Perancangan Spesifikasi Keamanan pada Aplikasi Persiapan Penyelenggaraan Sertifikasi Keamanan Perangkat Teknologi Informasi (SIAGASIKAT) Versi 1.0.0 Berdasarkan SNI ISO/IEC 15408:2014

Mahendra Yudhistira [1], Esti Rahmawati A[2], Alfred Saut S[3]
[1,2,3]Badan Siber dan Sandi Negara
[1,2,3]Jalan Muchtar Raya No 70, Kelurahan Duren Mekar, Kecamatan Bojongsari, Kota Depok, Jawa Barat
mahendra.yudhistira@bssn.go.id, esti.rahmawati@bssn.go.id , alfred.saut@bssn.go.id

Abstract—**Salah satu tugas pokok dan fungsi Deputi Bidang Pemantauan dan Pengendalian adalah untuk menyelenggarakan sertifikasi produk keamanan teknologi informasi (TI). Sampai dengan tahun 2020, penyelenggaraan sertifikasi ini belum optimal. Berbagai hal harus disiapkan antara lain penyiapan sistem manajemen mutu, kompetensi sumber daya manusia, dan peralatan pengujian. Untuk menyediakan informasi yang valid dan akurat terkait hal – hal tersebut maka dikembangkanlah suatu aplikasi dengan nama Persiapan Penyelenggaraan Sertifikasi Keamanan Perangkat TI (SIAGASIKAT) versi 1.0.0. Dalam tahap perencanaan dan analisis kebutuhan, didefinisikanlah kebutuhan *functional* dan *non-functional*. Salah satu persyaratan *non-functional* adalah spesifikasi keamanan. Dalam paper ini, kami merancang fungsi keamanan aplikasi SIAGASIKAT berdasarkan SNI ISO/IEC 15408:2014. Metode perancangan yang digunakan adalah ISO/IEC TR 15446:2017. Perancangan ini menghasilkan spesifikasi keamanan yaitu *identification and authentication* (FIA), *cryptographic support* (FCS), dan *security audit* (FAU).**

Kata kunci: SIAGASIKAT versi 1.0.0; spesifikasi keamanan; SNI ISO/IEC 15408:2014; ISO/IEC TR 15446:2017

Abstract—**One of the main tasks and functions of the Deputy of Monitoring and Control, BSSN is to hold IT security product certification. Until 2020, the IT security product certification has not been carried out optimally yet. Various matters must be prepared for conducting product certification, including the quality management system, human resource competencies, and testing equipment. To provide valid and accurate information about various matters that should be handled in the preparation of IT security product certification, an application with the name Persiapan Penyelenggaraan Sertifikasi Keamanan Perangkat Teknologi Informasi (SIAGASIKAT) version 1.0.0 was built. In the planning and needs analysis phase, the functional and non-functional requirements of the application are defined. One non-functional requirement is a system security specification. In this paper, we identified the security specification of SIAGASIKAT version 1.0.0 based on SNI ISO / IEC 15408: 2014. The design method follows the steps outlined in ISO / IEC TR 15446: 2017. The design results have obtained security specifications i.e. identification and authentication (FIA), cryptographic support (FCS), and security audit (FAU).**

Keywords-component: SIAGASIKAT version 1.0.0; security specification; SNI ISO/IEC 15408:2014; ISO/IEC TR 15446:2017

I. PENDAHULUAN

Badan Siber dan Sandi Negara (BSSN) merupakan salah satu Lembaga Pemerintah Non – Kementerian (LPNK) yang mempunyai tugas pokok dan fungsi dalam keamanan siber dan persandian [1]. Deputi Bidang Pemantauan dan Pengendalian menyelenggarakan tugas pokok dan fungsi untuk menjalankan pemantauan dan pengendalian dalam bidang keamanan siber dan persandian. Salah satu tugasnya adalah penyelenggaraan sertifikasi dan produk. Salah satu layanan sertifikasi yang diberikan adalah sertifikasi keamanan perangkat TI berdasarkan SNI ISO / IEC 15408: 2014 and SNI ISO / IEC 18045: 2015 atau yang lebih dikenal dengan istilah *Common Criteria.* Layanan sertifikasi ini akan dilakukan oleh Lembaga Sertifikasi Produk (LSPro) dan Laboratorium Pengujian (Lab Uji). Beberapa hal yang harus disiapkan dalam operasional LSPro dan Lab Uji adalah dokumentasi sistem manajemen, kompetensi Sumber Daya Manusia (SDM), dan peralatan pengujian [3].

Untuk menyediakan infomasi yang valid dan akurat terkait dengan hal – hal yang perlu disiapkan menuju operasional layanan sertifikasi, maka dikembangkanlah suatu aplikasi berbasis web dengan nama Aplikasi Persiapan Penyelenggaraan Sertifikasi Keamanan Perangkat TI (SIAGASIKAT) versi 1.0.0. Pengembangan aplikasi ini mengikuti kerangka kerja *System Development Life Cycle* (SDLC). Dalam tahap perencanaan dan analisis kebutuhan disusunlah kebutuhan fungsional dan non-fungsional aplikasi. Salah satu kebutuhan non-fungsional adalah spesifikasi keamanan aplikasi [5]. Spesifikasi keamanan menjadi bagian yang penting dari suatu aplikasi karena data pada aplikasi harus diamankan dari pihak yang tidak berwenang.

