Seminar Nasional Sains dan Teknologi Informasi (SENSASI)
SENSASI 2021

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 108 - 116

Perancangan Spesifikasi Fungsi Keamanan Aplikasi *File Encryption (Filtion)* Versi 1.0.0 berdasarkan SNI ISO/IEC 15408:2014

Yhufi Swastantri Gustiviana, Esti Rahmawati Agustina*

Badan Siber dan Sandi Negara, Jakarta, Indonesia
Email: [1]yhufi.swastantri@bssn.go.id, [2,*]esti.rahmawati@bssn.go.id

Abstrak

Laboratorium Pengujian BSSN mempunyai peran yang signifikan sebagai pelaksana proses determinasi atau pengujian. Untuk mendapatkan kepercayaan pelanggan dan pengakuan secara formal, Lab uji harus sesuai dengan SNI ISO/IEC 17025:2017. Dalam pemenuhan persyaratan tersebut, salah satu hal yang dikembangkan yaitu pemenuhan sistem informasi berupa *file encryption* untuk pengelolaan, pengendalian informasi dan data Laboratorium secara elektronik. Metode pengembangan aplikasi menerapkan *framework SDLC* yang mana dilakukan pendefinisian kebutuhan fungsional dan non-fungsional pada tahap perencanaan dan analisis kebutuhan. Paper ini membahas perancangan fungsi keamanan *file encryption* berbasis klien-server berdasarkan SNI ISO/IEC 15408:2014. Sedangkan metode penyusunan spesifikasi fungsi keamanan berdasar pada ISO/IEC TR 15446:2017. Perancangan ini menghasilkan spesifikasi fungsi keamanan yang diantaranya meliputi *Functional Security Audit (FAU), Functional Cryptographic Support (FCS), Functional Identification and Authentication (FIA), Functional Security Management (FMT), Functional Protection of the TSF (FPT), dan Functional TOE Access (FTA).*

Kata Kunci: *File Encryption; Spesifikasi Fungsi Keamanan; SNI ISO/IEC 15408:2014; ISO/IEC TR 15446:2017*

1. PENDAHULUAN

Laboratorium Pengujian (Lab Uji) Badan Siber dan Sandi Negara (BSSN) adalah organisasi inklusif di BSSN yang menyelenggarakan evaluasi produk keamanan perangkat teknologi informasi sesuai dengan Skema *Common Criteria* Indonesia (SCCI) [1]. Untuk mendapatkan kepercayaan pelanggan dan pengakuan secara formal, Lab Uji harus terakreditasi oleh pihak independen yang menyelenggarakan layanan akreditasi untuk Lembaga Penilaian Kesesuaian (LPK) [2], [3]. Dalam hal ini, akreditasi Lab Uji dilakukan oleh Komite Akreditasi Nasional (KAN) berdasarkan SNI ISO/IEC 17025:2017 tentang Persyaratan Umum Kompetensi Laboratorium Pengujian dan Laboratorium Kalibrasi [4].

Salah satu persyaratan proses yang tercantum pada klausul 7.11 yaitu tentang Pengendalian Data dan Manajemen Informasi [4]. Pengembangan persyaratan pada klausul ini dapat berupa pengelolaan pengendalian data dan informasi Laboratorium dengan memanfaatkan Teknologi Informasi (TI). Salah satu upaya Lab Uji BSSN dalam pemenuhan klausul tersebut adalah dengan mengembangkan aplikasi *File Encryption (Filtion)* versi 1.0.0 yang dapat mendukung pengelolaan laboratorium secara elektronik.

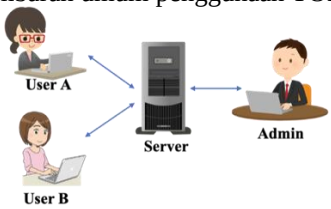
Metode pengembangan aplikasi menerapkan *framework System Development Life Cycle* (SDLC). Identifikasi kebutuhan fungsional dan non-fungsional aplikasi disusun pada tahap perencanaan dan analisis. Pada tahap ini, identifikasi spesifikasi keamanan aplikasi merupakan salah satu contoh dari identifikasi kebutuhan non-fungsional aplikasi [5]. Spesifikasi keamanan ini menjadi bagian yang penting dari suatu aplikasi karena data pada aplikasi harus diamankan dari pihak yang tidak berwenang.

Dalam pengembangannya, penyusunan spesifikasi keamanan mengacu pada standar nasional SNI ISO/IEC 15408:2014 tentang kriteria evaluasi keamanan suatu produk, sistem atau aplikasi. Adapun penelitian pendahulu yang menerapkan standar tersebut, diantaranya penelitian [6] merancang spesifikasi keamanan pada akses control. Selain itu penelitian [7] menerapkannya pada aplikasi *file encryption* yang bersifat *stand-alone* dan pada [8]–[10] pada web aplikasi. Karya tulis ini akan mendeskripsikan perancangan spesifikasi fungsi keamanan aplikasi *File Encryption* (*Filtion)* versi 1.0.0 untuk pengelolaan pengendalian data dan informasi Lab Uji BSSN berdasarkan SNI ISO/IEC 15408:2014.

