Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 2, April 2023, hlm. 265-277

DOI: https://doi.org/10.52436/1.jutif.2023.4.2.741
p-ISSN: 2723-3863
e-ISSN: 2723-3871

DEVELOPMENT OF PROTECTION PROFILE FOR SECOND-LEVEL E-KTP CARD READER BASED ON ISO/IEC 15408:2022 AND ISO/IEC TS 19608:2018

Yhufi Swastantri Gustiviana [*1], Yohan Suryanto[2]

[1,2]Teknik Elektro, Fakultas Teknik, Universitas Indonesia, Indonesia
Email: [1]yhufi.swastantri@ui.ac.id, [2]yohan.suryanto@email.ac.id

(Naskah masuk: 09 Desember 2022, Revisi : 22 Desember 2022, diterbitkan: 23 Maret 2023)

Abstract

The second level e-KTP reader device is an electronic data reader device stored in the e-KTP chip by applying a verification device in the form of a fingerprint/face scan. The data stored in the e-KTP chip is personal data that is general and specific, as stated in Law Number 27 of 2022. Therefore, users of e-KTP readers as controllers and processors of personal data are obliged to prevent unauthorised access lawfully by using a security system reliably, safely and responsibly. Permendagri Number 76 of 2020 requires compliance with product standards by involving relevant K/L agencies in the security sector as a form of supervision. Based on BSSN Regulation 15 of 2019, implementing the evaluation process in Indonesia's common criteria scheme requires a Protection Profile document to support the evaluation of IT device security. However, there is no Protection Profile document for e-KTP reader devices that have been certified so that it can be used as a reference in developing IT devices to support the evaluation of IT device security. Therefore, in this study, developing Protection Profiles for e-KTP readers based on ISO/IEC 15408 and ISO/IEC TS 19608: 2018 was carried out to prepare functional security requirements and security guarantees by considering the protection of personal data. While the developing method used is based on ISO/IEC TR 15446:2017. The results of this study are preparing a Protection Profile document consisting of 25 functional security requirements to fulfil 8 device security objectives with a level of security assurance at Evaluation Assurance Level (EAL) 4. Then the design results are tested based on the Assurance Protection Profile Evaluation class (APE) ISO/IEC 18045:2022 and declared to meet the criteria based on the ISO/IEC 15408 series.

Keywords: *e-KTP reader device, functional requirement, ISO/IEC 15408:2022, ISO/IEC TS 19608:2018, ISO/IEC 18045:2022, protection profile, security.*

PENGEMBANGAN *PROTECTION PROFILE* PERANGKAT PEMBACA KTP-EL TINGKAT KEDUA BERDASARKAN ISO/IEC 15408:2022 DAN ISO/IEC TS 19608:2018

Abstrak

Perangkat pembaca KTP-el tingkat kedua merupakan perangkat pembaca data elektronik yang tersimpan di dalam cip KTP-el dengan menerapkan satu perangkat verifikasi berupa pemindaian sidik jari/wajah. Data yang tersimpan dalam cip KTP-el merupakan data pribadi yang bersifat umum dan bersifat spesifik sebagaimana tercantum dalam Undang-undang Nomor 27 Tahun 2022. Oleh karena itu, pengguna perangkat pembaca KTP-el sebagai pengendali dan pemroses data pribadi wajib untuk mencegah pengaksesan yang tidak sah dengan menggunakan sistem keamanan secara andal, aman dan bertanggung jawab. Sebagai bentuk pengawasan, Permendagri Nomor 76 Tahun 2020 mensyaratkan untuk dilakukan kesesuaian standar produk dengan melibatkan instansi K/L terkait dalam bidang keamanan. Berdasarkan Peraturan BSSN Nomor 15 Tahun 2019, penyelenggaraan proses evaluasi dalam skema *common criteria* Indonesia membutuhkan dokumen *Protection Profile* untuk mendukung evaluasi keamanan perangkat TI. Namun, belum ada dokumen *Protection Profile* perangkat pembaca KTP-el yang telah tersertifikasi yang dapat dijadikan sebagai acuan dalam pengembangan perangkat TI untuk mendukung evaluasi keamanan perangkat TI. Oleh karena itu, pada penelitian ini dilakukan penyusunan *Protection Profile* perangkat pembaca KTP-el berdasarkan ISO/IEC 15408 dan ISO/IEC TS 19608:2018 untuk penyusunan persyaratan fungsional keamanan dan jaminan keamanan dengan mempertimbangkan pelindungan data pribadi. Sedangkan metode penyusunan yang digunakan berdasarkan ISO/IEC TR 15446:2017. Adapun hasil dari penelitian ini yaitu tersusunnya dokumen *Protection Profile* yang terdiri atas 25 persyaratan fungsional keamanan untuk memenuhi 8 (delapan) tujuan keamanan TOE dengan tingkat jaminan keamanan pada *Evaluation Assurance Level* (EAL) 4.