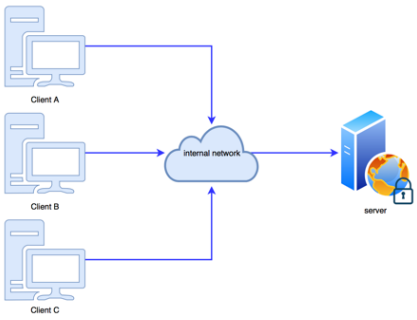
Di Indonesia, telah ada standar yang mengatur tentang spesifikasi keamanan pada suatu produk, sistem atau aplikasi teknologi informasi. Beberapa penelitian telah menggunakan standar ini untuk menentukan spesifikasi keamanan pada suatu sistem/aplikasi yang dirancang. Pada [6] telah dilakukan perancangan spesifikasi

keamanan pada aplikasi akses kontrol, pada [7] pada aplikasi *file encryption* dan pada [8] pada web aplikasi. Dalam makalah ini akan dideskripsikan bagaimana perancangan spesifikasi keamanan aplikasi SIAGASIKAT versi 1.0.0 berdasarkan standar tersebut yaitu SNI ISO/IEC 15408:2014.

II. LANDASAN TEORI

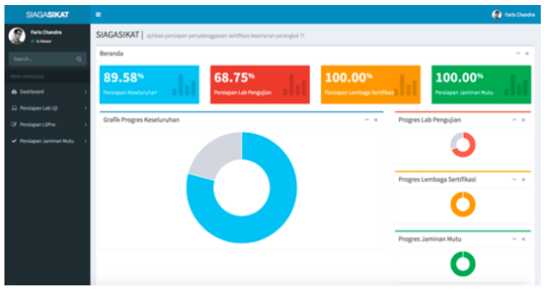
A. *Aplikasi SIAGASIKAT versi 1.0.0*

Aplikasi SIAGASIKAT versi 1.0.0 dirancang untuk melindungi data yang tersimpan dari pihak yang tidak berwenang untuk melakukan pencurian data. Aplikasi ini merupakan web application dengan arsitektur aplikasinya adalah klien–server. Gambar 1 menunjukkan asristektur aplikasi SIAGASIKAT versi 1.0.0.

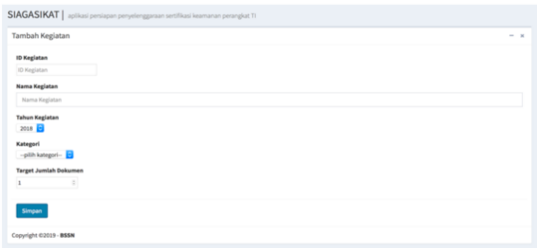


Gambar 1. Arsirektur Aplikasi SIAGASIKAT versi 1.0.0

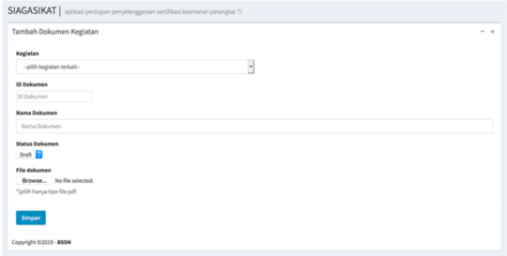
Klien dapat mengakses aplikasi ini melalui jaringan internal. Server merupakan tempat pengolahan dan penyimpanan data pengguna dari aplikasi ini. Klien sesuai dengan *role* yang dimiliki dapat melihat dan/atau merekam data kegiatan persiapan penyelenggaraan sertifikasi keamanan perangkat TI dan aplikasi akan menampilkan data progress persiapan tersebut. Berikut adalah Gambar 2 yang menyajikan tampilan dashboard SIAGASIKAT dan Gambar 3 yang menyajikan tampilan form isian kegiatan persiapan serta Gambar 4 menyajikan tampilan form isian dokumentasi sistem manajemen yang harus disiapkan.



Gambar 2. Tampilan Aplikasi SIAGASIKAT versi 1.0.0



Gambar 3. Tampilan Form Isian Kegiatan

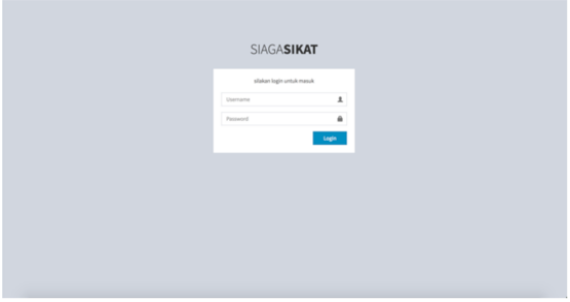


Gambar 4. Tampilan Form Isian Dokumen

Untuk mendukung tujuan perancangannya, aplikasi ini dilengkapi dengan fitur-fitur sebagai berikut

1) *Fitur Login*

Fitur ini menjamin bahwa hanya pengguna yang mempunyai *username* dan *password* yang berkesesuaian yang dapat login ke sistem dan mengakses aplikasi SIAGASIKAT versi 1.0.0. Gambar 5 menunjukkan tampilan login aplikasi.



