanpun, dimanapun dan oleh siapapun secara *real time*.

Keberhasilan sebuah transaksi bisnis secara elektronik dapat dinilai dari tiga criteria, 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 (*expand 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 berjalan dalam sebuah infastruktur/sarana teknologi informasi dan komunikasi, yaitu internet. Meskipun ditunjang dengan kecanggihan sarana komunikasi modern, internet sangat rentan terhadap serangan keamanan informasi. Tanpa adanya system keamanan informasi, transaksi elektronik menjadi sangat rentan terhadap gangguan keamanan informasi yang dapat menimbulkan rasa ketidaknyamanan bagi pelaku transaksi elektronik. Ketidaknyamanan dalam transaksi elektronik menyebabkan berkembangnya isu-isu mengenai *trust* dalam transaksi elektronik baik dalam lingkup nasional, regional dan global. Terdapat empat kriteria keamanan informasi dalam transaksi elektronik, yaitu: kerahasiaan (*confidentiality*), keotentikan (*authenticity*), integritas (*integrity*) dan nir-sangkal (*non-repudiation*).

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), definis Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya (UU No.11, 2008, PP No.82, 2012). 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, penyelenggaran negra, 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) .

Lebih lanjut lagi dalam Pasal 15 UU ITE disebutkan bahwa Penyelenggara Sistem Elektronik memiliki kewajiban untuk menyelenggarakan sistem elektronik yang andal, aman dan bertanggungjawab. Meskipun demikian, ketentuan tersebut diatas tidak berlaku dalam keadaan memaksa (*force majeur*), dan/atau kelalaian pihak pengguna Sistem Elektronik yang kejadiaanya dapat dibuktikan. Dengan ketentuan tersebut, maka Penyelenggara Sistem Elektronik memiliki persyaratan yang wajib dipenuhi, antara lain:

1. Dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh
2. Melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan dan keteraksesan Informasi Elektronik
3. Beroperasi sesuai prosedur
4. Dilengkapi dengan petunjuk penggunaan yang dapat dipahami
5. Dilengkapi dengan mekanisme pembaruan prosedur/petunjuk

Untuk menyelenggarakan transaksi elektronik yang terpercaya (*trusted e-tansaction*) tersebut, regulasi mengatur bahwa Pelaku usaha yang menawarkan produk melalui Sistem Elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan (Pasal 9 UU ITE). Selain itu, regulasi juga mengatur agar pelaku usaha yang menyelenggarakan sistem elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan (Pasal 10 UU ITE). Dalam Pasal 41 PP PSTE juga dijelaskan bahwa Penyelenggaraan Transaksi Elektronik dalam lingkup publik atau privat yang menggunakan Sistem Elektronik untuk kepentingan pelayanan publik wajib menggunakan Sertifikat Keandalan dan/atau Sertifikat Elektronik.

Transaksi elektronik harus aman dan andal. Karena itu, setiap penyelenggaraan transaksi elektronik yang menggunakan sistem elektronik wajib memiliki sertifikat keandalan dan sertifikat elektronik. Demikian amanat Pasal 41 dan 42 Peraturan Pemerintah (PP) No.82 Tahun 2012 tentang Peyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Standar keamanan informasi menekankan pada aspek syarat, prosedur, kebijakan, pengelolaan serta pendidikan dan pelatihan. Standarisasi yang dimaksud disini bukanlah standar teknis (spesifikasi), pengarahan suatu teknologi atau produk, dan kumpulan tip serta bukan sebagai jaminan berfungsinya sebuah alat keamanan informasi. Pendekatan ini memungkinkan standar keamanan informasi dapat diaplikasikan dalam berbagai tipe organisasi.

Salah satu satndar yang diperlukan untuk memfasilitasi system transaksi elektronik adalah adanya standar sertifikasi keandalan (*trust mark*). Sertifikat Keandalan akan dimiliki pelaku usaha jika memenuhi beberapa persyaratan. Seperti lolos standar perangkat keras, perangkat lunak, standar tenaga ahli, keamanan data, dan pengelola data. Terkait hal ini, sertifikasi bagi pelaku usaha dapat diperoleh dari lembaga sertifikasi keandalan Indonesia dan asing.

Terkait dengan kegiatan transaksi elektronik yang lebih luas, saat ini pemerintah Indonesia belum memiliki standar yang dapat digunakan sebagai arahan yang spesifik untuk kegiatan transaksi elektronik. Dengan dikeluarkannya UU ITE dan PP PSTE sebagai kebijakan yang mengatur kegiatan transaksi elektronik, maka dapat dijadikan acuan untuk pembuatan standar keamanan informasi untuk transaksi elektronik. Oleh karena itu, studi/kajian ini ditujukan untuk menggali dan mempelajari standar yang dibutuhkan oleh PP PSTE untuk memberikan arahan dalam kegiatan transaksi elektronik yang andal dan terpercaya. Dengan demikian permasalahan yang akan dibahas dalam kajian ini adalah; ”Bagaimanakah strategi penerapan kebijakan sertifikasi keandalan untuk penyelenggaraan sistem transaksi elektronik di Indonesia untuk mendukung tumbuh-kembangnya industri dan ekosistem Sertifikat Elektronik di Indonesia?”

Dengan memperhatikan hal tersebut diharapkan kajian ini dapat memberikan manfaat, yaitu dapat dijadikan sebuah rekomendasi untuk Direktorat Standarisasi, Ditjen SDPPI dalam membuat strategi dalam menerapkan standar dibidang keamanan informasi untuk transaksi elektronik. Disamping 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 standar sertifikat elektronik dan keandalan yang digunakan dalam kegiatan transaksi elektronik agar mendukung tumbuh-kembangnya industri sertifikat elektronik di IndonesiaSelain itu juga tersedianya peta jalan implementasi standar sertifikasi elektronik dan keandalan sebagai amanat PP no 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

II. TINJAUAN PUSTAKA

A. Strategi Keamanan Informasi Nasional

Strategi keamanan informasi menentukan arah semua kegiatan keamanan informasi. Komponen Kebijakan keamanan informasi adalah dokumen rencana tingkat tinggi dari keamanan informasi seluruh organisasi. Kebijakan berisi kerangka kerja untuk membuat keputusan spesifik, seperti rencana keamanan fisik dan administratif. ini merupakan rumusan untuk mengatasi permasalah Keamanan Informasi Nasional. Dengan adanya peraturan dan strategi maka akan mempertegas serta memperjelas cara untuk mengatasi permasalahan keamanan informasi.

