Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.202183637
Vol. 8, No. 6, Desember 2021, hlm. 1215-1226 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

PERANCANGAN SPESIFIKASI KEAMANAN UNTUK PENGEMBANGAN APLIKASI SECURE CHAT BERDASARKAN COMMON CRITERIA FOR IT SECURITY EVALUATION

Amiruddin Amiruddin [*1], Muhammad Faqih Rohmani[2]

[1]Politeknik Siber dan Sandi Negara, Bogor
[2]Badan Siber dan Sandi Negara, Jakarta
Email: [1]muhammad.faqih@bssn.go.id, [2]amir@poltekssn.ac.id
[*]Penulis Korespondensi

(Naskah masuk: 16 Juni 2020, diterima untuk diterbitkan: 17 November 2021)

Abstrak

Spesifikasi keamanan sangat penting bagi pengembangan aplikasi *chatting* karena dapat menentukan tingkat keamanan aplikasi yang tentunya akan berdampak pada kepercayaan pengguna. Namun, pengembangan fitur keamanan pada aplikasi yang beredar belum semua didasarkan pada suatu spesifikasi kebutuhan keamanan yang jelas. Misanya, aplikasi Mxit dan QQ Mobile tidak memenuhi satu pun dari tujuh kategori keamanan untuk *secure chat* yang dikeluarkan oleh Electronic Frontiers Foundtaion (EFF). Bahkan, Yahoo! Messenger belum menerapkan disain keamanan yang baik, misalnya kita tidak dapat memverifikasi identitas kontak kita. Selain itu, Yahoo! Messenger tidak menerapkan *perfect forward secrecy*. Artinya, fitur keamanan pada beberapa aplikasi *chat* dikembangkan tidak berdasarkan pada rancangan spesifikasi keamanan. Pada penelitian ini, dilakukan perancangan spesifikasi keamanan untuk pengembangan aplikasi *secure chat* dengan mengacu pada *Common Criteria for IT Security Evaluation Version 3.1:2017*. Pada hasil rancangan tersebut, telah ditentukan 28 famili dari 7 kelas *Secure Functional Requirement* (SFR) yang harus dipenuhi dalam pengembangan aplikasi secure chat. Hasil rancangan telah divalidasi dengan metode *expert judgment*.

Kata kunci: *aplikasi mobile, Common Criteria, secure chat, Security Functional Requirements*

SECURITY FUNCTIONAL REQUIREMENTS FOR DEVELOPING SECURE CHAT APPLICATION BASED ON COMMON CRITERIA FOR IT SECURITY EVALUATION

Abstract

Security specifications are very important for chat application development because they can determine the level of its security which, of course, will have an impact on user trust. However, the development of outstanding application security features is not all based on a clear security requirement specification. For example, the Mxit and QQ Mobile applications do not meet any of the seven security categories for secure chat issued by the Electronic Frontier Foundation (EFF). In fact, Yahoo! Messenger has not implemented a good security design, for example, we cannot verify the identity of our contacts and do not apply perfect forward secrecy. This means that security features in some chat applications are developed not based on security specification designs. In this study, the design of security specifications for secure chat application development was carried out by referring to the Common Criteria for IT Security Evaluation Version 3.1: 2017. In the design results, 28 families of 7 classes of Secure Functional Requirements (SFR) have been determined that must be met in the development of secure chat applications. The design result has been validated using expert judgment method.

Keywords: *Common Criteria, mobile application, secure chat, Security Functional Requirements*

1. PENDAHULUAN

Spesifikasi keamanan sangat penting bagi pengembangan sebuah aplikasi *chatting* karena dapat menentukan tingkat keamanan aplikasi yang dapat meningkatkan kepercayaan pengguna. Namun, pengembangan aplikasi *chatting* belum sepenuhnya memperhatikan aspek keamanan. Aplikasi Mxit dan QQ Mobile, misalnya, tidak memenuhi satu pun dari tujuh kategori keamanan untuk *secure chat* yang dikeluarkan oleh Electronic Frontiers Foundtaion (EFF). Bahkan, Yahoo! Messenger belum menerapkan disain keamanan yang baik, misalnya

kita tidak dapat memverifikasi identitas kontak kita dan tidak menerapkan *perfect forward secrecy* [Donohue, 2014], yaitu suatu jaminan bahwa kunci sesi tidak dapat digunakan untuk melakukan serangan walaupun kunci privat diketahui. Hal tersebut menjadi rumor yang mengganggu kenyamanan pengguna [Unger, 2015]. Hal tersebut ditunjukkan dengan hasil survei persepsi publik tentang privasi dan keamanan yang dilakukan oleh Pew Research Center pada tahun 2014 yang menyatakan bahwa 68% pengguna merasa tidak aman menggunakan layanan aplikasi *chatting* untuk berbagi informasi pribadi [Madden, 2014].

Salah satu upaya untuk mengatasi masalah tersebut adalah melakukan perancangan spesifikasi keamanan dalam bentuk *Security Functional Requirements* (SFR). *Common Criteria* yang merupakan dokumen acuan dalam standardisasi dan sertifikasi keamanan perangkat TI oleh berbagai negara, termasuk Indonesia, dapat digunakan untuk merancang SFR [Common Criteria2, 2017]. Rancangan SFR tersebut selanjutnya dapat dikembangkan menjadi dokumen *Protection Profile* (PP) atau *Security Target* (ST) sebagai dokumen acuan dalam proses standardisasi dan sertifikasi perangkat TI [Common Criteria1, 2017]. SFR terdiri atas 11 kelas dan 64 famili fungsional keamanan. Kelas dan famili tersebut tidak harus dipilih secara keseluruhan, melainkan dipilih berdasarkan kesesuaian fitur keamanan pada perangkat terkait.

Pada penelitian ini dilakukan perancangan spesifikasi keamanan pengembangan aplikasi secure chat berbasis Android berdasarkan *Common Criteria for IT Security Evaluation Version 3.1:2017* [Common Criteria2, 2017].

2. METODE PENELITIAN

Pada penelitian ini, perancangan SFR aplikasi *secure chat* dilakukan berdasarkan *Profile Protection* (PP) yang sudah ada dan mengikuti tahapan pada *ISO/IEC TR 15446-Information Technology-Security techniques-Guidance for the protection profiles and security targets* [ISO, 2017]. Setelah itu, rancangan SFR divalidasi dengan metode *expert judgment* dari pihak-pihak yang disebutkan dalam CC yaitu pengembang aplikasi secure chat, regulator, dan pakar CC.

Jadi, tahapan penelitian ini secara lengkap adalah sebagai berikut:

1. *TOE overview and conformance claim;*
2. *Security problem definition;*
3. *Security objectives;*
4. *Extended components;*
5. *Security Functional Requirements;*
6. *Expert judgment*

3. LANDASAN TEORI

3.1. Aplikasi Secure Chat

Secure chat merupakan aplikasi *instant messaging* yang menerapkan *end-to-end encryption* [Unger, 2015] untuk mencapai tujuan kerahasiaan, keaslian data, otentikasi entitas, otentikasi sumber data, dan nir-penyangkalan. Penelitian ini menggunakan karakteristik kripto pada 5 (lima) aplikasi *secure chat* populer berbasis *end-to-end encryption* yaitu WhatsApp [WhatsApp, 2017], Telegram [Nobari, 2017][Telegram, 2019], Signal Private Messenger [Signal, 2019], Rakuten Viber [Viber1, Viber2, 2019], dan PeSankita [XecureIT, 2017], seperti dirangkum dalam Tabel 1.