Kemudian hasil rancangan tersebut diuji berdasarkan kelas *Assurance Protection Profile Evaluation* (APE) ISO/IEC 18045:2022 dan dinyatakan memenuhi kriteria berdasarkan seri ISO/IEC 15408.

Kata kunci: *Perangkat Pembaca KTP-el, Persyaratan Fungsional Keamanan, Protection Profile, ISO/IEC 15408:2022, ISO/IEC TS 19608:2018, ISO/IEC 18045:2022, .*

1. PENDAHULUAN

Jaminan tertulis suatu sistem, proses, barang, jasa, atau personal terhadap suatu standar dan/atau regulasi diperoleh melalui kegiatan sertifikasi [1] sebagai rangkaian kegiatan Penilaian Kesesuaian. Adapun penyelenggara kegiatan sertifikasi dilakukan oleh Lembaga Sertifikasi sesuai dengan ruang lingkupnya. Dalam ruang lingkup barang atau produk, kegiatan sertifikasi diselenggarakan oleh Lembaga Sertifikasi Produk (LSPro).

Badan Siber dan Sandi Negara (BSSN) merupakan Lembaga Pemerintah Non Kementerian (LPNK) yang bertugas untuk membantu Presiden dalam melaksanakan tugas pemerintahan pada bidang keamanan siber dan sandi [2]. Dalam menjalankan tugas tersebut, Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi (Dit.KTKSS) merupakan unit kerja eselon 2 BSSN yang mempunyai tugas pokok dan fungsi dalam perumusan kebijakan teknis di bidang standardisasi, pengujian, sertifikasi, pengawasan dan pengendalian teknologi keamanan siber dan sandi [3]. Adapun salah satu upaya pemenuhan tugas pokok dan fungsi tersebut yaitu penyelenggaraan layanan sertifikasi dan pengujian keamanan perangkat TI melalui LSPro dan Laboratorium Pengujian dengan menyelenggarakan Skema *Common Criteria* Indonesia (SCCI). Selain itu, penyelenggaraan SCCI ini juga merupakan salah satu implikasi dari keanggotaan Indonesia yang tergabung dalam *Common Criteria Recognition Arrangement* (CCRA).

Penyelenggara SCCI terdiri dari Laboratorium Pengujian, LSPro dan komite skema. Proses sertifikasi Keamanan Perangkat TI (KPTI) dilaksanakan oleh LSPro, sedangkan proses pengujian kesesuaian KPTI dilaksanakan oleh Laboratorium Pengujian. Adapun operasional penyelenggara SCCI mengacu pada ISO/IEC 15408 dan ISO/IEC 18045 [4].

Pelaksanaan evaluasi produk TI yang kemudian disebut sebagai *Target of Evaluation* (TOE) meliputi kegiatan pemeriksaan dokumen bukti evaluasi, pengujian fungsionalitas dan pengujian penilaian kerentanan. Pada kegiatan pemeriksaan dokumen bukti evaluasi, terdapat unit pengujian yang menentukan apakah produk yang diuji tersebut mempunyai kesesuaian dengan *Protection Profile* tertentu. *Protection Profile* (PP) merupakan dokumen standar keamanan suatu tipe TOE tertentu sesuai dengan tingkat jaminan keamanan yang ingin dicapai dalam sertifikasi TOE yang ditentukan [4]. Dokumen PP merupakan kriteria teknis yang dapat disusun oleh beberapa unsur, diantaranya yaitu asosiasi, produsen dan regulator. Unsur asosiasi melakukan penyusunan dokumen PP untuk mencapai konsensus tentang persyaratan jenis TOE tertentu. Sedangkan unsur produsen atau pengembang TOE melakukan penyusunan dokumen PP untuk menetapkan persyaratan minimum jenis TOE tertentu. Selanjutnya, unsur pemerintah yang bertindak sebagai regulator dapat melakukan pengembangan dokumen PP untuk menentukan standar/persyaratan keamanan untuk kepentingan nasional [5].

Perangkat pembaca KTP-el merupakan alat pembaca data elektronik yang tersimpan di dalam cip KTP-el [6] yang memuat identitas resmi penduduk. Perangkat ini terdiri dari 3 (tiga) jenis, yaitu tingkat pertama, tingkat kedua dan tingkat ketiga yang mana masing-masing jenis tersebut dibedakan berdasarkan penerapan mekanisme autentikasinya. Sedangkan fungsi perangkat pembaca KTP-el diantaranya yaitu untuk memastikan keabsahan data dari cip KTP-el, melakukan autentikasi visual keabsahan data yang tercetak pada KTP-el, dan memastikan data penduduk dari cip KTP-el dapat diakses.