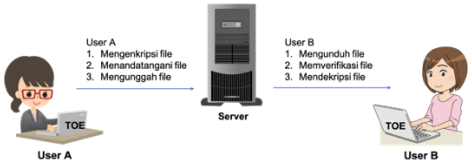
2. LANDASAN TEORI

2.1 Aplikasi *File Encryption (Filtion)* versi 1.0.0

Aplikasi *File Encryption (Filtion) versi 1.0.0* yang selanjutnya disebut sebagai *Target of Evaluation* (TOE) merupakan aplikasi enkripsi dan dekripsi file untuk melindungi data dari pihak yang tidak berwenang berupa pencurian dan modifikasi data. Adapun arsitektur yang diterapkan berbasis *client-server*. Gambar 1 menunjukkan arsitektur TOE, sedangkan gambaran umum penggunaan TOE ditampilkan pada gambar 2.



Gambar 1. *Arsitektur TOE*



Gambar 2*. Gambaran Umum Penggunaan TOE*

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 108 - 116

Pengguna dapat mengakses TOE hanya jika terhubung dengan jaringan internet. Pengolahan dan penyimpanan data pengguna TOE dilakukan oleh Server. Pengguna sesuai dengan *role* yang dimiliki dapat mengenkripsi dan mendekripsi file serta melakukan *signing* dan verifikasi file. Terdapat beberapa fitur keamanan yang diterapkan untuk mendukung tujuan TOE, diantaranya yaitu:

a. Penerapan Mekanisme *Login*
Tujuan penggunaan layanan ini yaitu untuk memberikan jaminan bahwa hanya pengguna yang sah yang dapat mengakses TOE, yang mana username dan password yang diinputkan oleh pengguna saling berkesesuaian.

b. Pembagian Role sebagai User dan Admin
Terdapat 2 (dua) peran dalam TOE, yaitu *Admin* dan *User*. *Admin* merupakan *role* yang mempunyai kewenangan untuk menambah, mengubah dan menghapus klien. Sedangkan *User* merupakan *role* yang dapat melakukan enkripsi dan *signing* file, serta mendekripsi dan verifikasi file.

c. Implementasi Algoritma Kriptografi
Implementasi algoritma kriptografi melekat pada fitur-fitur yang disediakan oleh TOE. Adapun algoritma kriptografi yang diimplementasikan sebagai berikut:

1. Pada fitur *login*, mekanisme perlindungan *password* menerapkan implementasi SHA 256 bit [9];
2. Pada fitur enkripsi dan dekripsi file, TOE mengimplementasikan algoritma kriptografi AES 256 bit. Sedangkan pada proses pembangkitan kunci enkripsi dan dekripsi menerapkan *Password Based Key Derivation Function (PBKDF)2* dengan inputan *passphrase* dari *user* [7]; dan
3. Pada fitur *signing file*, diimplementasi algoritma *hash function* yaitu SHA 256 dan algoritma RSA 2048 bit untuk melindungi integritas file [10].

2.2 SNI ISO/IEC 15408:2014 tentang Kriteria Evaluasi Keamanan Teknologi Informasi

SNI ISO/IEC 15408:2014 adalah standar nasional yang menjelaskan kriteria evaluasi keamanan dan spesifikasi keamanan suatu produk keamanan perangkat TI. Dalam standar tersebut, spesifikasi keamanan yang harus dimiliki suatu produk keamanan perangkat TI disebut sebagai *Security Functional Requirement (*SFR). Adapun spesifikasi keamanan ini terdiri 11 (sebelas) kelas keamanan yang masing masing menjelaskan tujuan keamanan tertentu [11], diantaranya yaitu identifikasi dan otentikasi, dukungan kriptografi, manajemen keamanan, audit keamanan dan lain sebagainya. Spesifikasi detil untuk memenuhi kesesuaian dengan tujuan keamanan suatu TOE dijelaskan pada komponen dari setiap kelas.

3. METODOLOGI PENELITIAN

Pada penelitian ini, perancangan *Security Functional Requirement (SFR)* merujuk pada ISO/IEC TR 15446 tentang panduan penyusunan *Protection Profile* dan *Security Target* [12], dengan tahapan-tahapan sebagai berikut:

a. Mendefinisikan permasalahan keamanan.
b. Mengidentifikasi tujuan keamanan.
c. Mendefinisikan spesifikasi keamanan untuk memenuhi tujuan keamanan.
d. Memilih spesifikasi keamanan untuk memenuhi persyaratan keamanan berdasar pada SNI ISO/IEC 15408: 2014.

4. HASIL DAN PEMBAHASAN

Pada subbagian ini akan menjelaskan tahapan-tahapan penentuan SFR sesuai dengan yang disebutkan pada subbagian 3, yaitu sebagai berikut:

4.1 Mendefinisikan Permasalahan Keamanan

Permasalahan keamanan dapat didefinisikan dari sifat dan ruang lingkup yang akan dicegah dan/atau ditanggulangi oleh TOE. Adapun hal-hal yang didefinisikan terdiri dari asumsi, ancaman dan kebijakan keamanan organisasi.

4.1.1 Asumsi terhadap Lingkungan Operasional TOE

Pendefinisian asumsi berfokus pada fungsi teknis di luar TOE,kondisi personil dan pemenuhan prosedur, serta perlindungan fisik TOE seperti yang tercantum pada tabel 1 berikut.