3.2. Common Criteria (CC)

CC adalah pedoman dan prosedur internasional yang berfokus pada fungsi standardisasi dan sertifikasi keamanan perangkat teknologi informasi. Salah satu produknya yang menunjang fungsi tersebut adalah dokumen *Common Criteria for IT Security Evaluation Version 3.1:2017* yang merupakan standar evaluasi keamanan produk TI, yang terdiri atas tiga bagian, yaitu CC Part 1 yang membahas konsep terminologi, deskripsi metodologi, sejarah perkembangan, dan organisasi pendukung dari CC [Common Criteria1, 2017]; CC Part 2 yan membahas *Security Functional Requirements* [Common Criteria2, 2017]; dan CC Part 3 yang membahas *Security Assurance Requirements and Evaluation Assurance Level* [Common Criteria3, 2012].

Tabel 1. Perbandingan Algoritme Kriptografi Pada Beberapa Aplikasi *Secure Chat*

Aplikasi	*Algoritme Enkripsi*	*Key Exchange*	*Key Gen.*	*Fungsi Hash*
Whatsapp	AES-256	*Diffie-Hellman*	*Curve 25519*	SHA-256
Telegram	AES-256	*Diffie-Hellman*	RSA 2048	SHA-256
Signal Private Messenger*]*	AES-256	*Double-Ratchet*	X3DH	SHA-256
PeSankita	AES-256	*Double-Ratchet*	X3DH	SHA-256
Rakuten	Salsa20	*Diffie-Hellman*	*Curve 25519*	SHA-256

3.3. Security Functional Requirements

SFR dibahas pada dokumen *Common Criteria for IT Security Evaluation Part 2 Version 3.1:2017* [Common Criteria2, 2017]. SFR merupakan bagian inti dari dokumen PP dan ST yang menggambarkan persyaratan keamanan pada perangkat TI yang dievaluasi atau dikenal dengan sebutan *Target of Evaluation* (TOE). SFR tersebut dirancang sesuai dengan tujuan keamanan yang ditentukan sebagai respon terhadap permasalahan keamanan pada produk TI terkait.

4. PEMBAHASAN

4.1. TOE Overview and Conformance Claim

Pada penelitian ini, yang menjadi target evaluasi (TOE) adalah aplikasi *secure chat* berbasis Android yang menerapkan *end-to-end encryption*.

Ada 3 (tiga) komponen utama pada TOE: Pertama, server aplikasi *secure chat* yang merupakan komponen untuk melakukan pengelolaan dan proses otentikasi dan otorisasi terhadap pengguna berdasarkan peran pengguna dalam TOE; Kedua, perangkat *smartphone* Android yang bersistem operasi android sebagai *platform* utama TOE; dan ketiga, aplikasi *secure chat* berbasis Android sebagai user interface dalam kirim terima pesan secara aman. Aset pada TOE adalah data TSF yaitu data yang mendukung fitur keamanan aplikasi *secure chat*. SFR dirancang berdasarkan *Common Criteria for IT Security Evaluation Version 3.1:2017 Revision 5 Part 2: Security Functional Components* [Common Criteria2, 2017].

4.2. Security Problem Definitions

4.2.1. Asumsi Lingkungan TOE

Asumsi lingkungan TOE dibuat berdasarkan fitur keamanan dari aplikasi *secure chat*. Asumsi-asumsi (diawali dengan huruf **A.**) pada setiap ruang lingkup dirangkum pada Tabel 2.

Tabel 2. Asumsi Lingkungan TOE

#	Asumsi	Deskripsi
1	A.PLAT-FORM	*Platform* memiliki spesifikasi, jaringan Internet, dan sistem operasi yang mendukung fungsional TOE.
2	A.FISIK	Lingkungan TOE seperti *hardware* dan *firmware* berada di bawah kendali keamanan oleh pihak yang sah.
3	A.KUNCI	Kunci yang disediakan oleh *Key Scheduling Algorithm* sesuai dengan tingkat layanan keamanan TOE.
4	A.BASIS-DATA	Sistem basis data pada *server* dan CA *server* TOE adalah terpercaya, aman, dan bekerja sesuai fungsinya.
5	A.ADMIN	Admin pada TOE merupakan pihak terpercaya dan di bawah pengelolaan dari *developer* aplikasi *secure chat*.
6	A.SERVER	*Server* pada TOE merupakan pihak terpercaya dan di bawah pengelolaan dari *developer* aplikasi *secure chat*.
7	A.USER	Pengguna TOE telah terlatih dan menguasai pengoperasian aplikasi.
8	A.PRO-SEDUR	Prosedur keamanan penggunaan aplikasi *secure chat* telah dirancang, diterbitkan dan diterapkan para pihak yang terlibat di TOE.

4.2.2 Ancaman pada Aset

Penentuan ancaman aset dilakukan dengan studi literatur dan merujuk OWASP Top Ten Risks Mobile Application 2016 [OWASP, 2016]. Ancaman tersebut (yang diawali dengan huruf **T.**) adalah T.CURI_DATA [Aminanto, 2014, Persson, 2017], T.MITM_KOM [eVAULT, 2017, Persson, 2017, Harpe, 2018], T.EAVS_KOM [Persson, 2017, Harpe, 2018], T.MAR_AUTH [eVAULT, 2017, Persson, 2017, Harpe, 2018], T.MALFUNGSI [Aminanto, 2014], T.MALWARE [Aminanto, 2014], T.MODIFIKASI [Aminanto, 2014, Harpe, 2018], dan T.AKSES_TS [Harpe, 2018] yang dijelaskan lebih rinci pada Tabel 3.

Tabel 3. Daftar Ancaman TOE

No	Deskripsi Ancaman	Ancaman pada OWASP
1	**T.CURI_DATA**	
	Penyerang mencuri data pada memori aplikasi, *server*, dan jalur komunikasi aplikasi *secure chat.*	Penyimpanan/ komunikasi data tidak aman, *reverse engineering, code tampering*, *extraneous functionality*
2	**T.MITM_KOM**	
	Penyerang melakukan akses/ manipulasi secara tidak sah pada data yang dikomunikasikan.	Komunikasi tidak aman
3	**T.EAVS_KOM**	
	Penyerang menyadap data yang dikomunikasikan pada jalur komunikasi.	Komunikasi tidak aman
4	**T.MAR_AUTH**	
	Penyerang melakukan penyamaran sebagai pihak pengguna sah dari suatu akun.	Otentikasi/ otorisas tidak aman
5	**T.MALFUNGSI**	
	Beberapa fungsi aplikasi tidak dapat berjalan.	Fungsi kriptografi tidak memadai, *client code quality*, *code tampering* dan *reverse engineering*
6	**T.MALWARE**	
	Penyerang menyisipkan *malware* pada saat proses instalasi aplikasi *secure chat*.	*client code quality*, *code tampering* dan *reverse engineering*
7	**T.MODIFI-KASI**	
	Penyerang memodifikasi pada aset yang terdapat pada TOE secara tidak sah.	Otorisasi/otorisasi tidak aman, *client code quality*, *code tampering* dan *reverse engineering*
8	**T.AKSES_TS**	
	Penyerang berbuat curang pada pengelolaan otorisasi pihak yang terlibat pada TOE sehingga dapat mengakses TOE.	Otorisasi tidak aman

4.2.3 Kebijakan Keamanan Organisasi

Kebijakan keamanan organisasi harus dipatuhi dan diterapkan pada proses bisnis TOE dan lingkungannya. Pada TOE ini, terdapat beberapa kebijakan (yang diawali dengan huruf **P.**) keamanan organisasi yang dijelaskan pada Tabel 4.