Gambar 5 Tampilan Login

2) *Pembagian Role Admin, Author dan Viewer*

Terdapat 3 peran dalam SIAGASIKAT yaitu *role Admin, Author*, dan *Viewer*. *Admin* merupakan *role* yang mempunyai hak untuk menambah, mengubah, dan menghapus data pengguna. *Author* merupakan *role* yang mempunyai hak untuk menambah, mengubah, dan menghapus data kegiatan maupun data dokumen. Sedangkan *Viewer* merupakan *role* yang hanya dapat mengakses dan melihat data nilai progres persiapan maupun data kegiatan dan dokumen.

3) *Implementasi Algoritma Kriptografi*

Algoritma kriptografi diimplementasikan untuk melindungi *password* pengguna, yaitu MD5 128 bit.

B. *SNI ISO/IEC 15408:2014 tentang Kriteria Evaluasi Keamanan Teknologi Informasi*

Security Functional Requirements (SFR) merupakan spesifikasi keamanan yang harus dipunyai oleh suatu produk keamanan. SNI ISO/IEC 15408:2014 merupakan standar nasional untuk spesifikasi sebuah produk keamanan [9]. Spesifikasi keamanan ini terdiri dari berbagai kelas yaitu *security audit (FAU), commucation, cryptographic support (FCS), user data protection (FDP), identification* dan *authentication (FIA), security management (FMT), privacy (FPR), protection of the ToE Security Functionality (FPT), Resource Utilisation (FRU), Target of Evaluation (TOE) access (FTA),* dan *Trusted Path/Channels (FTP)*. Setiap kelas mempunyai komponen yang lebih detil sesuai dengan tujuan keamanannya.

Berikut adalah Tabel I yang menunjukkan kelas yang berkesesuaian dengan penelitian ini.

TABLE I. KELAS SFR, KOMPONEN, DAN TUJUAN KEAMANANNYA

SFR	Komponen	Tujuan Keamanan
FAU	Audit keamanan yang meliputi kegiatan untuk mengenali, merekam, menyimpan dan menganalisa informasi yang berhubungan dengan kegiatan yang relevan dengan keamanan. Hasil dari penyimpanan audit dapat diperiksa untuk menentukan aktivitas keamanan apa yang berjalan dan siapa yang bertanggung jawab melakukan hal tersebut.	
	Security audit data generation (FAU_GEN)	Mendefinisikan persyaratan untuk merekam kejadian keamanan yang relevan yang terjadi di bawah kendali TSF, misalnya tingkat audit, menyebutkan jenis peristiwa yang harus diaudit oleh TSF, dan mengidentifikasi kumpulan minimum informasi terkait audit yang harus disediakan dalam berbagai jenis catatan audit
FCS	Kelas ini membahas persyaratan untuk pengimplementasian fungsi kriptografi,	
	Cryptographic key management (FCS_CKM)	Mendukung *key management life cycle* yaitu: pembangkitan kunci kriptografi, distribusi kunci kriptografi, akses kunci kriptografi, dan penghancuran kunci kriptografi
	Cryptographic operation (FCS_COP)	Agar operasi kriptografi berfungsi dengan benar, operasi harus dilakukan sesuai dengan algoritma yang ditentukan dan dengan Panjang kunci yang sesuai.
FIA	Kelas ini membahas persyaratan untuk fungsi-fungsi untuk membangun dan memverifikasi identitas pengguna yang diklaim.	
	Authentication failures (FIA_AFL)	Berisi persyaratan untuk menentukan nilai untuk sejumlah upaya otentikasi yang gagal dan tindakan TSF dalam kasus kegagalan upaya otentikasi
	User atribute definition (FIA_ATD)	Menetapkan persyaratan untuk mengaitkan atribut keamanan pengguna dengan pengguna sebagaimana diperlukan untuk mendukung TSF dalam membuat keputusan keamanan
	Specification of secrets (FIA_SOS)	Mendefinisikan persyaratan untuk mekanisme yang menegakkan metrik kualitas yang ditetapkan pada rahasia yang disediakan dan menghasilkan rahasia untuk memenuhi metrik yang ditentukan.
	User authentication (FIA_UAU)	Mendefinisikan jenis mekanisme otentikasi pengguna yang didukung oleh TSF
	User identification (FIA_UID)	Mendefinisikan kondisi di mana pengguna harus mengidentifikasi diri sebelum melakukan tindakan lain yang akan dimediasi oleh TSF dan yang memerlukan identifikasi pengguna.
	User-subject binding (FIA_USB)	Menetapkan persyaratan untuk membuat dan memelihara asosiasi atribut keamanan pengguna dengan subjek yang bertindak atas nama pengguna
FMT	Kelas ini dimaksudkan untuk menentukan manajemen beberapa aspek TSF: atribut keamanan, data dan fungsi TSF. Peran manajemen yang berbeda dan interaksinya, seperti pemisahan kemampuan, dapat ditentukan.	
	Management of security attributes (FMT_MSA)	Memungkinkan pengguna yang berwenang mengontrol manajemen atribut keamanan. Manajemen ini mungkin mencakup kemampuan untuk melihat dan memodifikasi atribut keamanan.
	Specification of Management Functions (FMT SMF)	Memungkinkan spesifikasi fungsi manajemen disediakan oleh TOE