Tabel 1. Asumsi Lingkungan Operasional TOE

Asumsi	Deskripsi
A.KONEKSI	Diasumsikan PC/desktop yang digunakan untuk mengoperasionalkan TOE aman hanya jika terkoneksi pada jaringan yang terlindung dari serangan dan terpercaya
A.TIMESTAMP	Diasumsikan bahwa Server menyediakan stempel waktu terpusat yang terpercaya untuk TOE.
A.PASSPHRASE	Diasumsikan bahwa passphrase memenuhi persyaratan keamanan dan didistribusikan secara offline dengan kurir terpercaya.
A.PROSEDUR	Diasumsikan bahwa pihak yang berwenang telah menyusun dan menerbitkan prosedur-prosedur yang dibutuhkan untuk mengoperasionalkan TOE
A.PENGGUNA	Diasumsikan bahwa TOE dioperasionalkan oleh pengguna yang terlatih dan terpercaya untuk mengoperasionalkan TOE tersebut.

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 108 - 116

Asumsi	Deskripsi
A.TUNGGAL	Diasumsikan bahwa TOE berjalan pada mesin pengguna tunggal dengan akses yang dilindungi oleh lingkungan TOE, yaitu hanya pengguna yang berwenang dari lingkungan TOE yang dapat mengakses TOE
A.PLATFORM	Diasumsikan bahwa TOE bergantung pada platform dan perangkat keras yang dapat dipercaya
A.PHYSICAL	Diasumsikan bahwa lingkungan operasional TOE aman dan dikelola dengan baik.

4.1.2 Ancaman terhadap Asset yang akan Diatasi oleh TOE

Aset TOE terdiri dari password, kunci, data pengguna, integritas data dan log data. Pendefinisian ancaman ini ditujukan untuk mengidentifikasi kapabilitas TOE dalam mengatasi beberapa ancaman yang mungkin terjadi seperti yang ditunjukkan pada Tabel 2 berikut.

Tabel 2. Ancaman terhadap asset

Ancaman	Deskripsi
T.TBKPSWD	Penyerang berusaha mendapatkan password pengguna (admin dan/atau user) yang sah untuk dapat mengoperasionalkan TOE. Username dan password yang berkesesuaian hanya dimiliki oleh pengguna yang sah untuk dapat mengoperasionalkan TOE.
T.AUDIT_LOG	Penyerang berusaha untuk mengakses data log pada server
T.DISCLOSURE	Penyerang berusaha untuk mencuri komunikasi pada jaringan untuk mendapatkan asset yang diproses dan dikirim menggunakan TOE antara client dan server. Penyerang berusaha mendekripsi file sehingga penyerang dapat membaca isinya.
T.TEMPER	Ancaman ini berusaha untuk mengkompromikan integritas data dengan mengganti atau memodifikasi asset
T.AKUN	Penyerang mencoba untuk mengorespondensikan *username* dan *password* pengguna TOE untuk dapat mengoperasionalkan TOE sebagai pengguna yang sah.

4.1.3 Kebijakan Keamanan Organisasi

Tabel 3 mendeskripsikan daftar kebijakan keamanan organisasi untuk TOE.

Tabel 3. Kebijakan Keamanan Organisasi

Kebijakan	Deskripsi
P.ADMIN	Pernyataan yang menegaskan bahawa TOE hanya dikelola oleh administrator yang berwenang
P.AKSES	Pernyataan yang menegaskan bahwa hanya pengguna yang berwenang yang memiliki akses untuk operasional TOE.
P.GANTIPWD	Pernyataan yang menegaskan bahwa pengguna harus melakukan mekanisme perubahan password secara periodik
P.ATURPWD	Pernyataan yang menegaskan bahwa pengguna harus menerapkan pengelolaan password untuk kategori kuat

4.2 Mengidentifikasi Tujuan Keamanan

Tanggapan terhadap permasalahan keamanan dapat dinyatakan sebagai tujuan keamanan. Pada tahapan ini dilakukan identifikasi terhadap tujuan keamanan untuk lingkungan operasional non-IT dan IT, serta tujuan keamanan untuk TOE. Tahapan akhir dari bagian ini adalah dengan disusunnya tabel rasional yang mengkorespondensikan permasalahan keamanan terhadap tujuan keamanan.

4.2.1 Daftar Asumsi, Ancaman dan Kebijakan

Asumsi, ancaman dan kebijakan keamanan organisasi sebagaimana yang telah didefinisikan pada subbab 4.1.

4.2.2 Tujuan Keamanan untuk Lingkungan Operasional Non-IT

Identifikasi yang dilakukan mencakup hal-hal yang berkaitan dengan prosedur dan metode administrasi TOE. Tabel 4 mendeskripsikan tujuan keamanan untuk lingkungan operasional non-IT.

Tabel 4. Tujuan Keamanan untuk Lingkungan Operasional Non-IT

Tujuan Keamanan	Deskripsi
OE.PROSEDUR	Pihak yang berwenang menyusun dan menerbitkan prosedur prosedur-prosedur yang dibutuhkan untuk mengoperasionalkan TOE
OE.PENGGUNA	Pengguna TOE telah terlatih dan terpercaya untuk mengeoperasionalkan TOE tersebut.