4.3. Security Objective

4.3.1 Security Objective pada TOE dan Lingkungan TOE

Dari hasil identifikasi, ada 11 *security objective* (diawali dengan huruf **O.**) pada TOE (dirangkum dalam Tabel 5) dan 11 *Security Objective* (diawali dengan huruf **OE.**) pada lingkungan TOE (dirangkum dalam Tabel 6).

Tabel 4. Kebijakan Keamanan Organisasi TOE

No	Kebijakan	Deskripsi
1	P.ANTIVIRUS	*Platform* TOE harus menyediakan antivirus untuk menanggulangi *malware*.
2	P.TERTUTUP	TOE harus menjamin bahwa aplikasi *secure chat* melakukan layanan *secure call* dan *secure chat* hanya pada kontak yang tersedia pada perangkat TOE.
3	P.PRIVATE-KEY	TOE dapat membangkitkan pasangan kunci privat dan publik milik pengguna.
4	P.KELOLA	TOE harus dapat menerapkan ketentuan

No	Kebijakan	Deskripsi
		keamanan dan mengatur pembaharuan dari sertifikat dan kontak telepon.
5	P.BUKU-KONTAK	TOE harus menjamin kontak yang tersimpan pada perangkat tidak dapat diganti secara lokal.
6	P.PEMBA-RUAN	TOE harus menjamin bahwa buku kontak pada perangkat diperbarui setiap ada pembaharuan.
7	P.MANA-JEMEN	Admin pada TOE harus melakukan pengelolaan operasi aplikasi dengan menerapkan aspek keamanan informasi.
8	P.PENGHA-PUSAN	Pesan akan terhapus secara permanen bila pengguna menghapus pesan.
9	P.LOGIN	Operasi pada pesan hanya dapat dilakukan oleh pihak pengguna dan pengelola yang terverifikasi melalui tahapan *login* yang sah.
10	P.USER	Pengguna harus memasukkan data yang benar pada saat registrasi.

Tabel 5. *Security Objective* pada TOE

#	Sec Object.	Deskripsi
1	O.AUTH	TOE harus menjamin informasi atau data yang dikirim atau pun diterima dalam proses bisnis aplikasi *secure chat* berasal dari pihak yang sah.
2	O.CONF	TOE harus menjamin bahwa informasi atau data yang dikirim atau diterima dalam proses bisnis aplikasi *secure chat* hanya dapat diketahui dan diakses oleh pihak yang sah.
3	O.FORWA RD_SEC	TOE harus menjamin bahwa setiap sesi komunikasi, sistem pengamanan informasi pada data TSF diperbaharui, sehingga penyerang tidak mampu memanfaatkan informasi pada suatu sesi komunikasi untuk melakukan serangan pada sesi komunikasi sebelumnya.
4	O.INT	TOE harus menjamin data TSF yang dikomuni-kasikan memiliki integritas dan terhindar dari akses atau pun modifikasi dari pihak tidak sah.
5	O.OFF-LINE	TOE harus menjamin ketersediaan fungsionalitas keamanan saat pengguna dalam keadaan *offline*.
6	O.AVAILA BILITY	TOE haru menjamin ketersediaan fungsionalitas dalam penggunaan aplikasi *secure chat*.
7	O.PRIVAT EKEY	TOE dapat melakukan pembangkitan pasangan kunci privat dan publik milik pengguna sesuai dengan akun terdaftar.
8	O.MANAG E	TOE harus menyediakan pihak admin layanan keamanan yang untuk mengelola data TSF.
9	O.ANTI-VIRUS	TOE harus menjamin bahwa TOE terhindar dari *malware* seperti virus, bot, dan sebagainya.
10	O.PHONE BOOK	TOE harus menjamin bahwa kontak pada aplikasi tidak dapat diganti secara lokal atau sebagian sehingga kontak yang tersedia merupakan kontak yang sesuai.
11	O.OTORI-SASI	TOE harus menjamin pengguna yang memiliki akses hanya dapat melakukan operasi sesuai dengan hak akses yang diperoleh.

4.3.3 Security Objective Rationale

Security Objective Rationale adalah gambaran hubungan antara *Security Objective* dengan *Security Problem Defintion*, yang tujuannya untuk menjamin kesesuaian hubungan *Security Objective* dengan *Security Problem Definition* yang telah ditentukan. *Security Objective Rationale* terdiri atas dua bagian yang meliputi: *Security Objective Rationale* untuk TOE dan *Security Objective Rationale* untuk lingkungan TOE. *Security Objective Rationale* untuk TOE ditunjukkan pada Tabel 7.

Tabel 6. *Security Objective* pada Lingkungan TOE

#	Sec Objective	Deskripsi
1	OE.ANTI-VIRUS	Lingkungan TOE harus menjamin bahwa aplikasi terhindar dari *malware*.
2	OE.ADMIN	Lingkungan TOE harus menjamin bahwa admin sebagai pengelola TOE adalah terpercaya, terlatih sesuai proses bisnis TOE.
3	OE.APLI-KASI	Lingkungan TOE harus menjamin bahwa aplikasi yang dapat berjalan pada proses bisnis adalah yang diizinkan oleh admin.
4	OE.PLAT-FORM	Lingkungan TOE harus menjamin bahwa *platform* yang mendukung proses bisnis TOE merupakan *platform* yang sesuai.
5	OE.BACK-END	Lingkungan operasional harus menjamin bahwa *hardware*, *firmware* atau *software* yang bekerja pada TOE sesuai fungsinya, aman secara fisik, dan terkelola dengan baik.
6	OE.KUNCI	Lingkungan operasional harus menjamin bahwa bilangan acak yang tersedia pada *platform* memiliki kualitas yang baik dan sesuai tingkat keamanan yang akan dicapai.
7	OE.SINGLE-USER	Lingkungan operasional harus menjamin bahwa TOE dioperasikan di bawah kendali pihak tunggal yang sah.
8	OE.USER	Lingkungan operasional harus menjamin pengguna TOE terpercaya dan terbiasa menjalankan proses bisnis aplikasi sesuai dengan kebijakan aplikasi terkait.
9	OE.FISIK	Lingkungan operasional harus menjamin bahwa TOE berlokasi pada lingkungan yang aman di bawah kendali organisasi.
10	OE.KELOLA	Lingkungan operasional harus menyediakan keamanan bagi admin dalam mengelola TOE.
11	OE.BASIS-DATA	Lingkungan operasional harus menjamin sistem basis data yang disediakan terpercaya dan bekerja sesuai fungsinya.