Kebijakan atau regulasi merupakan langkah antisipatif, pemerintah Indonesia terhadap adanya ancaman keamanan informasi. Regulasi yang telah dikeluarkan pemerintah Indonesia seputar keamanan informasi, antara lain;

1. Undang-undang Republik Indonesia No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik: Undang-undang tentang Informasi dan Transaksi Elektronik (ITE) telah mengamanatkan kewajiban penyelenggara sistem elektronik baik privat maupun publik untuk mengoperasikan sistem elektronik yang dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronis
2. Surat Keputusan Menteri Komunikasi dan Informatika Nomor: 133/KEP/M/KOMINFO/04/2010: Surat keputusan yang dikeluarkan oleh Menkominfo ini berisi pembentukan Tim Koordinasi Keamanan Informasi Indonesia yang mempunyai tugas melakukan koordinasi, menyusun kebijakan, menyusun petunjuk teknis, menyelenggarakan kampanye kesadaran (*awareness*), serta melakukan monitoring dan menyampaikan laporan pelaksanaan mengenai keamanan informasi di Indonesia.
3. Surat Edaran Menteri Komunikasi dan Informatika Nomor: 01/SE/M.KOMINFO/02/2011: Surat edaran ini berisikan tentang Penyelenggaraan Sistem Elektronik Untuk Pelayanan Publik Di Lingkungan Instansi Penyelenggara Negara.
4. Surat Edaran Menteri Komunikasi dan Informatika Nomor: 5/SE/M.KOMINFO/07/2011 tentang Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik
5. PP no 82, tahun 2012 tentang Penyelenggaraan Sistem dan Transakti Elektronik (PSTE). Peraturan ini mengatur tentang penyelenggaraan sistem elektronik, penyelenggaraan transaksi elektronik, tanda tangan elektronik, penyelenggaraan sertifikasi elektronik dan lembaga sertifikasi keandalan (*trustmark*) dan pengelolaan nama domain

B. Standarisasi Keamanan Informasi

Keberadaan regulasi tersebut dapat menjadi payung hukum pengamanan sistem informasi nasional dan menunjukkan tingkat kepedulian (*awareness*) pemerintah dalam hal keamanan informasi. Meskipun peraturan dan perundang-undangan di bidang keamanan informasi masih termasuk lemah. Kegiatan keamanan informasi tidak dapat dilakukan secara efektif tanpa mobilisasi rencana administrasi, fisik dan teknis yang menyatu.

Setiap elemen dalam memujudkan kemanan informasi harus mengacu pada standar keamanan yang telah ditetapkan. Standar keamanan informasi harus khusus dan spesifik sehingga mereka dapat diterapkan ke semua bidang keamanan informasi. Setiap negara perlu mengembangkan standar sesudah menganalisis standar keamanan administratif, fisik dan teknis yang banyak digunakan di dunia. Standar haruslah sesuai dengan lingkungan TIK yang umum.

Standar keamanan informasi bertujuan untuk merekomendasikan kegiatan keamanan informasi yang menyatu, seperti perumusan kebijakan keamanan informasi, penyusunan dan operasi organisasi keamanan informasi, manajemen sumber daya manusia, manajemen keamanan fisik, manajemen keamanan teknis, manajemen audit keamanan dan keberlanjutan bisnis (Ramakrishnan, 2004). Banyak organisasi telah merekomendasikan standar keamanan informasi. Contohnya antara lain persyaratan keamanan informasi dari *International Organization for Standardization and*

International Electrotechnical Commission (ISO / IEC) dan daftar evaluasi dari *Certified Information Systems Auditor* (CISA), dan *Certified Information Systems Security Professional* (CISSP) dari *Information Systems Audit and Control Association* (ISACA) (CSPP, 1998).

C. Konsep Soft Systems Methodology

Soft systems methodology (SSM) merupakan sebuah pendekatan untuk memecahkan situasi masalah kompleks yang tidak terstruktur berdasarkan analisis *holistic* 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 system 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 fikir 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).

Dalam 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) pendefisian 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.

D. Strategic Assumption Surfacing and Testing (SAST)

Metode SAST merupakan salah satu metode yang digunakan dalam menyusun alternatif-alternatif kebijakan berdasarkan asumsi–asumsi untuk rancang bangun model kebijakan. Terdapat empat tahapan dalam metode ini: (1) pembentukan kelompok (*group formation*), bertujuan menginventarisir opini-opini dan fakta apa saja yang muncul dalam kaitan objek kajian. Dalam kelompok diskusi tersebut melibatkan pihak pemangku kepentingan, pakar dan pihak yang terlibat langsung dalam permasalahan tersebut; (2) Pengedepanan (memunculkan) asumsi (*assumption surfacing*), menggali berbagai asumsi yang paling signifikan melalui diskusi kelompok untuk mendukung kebijakan dan strategi yang diinginkan.

Dalam tahap ini peserta melakukan analisa terhadap beberapa parameter melalui FGD, sehingga diperoleh asumsi-asumsi dasar yang secara signifikan berpengaruh terhadap penyusunan kebijakan; (3) pembahasan dialetik, untuk membuat kasus kemungkinan strategi terbaik yang diinginkan melalui diskusi pakar; dan (4) sintesis, untuk mencapai kompromi atas asumsi-asumsi yang dapat menghasilkan strategi baru yang mampu mengungguli strategi lama (Eriyatno dan Sofyan, 2007).

E. Pemodelan Sistem

Pemodelan adalah suatu terjemahan bebas dari istilah *modelling* untuk menghindari berbagai pengertian atau penafsiran yang berbeda-beda, pemodelan dapat diartikan sebagai suatu gugus aktifitas 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 didukung oleh asumsi strategis dari metode SAST *(Strategic Assumption Surfacing and Testing)* atau matriks kebijakan lainnya.

Elemen asumsi strategis hasil proses SAST menjadi input dalam proses transformasi, dibangun *Root Definition* sebagai *framework* dari model. Berdasarkan *framework Root*

Definition dibangun *Rich Picture* yang merupakan konsep dasar model. Berdasarkan *Rich Picture* dapat diindentifikasi elemen – elemen sistem yang berpengaruh terhadap tujuan sistem, kemudian meng gunakan *logical thinking process* dikonvergensikan menjadi suatu model konseptual.

F. Penelitian yang Pernah Dilakukan

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

1. 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 *Fokus 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)
2. 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)

G. Kerangka Kerja Penelitian

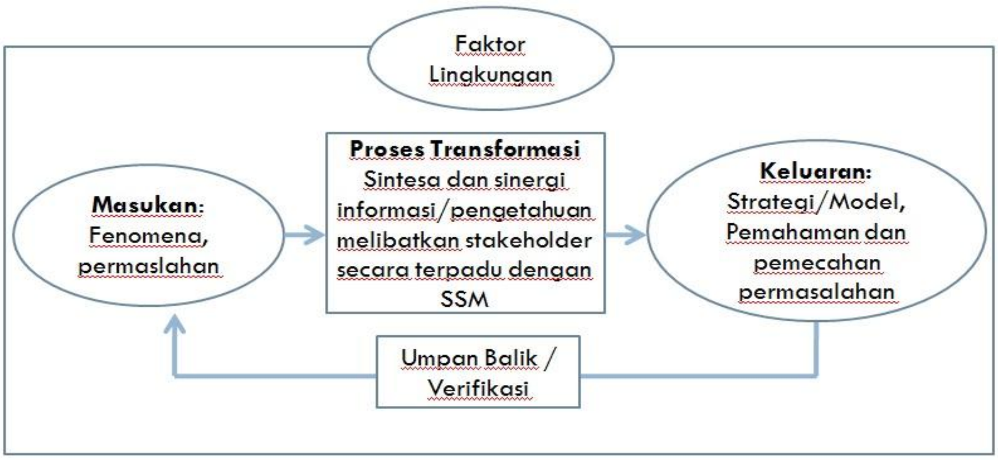
Dalam konteks *Soft System Methodology*, menurut Jackson (2003), sistem adalah suatu keutuhan yang komplek dimana kefungsiannya tergantung pada bagian-bagian dan interaksi antar bagian tersebut. Pemikiran sistematis dalam konteks penyelesaian permasalahan yang kompleks adalah pemikiran mengenai hubungan 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 berikut ini.

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 factor 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 dilakuna dengan *Soft System Methodology* (SSM).



Gambar 1. Skema Kerangka Kerja Penelitian

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.

III. Metode Penelitian

A. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan *Soft System Methodology* (SSM) melalui teknik *Strategic Assumption Surfacing and Testing* (SAST). Soft Systems Methodology (SSM) adalah 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.