Data KTP-el dapat diakses melalui proses autentikasi dua arah *(mutual authentication)* antara perangkat pembaca KTP-el yang dilengkapi dengan *Secure Access Module* (SAM) dengan KTP-el melalui metode umpan balik *(challenge/response)*. Metode ini dilakukan untuk menguji keabsahan perangkat pembaca KTP-el dan kartu cerdas nirkontak KTP-el. Selanjutnya jika proses verifikasi cip KTP-el berhasil, maka akan dilakukan proses verifikasi sidik jari pemilik KTP-el. Ketika proses verifikasi berhasil, maka akan dilakukan pembacaan rekaman elektronik data penduduk yang mana akan ditampilkan melalui monitor pada perangkat pembaca KTP-el ataupun pada komputer pengguna.Pengguna perangkat pembaca KTP-el juga dapat menyimpan data hasil pembacaan cip KTP-el ke dalam sistem informasi pengguna untuk kebutuhan pemrosesan lebih lanjut dalam rangka pelayanan administrasi pemerintahan dan/atau publik. Namun data biometrik hanya dapat digunakan untuk kepentingan verifikasi kepemilikan KTP-el sehingga tidak dapat dimanfaatkan untuk pemrosesan lebih lanjut.

Data yang termuat dalam cip KTP-el merupakan data pribadi yang bersifat umum, sedangkan informasi biometrik yang dimanfaatkan untuk memverifikasi pemilik KTP-el merupakan data pribadi yang bersifat spesifik. Atas hal tersebut, maka perangkat pembaca KTP-el erat kaitannya dengan pelindungan informasi identifikasi pribadi – *Personal Identifiable Information* (PII) baik itu data pribadi

yang bersifat umum maupun yang data pribadi yang bersifat spesifik, sehingga pengguna perangkat pembaca KTP-el baik itu sebagai pengendali ataupun pemroses data pribadi wajib untuk mencegah pengaksesan yang tidak sah dengan menggunakan sistem keamanan secara aman, andal dan bertanggung jawab [7].

Penerapan pengawasan perangkat pembaca KTP-el merupakan salah satu upaya untuk pemastian kesesuaian spesifikasi teknis dalam pelaksanaan pengujian teknis [6]. Adapun pelaksana pengujian teknis keamanan perangkat dilakukan oleh LPNK yang membidangi keamanan siber dan sandi. Dalam hal ini, pengampu tugas tersebut dilaksanakan oleh BSSN sesuai dengan Peraturan Presiden Nomor 28 Tahun 2021.

Berdasarkan data pada tahun 2021 - 2022, LSPro BSSN belum pernah menyelenggarakan kegiatan sertifikasi untuk perangkat pembaca KTP-el berdasarkan SCCI. Salah satu penyebabnya adalah belum adanya dokumen PP terkait perangkat pembaca KTP-el yang telah tersertifikasi yang dapat dijadikan sebagai acuan dalam pengembangan perangkat TI ataupun evaluasi keamanan perangkat TI. Hal ini menjadi indikasi urgensi dokumen PP Perangkat Pembaca KTP-el untuk mendukung evaluasi keamanan perangkat TI (KPTI).

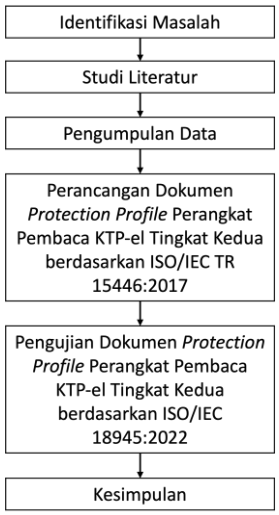
Beberapa penelitian telah membahas terkait pengembangan perangkat pembaca KTP-el [8] dan pengembangan PP untuk KTP-el [9], pelindungan informasi privasi [10], dan perangkat pembaca KTP-el [11]. Pada tahun 2014, Aminanto et al telah melakukan penelitian terkait pengembangan dokumen *Protection Profile* dan *Security Target* untuk Perangkat Pembaca KTP-el berdasarkan *Common Criteria* V.3.1:2012/ SNI ISO/IEC 15408:2014 [11]. Namun dalam penelitian tersebut belum menggunakan standar dan regulasi termutakhir yaitu ISO/IEC 15408:2022 dan Permendagri Nomor 76 Tahun 2020 serta tidak dilakukan pengujian pada kelas *Assurance Protection Profile Evaluation* (APE) berdasarkan ISO/IEC 18045. Selain itu, persyaratan keamanan fungsional yang disusun belum mempertimbangkan persyaratan keamanan yang berkaitan dengan data pribadi. Padahal, sebagaimana yang diketahui bahwa perangkat pembaca KTP-el erat kaitannya dengan pelindungan data pribadi.