4.2.3 Tujuan Keamanan untuk Lingkungan Operasional IT

Identifikasi yang dilakukan mencakup lingkup dan/ atau spesifikasi operasional TOE. Tabel 5 menyatakan tujuan keamanan untuk lingkungan operasional IT.

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 108 - 116

Tabel 5. Tujuan Keamanan untuk Lingkungan Operasional IT

Tujuan Keamanan	Deskripsi
OE.KONEKSI	PC/desktop yang digunakan untuk mengoperasionalkan TOE aman hanya jika terkoneksi pada jaringan yang terlindung dari serangan dan terpercaya
OE.TIMESTAMP	Server menyediakan stempel waktu terpusat yang terpercaya untuk TOE.
OE.PASSPHRASE	Passphrase memenuhi persyaratan keamanan dan didistribusikan secara offline dengan kurir terpercaya.
OE.TUNGGAL	Setiap pengguna bertanggung jawab atas TOE yang dijalankan pada mesin pengguna tunggal dengan akses yang dilindungi oleh lingkungan TOE, yaitu hanya pengguna yang berwenang dari lingkungan TOE yang dapat mengakses TOE
OE.PLATFORM	TOE berjalan pada platform dan perangkat keras yang dapat dipercaya
OE.PHYSICAL	TOE berada pada lingkungan operasional yang dikelola dengan baik dan aman

4.2.4 Tujuan Keamanan untuk TOE

Identifikasi tujuan keamanan untuk TOE disajikanpada tabel 6 berikut.

Tabel 6. Tujuan Keamanan untuk TOE

Tujuan Keamanan	Deskripsi
O.USEROTNK	TOE hanya dapat dioperasionalkan oleh user yang terotorisasi sebagai pengguna yang sah yang dibuktikan melalui mekanisme verifikasi
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 mampu menyajikan data yang berisi laporan pengguna saat melakukan proses login baik itu sukses maupun gagal
O.RAHASIA	TOE memiliki mekanisme untuk melindungi informasi dari file yang ditransmisikan sedemikian rupa sehingga isinya dilindungi kerahasiaannya dan hanya dapat diakses oleh pengguna yang berwenang
O.SIGNING	TOE memiliki mekanisme untuk menjamin integritas file yang ditransmisikan (baik itu mengganti atau memodifikasi konten)
O.PWD	TOE harus menyediakan mekanisme bahwa password yang digunakan untuk melindungi akses TOE cukup kuat
O.SESSION	TOE harus menyediakan mekanisme untuk mengakhiri *session* login setelah interval waktu yang diizinkan

4.2.5 Menyusun Matriks Rasional Keamanan dan Tujuan Keamanan

Tabel 7 menyajikan korespondensi tujuan keamanan dan bagaimana hal tersebut dapat menyatakan bahwa pemasalahan keamanan yang diidentifikasi telah diatasi oleh tujuan keamanan tersebut

Tabel 7. *Tabel Rasional Permasalahan Keamanan dan Tujuan Keamanan*

	T.TBKPSWD	T.AUDIT_LOG	T.DICLOSURE	T.TEMPER	T.AKUN	PADMIIN	P.AKSES	P.GANTI PWD	P.ATURPWD	A.KONEKSI	A.TIMESTAMP	A.PASSPHRASE	A.PROSEDUR	A.PENGGUNA	A.TUNGGAL	A.PLATFORM	A.FPHYSICAL
O. USEROTNK	✓				✓												
O. ADMIN		✓				✓											
O. AUDIT		✓															
O. RAHASIA			✓														
O.SIGNING				✓													
O. PWD					✓												
O. SESSION					✓												
OE.KONEKSI										✓							
OE.TIMESTAP											✓						
OE.PASSPHRASE												✓					
OE. PROSEDUR						✓	✓	✓	✓				✓				
OE. PENGGUNA	✓	✓												✓			
OE.TUNGGAL															✓		
OE.PLATFORM																✓	

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 108 - 116

OE.PHYSICAL																	✓

Korespondensi antara permasalahan keamanan dan tujuan keamana ditunjukkan dengan penggunaan tanda "✓". Hal ini merupakan justifikasi bahwa suatu permasalahan keamanan diatasi dengan sesuai oleh tujuan keamanan yang berkaitan. Tabel 8 menyajikan justifikasi permasalahan keamanan terhadap tujuan keamanan.