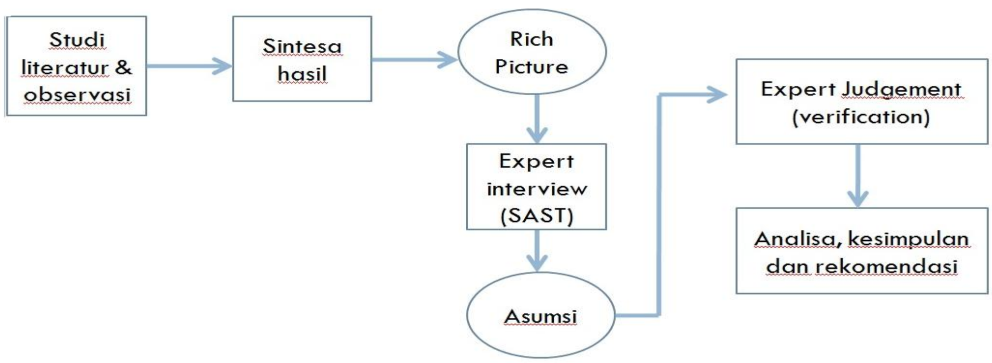
Sementara itu, teknik SAST adalah suatu metode yang digunakan untuk menyelesaikan masalah yang saling terkait dan rumit, dengan ketidak jelasan tentang tujuan, adanya konflik kepentingan, serta ketidak pastian lingkungan, maupun kendala sosial. (Jackson, 2003*).* Prinsip yang digunakan dalam landasan SAST *(*Mason & Mittrof, 1981*)* adalah: *partisipatif*, *adversarial*, *integrative*, dan *managerial mind suporting*.Dalam memperoleh data dan informasi dilakukan penelitian langsung di lapangan dengan metode wawancara melalui wawancara mendalam (*deep interview*) dan survey 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

1. 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) survey pengumpulan data di beberapa lokasi yang ditentukan serta survai pakar untuk mengakuisisi pengetahuan *thinking respondent* secara *purposive sampling* (Cooper dan Schindler, 2008).
2. Tahap survai pakar yang dilakukan melalui indepth interview (IDI) dan diskusi terfokus (FGD), serta pengisian kuesioner untuk analisis SAST. Metode SAST (Mason dan Mitroff, 1981) ditujukan untuk memunculkan dan menguji asumsi strategis yang merupakan kondisi ideal atau prasyarat yang harus dipenuhi dalam sistem. Kondisi riil yang dihadapi implementasi kebijakan disajikan dalam bentuk analisis kebijakan terhadap permasalahan yang terkait dengan implementasi standarisasi sertifikat keandalan dalam penyelenggaraan sistem transaksi elektronik. Pengetahuan pakar yang telah diserap, dipahami dan pendalaman terhadap kompleksitas sistem transaksi elektronik secara grafis dapat digambarkan dalam rich picture. Terhadap input elemen, asumsi strategis model yang dikembangkan serta analisis CATWOE, yaitu: C (*Customers*); A (*Actors*); T (*Transformation process*); W (*Worldview*); O(*Owners*); dan E (*Environmental constraints*), selanjutnya dilakukan penyusunan *root definition* (RD). Setelah melalui logical thinking process, disusun pemodelan sistem, yaitu model implementasi kebijakan standarisasi sertifikat elektronik dalam perspektif keamanan informasi, kemudian model integrasi kebijakan tersebut divalidasi dengan *expert judgement*. Gambar 2 adalah skema motode penelitian yang dilakukan.



Gambar 2. Skema Kerangka Kerja Penelitian

IV. Hasil Penelitian dan Pembahasan

A. *Sertifikat Elektronik dan Sertifikat Keandalan*

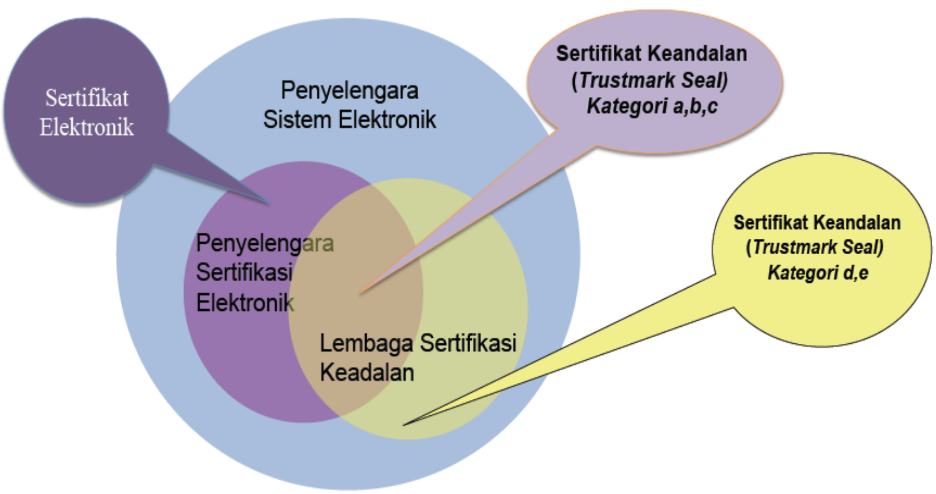
Sertifikat Elektronik adalah sertifikat yang bersifat elektronik dan memuat Tanda Tangan Elektronik serta identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik (PSrE). Adapun Kewenangan PSrE berdasarkan Pasal 60 PP PSTE, antara lain :

- Pemeriksaan calon pemegang Sertifikat Elektronik
- Penerbitan Sertifikat Elektronik
- Perpanjangan masa berlaku Sertifikat Elektronik
- Pemblokiran dan pencabutan Sertifikat Elektronik
- Validasi Sertifikat Elektronik
- 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 Sertfikasi Keandalan (LSK) adalah lembaga independen yang dibentuk oleh professional 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).

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 3 .Contoh Sertifikat Keandalan dan Sertifikat Elektronik



Gambar 4. Interelasi antara LSK dengan PSrE

Penyelenggaraan Transaksi Elektronik dalam lingkup public 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 public 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).

Standarisasi keamanan informasi pada dasarnya adalah mengenai pengelolaan resiko yang dilakukan dengan cara mengembangkan manajemen risiko dan strategi mitigasi melalui pengidentifikasian aset, ancaman dan *vulnerabilities* serta pengukuran resiko. Adanya standar keamanan informasi dapat diterapkan untuk menetapkan syarat-syarat keamanan informasi dan jenis pengendalian yang diperlukan untuk meminimalisir ancaman dan risiko tersebut yang disesuaikan dengan keuntungan organisasi yang paling optimal.

Tujuan utama penerapan Standar Keamanan Informasi adalah agar kegiatan pengamanan informasi pemerintah menjadi efisien dan efektif, sehingga tidak mudah untuk dibongkar pihak asing. Selain itu, Standar Keamanan Informasi akan memudahkan dalam menciptakan regulasi yang dapat memberikan keputusan apakah sebuah kegiatan keamanan informasi sudah baik atau belum, apakah sebuah informasi perlu mendapat perlakuan pengamanan atau tidak dan juga dapat menentukan sampai tingkat berapa pengamanan yang diperlukan, dan sebagainya (Calder & Watkins, 2003). Sehingga regulasi tentang keamanan informasi tidak perlu menciptakan badan/institusi lagi yang khusus untuk mengambil keputusan keamanan informasi atau tingkat kerahasiaan sebuah data/informasi.