Berdasarkan latar belakang tersebut, maka perlu dilakukan penyusunan dokumen PP perangkat pembaca KTP-el dengan pemenuhan persyaratan keamanan dan jaminan keamanan berdasarkan standar yang berlaku dan mempertimbangkan pengaturan terkait lainnya, seperti keterkaitan dengan pelindungan data pribadi sehingga dapat termanfaatkan oleh produsen, konsumen dan regulator. Adapun jenis perangkat pembaca KTP-el yang menjadi TOE pada dokumen PP ini adalah perangkat pembaca KTP-el tingkat kedua. Mekanisme autentikasi yang diterapkan pada jenis ini yaitu menggunakan 1 (satu) perangkat verifikasi berupa pemindaian sidik jari atau wajah. Pada penelitian ini, perangkat pembaca menerapkan mekanisme verifikasi melalui pemindaian sidik jari dengan mempertimbangkan jenis perangkat yang diproduksi oleh produsen KTP-el di Indonesia.

Proses penyusunan dokumen *Protection Profile* mengacu pada standar internasional ISO/IEC 15446:2017 tentang panduan dalam penyusunan *Protection Profile* dan *Security Target* [12]. Sedangkan persyaratan keamanan didefinisikan berdasarkan ISO/IEC 15408-2:2022 tentang komponen fungsional keamanan teknologi informasi [13]. Persyaratan jaminan keamanan disusun berdasarkan ISO/IEC 15408-5:2022 tentang paket untuk persyaratan keamanan [14]. Selain itu, karena perangkat pembaca KTP-el memiliki keterkaitan dengan pelindungan data pribadi, maka fungsi persyaratan fungsional keamanan privasi disusun berdasarkan ISO/IEC TS 19608:2018 tentang panduan untuk mengembangkan fungsi persyaratan keamanan dan privasi berdasarkan ISO/IEC 15408 [15]. Sedangkan rancangan yang telah disusun akan diuji berdasarkan ISO/IEC 18045:2022 tentang metode untuk mengevaluasi kriteria keamanan TI pada kelas *Assurance Protection Profile Evaluation* (APE) [16]. Hasil dari penelitian ini dapat dijadikan sebagai rekomendasi kebijakan terkait kriteria teknis persyaratan keamanan perangkat pembaca KTP-el tingkat kedua untuk mendukung evaluasi keamanan perangkat TI.

2. METODE PENELITIAN

Penelitian ini terdiri dari 6 (enam) tahapan sebagaimana ditunjukkan pada gambar 1, yaitu dilakukan identifikasi masalah, melakukan studi literatur, melakukan pengumpulan data, melakukan perancangan dan pengujian serta menyusun kesimpulan.



Gambar 1. Tahapan Penelitian

Adapun deskripsi kegiatan penelitian yang dilakukan pada setiap tahapan sebagaimana ditunjukkan pada gambar 1 yaitu:

1. Proses identifikasi masalah dilakukan untuk menentukan latar belakang penelitian. Adapun permasalahan yang teridentifikasi pada penelitian ini yaitu perlu adanya *Protection Profile* perangkat pembaca KTP-el baik itu sebagai bentuk pelaksanaan standardisasi teknologi keamanan siber dan sandi, pedoman untuk mengembangkan perangkat pembaca KTP-el, ataupun sebagai gambaran kebutuhan keamanan pengguna.
2. Melakukan studi literatur terkait fungsi keamanan yang diterapkan pada perangkat pembaca KTP-el tingkat kedua. Pada tahap ini dilakukan studi literatur fungsi keamanan perangkat pembaca KTP-el tingkat kedua yang kemudian disebut sebagai TOE dengan mempertimbangkan pemenuhan pelindungan data pribadi yang berasal dari penelitian sebelumnya dan Permendagri Nomor 76 Tahun 2020.
3. Pengumpulan data yang dilakukan dalam penelitian ini yaitu telaah dokumen berupa pengambilan data dari penelitian ilmiah dan/atau peraturan atau ketentuan lain yang terkait dengan pelaksanan tugas pokok K/L yang berkaitan dengan Permendagri 76 Tahun 2020, perangkat pembaca KTP-el dan pelindungan data pribadi, penyusunan *Protection Profile* dan persyaratan fungsional keamanan serta standar nasional dan/atau internasional yang berlaku.
4. Perancangan dokumen *Protection Profile* Perangkat Pembaca KTP-el tingkat kedua. Tahapan penyusunan *Protection Profile* dilakukan berdasarkan ISO/IEC TR 15446:2017 tentang panduan penyusunan *Protection Profile* dan *Security Target*, meliputi:
    a. Menentukan permasalahan keamanan melalui pendefinisian ancaman yang relevan dengan TOE, kebijakan keamanan organisasi dan asumsi untuk operasional TOE;
    b. Mengidentifikasi tujuan keamanan TOE dan lingkungan operasional TOE;
    c. Menentukan spesifikasi keamanan melalui matriks rasional untuk setiap tujuan keamanan terhadap permasalahan keamanan;
    d. Memilih fungsi keamanan, melalui identifikasi persyaratan fungsi keamanan yang perlu disediakan oleh TOE untuk memenuhi tujuan keamanan berdasarkan ISO/IEC 15408-2:2022 dan ISO/IEC TS 19608:2018
5. Pengujian dokumen *Protection Profile* Perangkat Pembaca KTP-el tingkat kedua terhadap kelas APE berdasarkan ISO/IEC 18045:2022.