Tabel 7 menunjukkan *Security Objective Rationale* pada TOE. Seluruh ancaman dan satu kebijakan yang telah didefinisikan pada *Security Problem Definition* memiliki hubungan dengan *Security Objective* pada TOE, dan begitu juga sebaliknya. Selain itu, tidak terdapat ancaman yang tidak direspon oleh *Security Objective* untuk TOE, dan begitu juga sebaliknya. Hubungan keterkaitan tersebut (ditandai dengan 'X') dijelaskan sebagai berikut. *Security Objective Rationale* untuk lingkungan TOE bertujuan untuk memastikan kesesuaian hubungan antara asumsi dan kebijakan yang telah didefinisikan dengan *Security Objective* untuk lingkungan TOE yang telah didefinisikan. Dengan kata lain, seluruh asumsi dan kebijakan harus memiliki hubungan keterkaitan dengan *Security Objective* untuk lingkungan TOE dan begitu juga sebaliknya.

Tabel 7. *Security Objective Rationale* TOE

Ancaman / Kebijakan	*Security Objective* untuk TOE									
	O.AUTH	O.CONF	O.FORWARD_SEC	O.INT	O.OFFLINE	O.AVAILABILITY	O.PRIVATE_KEY	O.MANAGE	O.ANTIVIRUS	O.PHONEBOOK	O.OTORISASI
T.CURI_DATA		X			X						
T.MITM_KOM	X		X	X							
T.EAVS_KOM		X	X								

Ancaman / Kebijakan	*Security Objective* untuk TOE										
	O.AUTH	O.CONF	O.FORWARD SEC	O.INT	O.OFFLINE	O.AVAILABILITY	O.PRIVATE KEY	O.MANAGE	O.ANTIVIRUS	O.PHONEBOOK	O.OTORISASI
T.MAR_AUTH	X						X			X	
T.MALFUNGSI					X	X					
T.MALWARE									X		
T.MODIFIKASI				X							
T.AKSES_TS											X
P.PEMBARUAN	X	X				X		X			

Pada Tabel 8 ditunjukkan *Security Objective Rationale* untuk lingkungan TOE. Seluruh asumsi dan beberapa kebijakan yang telah didefinisikan pada *Security Problem Definition* memiliki hubungan dengan *Security Objective* pada lingkungan TOE (ditandai dengan 'X'), dan begitu juga sebaliknya. Selain itu, tidak terdapat asumsi dan kebijakan yang tidak berketerkaitan dengan *Security Objective* untuk lingkungan TOE yang telah didefinisikan, dan begitu juga sebaliknya.

Tabel 8. *Security Objective Rationale* Lingkungan TOE

Asumsi / Kebijakan	*Security Objective* pada lingkungan TOE										
	OE.ANTIVIRUS	OE.ADMIN	OE.APLIKASI	OE.PLATFORM	OE.BACKEND	OE.KUNCI	OE.SINGLEUSER	OE.USER	OE.FISIK	OE.KELOLA	OE.BASISDATA
A.PLATFORM				X	X						
A.FISIK									X		
A.KUNCI						X					
A.BASIS-DATA											X
A.ADMIN		X									
A.SERVER										X	
A.USER								X			
A.PROSEDUR		X	X					X		X	
P.ANTIVIRUS	X										
P.TERTUTUP		X					X		X	X	
P.PRIVATEKEY						X		X		X	
P.KELOLA					X					X	
P.BUKU-KONTAK										X	X
P.PEMBARUAN				X						X	X
P.MANAJEMEN		X			X	X				X	X
P.PENGHAPUSAN										X	X
P.LOGIN		X	X				X	X		X	
P.USER								X			

Pada Tabel 8 dapat dilihat bahwa seluruh asumsi lain, dari A.PLATFORM hingga A.PROSEDUR, sudah ditanggapi dengan *security objective* tertentu pada lingkungan TOE.

4.4 Extended Components

Pada TOE ini, terdapat beberapa *Extended Components* yaitu FDP_DEL_EXT.1, FDP_DEL_ EXT.2, FIA_IDP_EXT.1, FIA_IDP_EXT.2. FIA_ IDP_EXT.3. FCS_TLSS_EXT.1 dan FCS_RBG_ EXT.1 yang didefinisikan langsung dari *extended components* pada bagian spesifikasi protokol TLS dan pembangkitan bilangan acak pada bagian SFR.

4.5. Security Functional Requirements

4.5.1 SFR Rationale

SFR ditentukan berdasarkan *rationale* berupa hubungan antara SFR dengan *Security Objective* yang diberikan dalam Tabel 9. Hasil pemetaan tersebut menunjukkan bahwa setiap SFR yang dipilih sudah bersesuaian dengan *Security Objective*. Penjelasan SFR *Rationale* dan justifikasi berdasarkan *Security Objective* diuraikan sebagai berikut. (**Catatan:** karena keterbatasan ruang, seluruh famili SFR yang memenuhi setiap *objective* hanya dirangkum tanpa penjelasan fungsi atau kaitannya dengan *security objective* tertentu.)

Tabel 9. SFR Rationale

SFR pada TOE	*Security Objective* pada TOE										
	O.AUTH	O.CONF	O.FORWARD SEC	O.INT	O.OFFLINE	O.AVAILABILITY	O.PRIVATE KEY	O.MANAGE	O.ANTIVIRUS	O.PHONEBOOK	O.OTORISASI
FAU_GEN.1						X					
FAU_GEN.2						X					
FCS_CKM.1				X		X	X				
FCS_CKM.2		X	X			X					
FCS_CKM.4		X	X								
FCS_COP.1	X	X		X		X					
FCS_RBG_EXT.1		X				X					
FCS_TLSS_EXT.1		X				X		X			
FDP_ACC.1											X
FDP_ACF.1											X
FDP_DEL_EXT.1					X						
FDP_DEL_EXT.2					X						
FIA_ATD.1	X										X
FIA_IDP_EXT.1	X										
FIA_IDP_EXT.2	X										X
FIA_IDP_EXT.3	X										
FIA_UAU.1	X										
FIA_UAU.5	X										
FIA_UAU.6	X										
FIA_UID.1	X										
FIA_USB.1	X										
FMT_MTD.1								X		X	X
FMT_SMF.1								X		X	
FMT_SMR.1								X			X
FPT_PHP.1									X		
FPT_PHP.2									X		
FPT_PHP.3									X		
FTP_ITC.1	X	X									

O.AUTH
Objective: TOE dapat menjamin bahwa pengguna benar-benar sah karena telah teridentifikasi dan terotentikasi sebelum melakukan akses pada layanan *secure chat*. *Objective* ini dipenuhi oleh 11 *corresponding* atau famili SFR yaitu: FCS_COP.1, FIA_ATD.1, FIA_IDP_ EXT.1, FIA_IDP_EXT.2,

FIA_IDP_EXT.3, FIA_UAU.1, FIA_UAU.5, FIA_UAU.6, FIA_UID.1, dan FIA_USB.1.