Standar keamanan informasi menekankan pada aspek syarat, prosedur, kebijakan, pengelolaan serta pendidikan dan pelatihan. Standarisasi yang dimaksud disini bukanlah standar teknis (spesifikasi), pengarahan suatu teknologi atau produk, dan kumpulan tip serta bukan sebagai jaminan berfungsinya sebuah alat keamanan informasi. Pendekatan ini memungkinkan standar keamanan informasi dapat diaplikasikan dalam berbagai tipe organisasi.

B. Standarisasi Bidang TIK

Standar adalah spesifikasi teknis atau sesuatu yang dibakukan dan disusun berdasarkan konsensus semua pihak terkait dengan memperhatikan berbagai syarat (kesehatan, keselamatan, dan perkembangan iptek) berdasarkan pengamaman, perkembangan masa kini dan masa depan. Standardisasi di bidang TIK diperlukan untuk memberikan suatu cara yang tetap bagi sistem-sistem *hardware* dan/atau *software* untuk berkomunikasi. Dengan memungkinkan hardware dan software dari pabrikan-pabrikan yang berbeda untuk berinterkoneksi, standard membantu meningkatkan persaingan. Dalam kaitan transaksi elektronik, pemberlakuan standar bertujuan untuk melindungi masyarakat dari kemungkinan kerugian yang ditimbulkan akibat transaksi elektronik dan terciptanya ekosistem bisnis yang kondusif, aman dan terpercaya

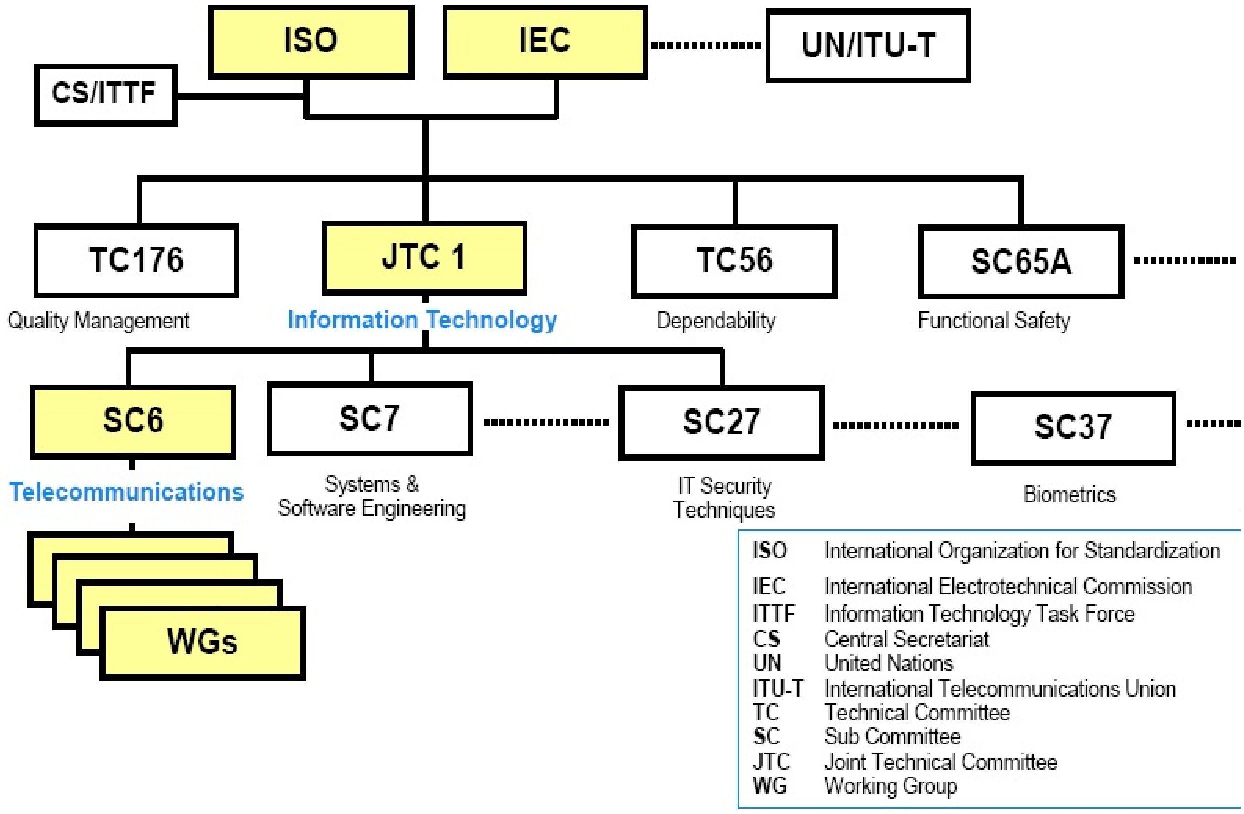
Terdapat dua jenis standar, antara lain: ***De facto*,** yaitu: standar-standar yang muncul di pasar dan diterima luas. Contoh jenis tersebut adalah berikut: QWERTY, ASCII, MS-DOS & Microsoft Windows operating systems, MP3. Jenis standard lainnya adalah ***De Jure*** **(Formal)**, yaitu: suatu standar yang dikembangkan oleh badan pembuat standar milik industri atau milik pemerintah. Pemerintah atau badan regulasi dapat mewajibkan pemberlakuan standar-standar sukarela (baik *de facto* maupun *de jure*). Standar yang diwajibkan oleh pemerintah atau badan regulasi disebut regulasi teknis.

Berdasarkan proses, terdapat tiga tahap dalam proses standardisasi (International Organization for Standardization/International Electrotechnical Commission, 1996), yaitu sebagai berikut:

1. ***Specification***: mengembangkan nomenklatur dan mengidentifikasi masalah yang akan diangkat.
2. ***Identification of choices***: mengidentifikasi solusi masalah dan memilih solusi yang "*optimum*".
3. ***Acceptance***: menetapkan solusi, menjadikannya diketahui oleh industri sehingga diterima suatu solusi yang seragam.

Standardisasi bidang elektronik dan telekomunikasi yang digunakan selama ini dibuat oleh Badan pembuat standard (*International Organization for Standardization/International Electrotechnical Commission*, 2000). Beberapa Badan Pembuat Standar, baik internasional maupun nasional adalah sebagai berikut:

1. Internasional:
   a. **ISO**: *International Organization for Standardization* (www.iso.ch)
   b. **IEC**: *International Electrotechnical Commission* (www.iec.ch)
   c. **ITU-T**: *International Telecommunications Union – Telecom Sector* (www.itu.int)
   d. **ETSI**: *European Telecommunications Standards Institute* (http://www.etsi.org/)
   e. **ANSI**: *American National Standards Institute* (www.ansi.org)



Gambar 5. Lingkup Standarisasi ISO/IEC

f. **IEEE**: *Institute of Electrical and Electronic Engineers* (standards.ieee.org)
g. **IETF**: *Internet Engineering Task Force* (www.ietf.org)

2. Nasional**:**
   a. **BSN**: Badan Standardisasi Nasional (www.bsn.go.id)

Kementerian Kominfo sebagai instansi teknis dapat memberlakukan penggunaan wajib standar tersebut yang sebelumnya bersifat sukarela (rekomendasi ITU, standar-standar ISO/IEC, ETSI, BSN, dll.) melalui kebijakan-kebijakan yang dikeluarkan Pemerintah. Dalam PP 102 Tahun 2000 tentang Standardisasi Nasional menyatakan bahwa pemberlakuan Standar Nasional Indonesia adalah keputusan pimpinan instansi teknis yang berwenang untuk memberlakukan Standar Nasional Indonesia secara wajib terhadap barang dan atau jasa. Standar yang diberlakukan wajib oleh Pemerintah/regulator disebut regulasi teknis. UU 36/1999 dan PP 52/2000 menyebut regulasi teknis sebagai persyaratan teknis. Merujuk pada pasal 72 PP 52/2000, tujuan Persyaratan Teknis adalah:

1. menjamin keterhubungan dalam jaringan telekomunikasi;
2. mencegah saling mengganggu antar alat dan perangkat telekomunikasi;
3. melindungi masyarakat dari kemungkinan kerugian yang ditimbulkan akibat pemakaian alat dan perangkat telekomunikasi;
4. mendorong berkembangnya industri, inovasi dan rekayasa teknologi telekomunikasi nasional.