III. METODOLOGI PENELITIAN

Penyusunan SFR aplikasi SIFER ini mengikuti langkah – langkah penyusunan SFR yang tertuang pada ISO/IEC TR 15446 – *Information technology – Security techniques – Guidance for the production profiles and security targets* [10]. Langkah – langkah tersebut adalah sebagai berikut:

1. Mendefinisikan permasalahan keamanan.

   Pada langkah ini didefinisikan permasalahan keamanan pada aplikasi SIAGASIKAT yang meliputi ancaman yang akan diatasi oleh aplikasi, asumsi untuk operasional aplikasi dan kebijakan organisasi yang disusun, diberlakukan dan dipatuhi oleh pengguna SIAGASIKAT.

2. Mengidentifikasi tujuan keamanan untuk mengatasi permasalahan keamanan pada langkah pertama.

   Pada langkah ini diidentifikasi tujuan keamanan untuk lingkungan operasional IT maupun non IT dari aplikasi juga tujuan keamanan dari aplikasi SIAGASIKAT.

3. Mendefinisikan persyaratan keamanan untuk memenuhi tujuan keamanan pada langkah sebelumnya;

   Pada langkah ini didefinisikan spesifikasi keamanan yang memenuhi tujuan keamanan. *Output* dari langkah ini adalah matriks rasional untuk setiap tujuan keamanan terhadap permasalahan keamanan.

4. Memilih SFR untuk memenuhi persyaratan keamanan pada langkah sebelumnya.

IV. PEMBAHASAN

Tahapan yang dilakukan dalam penyusunan SFR adalah mengidentifikasi permasalahan keamanan, mengidentifikasi tujuan keamanan untuk mengatasi permasalahan tersebut, mendefinisikan persyaratan keamanan untuk memenuhi tujuan keamanan tersebut, dan memilih SFR untuk memenuhi persyaratan keamanan tersebut. Berikut adalah deskripsi dari pelaksanaan tahap – tahap tersebut:

A. Mengidentifikasi Permasalahan Keamanan

Tujuan dari tahap ini adalah untuk mendefinisikan sifat dan ruang lingkungan permasalahan keamanan yang akan diatasi oleh aplikasi yang selanjutnya pada makalah ini disebut Target of Evaluation (TOE). Permasalahan keamanan ini terdiri dari asumsi tentang lingkungan

operasional TOE, ancaman terhadap aset, dan kebijakan keamanan organisasi.

1) Asumsi tentang lingkungan operasional TOE

Asumsi terkait dengan lingkungan operasional TOE dibagai kedalam 3 (tiga) area yaitu perlindungan fisik, personil dan prosedur, dan fungsi teknis di luar TOE. Berikut adalah Tabel II yang mendeskripsikan kondisi yang diasumsikan dalam lingkungan operasional TOE.

TABLE II. ASUMSI LINGKUNGAN OPERASIONAL TOE

Asumsi	Penjelasan
A.FISIK	Disasumsikan bahwa TOE dioperasikan pada lingkungan yang aman dan dikelola dengan baik.
A.PENGGUNA	Diasumsikan bahwa pengguna TOE terpercaya dan terlatih untuk menggunakan TOE.
A.PROSEDUR	Diasumsikan bahwa prosedur penggunaan TOE dan prosedur lain yang dibutuhkan telah dirancang dan diterbitkan oleh pihak yang berwenang..
A.KONEKSI	Diasumsikan bahwa PC/desktop dimana TOE berjalan hanya terkoneksi pada jaringan yang terpercaya.dan terlindungi dari serangan.

2) Ancaman terhadap aset

Aset yang dilindungi oleh TOE adalah password dan data pengguna yaitu data terkait dengan kompetensi personil. Ancaman yang didefinisikan merupakan ancaman yang akan diatasi oleh TOE. Berikut adalah Tabel III yang mendeskripsikan daftar ancaman yang akan diatasi oleh aplikasi SIAGASIKAT.