Selanjutnya hasil dari perancangan dan pengujian dokumen *Protection Profile* Perangkat Pembaca KTP-el tingkat kedua ini menjadi simpulan penelitian.

2.1. ISO/IEC 15408-2:2022 Keamanan Informasi, Keamanan Siber dan Pelindungan Privasi – Kriteria Evaluasi untuk Keamanan TI Bagian 2: Komponen Fungsional Keamanaan

Standar ini mendefinisikan komponen fungsional keamanan untuk evaluasi keamanan yang terdiri dari 11 (sebelas) kelas keamanan, meliputi:

a. *Functional Security Audit* (FAU), merupakan persyaratan audit keamanan yang melibatkan perekaman, penyimpanan dan analisis informasi yang terkait dengan aktivitas keamanan;
b. *Functional Communication* (FCO), merupakan persyaratan untuk memastikan identitas pengirim (bukti pengirim) dan penerima informasi (bukti penerima);
c. *Functional Cryptographic Supports* (FCS), merupakan persyaratan fungsional kriptografi untuk memenuhi tujuan keamanan, termasuk identifikasi dan autentikasi, nir-sangkal, *trusted path*, *trusted channel* dan pemisahan data;
d. *Functional User Data Protection* (FDP), merupakan persyaratan untuk melindungi data pengguna selama impor, ekspor dan penyimpanan atribut keamanan yang terkait langsung dengan pengguna;
e. *Functional Identification and Authentication* (FIA), merupakan persyaratan untuk menetapkan dan memverifikasi identitas pengguna;
f. *Functional Security Management* (FMT), merupakan persyaratan untuk melakukan pengelolaan data TSF, pengelolaan atribut keamanan, pengelolaan fungsi TSF dan definisi peran keamanan;
g. *Functional Privacy (FPR),* merupakan persyaratan perlindungan pengguna terhadap penemuan dan penyalahgunaan identitas oleh pengguna lain;
h. *Functional Protection of the TSF* (FPT), merupakan persyaratan yang berhubungan dengan integritas dan mekanisme manajemen yang membentu TSF dan integritas data TSF;
i. *Functional Resource Utilization* (FRU), merupakan persyaratan ketersedian sumber daya yang diperlukan;
j. *Functional TOE Access* (FTA), merupakan persyaratan untuk mengontrol pembentukan sesi pengguna;
k. *Functional Trusted Path/Channels* (FTP), merupakan persyaratan untuk jalur komunikasi terpercaya antara pengguna dan TSF dan jalur komunikasi terpercaya antara TSF dan produk TI terpercaya lainnya.

2.2. ISO/IEC TS 19608:2022 Panduan untuk Pengembangan Persyaratan Fungsional

Keamanan dan Privasi berdasarkan ISO/IEC 15408

Standar ini berisikan panduan untuk memilih dan menentukan persyaratan fungsional keamanan untuk melindungi informasi informasi pengidentifikasi personal sebagai komponen tambahan berdasarkan prinsip yang didefinisikan dalam ISO/IEC 29100 melalui paradigma yang dijelaskan dalam ISO/IEC 15408-2. Adapun komponen tambahan untuk privasi, meliputi prinsip persetujuan dan pilihan, legitimasi tujuan dan spesifikasi, batasan koleksi, minimisasi data dan pembatasan penggunaan, retensi dan penggunaan, keterbukaan, transparansi, dan pemberitahuan, partisipasi dan akses individu, akurasi dan kualitas, akuntabilitas dan kepatuhan privasi, serta keamanan informasi.