Dalam PP 52/2000 disebutkan bahwa Setiap alat dan perangkat telekomunikasi yang dibuat, dirakit, dimasukkan, untuk diperdagangkan dan atau digunakan di wilayah Negara Republik Indonesia wajib memenuhi persyaratan teknis. Persyaratan teknis alat dan perangkat telekomunikasi meliputi persyaratan teknis alat dan perangkat telekomunikasi untuk keperluan penyelenggaraan jaringan, penyelenggaraan jasa telekomunikasi dan penyelenggaraan telekomunikasi khusus.

C. *Sertifikat Elektronik dan Sertifikat Keandalan*

Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik. Sertifikat tersebut dikeluarkan oleh Penyelenggara Sertifikasi Elektronik (PSrE). Dengan demikian, sertifikat elektronik menduduki peran layaknya "paspor elektronik", ia tidak dapat dipisahkan dari praktek tanda tangan elektronik, ia membawa kekuatan hukum yang kuat karena dapat meyakinkan identitas Penandatangan. Sertifikat elektronik mempunyai sebuah struktur internal, artinya ada beberapa bagian yang diwajibkan untuk diinformasikan atau dilekatkan pada sertifikat tersebut untuk memberikan kekuatan hukum pada sertifikat tersebut Syarat-

syarat ini akan diatur lebih lanjut di Peraturan Pemerintah berdasarkan Pasal 13 ayat (2) UU ITE.

Struktur internal ini didefinisikan oleh sebuah standar internasional yang disebut *recommendation* X-509 V.3 *de l'Union internationale des telecommunications* (JTC 1 TAG, 2002). Standar internasional ini kemudian dikembangkan oleh *Internet Engineering Task Force* untuk diaplikasikan pada teknologi tanda tangan elektronik. Sebuah sertifikat elektronik, menurut standar X-509 V.3 tersebut, hendaknya memuat minimal keterangan-keterangan sebagai berikut :

1. Versi sertifikat;
2. Nomor seri sertifikat;
3. Algoritma yang dipergunakan;
4. Nama pemilik sertifikat digital, temasuk didalamnya keterangan tentang negara asal, organisasi dan seterusnya;
5. Nama lembaga yang menerbitkan sertifikat elektronik:
6. Ekstensi, disesuaikan dengan kebutuhan.

UU ITE maupun PP PSTE tidak mempresisikan keterangan-keterangan apa saja yang harus dimuat dalam sebuah sertifikat elektronik, tetapi dalam kedua regulasi tersebut menyerahkan kepada Peraturan Pemerintah untuk menentukan lebih lanjut mengenai penyelenggaraan sertifikasi elektronik. Namun, sebagai perbandingan, standardisasi tersebut dapat mencontoh atau mereferensi kepada Dekrit Komisi Negara Perancis 2001-272 tanggal 30 Maret 2001 tentang "aplikasi Pasal 1316-4 *Code civil* dan tentang tanda tangan elektronik" (Fleischmann, 1995). Pasal 6 dekrit ini menentukan keterangan-keterangan yang harus dimuat dalam sebuah sertifikat elektronik terkualifikasi adalah sebagai berikut :

1. Keterangan yang mengindikasikan bahwa sertifikat ini dikeluarkan sebagai sertifikat elektronik terkualifikasi;
2. Identitias dari Penyelenggara Sertifikasi Tanda Tangan Elektronik serta Negara di mana ia berada;
3. Nama Penandatangan atau nama aliasnya, disertai dengan bukti-bukti identitas Penandatangan ;
4. Bila keadaan memungkinkan, keterangan kualitas si Penandatangan sesuai dengan penggunaan daripada tujuan pemakaian sertifikat elektronik itu ditujukan;
5. Data-data pemeriksa kebenaran/keabsahan tanda tangan elektronik yang sesuai dengan data-data pembuatan tanda tangan elektronik;
6. Indikasi awal berlaku dan berakhirnya validitas dari sertifikat elektronik;
7. Kode identitas dari sertifikat elektronik;
8. Tanda tangan elektronik dari Penyelenggara Sertifikasi Tanda Tangan Elektronik yang mengeluarkan sertifikat elektronik tersebut ;
9. Bila keadaan memungkinkan, disertakan kondisi-kondisi penggunaan sertifikat elektronik, khususnya besarnya transaksi maksimal yang dapat dilakukan dengan menggunakan sertifikat elektronik tersebut.

Sementara itu, Sertifikat Keandalan (*trustmark*) adalah dokumen yang menyatakan pelaku usaha yang menyelenggarakan transaksi secara elektronik telah lulus audit atau uji kesesuaian dari Lembaga Sertifikasi Keandalan. Tujuan digunakannya Sertifikat Keandalan adalah untuk melindungi komsumen dalam transaksi elektronik. Jaminan bahwa pelaku usaha telah memenuhi kriteria yang ditentukan oleh Lembaga Sertifikasi Keandalan (LSK). Sertifikat keandalan digunakan pada web site dan/atau sistem elektronik lainnya.

D. Penyelenggara Sertifikat Elektronik dan Lembaga Sertifikat Keandalan untuk meningkatkan Keamanan Transaksi Elektronik

Penyelenggara Sertifikasi Elektronis (PSrE), menurut UU ITE, adalah subyek hukum yang berfungsi sebagai pihak ketiga yang layak dipercaya untuk menyelenggarakan tanda tangan elektronik untuk memastikan identitas dan status subyek 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 subyek hukum pemilik tanda tangan dipastikan ketika diterbitkannya sertifikat elektronik.

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.

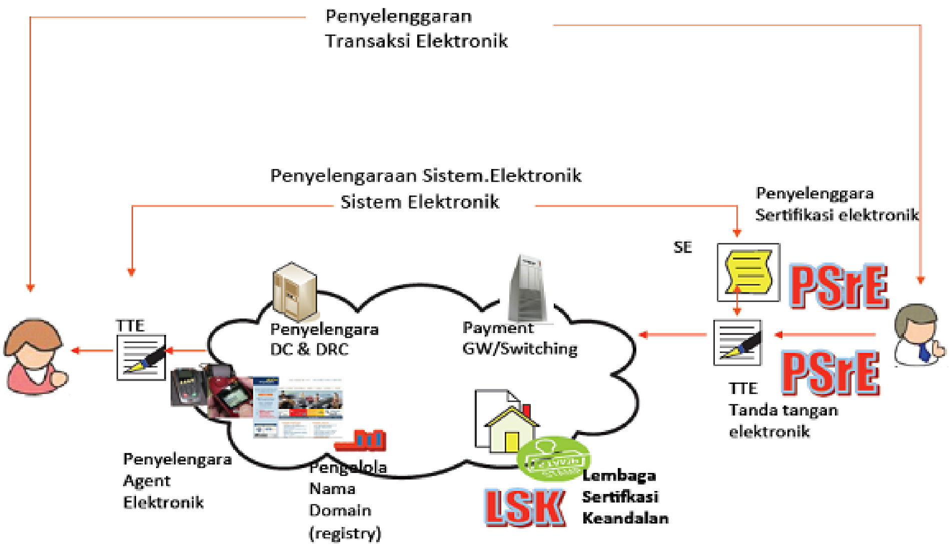
E. Analisa Standarisasi Sertifikat Elektronik dan Keandalan

Metode SSM berfokus untuk menciptakan sistem aktivitas dan hubungan manusia dalam sebuah organisasi atau kelompok dalam rangka mencapai tujuan bersama. Berpikir dengan system merupakan suatu bidang transdisiplin yang muncul sebagai respon terhadap keterbatasan dari pendekatan teknikal dalam proses reduksi untuk memecahkan masalah. Pemikiran sistem dalam konteks pemecah-an 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 6.