Tabel 8. Justifikasi Permasalahan Keamanan terhadap Tujuan Keamanan

Permasalahan Keamanan	Justifikasi
T.TBKPSWD	O.USEROTNK mewajibkan TOE hanya dapat dioperasionalkan oleh user yang terotorisasi sebagai pengguna yang sah yang dibuktikan melalui mekanisme verifikasi. Jika username dan password yang dimasukkan oleh pengguna tidak berkesesuaian, maka TOE tidak dapat dioperasionalkan. OE. PENGGUNA mensyaratkan bahwa setiap telah terlatih dan terpercaya untuk mengeoperasionalkan TOE. Maka O.USEROTNK dan OE.PENGGUNA dapat mencegah/meminimalisir terjadinya T.TBKPWD
T.AUDIT_LOG	O.ADMIN mensyaratkan bahwa 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 mensyaratkan bahwa TOE mampu menyajikan data yang berisi laporan pengguna saat melakukan proses login baik itu sukses maupun gagal, file yang dienkripsi dan ditandatangan serta file yang diverifikasi dan didekripsi. OE. PENGGUNA mensyaratkan bahwa setiap telah terlatih dan terpercaya untuk mengeoperasionalkan TOE. Maka O.ADMIN, O.AUDIT dan OE.PENGGUNA dapat mencegah/meminimalisir terjadinya T.AUDITLOG
T.DISCLOSURE	O.RAHASIA mewajibkan TOE harus memiliki mekanisme untuk melindungi informasi dari file yang ditransmisikan sedemikian rupa sehingga isinya dilindungi kerahasiaannya dan hanya dapat diakses oleh pengguna yang berwenang. Maka O.RAHASIA dapat mencegah/meminimalisir terjadinya T.DISCLOSURE
T.TEMPER	O.SIGNING mensyaratkan bahwa TOE harus menyediakan mekanisme yang menjamin integritas file yang ditransmisikan (baik itu mengganti atau memodifikasi konten) Maka O.SINGING dapat mencegah/meminimalisir terjadinya T.TEMPER
T.AKUN	O.USEROTNK mensyaratkan bahwa TOE hanya dapat dioperasionalkan oleh user yang terotorisasi sebagai pengguna yang sah yang dibuktikan melalui mekanisme verifikasi. Jika username dan password yang dimasukkan oleh pengguna tidak berkesesuaian, maka TOE tidak dapat dioperasionalkan. O.PWD mewajibkan TOE harus memiliki mekanisme yang menyatakan bahwa password yang digunakan untuk melindungi akses TOE cukup kuat O.SESSION mensyaratkan bahwa TOE harus menyediakan mekanisme untuk mengakhiri *session* login setelah interval waktu yang diizinkan Maka O.USEROTNK, O.PWD dan O.SESSION dapat mencegah/meminimalisir terjadinya T.AKUN
P.ADMIN	O.ADMIN mensyaratkan bahwa 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 OE.PROSEDUR mensyaratkan bahwa TOE pihak yang berwenang dan/atau developer menyusun dan menerbitkan prosedur-prosedur yang dibutuhkan untuk mengoperasionalkan TOE, antara lain penggantian *password,* pengelolaan *password* dan akses pengguna terhadap TOE.
P.AKSES P.GANTIPWD P.ATURPWD A.PROSEDUR	OE.PROSEDUR mensyaratkan bahwa TOE pihak yang berwenang dan/atau developer menyusun dan menerbitkan prosedur-prosedur yang dibutuhkan untuk mengoperasionalkan TOE, antara lain penggantian *password,* pengelolaan *password* dan akses pengguna terhadap TOE. Dengan demikian maka P.AKSES, P.GANTIPWD dan P.ATURPWD mendukung A.PROSEDUR sehingga asumsi tersebut persis memenuhi OE.PROSEDUR. A PROSEDUR dinyatakan kembali sebagai OE.PROSEDUR
A.KONEKSI	OE.KONEKSI mewajibkan PC/desktop yang digunakan untuk mengoperasionalkan TOE aman hanya jika terkoneksi pada jaringan yang terlindung dari serangan dan terpercaya. Dengan demikian maka A.KONEKSI persis memenuhi OE.KONEKSI, sehingga A.KONEKSI dinyatakan kembali sebagai OE.KONEKSI
A.TIMESTAMP	OE.TIMESTAMP mensyaratkan bahwa Server menyediakan stempel waktu terpusat yang

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 108 - 116

	terpercaya untuk TOE. Dengan demikian maka A. TIMESTAMP persis memenuhi OE. TIMESTAMP, sehingga A. TIMESTAMP dinyatakan kembali sebagai OE. TIMESTAMP
A.PASSPHRASE	OE.PASSPHRASE mewajibkan passphrase memenuhi persyaratan keamanan dan didistribusikan secara offline dengan kurir terpercaya. Dengan demikian maka A.PASSPHRASE persis memenuhi OE.PASSPHRASE, sehingga A.PASSPHRASE dinyatakan kembali sebagai OE.PASSPHRASE
A.PENGGUNA	OE. PENGGUNA mensyaratkan bahwa setiap telah terlatih dan terpercaya untuk mengeoperasionalkan TOE. Dengan demikian maka A.PENGGUNA persis memenuhi OE.PENGGUNA, sehingga A.PENGGUNA dinyatakan kembali sebagai OE.PENGGUNA
A.TUNGGAL	OE. TUNGGAL mensyaratkan bahwa TOE berjalan pada mesin pengguna tunggal dengan akses yang dilindungi oleh lingkungan TOE, yaitu hanya pengguna yang pengguna yang memiliki otorisasi TOE yang dapat mengakses TOE. Dengan demikian maka A.TUNGGAL persis memenuhi OE.TUNGGAL, sehingga A.TUNGGAL dinyatakan kembali sebagai OE.TUNGGAL
A.PLATFORM	OE.PLATFORM mensyaratkan bahwa TOE bergantung pada platform dan perangkat keras yang dapat dipercaya. Dengan demikian maka A.PLATFORM persis memenuhi OE. PLATFORM, sehingga A.PLATFORM dinyatakan kembali sebagai OE. PLATFORM
A.PHYSICAL	OE.PHYSICAL mewajibkan TOE berada pada lingkungan operasional yang dikelola dengan baik dan aman. Dengan demikian maka A.PHYSICAL persis memenuhi OE.PHYSICAL, sehingga A.PHYSICAL dinyatakan kembali sebagai OE. PHYSICAL