2.3. ISO/IEC 15048-3:2022 Keamanan Informasi, Keamanan Siber dan Pelindungan Privasi – Kriteria Evaluasi untuk Keamanan TI Bagian 3: Komponen Jaminanl Keamanaan

Standar ini mendefinisikan kelas komponen jaminan keamanan, meliputi:

a. Kelas ASE: *Assurance Security Target Evaluation*, menunjukkan bahwa dokumen *Security Target* (ST) merupakan identitias produk yang berisi nama produk, versi, serta klaim fitur keamanan dari pengembang produk TI telah disusun dengan konsisten dan tepat;
b. Kelas ADV: *Assurance Development*, memberikan informasi tentang pengembangan produk sebagai dasar dalam melakukan analisis kerentanan dan pengujian TOE yang mana setidaknya mencakup deskripsi terkait desain dan implementasi serta deskripsi arsitektur;
c. Kelas AGD: *Assurance Guidance Document*, menyediakan persyaratan untuk dokumentasi panduan TOE untuk seluruh peran pengguna;
d. Kelas ALC: *Assurance Life-cycle support*, menyediakan dan mendukung siklus hidup sebagai aspek untuk membangun kontrol keamanan yang tepat dalam pengembangan, produksi pengiriman dan pemeliharaan TOE;
e. Kelas ATE: *Assurance Testing*, memberikan jaminan bahwa TSF berperilaku sebagaimana yang dijelaskan dalam spesifikasi fungsional, desain TOE, representasi implementasi dan memungkinkan ketelusuran SFR pada skenario pengujian;
f. Kelas AVA: *Assurance Vulnerability Assessment*, melakukan penilaian untuk mengidentifikasi kerentanan selama evaluasi TOE.

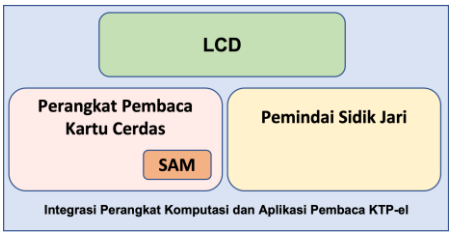
2.4. ISO/IEC 18045:2022 Keamanan Informasi, Keamanan Siber dan Pelindungan Privasi – Kriteria Evaluasi untuk Keamanan TI – Metodologi untuk Evaluasi Keamanan TI

Standar ini menjelaskan tindakan minimum yang harus dilakukan oleh evaluator untuk melakukan evaluasi berdasarkan kriteria dan bukti evaluasi yang ditentukan dalam seri ISO/IEC 15408. *Assurance Protection Profile Evaluation* (APE) merupakan klausul untuk melakukan evaluasi PP. Metodologi evaluasi dalam klausul ini didasarkan pada persyaratan PP sebagaimana ditentukan dalam ISO/IEC 15408-3:2022 kelas APE. Adapun sub aktivitas yang dilakukan dalam pengujian pada kela sini yaitu:

a. APE_INT. 1 bertujuan untuk menentukan apakah *Protection Profile* (PP) diidentifikasi dengan benar dan apakah referensi PP dan gambaran umum TOE konsisten antara satu dengan yang lainnya;
b. APE_CCL.1 bertujuan untuk untuk menentukan validitas dari klaim kesesuaian terhadap ISO/IEC 15408 yang diklaim PP;
c. APE_SPD.1 bertujuan untuk menentukan bahwa masalah keamanan yang dimaksudkan untuk ditangani oleh TOE dan lingkungan operasionalnya didefinisikan dengan jelas;
d. APE_OBJ.2 bertujuan untuk menentukan apakah tujuan keamanan secara memadai dan lengkap mampu mengatasi definisi masalah keamanan dan pembagian masalah antara TOE dan lingkungan operasionalnya didefinisikan dengan jelas;
e. APE_ECD.1 bertujuan untuk menentukan apakah *extended component definition* telah didefinisikan dengan jelas dan tidak ambigu, dan apakah komponen tersebut diperlukan, yaitu tidak dapat dinyatakan dengan jelas menggunakan komponen ISO/IEC 15408-2 atau ISO/IEC 15408-3 yang ada;
f. APE_REQ.2 bertujuan untuk menentukan apakah SFR dan SAR jelas, tidak ambigu dan terdefinisi dengan baik, apakah konsisten secara internal, dan apakah SFR memenuhi tujuan keamanan TOE.

3. HASIL DAN PEMBAHASAN

Target of Evaluation (TOE) pada PP ini adalah perangkat pembaca KTP-el tingkat kedua dengan menerapkan perangkat verifikasi berupa pemindai sidik jari. TOE terdiri dari perangkat keras berupa perangkat pembaca kartu cerdas yang disertai dengan *Secure Access Module* (SAM), perangkat komputasi, pemindai sidik jari dan perangkat lunak sebagai pembaca KTP-el. Adapun gambar 2 menunjukkan lingkungan operasional TOE yang mana merupakan integrasi antara perangkat komputasi dan aplikasi pembaca KTP-el.