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 system 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. 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.



Gambar 6. *Rich Picture* Sistem Transaksi Elektronik

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 professional
6.	mengembangkan inkubator industri CA di Indonesia yang menggunakan standarisasi milik bangsa
World View	
1.	Penerapan standard 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

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.

Aplikasi pendekatan sistem lunak pada penelitian ini menggunakan teknik SAST (*Strategic Assumption Surfacing and Testing*) yang melibatkan para praktisi senior perusahaan melalui teknik wawancara mendalam dan FGD (Berta-lanffy, 1968). Teknik SAST digunakan, dengan melibat-kan praktisi senior/pakar melalui wawancara mendalam dan juga *Focus Grouyp Discndarussion* (FGD) untuk pengidentifikasian dan pemeringkatan asumsi-asumsi model implementasi standarisasi sertifikasi elektronik bagi penyelengara system elektronik. Responden yang dilibatkan dalam proses rancang bangun model adalah: unsur pemerintah, praktisi operator telekomunikasi, praktisi atau pakar bidang TI dan keamanan TI, pakar di bidang hukum IT (*cyber law*), akademisi bidang TI dan keamanan TI serta praktisi bidang keuang dan perbankan.

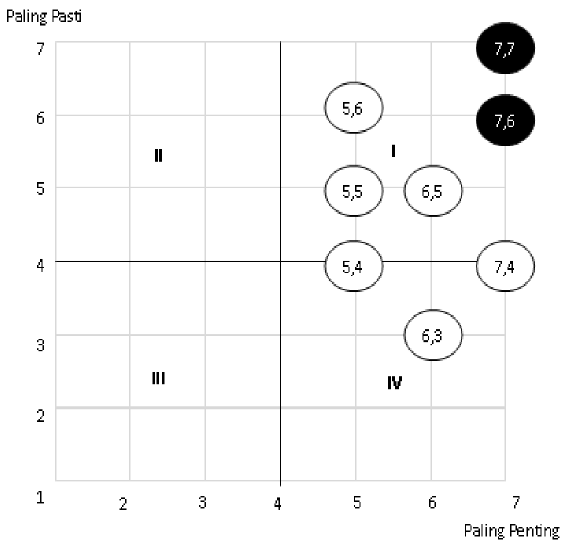
Menurut Mason & Mitroff (1981) ada empat (4) prinsip yang mendasari metode SAST: *(1) Participative, (2) Adversarial, (3) Integrative, (4)* Managerial and mind supporting. Berdasarkan empat prinsip tersebut dikembangkan empat tahap penggunaan teknik SAST, yaitu: (1) *Group formation*; (2) *Assumption surfacing*; (3) *Dialectical debate*; (4) *Synthesis*. Berdasarakan hasil kajian literatur dan wawancara dengan praktisi yang berkompeten dengan strategi standarisasi sertifikat elektronik, maka dilakukan modifikasi asumsi, kemudian melalui pengujian pakar lainnya lebih lanjut lagi ditentukan nilai kepentingan dan kepastian dengan skala ordinal untuk kepentingan skala 1-7 (sangat tidak penting – sangat penting). Demikian juga untuk kepastian digunakan skala ordinal 1-7 (sangat tidak pasti - sangat pasti). Dari proses tersebut diperoleh asumsi strategis seperti pada table 2.

TABEL 2. ASUMSI STRATEGIS IMPLEMENTASI STANDARISASI SERTIFIKASI ELEKTRONIK

Pencapaian Tujuan Standariasi Sertifikasi Keandalan	
A1	Penyelenggaraan transaksi elektronik yang terpercaya (*trusted e-tansaction*)
A2	Komitmen terhadap penerapan standard dan regulasi
A3	Peningkatan kesadaran masyarakat terhadap keamanan informasi
A4	Meningkatkan kenyamanan bertransaksi elektronik
A5	Tumbuhnya industri dan ekosistem bisnis sertifikat elektronik
A6	Persaingan pasar yang kondusif
A7	Meningkatkan daya saing
A8	Kemandirian industri sertifikat elektronik nasional
A9	Kemudahan dalam berbisnis on-line
Pemenuhan Prasyarat Input	
B1	Adanya komitmen penerapan regulasi dan kebijakan dalam mendorong penerapan standar sertifikasi elektronik dan keandalan
B2	Tersedianya komunitas bisnis industri sertifikat elektronik dan sertifikat keandalan
B3	Ada kebijakan yang mengatur keterlibatan pihak ketiga (penyelenggara sertifikat elektronik dan keandalan) multinasional dalam penerbitan sertifikat elektronik
B4	Kerjasama dengan pihak ketiga (penyelenggara sertifikat elektronik dan keandalan) multinasional
B5	Adopsi standar internasional untuk standar nasional
B6	Tersedianya iklim bisnis industri sertifikat elektronik yang kondusif
B7	Peran serta penelitian dan pengembangan untuk penyelenggaraan ekosistem sertifikat elektronik nasional
B8	Penyediaan inkubator bisnis penyelenggaraan sertifikasi elektronik nasional
B9	Pelatihan dan Pengembangan SDM terkait dengan transaksi elektronik

Pemenuhan Prasyarat Proses	
C1	Penyediaan infrastruktur teknologi keamanan informasi dan sarana komunikasi sebagai pendukung transaksi elektronik sesuai UU ITE dan PP PSTE
C2	Tata kelola bisnis sertifikasi elektronik dan sertifikasi keandalan dan menerapkan mekanisme ISMS
C3	Tersedianya pusat data (data center) berikut DRC dan *collocation*
C4	Terdapat mekanisme pasar bisnis sertifikat elektronik yang kondusif
C5	Tersedia standard dan prosedur audit atau uji Kesesuaian dari Lembaga Sertifikasi Keandalan
C6	Tersedia lembaga akreditasi untuk sertifikasi elektronik
C7	Proteksi pemerintah (regulator) terhadap munculnya sertifikat kenadalan (*trust mark*) palsu
C8	standar yang mengatur layanan dasar Penyelenggara Sertifikasi Elektronik (PSrE)
C9	Konsorsium Penyelenggara Sertifikasi Elektronik
C10	Badan Regulator Transaksi Elektronik
C11	Layanan Kunci Publik Nasional

Hasil pemunculan (*surfacing*) dan pengujian (*testing*) asumsi tersebut bertujuan untuk memperoleh tingkat kepastian dan kepentingan asumsi. Penentuan asumsi strategis digambarkan dalam kuadran kartesius (Mason dan Mitroff, 1981), dimana kuadran I untuk rencana yang pasti sebagai penggerak keberhasilan model kebijakan serta asumsi untuk rencana yang bermasalah (kuadran IV) sebagai solusi pencegahannya. Dari kedua kuadran tersebut teridentifikasi asumsi strategis yang diperlukan untuk mendukung suatu kesimpulan atau validasi argumen untuk implementasi standarisasi sertifikasi elektronik untuk system transaksi elektronik. Dengan adanya asumsi strategis ini model yang dirancang dapat diarahkan untuk pencapaian tujuan tumbuhnya ekosistem bisnis transaksi elektronis yang handal dan terpercaya. Selanjutnya asumsi-asumsi tersebut diperingkat berdasarkan tingkat kepentingan dan kepastian, menggunakan skala stapel dan hasilnya digunakan sebagai pertimbangan dalam rancang bangun model, sebagai mana ditunjukkan pada Gambar 7.