4.3 Menentukan SFR yang sesuai dengan Tujuan Keamanan

Didefinisikan 7 (tujuh) tujuan keamanan, yaitu O.USEROTNK, O.ADMIN, O.AUDIT, O.RAHASIA, O.SIGNING, O.PWD, dan O.SESSION. Kemudian, berikut adalah SFR yang ditentukan untuk tujuan keamanan yang telah diidentifikasi.

a. SFR untuk O.USEROTNK
   SFR yang bersesuaian diantaranya yaitu *Functional Identification and Authentication (FIA)* dan *Functional Cryptographic Support (FCS).*
   1. *Functional Identification and Authentication (FIA)*
      Dalam kelas FIA, SFR yang berkesesuaian adalah:
      a) *Identification of users before operating TOE (FIA_UID)*
      SFR ini berhubungan karena pengguna akan diidentifikasi terlebih dahulu menggunakan *username*-nya sebelum mengoperasikan TOE
      b) *Authentication of users before operating TOE* (FIA_UAU)
      SFR ini berhubungan karena pengguna akan diotentikan terlebih dahulu menggunakan *password-nya* sebelum mengoperasikan TOE
   2. *Functional Cryptographic Support (FCS)*
      SFR yang berkaitan yaitu *cryptopgraphic operation* yaitu FCS_COP. SFR ini berhubungan karena TOE mengimplementasikan algoritma kriptografi yaitu SHA-256 dalam proses pengamanan *password.* Jadi nilai yang disimpan oleh TOE adalah *hash* dari *password* tersebut.

b. SFR untuk O.ADMIN
   SFR yang bersesuaian adalah *Functional Management* (FMT), diantaranya yaitu:
   1. *Specification of management function (FMT_SMF)*
      SFR ini berhubungan karena admin dapat mengelola pengguna.
   2. *Maintenance of security roles (FMT_SMR)*
      SFR ini berhubungan karena apliasi mengelola 2 (dua) jenis *role* yaitu *admin* dan *user.*

c. SFR untuk O.AUDIT
   SFR yang bersesuaian adalah *Functional Audit (FAU)* yaitu FAU_GEN (*Security audit data generation).* TOE akan menghasilkan catatan audit yang memuat informasi gagal ataupun suksesnya proses login yang dilakukan oleh pengguna, sehingga file yang dienkripsi dan di-*signing*, serta file yang diverifikasi dan didekripsi sesuai FAU_SAR (*Security review*)

d. SFR untuk O.RAHASIA
   SFR yang bersesuaian adalah *Functional Cryptographic (FCS)* dan *Functional Protection of TSF (FPT)*
   1. *Functional Cryptographic (FCS)*
      SFR yang berkesesuaian diantaranya yaitu:
      a) *Cryptographic Key Management (FCS_CKM)*

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 108 - 116

SFR ini berhubungan karena TOE mengimplementasikan algoritma PBKDF2 untuk membangkitkan kunci enkripsi dan dekripsi.

b) *Cryptographic Operation (FCS_COP)*
SFR ini berhubungan karena TOE mengimplementasikan algoritma kriptografi AES-256

2. *Functional Protection of TSF (FPT)*
Pada kelas FPT, SFR yang besesuaian adalah *Internal TOE TSF Data Transfer (*FPT_ITT). SFR ini berhubungan karena menggunakan protokol komunikasi *Hypertext Transfer Protocol Secure (https).*

e. SFR untuk O.SIGNING
SFR yang bersesuaian diantaranya yaitu *Cryptographic Operation (FCS_COP).* SFR ini berhubungan karena TOE mengimplementasikan algoritma kriptografi yaitu SHA 256 untuk *hashing* dan RSA 2048 dalam proses pembangkitan kunci publik dan privat yang selanjutnya kunci privat inilah yang digunakan dalam proses *signing.*

f. SFR untuk O.PWD
SFR yang bersesuaian adalah *Functional Identification and Authentication (FIA)* yaitu *Spesicification of Secrets* (FIA_SOS). TOE menerapkan 8 karakter sebagai minumum panjang password.

g. SFR untuk O.SESSION
SFR yang bersesuaian adalah *Functional TOE Access (FTA)* yaitu *Session Locking and Termination (FTA_SSL).* TOE menerapkan *interactive session* selama 30 menit.

4.4 Menentukan Spesifikasi Keamanan untuk Memenuhi Persyaratan Keamanan

Dari hasil penentuan SFR yang telah ditentukan pada subbab 4.3, pernyataan SFR yang berkesuaian dengan SNI ISO/IEC 15408:2014 sebagai berikut:

1. *FIA_UID 1. Timing of Identification*
   a. FIA_UID.1.1
      TSF harus mengizinkan **[Login ke TOE]** atas nama pengguna yang dilakukan sebelum pengguna diidentifikasi.
   b. FIA UID.1.2
      SF harus mewajibkan setiap pengguna untuk berhasil diidentifikasi sebelum memperbolehkan tindakan TSF lainnya atas nama pengguna tersebut.
2. *FIA_UID.2 User Identification before any action*
   FIA_UID.2.1
   TSF harus mewajibkan setiap pengguna untuk berhasil diidentifikasi sebelum memperbolehkan tindakan TSF lainnya atas nama pengguna tersebut.
3. *FIA_UAU 1. Timing of authentication*
   a. FIA_UAU.1.1
      TSF harus mengizinkan **[Login ke TOE]** atas nama pengguna yang dilakukan sebelum pengguna diautentikasi.
   b. FIA UAU.1.2
      TSF harus mewajibkan setiap pengguna untuk suskes terotentikasi sebelum memperbolehkan tindakan TSF lainnya atas nama pengguna tersebut.
4. *FIA_UAU.2 User Authentication before any action*
   TSF harus mewajibkan setiap pengguna untuk suskes terotentikasi sebelum memperbolehkan tindakan TSF lainnya atas nama pengguna tersebut.
5. *FCS_COP.1a Cryptographic Operation (password hashing)*
   TSF harus dapat menampilkan [**password hashing**] yang sesuai dengan algoritma kriptografi khusus [**SHA 256**] dan ukuran kunci kriptografi [-] yang memenuhi syarat berikut: [**FIPS 180-2**].
6. *FAU_GEN.1.Audit Data Generation*
   a. FAU_GEN.1.1
      TSF harus dapat menciptakan rekam audit sebagai berikut:
      1) Menghidupkan dan mematikan fungsi-fungsi audit
      2) Tingkatan peristiwa-peristiwa audit [tidak dispesifikasikan]; dan
      3) **[Proses Login]**
   b. FAU_GEN.1.2
      TSF harus merekam setiap hasil audit setidaknya untuk informasi berikut:
      1) Tanggal dan waktu peristiwa, jenis peristiwa, identitas subjek (jika ada), dan hasil (berhasil atau tidaknya) sebuah peristiwa; dan
      2) Untuk setiap jenis audit, berdasarkan definisi peristiwa ko,ponen fungsional yang bisa diaudit yang terdapat pada PP/ST, [**user login success/fail event, event type, date and time, user id**].
7. *FAU_GEN.2*
   Untuk peristiwa audit yang dihasilkan dari pengguna yang teridentifikasi, TSF harus dapat menghubungkan setiap peristiwa dengan identitas pengguna yang menyebabkannya.
8. *FAU_SAR.1. Audit Review*
   a. FAU SAR 1.1
      TSF harus memberi [**admin**] kemampuan untuk membaca [**audit log**] dari catatan audit.
   b. FAU_SAR.1.2

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 108 - 116

TSF harus memberikan catatan audit yang sesuai bagi pengguna untuk menginterpretasikan informasi

9. *FMT_SMF.1 Security of Management Function*
   FMT_SMF.1
   TSF harus mampu menampilkan fungsi-fungsi manajemen berikut: [**create, read, update, delete of clients account**].
10. *FMT_SMR.1.Security Roles*
    a. *FMT_SMR.1.1*
       TSF harus mempertahankan peran **[Admin and User].**
    b. *FMT_SMR.1.2*
       TSF harus dapat menghubungkan pengguna dengan perannya.
11. *FIA_SOS.1 Verification of Secrets*
    FIA_SOS.1.1
    TSF harus menyediakan mekanisme untuk memverifikasi bahwa rahasia memenuhi [**minimum length of eight (8) characters password**].
12. *FTA_SSL.3 TSF-Initiated Termination*
    FTA_SSL.3.1
    TSF akan mengakhiri sesi interaktif setelah **[30 menit].**
13. *FTA_SSL.4 User-Initiated Termination*
    FTA_SSL.4.1
    TSF harus mengizinkan penghentian sesi interaktif milik pengguna yang dimulai oleh pengguna
14. *FPT_ITT.1 Basic Internal TSF Data Transfer Protection*
    FPT_ITT.1.1
    TSF harus melindungan data TSF dari [*disclosure, modification*] Ketika ditransmisikan antara bagian-bagian TOE yang terpisah.
15. *FCS_CKM.1a Cryptographic Key Generation*
    FCS_CKM.1.1
    TSF harus membangkitkan kunci kriptografi yang behubungan dengan algoritma pembangkitan kunci kriptografi [**PBKDF2-HMACSHA1**] dan ukuran kuci kriptografi khusus [**256 bit**] yang memenuhi syarat berikut: [**RFC 6070**].
16. *FCS_CKM.4 Cryptographic Key Destruction*
    FCS_CKM.4.1
    TSF harus menghancurkan kunci kriptografi sesuai dengan metode penghancuran kunci kriptografi khusus [**key zeroize**] yang memenuhi syarat berikut: [**None**].
17. *FCS_COP.1b Cryptographic Operation (encryption and decryption)*
    FCS_COP.1.1
    TSF harus dapat menampilkan [**encryption and decryption**] yang sesuai dengan algoritma kriptografi khusus [**AES CBC Mode**] dan ukuran kunci kriptografi [**256 bit**] yang memenuhi syarat berikut: [**FIPS 197**].
18. *FCS_COP.1c Cryptographic Operation (file hashing)*
    FCS_COP.1.1
    TSF harus dapat menampilkan [**file signing]** yang sesuai dengan algoritma kriptografi khusus [**SHA 256**] dan ukuran kunci kriptografi [-] yang memenuhi syarat berikut: [**FIPS 180-2**].
19. *FCS_COP.1c Cryptographic Operation (signing)*
    FCS_COP.1.1
    TSF harus dapat menampilkan [**signing**] yang sesuai dengan algoritma kriptografi khusus [**RSA**] dan ukuran kunci kriptografi [**2048**] yang memenuhi syarat berikut: [**RFC 8017**].
20. *FCS_CKM.1b Cryptographic Key Generation (Signing)*
    FCS_CKM.1.1
    TSF harus membangkitkan kunci kriptografi yang behubungan dengan algoritma pembangkitan kunci kriptografi **[RSA]** dan ukuran kuci kriptografi khusus **[2048bit]** yang memenuhi syarat berikut: **[RFC 8017]**