Gambar 2. Lingkungan Operasional TOE

Data KTP-el dapat diakses melalui proses autentikasi dua arah (*mutual authentication)* antara perangkat pembaca KTP-el yang dilengkapi dengan *Secure Access Module* (SAM) dengan KTP-el melalui metode umpan balik *(challenge/response)*. Metode ini dilakukan untuk menguji keabsahan perangkat pembaca KTP-el dan kartu cerdas nirkontak KTP-el. Proses umpan balik tersebut dilakukan dalam format *Application Protocol Data Unit* (APDU) [17] dengan *secure messaging* melalui enkripsi *command* data dengan pemanfaatan algoritma kriptografi [18]. Sedangkan verifikasi keabsahan data dilakukan melalui proses verifikasi *digital signature* berbasis *Elliptic Curve Digital Signature Algorithm* (ECDSA) [8]. Selanjutnya jika proses verifikasi cip KTP-el berhasil, maka akan dilakukan proses verifikasi sidik jari pemilik KTP-el. Ketika proses verifikasi berhasil, maka akan dilakukan pembacaan rekaman elektronik data penduduk yang mana akan ditampilkan melalui monitor pada perangkat pembaca KTP-el ataupun pada komputer pengguna. Interaksi antara perangkat pembaca KTP-el dengan komputer pengguna membutuhkan *driver* perangkat lunak yang mendukung interoperabilitas TOE dan perangkat eksternal tersebut. Namun integrasi tersebut berada di luar ruang lingkup dalam pembahasan penelitian ini. Selain itu, SAM yang digunakan pada perangkat pembaca juga tidak termasuk dalam ruang lingkup TOE sehingga pengimplementasiannya dijadikan sebagai asumsi yang telah memenuhi spesifikasi keamanan sebagaimana yang dipersyaratkan dalam Permendagri Nomor 76 Tahun 2020.

Adapun fungsi dari TOE meliputi:

a. Memastikan penggunaan cip KTP-el yang sah;
b. Memastikan keabsahan kepemilikan melalui verifikasi sidik jari;
c. Menampilkan data rekaman elektronik yang tersimpan dalam cip KTP-el;
d. Memastikan keabsahan data melalui perbandingan verifikasi visual dari hasil pembacaan cip KTP-el untuk kondisi tertentu;
e. Memungkinkan untuk dapat menyimpan data hasil pembacaan dari cip KTP-el pada sistem informasi pengguna untuk kebutuhan pemrosesan lebih lanjut dalam rangka pemenuhan kepentingan pemerintahan dan publik. Sedangkan data biometrik penduduk hanya digunakan untuk kepentingan verifikasi kepemelikan KTP-el dan tidak dapat disimpan.

Dalam upaya pelindungan data pribadi pemilik KTP-el, maka TOE dianggap perlu menyediakan mekanisme untuk mendapat persetujuan pemrosesan data pribadi dari pemilik data pribadi dan menyediakan mekanisme untuk menghapus data pribadi yang tidak boleh disimpan sebagaimana peraturan perundang-undangan yang berlaku. Sedangkan spesifikasi perangkat keras dan perangkat lunak yang digunakan merujuk pada Lampiran Permendagri Nomor 76 Tahun 2020 Bagian II.A..

3.1. Penentuan Permasalahan Keamanan

Penentuan permasalajan keamanan mencakup ancaman yang dapat dimitigasi oleh TOE, kebijakan keamanan organisasi yang harus diterapkan untuk mendukung operasional TOE, dan asumsi yang harus dipenuhi untuk lingkungan IT maupun non-IT agar TOE dapat berjalan sebagaimana fungsinya.

a. Aset dan Ancaman

Pada penelitian ini, ancaman disusun berdasarkan analisis pohon ancaman dengan menentukan aset yang akan dilindungi sebagai puncak pohon. Selanjutnya setiap aset akan memiliki anak cabang untuk merepresentasikan mekanisme keamanan yang diterapkan untuk melindungi aset. Kemudian dilakukan identifikasi terhadap ancaman yang mungkin untuk masing-masing mekanisme keamanan. Tabel 1 menunjukkan identifikasi aset yang dilindungi oleh TOE.

Tabel 1. Aset yang Dilindungi TOE

Aset	Deskripsi	Pemilik Data
Kredensial	Atribut keamanan yang digunakan oleh user dan admin untuk melakukan proses autentikasi sebelum menjalankan operasional TOE	*User, admin*
Data KTP-el	Data penduduk yang akan diverifikasi mencakup biodata diri, NIK, foto, tanda tangan dan sidik jari	Pengguna perangkat pembaca KTP-el
Log data	Memuat informasi aktivitas admin dan user dalam mengoperasikan TOE	*User, admin*
Firmware	Perangkat lunak untuk operasional perangkat pembaca KTP-el serta pembaruan program	Pengguna perangkat pembaca KTP-el
Fisik Perangkat	Fisik perangkat untuk operasional pembaca KTP-el terintegrasi	Pengguna perangkat pembaca KTP-el

Tabel 1 memuat informasi terkait aset, deskripsi aset dan pemilik data aset. Berdasarkan identifikasi tersebut, maka tabel 2 menunjukkan identifikasi ancaman yang harus dimitigasi oleh TOE untuk melindungi aset.