Gambar 7. Pemeringkatan Asumsi Strategis dengan Teknik SAST

TABEL 3. NILAI ASUMSI STRATEGIS

Asumsi dengan nilai 7,7:
A1, A2, A4, B4, B8, C1, C5, C7, C8

Asumsi dengan nilai 7,6:
A5, B5, B6, B9, C2, C3, C6, C10

Asumsi-asumsi pada kuadran I yang memiliki tingkat kepentingan dan tingkat kepastian paling tinggi dengan nilai 7,7 dan 7,6 (amat sangat penting–amat sangat pasti), beberapa diantaranya yaitu: Penyelenggaraan transaksi elektronik yang terpercaya (*trusted e-tansaction*) (A1), Komitmen terhadap penerapan standard dan regulasi (A2), Meningkatkan kenyamanan bertransaksi elektronik (A4), Tumbuhnya industri dan ekosistem bisnis sertifikat elektronik (A5), Tersedianya komunitas bisnis industri sertifikat elektronik dan sertifikat keandalan (B3), Ada kebijakan yang mengatur keterlibatan pihak ketiga multinasional dalam penerbitan sertifikat elektronik (B4), Tersedianya iklim bisnis industri sertifikat elektronik yang kondusif (B5), Penyediaan infrastruktur teknologi keamanan informasi dan sarana komunikasi sebagai pendukung transaksi elektronik sesuai UU ITE dan PP PSTE (C1), tata kelola bisnis sertifikasi elektronik dan sertifikasi keandalan dan menerapkan mekanisme ISMS (C2), Tersedianya pusat data (*data center*) berikut DRC dan *collocation* (C3), standar yang mengatur layanan dasar Penyelenggara Sertifikasi Elektronik (PSrE) (C7).

Selain itu, juga teridentifikasi asumsi strategis untuk rencana yang dinilai tidak terlalu penting oleh responden. Asumsi tersebut adalah asumsi yang berada pada kuadran IV, yaitu: kemudahan dalam bisnis *on-line* (A9), dan Terdapat mekanisme pasar bisnis sertifikat elektronik yang kondusif (C4). Hal ini disebabkan karena, asumsi tersebut dapat terwujud jika asumsi-asumsi yang dinilai sangat penting dan krusial telah dilaksanakan. Permasalahan implementasi kebijakan standarisasi sertifikat elektronik dan keandalan untuk system transaksi elektronik sebagaimana yang teridentifikasi dapat dikendalikan dengan adanya dukungan dan komitmen kebijakan pemerintah serta inisiatif pemerintah untuk menyediakan sarana dan prasarana guna menumbuh-kembangkan iklim bisnis transaksi elektronik yang kondusif. Komitmen kebijakan pemerintah tersebut ditindaklanjuti dengan menyiapkan standard dan mekanisme evaluasi serta monitoring pelaksanaan kebijakan tersebut.

F. Integrasi Regulasi Teknis Sertifikasi Elektronik dan Keandalan

Berdasarkan seluruh tahapan penelitian yang tertuang dalam kerangka penelitian, maka dibentuklah Model manajemen terintegrasi yang melibatkan beberapa sector pemerintah yang terkait. Model manajemen 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 implementasi Standarisasi Sertifikat Elektronik dan Sertifikat Keandalan. Regulasi yang dikeluarkan bersifat mengikat kepada setiap entitas yang terlibat dalam ekosistem kelembagaan Sertifikasi Elektronik dan Sertifikasi Keandalan. 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 dan Sertifikasi Keandalan. Tujuan dilakukannya audit dan penilaian adalah untuk menilai kepatuhan Penyelenggara Sertifikasi Elektronik dan Sertifikasi Keandalan terhadap regulasi dan standard yang berlaku. Lembaga Audit dan Akreditasi melakukan kegiatan audit berdasarkan regulasi dan standard yang dikeluarkan oleh Pemerintah. Setelah dilakukan proses audit dan penilaian, maka dikeluarkan akreditasi terhadap institusi Penyelenggara Sertifikasi Elektronik dan Sertifikasi Keandalan. Akreditasi tersebut dapat membuktikan bahwa Penyelenggara Sertifikasi Elektronik (PSrE) dan Sertifikasi Keandalan 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*. Kepercayaan masyarakat terhadap Penyelenggara Sistem Transaksi Elektronik bergantung pada tingkat keamanan dan keandalan system. Dengan demikian setiap Penyelenggara Sistem Transaksi Elektronik membutuhkan Sertifikat Elektronik (PSrE) atau dikenal dengan *Certificate of Authority* (CA) dan Sertifikat Keandalan atau secara umum dikenal dengan *trust mark*. Standard yang digunakan:

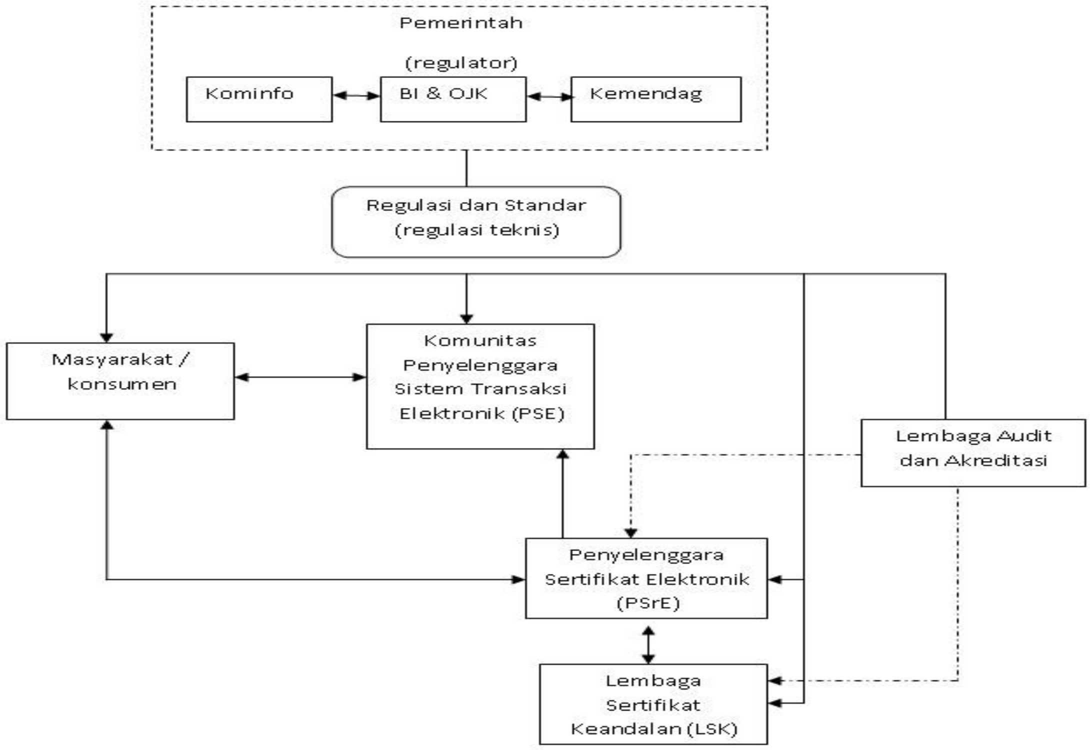
1. Profile Certificate : X.509.v3
2. CRL : X.509.v2
3. Enkripsi : RSA
4. Hashing : MD5, SHA
5. Key length : 1024 Bit
6. ISO 14516/2002 (SNI Kep BSN no 63/2005)

Tujuan utama dibangunnya model tata kelola implementasi standardisasi sertifikat elektronik dan sertifikat keandalan adalah untuk mempermudah implementasi kebijakan penerapan kebijakan standardisasi tersebut.