5. KESIMPULAN

Perancangan terhadap spesifikasi fungsi keamanan pada aplikasi *File Encryption (Filtion) versi 1.0.0 untuk* pengelolaan pengendalian data dan informasi untuk pemenuhan operasional Laboratorium Pengujian berdasarkan SNI ISO/IEC 15408:2014 telah dilakukan. Spesifikasi fungsi keamanan yang berhasil dirancang untuk TOE tersebut meliputi *Functional Security Audit (FAU), Functional Cryptographic Support (FCS), Functional Identification and Authentication (FIA), Functional Security Management (FMT), Functional Protection of the TSF (FPT), dan Functional TOE Access (FTA.*

REFERENCES

[1] Tim Penyiapan Sistem Manajemen Laboratorium Pengujian BSSN, “Pedoman Mutu Laboratorium Pengujian BSSN ,” *Tidak dipublikasikan*. Tidak dipublikasikan, Jakarta, 2021.

ISBN: 978-623-93614-6-4
Agustus 2021
Hal: 108 - 116

[2] A. E. Agustini, "KAN Ingatkan Pentingnya Kreditasi," *Bali Tribune*, 2018. https://balitribune.co.id/content/kan-ingatkan-pentingnya-akreditasi (accessed Jul. 20, 2021).
[3] Redaksi, "Lab dan Penyelenggara Uji Profisiensi Harus Terakreditasi KAN," *itechmagz*, Jun. 06, 2021. https://itechmagz.id/corporate-updates/lab-dan-penyelenggara-uji-profisiensi-harus-terakreditasi-kan/ (accessed Jul. 21, 2021).
[4] Badan Standardisasi Nasional, *SNI ISO/IEC 17025:2017 Persyaratan Umum Kompetensi Laboratorium Pengujian dan Laboratorium Kalibrasi*, vol. Issued Number 1. 2018.
[5] MateriDosen, "Perbedaan Kebutuhan Fungsional dan Non Fungsional, Lengkap Contoh dan Penjelasan." https://www.materidosen.com/2017/03/perbedaan-kebutuhan-fungsional-dan-non.html (accessed Jul. 20, 2021).
[6] F. Achmad and E. R. Agustina, "Perancangan Spesifikasi Keamanan Kontrol Akses Pada Aplikasi Layanan Informasi di Lingkungan Instansi Pemerintah," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 6, no. 2, pp. 195–200, Apr. 2019, doi: 10.25126/jtiik.201961304.
[7] A. Saut, F. Achmad, and E. R. Agustina, "Perancangan Spesifikasi Keamanan pada SIFER Berdasarkan SNI ISO/IEC 15408:2014 - Teknologi Infomasi - Teknik Keamanan - Kriteria Evaluasi Keamanan Teknologi Informasi," in *The 11th National Conference on Information Technology and Electrical Engineering* , Dec. 2019, pp. 276–283.
[8] E. R. Agustina, A. Saut, Christine Magdalena, and I. Fitriani, "Perancangan Spesifikasi Keamanan Aplikasi Sistem Kompetensi Personil LSPro BSSN 'SIKOMPRONAS' Versi 1.0.0 Berdasarkan SNI ISO/IEC 15408:2014," in *Embracing Industry 4.0: Towards Sustainable Smart Applications*, Oct. 2019, pp. 68–76.
[9] M. Yudhistira, E. Rahmawati, and A. Saut, "Perancangan Spesifikasi Keamanan pada Aplikasi Persiapan Penyelenggaraan Sertifikasi Keamanan Perangkat Teknologi Informasi (SIAGASIKAT) Bersi 1.0.0 Berdasarkan SNI ISO/IEC 15408:2014," in *Proceedings of The 12th National Conference on Information Technology and Electrical Engineering (CITEE)*, Oct. 2020, pp. 73–79.
[10] E. R. Agustina, "Perancangan Spesifikasi Keamanan Aplikasi Sistem Kompetensi Personil LSPro BSSN 'SIKOMPRONAS' versi 1.1.0 berdasarkan SNI ISO/IEC 15408:2014," *Tidak dipublikasikan*. Tidak dipublikasikan, Jakarta, 2021.
[11] Badan Standardisasi Nasional, *SNI ISO/IEC 15408:2014 Teknologi Informasi - Teknik Keamanan- Kriteria Evaluasi Keamanan Teknologi Informasi - Bagian 2: Komponen Fungsional Keamanan*. Badan Standardisasi Nasional, 2014.
[12] ISO, *ISO/IEC TR 15446: 2017 Information Technolofy - Security Techniques - Guidance for the Production of Protection Profiles and Security Targets*. ISO, 2017.