O.CONF
Objective: TOE dapat menjamin bahwa informasi atau data yang dikirim ataupun diterima dalam proses bisnis aplikasi secure chat hanya dapat diketahui dan diakses oleh pihak yang sah. *Objective* ini dipenuhi oleh 5 famili SFR yaitu FCS_CKM.2, FCS_CKM.4, FCS_COP.1, FCS_ RBG_EXT.1, dan FCS_TLSS_EXT.1.

O.FORWARD_SEC
Objective: TOE harus dapat menjamin bahwa pada setiap sesi komunikasi, sistem pengamanan informasi pada data TSF diperbaharui, sehingga penyerang tidak mampu memanfaatkan informasi pada suatu sesi komunikasi untuk melakukan penyerangan pada sesi komunikasi sebelumnya. *Objective* ini dipenuhi oleh 2 famili SFR yaitu FCS_CKM.2 dan FCS_CKM.4.

O.INT
Objective: TOE harus dapat menjamin bahwa data TSF yang dikomunikasikan memiliki integritas dan terhindar dari akses ataupun modifikasi dari pihak yang tidak sah. *Objective* ini dipenuhi oleh 2 famili SFR yaitu FCS_CKM.1 dan FCS_COP.1.

O.OFFLINE
Objective: TOE harus dapat menjamin ketersediaan fungsionalitas keamanan pada saat pengguna offline. *Objective* ini dipenuhi oleh 2 famili SFR yaitu FDP_DEL_EXT.1 dan FDP_DEL_EXT.2.

O.AVAILABILITY
Objective: TOE harus dapat menjamin ketersediaan fungsionalitas penggunaan aplikasi secure chat. Terdapat 7 corresponding SFR untuk O.AVAIL-ABILITY yaitu FAU_GEN.1, FAU_GEN.2, FCS_CKM.1, FCS_CKM.2, FCS_COP.1, FCS_ RBG_EXT.1, dan FCS_TLSS_EXT.1.

O.PRIVATEKEY
Objective: TOE dapat melakukan pembangkitan pasangan kunci privat dan publik milik pengguna sesuai dengan akun yang terdaftar. Terdapat hanya 1 corresponding SFR untuk O.PRIVATEKEY yaitu FCS_CKM.1.

O.ANTIVIRUS
Objective: TOE harus dapat menjamin bahwa TOE terhindar dari malware, seperti: virus, bot, dan sebagainya. Terdapat 3 corresponding SFR untuk O.ANTIVIIRUS yaitu FPT_PHP.1, FPT_PHP.2, dan FPT_PHP.3.

O.PHONEBOOK
Objective: TOE harus dapat menjamin bahwa kontak pada aplikasi tidak dapat terganti secara lokal ataupun sebagian. Terdapat 2 corresponding SFR untuk O.PHONEBOOK yaitu FMT_MTD.1 dan FMT_SMF.1.

O.OTORISASI
Objective: TOE dapat menjamin pengguna yang memiliki akses, hanya dapat melakukan operasi sesuai dengan hak akses yang diperoleh. *Objective* ini dipenuhi oleh 5 famili SFR yaitu FDP_ACC.1 dan FDP_ACF.1, FIA_ATD.1, FIA_IDP_EXT.2, FMT_MTD.1, dan FMT_SMR.1.

4.5.2 Security Functional Requirements

Berdasarkan rationale tersebut dipilih SFR untuk aplikasi secure chat sebagaimana dirangkum dalam Tabel 10 dan dijelaskan pada bagian selanjutnya.

Kelas FAU (Security Audit)

Famili: FAU_GEN 1.1
TSF dapat membangkitkan rekaman audit dari kejadian-kejadian seperti start-up dan shut-down dari fungsi audit. Juga pada seluruh kejadian yang dapat diaudit untuk level audit yang tidak dispesifikasi atau kejadian umum seperti: pengguna melakukan sign-up, log-in, dan log-out, operasi pada pesan (kirim, membaca, membalas, menghapus, meneruskan, mencabut, dan mengunduh), operasi-operasi pengelolaan, melakukan impor, pergantian, dan penghapusan TLS server key dan sertifikat.

Famili: FAU_GEN.1.2
TSF dapat merekam pada setiap rekaman audit, yang paling sedikit terkait informasi: tanggal dan waktu kejadian, tipe kejadian, identitas subjek (jika digunakan) dan hasil kejadian (gagal atau berhasil), dan setiap tipe kejadian audit, ditentukan berdasarkan definisi kejadian auditable dari komponen fungsional termasuk PP ataupun ST, dan informasi audit relevan lainnya.

Famili: FAU_GEN.2.1
TSF dapat mengaitkan setiap kejadian audit dengan identitas pengguna penyebab kejadian tersebut.

Kelas FCS (Cryptographic Support)

Famili: FCS_CKM.1.1
a. TSF dapat membangkitkan kunci kriptografi berdasarkan algoritme pembangkitan kunci yaitu ZRTP pada RFC 6189 dan SRTP pada RFC 3711 untuk AES-256 dengan mode operasi CBC ataupun CM mode, dan kunci HMAC SHA-1 dan HMAC SHA-256, dan kunci berukuran 256 bit yang telah ditentukan (AES-256 dan HMAC SHA-256) dan 160 bit (HMAC-SHA1) yang dijelaskan pada: FIPS-197, NIST SP 800-38A, RFC 2104, dan FIPS 180-4.

Tabel 10. SFR pada TOE

Kelas SFR	Famili	Nama SFR
FAU (*Security Audit*)	FAU_GEN.1	*Audit data generation*
	FAU_GEN.2	*User ID Association*
FCS (*Crypto-graphic Support*)	FCS_CKM.1	*Crypto-Key Generation*
	FCS_CKM.2	*Crypto-Key Distribution*
	FCS_CKM.4	*Crypto-Key Destruction*
	FCS_COP.1	*Crypto-Operation*
	FCS_RBG_EXT.1	*Random bit Generation*
	FCS_TLSS_EXT.1	TLS *Server Protocol*
FDP (*User Data Protection*)	FDP_ACC.1	*Subset Access Control*
	FDP_ACF.1	*Security Attribute Based Access Control*
	FDP_DEL_EXT.1	*Scheduled Data Deletion*
	FDP_DEL_EXT.2	*Event Triggered Deletion*
FIA (*Identifi-cation* dan *Authenti-cation*)	FIA_ATD.1	*User Attribute Definition*
	FIA_IDP_EXT.1	*Redirection to IDP*
	FIA_IDP_EXT.2	*Acceptance of User Information from* IDP
	FIA_IDP_EXT.3	*Authentication to the* TOE
	FIA_UAU.1	*Timing of Authenticat.*
	FIA_UAU.5	*Multiple Authentication Mechanisms*
	FIA_UAU.6	*Re-authenticating*
	FIA_UID.1	*Timing of Identification*
	FIA_USB.1	*User Subject Binding*
FMT (*Security Management*)	FMT_MTD.1	*Mgmt of* TSF *Data*
	FMT_SMF.1	*Spec of Mgmt Functions*
	FMT_SMR.1	*Security Roles*
FPT (TSF *Physical Protection*)	FPT_PHP.1	*Passive detection of Physical Attack*
	FPT_PHP.2	*Notif of Physical Attack*
	FPT_PHP.3	*Resistant to Physical Attack*
FTP (*Trusted Path/Channels*)	FTP_ITC.1	*Inter-TSF Confidentiality during Transmission*

b. TSF dapat membangkitkan kunci kriptografi sesuai dengan algoritme yang telah ditentukan sebagaimana didefinisikan dalam standar TLS v1.2 [RFC 5246] untuk AES-256 dalam Galois Counter Mode (GCM) dan kunci berukuran 256bit (AES-256) yang dijelaskan pada FIPS 197 dan NIST SP 800-38D.
c. TSF dapat membangkitkan kunci kriptografi asimetrik berdasarkan algoritme pembangkitan kunci yang telah dikhususkan yakni skema RSA mengunakan ukuran kunci minimal 2048 yang didefinisikan pada FIPS PUB 186-4.