TABEL 4. ASUMSI STRATEGIS IMPLEMENTASI STANDARISASI SERTIFIKASI ELEKTRONIK

No.	Hirarki	Teknik SAST	
		Asumsi Strategis	**Fokus Isu**
1	Direktif	Mengacu pada : UU 11/2008 tentang ITE, PP PSTE, UU 36/1999 tentang dan PP 52/2000, ISO/SNI 19-7125-2005	
2	Strategik	a. Regulasi teknis untuk sertifikasi elektronik dan keandalan b. Kebijakan yang mengatur keterlibatan pihak ketiga multinasional c. Standard dan prosedur audit atau uji Kesesuaian dari Lembaga Sertifikasi Keandalan d. Proteksi pemerintah (regulator) terhadap munculnya sertifikat kenadalan (trust mark) palsu e. Standar yang mengatur layanan dasar Penyelenggara Sertifikasi Elektronik (PSrE)	Kebijakan Teknis Sertifikasi Elektronik dan Keandalan yang terintegrasi dan ekosistem bisnis yang kondusif (*Integrated policy, Standardisation, condusive business ecosystem*)
3	Taktikal	Koordinasi dengan lintas stakeholder, seperti: a. Regulator: BI, OJK, Kementerian Perdagangan b. Bisnis: industri Perbankan, penyedia layanan internet/operator telco, pengelola domain, komunitas pelaku bisnis secara elektronis	Koordinasi tingkat kebijakan dan operasional (*high and middle level implementation plan*)

No.	Hirarki	Teknik SAST	
		Asumsi Strategis	Fokus Isu
4	Operasional	a. Penyediaan infrastruktur pendukung transaksi elektronik sesuai UU ITE dan PP PSTE b. Pusat data (*data center*) berikut DRC dan *collocation* c. Tersedianya komunitas bisnis industri sertifikat elektronik dan sertifikat keandalan d. Penyediaan inkubator bisnis penyelenggaraan sertifikasi elektronik nasional e. Pelatihan dan Pengembangan SDM terkait dengan transaksi elektronik	Ketersediaan infrastruktur dan dukungan teknis operasional (*availability and technical support*)



Gambar 8. Model Integrasi Regulasi Teknis Sertifikat Elektronik dan Keandalan

Adanya model tata kelola implementasi standardisasi sertifikat elektronik dan sertifikat keandalan dapat memperjelas tata hubungan dan kewajiban serta tanggung jawab dari masing-masing *stakeholder*. Berdasarkan hasil analisis menggunakan teknik SAST yang telah dilakukan, maka Tabel dibawah ini menunjukkan resume hasil analisis menggunakan teknik SAST.

Hasil analisis dengan Teknik SAST menunjukkan bahwa terdapat 4 (empat) hierarki/tingkatan tata kelola yang dikaitkan dengan isu strategis pada masing-masing tingkatan. Tingkatan direktif fokus terhadap regulasi yang bersifat makro dan berada pada level paling tinggi, seperti: UU 11/2008 tentang ITE, PP PSTE, UU 36/1999 tentang dan PP 52/2000, ISO/SNI 19-7125-2005. Sementara itu pada tingkatan Strategik, memiliki isu strategis dalam hal yang bersifat teknis penjabaran regulasi yang bersifat makro dalam mengimplementasikan regulasi standardisasi sertifikat elektronik dan sertifikat keandalan. Adapun pada tingkatan Taktikal mengatur hal-hal teknis yang bersifat koordisi antar lembaga yang terkait dalam ekosistem Penyelenggara Sistem Transaksi Elektronik dan pada tingkatan Operasional lebih fokus mengatur pada hal-hal yang bersifat teknis operasional implementasi standarisasi sertifikat elektronik dan sertifikat keandalan. Pada level ini menitikberatkan pada aspek ketersediaan infrastruktur dan dukungan teknis operasional.

V. SIMPULAN DAN SARAN

A. *Kesimpulan*

Berdasarkan hasil pembahasan dalam penelitian ini, dapat disimpulkan sebagai berikut:

1. Untuk membangun sebuah system, fokus yang pertama adalah pada aspek ketersediaan (*availability*). Ketika sebuah system dibangun, maka lambat laun masyarakat akan banyak yang akan mengakses system tersebut. Jika infrastruktur pendukung system tidak dipersiapkan dengan baik, maka akan memungkinkan terjadinya system tersebut menjadi down. Salah satu upaya yang dapat dilakukan adalah dengan membangun data center.

2. Lembaga Sertifikat Keandalan melakukan audit terhadap Informasi elektronik (pasal 66 PP PSTE ayat 3) dan sistem elektronik (PP PSTE pasal 66 ayat 2) untuk mendapatkan sertifikat keandalan.
3. Kajian sertifikat keandalan yang perlu dilakukan adalah kegiatan proses bisnis pelaku usaha dalam menggunakan system elektronik (informasi kegiatan usaha)
4. Model bisnis sebuah Lembaga Penyelenggara Sertifikat Elektronik bergantung pada kepercayaan kepercayaan. Oleh karena itu, setiap pelaku industry yang melakukan transaksi harus membangun dan mendapatkan kepercayaan (trust) dari masyarakat pelaku transaksi elektronik.

B. Saran

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

1. menyediakan infrastruktur: Lembaga *certificate of authority* (CA), infrastruktur teknis pendukung dan mengimplementasikan standar yang dapat digunakan oleh para pelaku tansaksi elektronik
2. komitmen pada perlindungan keamanan informasi dalam transaksi elektronik
3. kemandirian dalam infrastruktur teknologi keamanan informasi; munculnya industry pembuat CA dan lain-lain.
4. komitmen terhadap Law enforcement (penindakan hukum), yaitu dengan adanya punishment bagi yang tidak taat dan tidak mau dilakukan audit
5. membangun iklim kesadaran pada masyarakat mengenai pentingnya keamanan informasi dalam transaksi elektronik.
6. Strategi lainnya adalah inisiatif pemerintah untuk menjadi perintis (*pioneer*) sebuah Lembaga Penyelenggara Sertifikat Elektronik pertama yang terpercaya dengan membangun infrastruktur Sertifikat Elektronik sendiri dan mendorong seluruh masyarakat pelaku transaksi elektronik menggunakan Sertifikat Elektronik tersebut.

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., 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). Business Resarch Methods. New York: McGraw-Hill Companies,. Inc.

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

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

Eriyatno. (2012). 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.

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.

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.

PP No.82. Peraturan Pemerintah Republik Indonesia Nomor 82. Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Pub.L.No.82 Tahun 2012 (2012). Indonesia

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).

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.

UU RI No.11. Undang-Undang Republik Indonesia Nomor 11. Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pub.L.No.11 Tahun 2008 (2008). Indonesia