TABLE III. DAFTAR ANCAMAN

Ancaman	Penjelasan
T. TBKPASWDPENGGUNA	Ancaman ini berusaha untuk mendapatkan *password* pengguna yang sah (baik sebagai *admin*, *viewer*, maupun *author*) agar dapat masuk ke aplikasi SIAGASIKAT. Pada kenyataannya hanya pengguna yang mempunyai *username* dan *password* yang berkesesuaian yang dapat masuk dan menjalankan aplikasi SIAGASIKAT*)*.
T.TBKPASWDDATA	Ancaman ini berusaha untuk mendapatkan *password* sehingga dapat mengakses data aplikasi pada server.
T.AUDITLOG	Ancaman ini berusaha untuk mengakses data log pada server.

3) Kebijakan keamanan organisasi

Kebijakan keamaan organisasi merupakan kebijakan yang harus disusun, diberlakukan dan dipatuhi oleh para pengguna TOE agar TOE berjalan sebagaimana mestinya. Berikut adalah Tabel IV yang mendeskripsikan daftar kebijakan keamanan tersebut.

TABLE IV. DAFTAR KEBIJAKAN KEAMANAN ORGANISASI

Ancaman	Penjelasan
P.AKSES	Kebijakan ini mewajibkan TOE hanya diakses oleh pengguna yang berwenang.
P.GANTIPASSWD	Kebijakan ini mewajibkan pengguna untuk melakukan pergantian *password* secara berkala.
P.ATURPASWD	Kebijakan ini mewajibkan pengguna untuk mengatur *password* yang kuat.

B. Mengidentifikasi Tujuan Keamanan

Tujuan keamanan merupakan pernyataan singkat tentang respon yang dimaksudkan dalam menanggapi permasalahan keamanan yang telah ditetapkan pada langkah sebelumnya. Langkah – langkah dalam mengidentifikasi tujuan keamanan adalah menyusun daftar ancaman, kebijakan dan asumsi. Selanjutnya mengidentifikasi tujuan keamanan untuk lingkungan operasional non-IT. Langkah ketiga adalah mengidentifikasi tujuan keamanan untuk lingkungan operasional IT. Selanjutanya mengidentifikasi tujuan keamanan untuk TOE. Langkah terakhir adalah menyusun tabel rasional antara permasalahan keamanan dan tujuan keamanan.

1) Daftar Ancaman, Kebijakan, dan Asumsi

Ancaman, kebijakan dan asumsi telah didefinisikan pada subbab sebelumnya yaitu mengidentifikasi permasalahan keamanan. Terdapat 3 (tiga) ancaman yaitu T. TBKPASSWDPENGGUNA, T.TBKPASSWDDATA, dan T.AUDITLOG. Telah juga didefinisikan kebijakan yaitu P.AKSES, P.GANTIPASSWORD dan P.ATURPASWD. Terdapat 4 (empat) asumsi yaitu A.FISIK, A.PENGGUNA, A.PROSEDUR, dan A.KONEKSI.

2) Tujuan Keamanan untuk Lingkungan Operasional Non-IT

Tujuan keamanan yang berhubungan dengan Lingkungan Operasional Non-IT adalah tujuan keamanan yang berhubungan dengan metode administrasi atau prosedur yang harus berlaku. Berikut adalah Tabel V yang mendeskripsikan tujuan kemanan yang harus dipenuhi umtuk lingkungan operasional non-IT:

TABLE V. TUJUAN KEAMANAN UNTUK LINGKUNGAN OPERASIONAL NON-IT

Tujuan Keamanan yang Berhubungan dengan Lingkungan Operasional Non-IT	Penjelasan
OE.PENGGUNA	Setiap pengguna TOE tepercaya dan terlatih untuk dapat menggunakan TOE
OE.PROSEDUR	Prosedur penggunaan TOE dan prosedur lain yang dibutuhkan telah dirancang dan diterbitkan oleh pihak yang berwenang

3) Tujuan Keamanan untuk Lingkungan Operasional IT

Tujuan keamanan yang berhubungan dengan Lingkungan Operasional IT adalah tujuan keamanan yang berhubungan dengan IT dimana TOE berjalan. Berikut adalah Tabel VI yang mendeskripsikan tujuan kemanan yang harus dipenuhi umtuk lingkungan operasional IT:

TABLE VI. TUJUAN KEAMANAN UNTUK LINGKUNGAN OPERASIONAL IT

Tujuan Keamanan yang Berhubungan dengan Lingkungan Operasional IT	Penjelasan
OE.FISIK	TOE harus dioperasikan pada lingkungan yang aman dan dikelola dengan baik
OE.KONEKSI	PC/desktop dimana TOE berjalan hanya terkoneksi pada jaringan yang terpercaya dan terlindungi dari serangan

4) Mengidentifikasi Tujuan Keamanan untuk TOE

Berikut adalah Tabel VII yang mendeskripsikan tujuan keamanan yang harus dipenuhi oleh TOE:

TABLE VII. TUJUAN KEAMANAN UNTUK TOE

Tujuan Keamanan untuk TOE	Penjelasan
O.USEROTENTIK	TOE harus menyediakan mekanisme untuk membuktikan bahwa hanya *user* yang otentik yang dapat mengoperasikan aplikasi.
O.ADMIN	TOE harus menyediakan mekanisme untuk seluruh fungsi dan layanan untuk mendukung *admin* dalam mengelola keamanan dari TOE dan membatasi fungsi dan layanan tersebut dari pihak yang tidak berwenang.
O.AUDIT	TOE harus menyediakan laporan sukses dan gagal untuk proses login pengguna aplikasi

5) Menyusun Tabel Rasional Permasalahan Keamanan dan Tujuan Keamanan

Tabel VIII menunjukkan bagaimana tujuan keamanan dari TOE dapat menjawab permasalahan keamanan.