Famili: FCS_CKM.2.1
TSF dapat melakukan performa kriptografi key establishment berdasarkan metode-metode key establishment sebagai berikut:
a. Skema RSA-Based Key Establishment (NIST SP 800-56B Revision 1)
b. Skema Elliptic Curve Based Key Establishment (NIST SP 800-56A Revision 2)
c. Skema Finite Field Based Key Establishment (NIST SP 800-56A Revision 2)
d. Skema Key Establishment menggunakan Diffie-Hellman group 14 sesuai RFC 3526
e. Skema Password Based Key Derivation Function (PBKDF) (NIST SP 800-132)
f. Skema Zimmermann Real Time Transport Protocol (RFC 6189)
g. Skema kunci publik pengguna dengan metode TLS 1.2 (RFC 5246)

Famili: FCS_CKM.4.1
TSF dapat menghancurkan kunci kriptografi berdasarkan metode key destruction yang sesuai dengan TOE dan TOE Environment (metode dapat disesuaikan dengan standar terkait).

Famili: FCS_COP.1
a. TSF dapat melakukan operasi enkripsi dan dekripsi simetrik berdasarkan algoritme yang telah dispesifikasikan yakni AES dengan mode operasi CBC, CTR ataupun GCM dan dengan pilihan ukuran kunci 128 bit, 192 bit atau 256 bit. Mode CBC dijelaskan pada ISO 10116, CTR pada ISO 10116, dan GCM pada ISO 19772.
b. TSF dapat melakukan operasi pembangkitan tanda tangan digital dengan algoritme yang telah dispesifikasikan. Pilihan yang disarankan: RSA Digital Signature dan ukuran kunci kriptografi (modulus) minimal 2048 bit dan Elliptic Curve Digital Signature dan ukuran kunci kriptografi minimal 256 bit. Saran tersebut dijelaskan pada dokumen FIPS PUB 186-4.
c. TSF dapat melakukan operasi secure hash berdasarkan algoritme kriptografi, dengan pilihan SHA-1, SHA-256, dan SHA-384.
d. TSF dapat melakukan operasi keyed hash berdasarkan algoritme kriptografi yang telah ditetapkan (HMAC SHA-1, HMAC SHA-256, atau HMAC SHA-384) dan ukuran kunci terkait, dan ukuran message digest (160, 256, atau 384 bit) yang dijelaskan pada ISO/IEC 9797-2:2011, Section 7: MAC Algorithm 2.

Famili: FCS_RBG_EXT.1.1
TSF dapat melakukan seluruh layanan pembangkitan bilang acak deterministik berdasarkan ISO/IEC 18031:2011 dengan menggunakan beberapa pilihan algoritme yaitu: Hash_DRBG, HMAC_DRBG, atau CTR_DRBG (AES).

Famili: FCS_RBG_EXT.1.2
RBG deterministik dapat mengeluarkan hasil bilangan acak berdasarkan satu entropy source yang paling sedikit dan digabungkan dengan entropy dari sumber noise berdasarkan software [assignment: jumlah sumber noise berdasarkan software], sumber noise berdasarkan hardware [assignment: jumlah sumber noise berdasarkan hardware] dengan minimum [selection: 128 bit, 192 bit, dan 256 bit) dari entropy paling sedikit setara dengan kekuatan keamanan tertinggi, hal tersebut dijelaskan pada ISO/IEC 18031:2011 Tabel C.1: Security Strength

Table for Hash, dari kunci dan hash yang yang akan dibangkitkan.

Famili: FCS_TLSS_EXT.1.1
TSF dapat menerapkan TLS 1.2 (RFC 5246) dan menolak seluruh versi lainnya dari TLS dan SSL. Implementasi yang dapat mendukung yang didefinisikan dalam RFC 3268, 4492, 5246, 5288, 5289 adalah:

- TLS_RSA_WITH_AES_128/192/256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128/192/256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128/192/256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128/192/256_CBC_SHA256
- TLS_RSA_WITH_AES_128/192/256_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128/192_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128/192_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128/192_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128/192_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384.

Famili: FCS_TLS_EXT.1.2
TSF dapat menolak koneksi dari permintaan klien dengan SSL 2.0, SSL 3.0, TLS 1.0, dan TLS 1.1.

Famili: FCS_TLSS_EXT.1.3
TSF dapat melakukan *key establishment* RSA dengan ukuran kunci 2048, 3072, atau 4096 bit; pembangkitan parameter EC Diffie Hellman yang berkaitan dengan kurva NIST dengan pilihan kurva secp256r1 atau secp521r1 dan bukan kurva lainnya; dan pembangkitan parameter Diffie Hellman dengan ukuran 2048bit atau 3072 bit.

Kelas FDP (User Data Protection)

Famili: FDP_ACC.1
TSF dapat menjamin dan menegakkan kebijakan keamaan kontrol akses pesan pada subjek (pengguna), objek (pesan), dan operasi (kirim atau buat pesan baru, baca, balas, teruskan, unduh, hapus, dan cabut).

Famili: FDP_ACF.1.1
TSF dapat menjamin dan menegakkan kebijakan keamanan kontrol akses pesan berdasarkan aspek objek, meliputi subjek (pengguna), objek (pesan), atribut subjek keamanan (ID pengguna internal, nomor ponsel, peran [admin, pengguna internal dan pengguna eksternal], fungsi keanggotaan akun, atribut objek keamanan (ID pesan, nomor ponsel).

Famili: FDP_ACF.1.2
TSF dapat menjamin aturan yang diterapkan dapat menentukan kontrol dari subjek dan objek yang diperbolehkan.

Famili: FDP_ACF.1.3
TSF dapat melakukan otorisasi akses secara eksplisit dari subjek kepada objek berdasarkan aturan tambahan yakni aturan berdasarkan *security attribute*, yang secara eksplisit mengatur akses subjek terhadap objek.

Famili: FDP_ACF.1.4
TSF dapat menolak akses dari subjek kepada objek berdasarkan aturan tambahan yakni aturan yang berdasarkan *security attributes*, yang secara eksplisit menolak akses dari subjek ke objek.

Famili: FDP_DEL_EXT.1.1
TSF dapat menghapus pesan tersebut setelah periodik tertentu.

Famili: FDP_DEL_EXT.2
TSF dapat menghapus pesan ketika terdapat kejadian, seperti: pihak yang sah meminta untuk layanan penghapusan pesan; akun yang berkaitan dengan pesan terhapus, dan kejadian lainnya.

Kelas FIA (Identification and Authentication)

Famili: FIA_ATD.1.1
TSF dapat mengelola *daftar security attribute* yang tersedia, termasuk untuk pengguna individu: ID pengguna internal, satu ataupun lebih identifier pengguna, nomor ponsel, peran, fungsi keanggotaan akun, dan atribut tambahan lainnya.

Famili: FIA_IDP_EXT.1.1.
TSF dapat mengalihkan pengguna ke IDP terpercaya untuk keperluan identifikasi dan otentikasi.

Famili: FIA_IDP_EXT.2.
TSF dapat melakukan verifikasi sumber informasi pengguna untuk menjadi IDP terpercaya dengan menggunakan mekanisme otentikasi sumber; integritas dari informasi pengguna harus benar-benar terverifikasi menggunakan mekanisme verifikasi integritas; dan verifikasi tambahan lainnya sebelum menerima identitas pengguna, dan mengikuti atribut pengguna (jika terbukti): peran, fungsi keanggotaan anggota, dan atribut pengguna tambahan dari IDP terpercaya.

Famili: FIA_IDP_EXT.3.1
TSF dapat mengontentikasi identitas pengguna yang disediakan dari IDP dalam aturan berikut:

Pada saat Initial Sign-up. Untuk pengguna internal dan admin, identitas pengguna diterima tanpa tahapan otentikasi. Untuk pengguna eksternal berdasarkan invitation, identitas pengguna harus cocok dengan identifier pengguna yang disediakan oleh inviter atau pengundang. Untuk pengguna eksternal tanpa *invitation*, nomor ponsel yang disediakan oleh pengguna, dijadikan sebagai acuan untuk mengirimkan kode *challenge*, dan kode tersebut berfungsi sebagai parameter otentikasi

sebagai masukan dalam TOE, sehingga kode masukan harus cocok dengan kode yang disediakan oleh *server* TOE.

Pada saat Log-in. Untuk pengguna internal dan admin, identitas pengguna diterima tanpa tahapan otentikasi. Untuk pengguna eksternal, identitas pengguna harus cocok dengan identifier pengguna yang dikirimkan melalui nomor ponsel pengguna.

Famili: FIA.UAU.1.1
TSF dapat mengizinkan akses aplikasi TOE pada smartphone android dan pilihan dari layanan identitas sesuai dengan kepentingan pengguna sebelum pengguna terotentikasi.

Famili: FIA.UAU.1.2
TSF dapat mewajibkan seiap pengguna untuk berhasil terotentikasi, sebelum diperbolehkan mengizinkan fungsi TSF lainnya berada pada kendali pengguna.

Famili: FIA_UAU.5.1
TSF dapat menyediakan mekanisme *multiple authentication* untuk mendukung otentikasi pengguna.

Famili: FIA_UAU.5.2
TSF dapat mengotentikasi seluruh identitas pengguna berdasarkan aturan yang menjelaskan mekanisme *multiple authentication* untuk otentikasi.

Famili: FIA_UAU.6.1
TSF dapat melakukan reotentikasi pengguna dibawah kondisi-kondisi seperti permintaan pengguna, tingkat sensitivitas informasi yang tinggi, dan sebagainya.

Famili: FIA_UID.1.1.
TSF dapat mengizinkan akses aplikasi dari *smartphone* android dan pilihan dari layanan identitas sesuai kepentingan pengguna sebelum pengguna teridentifikasi.

Famili: FIA_UID.1.2.
TSF dapat mewajibkan seiap pengguna untuk berhasil teridentifikasi, sebelum diperbolehkan mengizinkan fungsi TSF lainnya berada pada kendali pengguna.

Famili: FIA_USB.1.1.
TSF dapat menghubungkan *security attributes* pengguna berikut dengan tindakan subjek sesuai dengan kepentingan pengguna, seperti ID pengguna internal, Identifier pengguna, dan nomor ponsel.

Famili: FIA_USB.1.2.
TSF dapat menjalankan aturan yang diikuti pada asosiasi awal dari *security attribute* pengguna dengan subjek berdasarkan kepentingan pengguna. Untuk pengguna internal dan admin, TOE dapat memberikan ID pengguna internal yang unik dan menghubungkan ID pengguna dan nomor ponsel yang disediakan oleh IDP internal kepada ID pengguna internal. Untuk pengguna eksternal yang melakukan *sign-up* dengan *invitation*, TOE dapat memberikan ID pengguna internal yang unik dan menghubungkan ID pengguna dan nomor ponsel yang disediakan oleh pengundang terhadap ID pengguna internal. Untuk pengguna eksternal yang melakukan *sign-up* tanpa *invitation*, TOE dapat memberikan ID pengguna internal yang unik dan menghubungkan ID pengguna yang disediakan oleh IDP eksternal dan nomor ponsel yang disediakan oleh pengguna eksternal terverifikasi.

Famili: FIA_USB.13.
TSF dapat menjalankan aturan yang diikuti dalam pengelolaan perubahan terkait *security attribute* pengguna yang terhubung dengan subjek yang berkepentingan: ID pengguna internal tidak dapat diganti dan aturan tambahan untuk perubahan atribut.

Kelas FMT (Security Management)

Famili: FMT_MTD.1.1
TSF dapat membatasi kemampuan untuk mengelola data TSF ke admin.

Famili: FMT_SMF.1.1
TSF dapat memiliki kemampuan untuk melakukan performa fungsi manajemen sebagai berikut: konfigurasi pengaturan sistem dengan pilihan: periode penyimpanan pesan dan tingkat perizinan untuk pengguna eksternal; konfigurasi daftar IDP terpercaya; pencarian dan penghapusan pengguna; membuat dan menghapus fungsi dari akun; melakukan impor kunci dan sertifikat untuk *server* TLS; dan daftar fungsi manajemen tambahan lainnya yang disediakan oleh TSF.

Famili: FMT_SMR.1.1
TSF dapat mengelola peran-peran dari admin, pengguna internal, dan pengguna eksternal.

Famili: FMT_SMR.1.2
TSF dapat menghubungkan pengguna dengan perannya masing-masing.

Kelas FPT (Physical Protection)

Famili: FPT_PHP.1.1
TSF dapat menyediakan deteksi yang jelas dari pengrusakan fisik yang dapat merusak fungsi TSF.

Famili: FPT_PHP.1.2
TSF dapat menyediakan kapabilitas untuk menentukan gangguan fisik dari perangkat TSF atau elemen dari TSF.

Famili: FPT_PHP.2.1
TSF dapat menyediakan deteksi yang jelas akan gangguan fisik yang mungkin mengganggu TSF.

Famili: FPT_PHP.2.2
TSF dapat menyediakan kapabilitas untuk menentukan gangguan fisik pada perangkat TSF atau elemen TSF.