TABLE VIII. TABEL RASIONAL PERMASALAHAN KEAMANAN DAN TUJUAN KEAMANAN

	T.TBKPASWDPENGGUNA	T.TBKPASSWDDATA	T.AUDITLOG	A.FISIK	A.PENGGUNA	A.PROSEDUR	A.KONEKSI	P.AKSES	P.GANTIPASWD	P.ATURPASWD
O.USEROTENTIK	X	X								
O.ADMIN		X	X							
O.AUDIT			X							
OE.PENGGUNA	X	X	X		X					
OE.PROSEDUR						X		X	X	X
OE.FISIK				X						
OE.KONEKSI							X			

Setiap tanda "X" yang diberikan merupakan keterhubungan antara permasalahan keamanan dan tujuan keamanan yang akan mengatasi permasalahan tersebut. Setiap keterhubungan ini kemudian dijustifikasi untuk menyatakan bahwa tujuan keamanan tersebut memang sesuai untuk mengatasi permasalahan keamanan yang berkaitan. Berikut adalah Tabel IX yang menunjukkan justifikasi tersebut:

TABLE IX. JUSTIFIKASI PERMASALAHAN KEAMANAN DAN TUJUAN KEAMANAN

Permasalahan Keamanan	Justifikasi
T.TBKPASWD PENGGUNA	O.USEROTENTIK mensyaratkan bahwa TOE harus menyediakan mekanisme untuk membuktikan bahwa hanya *user* yang otentik yang dapat mengoperasikan aplikasi. Jika *user* memasukkan *username* dan *password* yang tidak berkesesuaian maka *user* tersebut tidak dapat mengoperasikan TOE. OE.PENGGUNA mensyaratkan bahwa pengguna TOE merupakan pengguna yang tepercaya dan terlatih untuk dapat mengoperasionalkan TOE. Dengan demikian T.TBKPASWDPENGGUNA diminimalisir oleh O.USEROTENTIK dan OE.PENGGUNA.
T.TBKPASWD DATA	O.USEROTENTIK mensyaratkan bahwa TOE harus menyediakan mekanisme untuk membuktikan bahwa hanya *user* yang otentik yang dapat mengoperasikan aplikasi. Jika *user* memasukkan *username* dan *password* yang tidak berkesesuaian maka user tersebut tidak dapat mengoperasikan TOE.
	O.ADMIN mensyaratkan TOE untuk menyediakan mekanisme bahwa seluruh fungsi dan layanan untuk mendukung *admin* dalam mengelola keamanan dari TOE dan membatasi fungsi dan layanan tersebut dari pihak yang tidak berwenang. Terutama untuk data pengguna yang *password*nya hanya diketahui oleh *admin* yang berwenang. OE.PENGGUNA mensyaratkan bahwa pengguna TOE merupakan pengguna yang tepercaya dan terlatih untuk dapat mengoperasionalkan TOE. Dengan demikian T.TBKPASWDDATA diminimalisir oleh O.USEROTENTIK, O.ADMIN dan OE.PENGGUNA.
T.AUDITLOG	O.AUDITLOG mensyaratkan bahwa TOE harus menyediakan laporan sukses dan gagal untuk proses login pengguna aplikasi. T.AUDITLOG diminimalisir dengan mekanisme keamanan yang mengimplementasikan penggunaan *password* yang yang menyimpan data kredensial di Php MyAdmin. *Password* ini hanya diketahui oleh *admin* yang berwenang. Hal ini sejalan dengan O.ADMIN yaitu mensyaratkan TOE untuk menyediakan mekanisme bahwa seluruh fungsi dan layanan untuk mendukung *admin* dalam mengelola keamanan dari TOE dan membatasi fungsi dan layanan tersebut dari pihak yang tidak berwenang. OE.PENGGUNA mensyaratkan bahwa pengguna TOE merupakan pengguna yang tepercaya dan terlatih untuk dapat mengoperasionalkan TOE. Dengan demikian T.AUDITLOG diminimalisir oleh O.AUDITLOG, O.ADMIN dan OE.PENGGUNA.
T.TEBAKPASS PHRASE	O.VERIFIKASIPASSPHRASE mensyaratkan bahwa TOE harus menyediakan mekanisme untuk memverifikasi apakah passphrase yang dimasukkan oleh pengguna pada saat melakukan dekripsi merupakan passphrase yang dimasukkan saat enkripsi. Jike pengguna memasukkan passphrase yang salah maka proses dekripsi tidak dapat dijalankan. OE.PENGGUNA mensyaratkan bahwa pengguna TOE merupakan pengguna yang tepercaya dan terlatih untuk dapat mengoperasionalkan TOE. Dengan demikian T.TEBAKPASSPHRASE diminimalisir oleh O.VERIFIKASIPASSPHRASE dan OE.PENGGUNA.
A.FISIK	OE.FISIK mensyaratkan TOE harus dioperasikan pada lingkungan yang aman dan dikelola dengan baik. Sehingga OE.FISIK hanyalah pernyataan kembali dari A.FISIK yaitu OE.FISIK memenuhi persis asumsi A.FISIK

A.PENGGUNA	OE.PENGGUNA mensyaratkan pengguna TOE harus tepercaya dan terlatih untuk dapat menggunakan TOE. Sehingga OE. PENGGUNA hanyalah pernyataan kembali dari A. PENGGUNA yaitu OE. PENGGUNA memenuhi persis asumsi A. PENGGUNA
A.KONEKSI	OE.KONEKSI mensyaratkan PC/desktop dimana TOE berjalan hanya terkoneksi pada jaringan yang terpercaya dan terlindungi dari serangan. Sehingga OE. KONEKSI hanyalah pernyataan kembali dari A. KONEKSI yaitu OE.KONEKSI memenuhi persis asumsi A. KONEKSI.
A.PROSEDUR	OE.PROSEDUR mensyaratkan prosedur penggunaan TOE dan prosedur lain yang dibutuhkan telah dirancang dan diterbitkan oleh pihak yang berwenang, antara lain penggantian *password,* pengelolaan *password* dan akses pengguna terhadap TOE. Sehingga OE. PROSEDUR hanyalah pernyataan kembali dari A. PROSEDUR yaitu OE. PROSEDUR memenuhi persis asumsi A. PROSEDUR juga didukung oleh P.AKSES, P.GANTIPASWD, dan P.ATURPASWD.
P.AKSES	
P.GANTIPASWD	
P.ATURPASWD	

C. Menentukan SFR yang Sesuai Berdasarkan Tujuan Keamanan

Berdasarkan subbab sebelumnya telah didefinsikan 3 (tiga) tujuan keamanan yaitu O.USEROTENTIK, O.ADMIN, dan O.AUDITLOG. Selanjutnya ditentukanlah SFR dari setiap tujuan keamanan.

1) SFR untuk O.USEROTENTIK

SFR yang berkesesuaian adalah *Functional Identification and Authentication (FIA)* dan *Functional Cryptographic Support (FCS*).

a) Functional Identification and Authentication (FIA)

Dalam kelas FIA, SFR yang berkesesuaian adalah:

- *Identification of users before operating ToE (FIA_UID);*
  SFR ini berhubungan karena pengguna akan diidentifikasi terlebih dulu menggunakan *username*-nya sebelum mengoperasikan TOE.
- *Authentication of users before operating ToE (FIA_UAU);*
  SFR ini berhubungan karena pengguna akan diotentikasi terlebih dulu menggunakan *password*-nya sebelum mengoperasikan TOE

b) Functional Cryptographic Support (FCS)

Dalam kelas FCS, SRF yang berhugungan adalah *cryptographic operation* yaitu FCS_COP. SFR ini berhubungan karena TOE mengimplementasikan algorirma kriptografi yaitu MD5 dalam proses pengamanan *password*. Jadi nilai yang disimpan oleh TOE adalah *hash* dari *password* tersbeut.

2) SFR untuk O.ADMIN

SFR yang berhubungan dengan O.ADMIN adalah *Functional Management (FMT).* SFR yang berkaitan adalah sebagai berikut:

- *Specification of management function (FMT_SMF);*
  SFR ini berhubungan karena *admin* dapat mengelola pengguna dan data yang tersimpan dalam aplikasi.
- *Maintenance of security roles (FMT_SMR);*
  SFR ini berhubungan karena aplikasi mengelola 3 (tiga) jenis *role* yaitu *admin, author,* dan *viewer*.

3) SFR untuk O.AUDIT

SFR yang berhubungan dengan O.AUDIT adalah *Functional Audit (FAU)* yaitu FAU_GEN (*Security audit data generation*). Aplikasi ini membangkitkan rekaman audit untuk setiap proses login pengguna baik sukses maupun gagal juga FAU_SAR (*Security review*) karena hanya admin yang berwenang yang dapat mengakses data log tersebut.

Dari hasil penentuan SFR yang telah ditentukan sebelumnya, maka berikut adalah pernyataan (*statement*) SFR sesuai dengan SNI ISO/IEC 15408:2014.