Famili: FPT_PHP.2.3
Untuk aplikasi *secure chat* yang terinstal pada smartphone, TSF harus dapat melakukan pengawasan perangkat dan elemen dan memberikan notifikasi (sesuai peran pengguna) ketika terdapat pengrusakan pada perangkat TSF atau elemen TSF.

Famili: FPT_PHP.3
TSF dapat tahan dari skenario-skenario pengrusakan yakni penyisipan malware dan sebagainya pada: aplikasi TOE, sistem operasi TOE, dan sebagainya dengan melakukan respon secara otomatis, sehingga SFR TOE dapat berjalan sesuai dengan fungsinya.
Kelas FTP (Trusted Path/Channel)

Famili: FTP_ITC.1.1
TSF dapat menyediakan jalur komunikasi antara TOE dan produk IT terpercaya lainnya, yang secara logika, terlihat jelas dari jalur komunikasi lainnya dan menyediakan jaminan identifikasi dari titik akhirnya dan perlindungan jalur data dari modifikasi atau pencurian.

Famili: FTP_ITC.1.2
TSF dapat mengizinkan produk IT terpercaya lainnya untuk menginisiasi komunikasi melalui jalur terpercaya.

Famili: FTP_ITC.1.3
TSF dapat menginisiasi komunikasi melalui jalur terpercaya tanpa layanan fungsi apapun.

4.6 *Expert Judgment*

Tahap akhir dari penelitian ini adalah *expert judgment* (penilaian pakar) terkait dokumen SFR yang telah dibuat. Seluruh entitas evaluator yang dimaksudkan dalam CC yaitu pengembang, pakar CC, dan regulator/pemerintah sudah dipenuhi dalam proses validasi dokumen. Pengembang *secure chat*, pejabat fasilitasi standardisasi keamanan perangkat TI di BSSN, dan pakar CC sudah memberikan validasi terhadap dokumen melalui lembar pernyataan bahwa dokumen SFR yang dihasilkan dalam penelitian ini sudah valid. Namun, ada catatan tambahan yang diberikan validator yaitu perlunya pengembangan *thread* lebih lanjut sesuai dengan perkembangan TI dan juga perlunya penegasan pada SFR untuk menggunakan *multiple authentication* sebagai upaya penguatan keamanan.

5. KESIMPULAN

Pada penelitian ini telah dirancang spesifikasi keamanan (*Security Functional Requirements* / SFR) untuk pengembangan aplikasi *secure chat* berdasarkan Common Criteria for IT Security Evaluation. Berdasarkan hasil identifikasi *Security Problem Definition,* yang dikaitkan dengan *Security Objective* untuk TOE dan lingkungan TOE, kemudian ditentukan SFR yang sesuai untuk pengembangan aplikasi *secure chat*. Rancangan SFR tersebut terdiri atas tujuh kelas yaitu *security audit* (FAU), *cryptographic support* (FCS), *data protection* (FDP), *identification and authentication* (FIA), *security management* (FMT), *physical protection* (FPT), dan *trusted path/channel* (FTP). Rancangan SFR telah divalidasi menggunakan *metode expert judgment*.

DAFTAR PUSTAKA

ANDROID, “A sweet new take on Android 5.0, Lollipop,” Android, 2019. [Online]. https://android.com/versions/lollipop-5-0/

AMINANTO, M. E. and Sutikno, S., "Development of protection profile and security target for Indonesia electronic ID card (KTP-el) reader based on common criteria V3.1:2012/SNI ISO/IEC15408:2014", International Conference of Advanced Informatics: Concept, Theory and Application (ICAICTA), Bandung, 2014, pp. 1-6

Common Criteria1, “Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model, Revision 5, 2017

Common Criteria2, “Common Criteria for Information Technology Security Evaluation Part 2 : Security functional components, Revision 5, 2017

Common Criteria3, “Common Criteria for Information Technology Security Evaluation Part 3 : Security assurance components, 2012

DASHTINEJAD, P., “Security System for Mobile Messaging Applications,” KTH University, 2015. https://www.diva-portal.org/smash/get/diva/3A813095/fulltext01.pdf

DONOHUE, B., 11 Unsecure Mobile and Internet Messaging Apps, 2014 https://www.kaspersky.com/blog/11_unsecure_messengers/ 6806/ diakses 6 Agustus 2020

eVAULT, Technologies Sdn.Bhd, “SecureMi® Version 1.2 Security Target 0.13 4”, 2017, pp. 1–60 https://commoncriteriaportal.org/files/epfiles/SecureMi-1.2-Security-Target-v0.13.pdf

HARPE, R. “Secure Messages Protection Profile,” vol. 1, no. 44, pp. 1–44, 2018 https://commoncriteriaportal.org/files/epfiles/Secure-Messages-PP-v1.1.pdf

ISO, “ISO/IEC TR: 15446: Information Technology - Security Techniques - Guidance for the Production of Protection Profiles and Security Targets”, International Organization for Standardization, Geneva, 2017

MADDEN, M. et al., "Public Perceptions of Privacy and Security in the Post-Snowden Era", 2014, https://pewresearch.org/internet/2014/11/12/public-privacy-perceptions/

NOBARI,A. D. et al., "Analysis of Telegram, An Instant Messaging Service", Proceedings of the 2017 ACM on Conference on Information and Knowledge Management, 2017, pp.2035–2038,

OFFERMANN, P. and Platz, E.R., "Outline of a Design Science Research Process," Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, May 2009 Article No.: 7 pp. 1–11

OWASP, "Mobile Top 10 2016-Top 10," Open Web Application Security Project, 2016. [Online]. https://owasp.org/index.php/Mobile_Top_10_2016-Top_10.

PERSSON, S., "Security Target for Dencrypt Talk Version 1.0," pp. 1–39, 2017.

https://commoncriteriaportal.org/files/epfiles/Security-Target-for-Dencrypt-Talk-version-1.0.pdf

REMOND, M., "ejabberd Massive Scalability: 1 Node — 2+ Million Concurrent Users," ejabberd, XMPP, 2016. Online:

https://ejabberd.im/forum/25334/ejabberd-massive-scalability-1-node-__%E2%80%94-2-million-concurrent-users/index.html

SABAH, N. et al., "Developing an End-to-End secure chat Application," Int. J. Comput. Sci. Netw. Secur., vol. 17, no. 11, pp. 108–113, 2017

Signal, "Signal Specification," 2019. Online:

https://signal.org/docs

Telegram, "Telegram FAQ," 2019. Online: https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here.

UNGER, N. et al., "SoK: Secure Messaging," 2015 IEEE Symposium on Security and Privacy, San Jose, CA, 2015, pp. 232-249, doi: 10.1109/SP.2015.22.

Viber1, "Rakuten Viber Features," Rakuten Viber, 2019. Online: https://viber.com/features/

Viber2, "Viber Encryption Overview," 2019. https://viber.com/app/uploads/viber-encryption-overview.pdf

WhatsApp, "WhatsApp Encryption Overview", Technical White Paper, p. 11, 2017 https://whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

XecureIT, Pesankita, 2017, online: https://pesan.kita.id/

Halaman ini sengaja dikosongkan