- ***FIA_UID.1.1 Timing of identification***
  The TSF shall allow [Login into ToE] on behalf of the user to be performed before the user is identified.
- ***FIA_UID.1.2 User identification before any action***
  The TSF shall require each user to be successfully identified before following any other TSF-mediated actions on behalf of that user.
- ***FIA_UAU.2 User authentication before any action***
  The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
- ***FCS_COP .1 Cryptographic operation (password verification)***
  The TSF shall perform generation of password verification in accordance with a specified cryptographic algorithm MD5 and cryptographic key sizes - that meet the following: RFC 1321.
- ***FAU_GEN.1.1 Audit data generation The TSF shall be able to generate an audit record of the following auditable events:***
  a) Start-up and shutdown of the audit functions
  b) All auditable events for the [not specified] level of audit; and [assignments:login process]
- ***FAU_GEN.1.2 Audit data generation***
  a) The TSF shall record within each audit record at least the following information:
  b) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
- ***FAU_SAR 1.1 Audit Review***
  The TSF shall provide [admin] with the capability to read [audit log] from the audit records.

- ***FAU_SAR.1.1 Audit Review***

  The TSF shall provide the audit records in a manner suitable for the user to interpret the information
- ***FMT_SMF.1 Security of Management Function***

  The TSF shall be capable of performing the following management function: [create, read, update, delete of clients account]
- ***FMT_SMR.1.1Security Roles***

  The TSF shall maintain the roles [Admin, Author, Viewer].

- ***FMT_SMR.1.2 Security Roles***

  The TSF shall be able to associate users with roles.

V. KESIMPULAN

Telah dilakukan perancangan spesifikasi keamanan pada aplikasi SIAGASIKAT versi 1.0.0 berdasarkan SNI ISO/IEC 15408:2014. Spesifikasi keamanan yang berhasil dirancang untuk aplikasi tersebut adalah *FIA_UID Timing of identification, FIA_UAU User identification before any action, FCS_COP Cryptographic operation, FAU_GEN Audit data generation, FAU_SAR Audit Review, FMT_SMF Security of management function, and FMT_SMR Security Roles.*

REFERENCES

[1] K. H. d. HAM, "Jaringan Dokumentasi dan Informasi Hukum BSSN," 23 May 2017. [Online]. Available: https://jdih.bssn.go.id/arsip-hukum/perpres-nomor-53-tahun-2017-tentang-badan-siber-dan-sandi-negara. [Diakses pada 12 September 2019].

[2] B. S. d. S. Negara, "Jaringan Dokumentasi dan Informasi Hukum BSSN," 31 January 2017. [Online]. Available: https://jdih.bssn.go.id/arsip-hukum/peraturan-badan-siber-dan-sandi-negara-nomor-2-tahun-2018-tentang-organisasi-dan-tata-kerja-badan-siber-dan-sandi-negara. [Diakses pada 12 September 2019].

[3] B. S. d. S. Negara, "Jaringan Dokumentasi dan Informasi Hukum BSSN," 29 December 2019. [Online]. Available: https://jdih.bssn.go.id/arsip-hukum/peraturan-badan-siber-dan-sandi-negara-nomor-15-tahun-2019-tentang-penyelenggaraan-skema-common-criteria-indonesia. [Diakses pada 2 March 2020].

[4] B. University, "Tahapan - tahapan dalam SDLC," Binus University, 14 July 2016. [Online]. Available: http://scdc.binus.ac.id/himsisfo/2016/07/tahapan-tahapan-dalam-sdlcsistem-development-life-cycle/. [Diakses pada 2019 September 2019].

[5] M. Dosen, "Perbedaan Kebutuhan Fungsional dan Non Fungsional, Lengkap Contoh dan Penjelasan," Materi Dosen, 22 March 2017. [Online]. Available: http://www.materidosen.com/2017/03/perbedaan-kebutuhan-fungsional-dan-non.html. [Diakses pada 12 September 2019].

[6] F. A. Esti Rahmawati Agustina, "Perancangan Spesifikasi Keamanan Kontrol Akses pada Aplikasi Layanan Informasi di Lingkungan Instansi Pemerintah," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 6, no. 2, p. 195, 2019.

[7] F. A. E. R. Alfred Saut S, "Perancangan Spesifikasi Keamanan pada SIFER Berdasarkan SNI ISO/IEC 15408:2014 - Teknologi Informasi - Teknik Keamanan - Kriteria Evaluasi Keamanan Teknologi Informasi," in The 11th Conference on Information Technology and Electrical Engineering (CITEE 2019, Jogjakarta, 2019).

[8] E.R. A.S. M.C. Irma Fitriani, "Perancangan Spesifikasi Keamanan pada Aplikasi Sistem Kompetensi Personil LSPro (SIKOMPRONAS) Versi 1.0.0 Berdasarkan SNI ISO/IEC 15408:2014," in 2nd SEMINASTIKA 2019. Avaiable on https://journal.universitasmulia.ac.id/index.php/seminastika/article/view/93.

[9] B. S. Nasional, "SNI ISO/IEC 15408:2014," Badan Standardisasi Nasional, Jakarta, 2014.

[10] B. S. Nasional, "ISO/IEC TR 15446:2017," ISO Central Secretariat, Jakarta, 2017.