Tabel 2. Ancaman yang Dimitigasi TOE

Ancaman	Deskripsi	Aset yang Dituju
T.TEBAK_ PASSWORD	Penyerang mencoba untuk melakukan *login* berkali-kali untuk mendapatkan *username*	Kredensial *user* dan *admin*

Ancaman	Deskripsi	Aset yang Dituju
	dan *password* milik *user* dan/atau *admin* TOE untuk dapat mengoperasikan TOE sebagai pihak yang berwenang.	
T.COBA_ VERIFIKASI	Penyerang mencoba untuk melakukan verifikasi cip KTP-el dan/atau sidik jari seolah-olah sebagai pemilik yang sah.	Data KTP-el
T.PENGUNGKAPAN	Penyerang melakukan penyadapan pada kanal komunikasi untuk dapat mengakses ataupun membocorkan data KTP-el.	Data KTP-el
T. BACALOG	Penyerang mencoba untuk membaca log data yang berisi aktivitas *user* maupun *admin* aplikasi dalam mengoperasikan TOE serta memungkinkan untuk menghapus atau memodifikasi log data.	Log Data
T. GAGAL_ MEMBUAT_LOG	Penyerang menghabiskan media penyimpanan sehingga TOE gagal mencatat log data.	Log Data
T. MALWARE	Penyerang mengubah *firmware* dengan menyisipkan *malware* yang ada di TOE dengan cara mengubah atau menghapus konfigurasi TOE untuk mendapatkan akses fungsional TOE	*Firmware*
T. MALAFUNGSI	Adanya kegagalan fungsi TOE baik disengaja atau tidak sehingga TOE tidak dapat beroperasional sebagaimana mestinya	*Firmware*
T. TAMPERING	Penyerang melakukan *physical probing* untuk mendapatkan data pada perangkat pembaca KTP-el.	Fisik Perangkat

b. Kebijakan Keamanan Organisasi

Pendefinisian kebijakan keamanan organisasi bertujuan untuk mendukung operasional TOE. Tabel 3 telah mendefinisikan kebijakan keamanan organisasi, yang mana kebijakan disusun dan disahkan untuk ditaati dan dijalankan oleh pengguna TOE.

Tabel 3. Kebijakan Keamanan Organisasi

Kebijakan Keamanan Organisasi	Penjelasan
P. PENGGUNA	Operasional TOE didukung dengan tersedianya pengguna terotorisasi yang sesuai dengan perannya untuk mengelola TOE dengan aman
P. PASSWORD	Operasional TOE didukung dengan kebijakan terkait pengaturan *password* untuk pengguna TOE
P. VERIFIKASI_ VISUAL	Operasional TOE didukung dengan kebijakan untuk melakukan verifikasi secara visual untuk kondisi tertentu
P.SAM	Operasional TOE didukung dengan kebijakan terkait *crypto co-processor* pada SAM yang mendukung algoritma kriptografi dan paling rendah telah tersertifikasi *Common Criteria* EAL 5+ atau FIPS 140-2 tingkat 4
P.PENGGUNAAN	Operasional TOE didukung dengan kebijakan terkait petunjuk instalasi, konfigurasi dan penggunaan TOE
P. MANAJEMEN_ KUNCI	Operasional TOE didukung dengan kebijakan terkait manajemen dan pelindungan kunci yang digunakan untuk autentikasi cip KTP-el dan perangkat pembaca KTP-el

c. Asumsi

Asumsi berfokus pada hal-hal yang mendukung operasional TOE misalnya pengguna, lingkungan, koneksi, perangkat eksternal tambahan dan lain sebagainya. Tabel 4 mendekripsikan asumsi keamanan operasional TOE. Pernyataan pada setiap asumsi akan dijadikan sebagai justifikasi untuk menyatakan bahwa tujuan keamanan lingkungan operasional TOE dipenuhi oleh asumsi keamanan operasional TOE.

Tabel 4. Asumsi Keamanan Operasional TOE

Asumsi	Pernyataan
A. PENGGUNA	Diasumsikan pengguna TOE tidak ceroboh, pertanggung jawab atas pengeoperasian TOE yang aman dan patuh pada kebijakan penggunaan TOE
A. KONEKSI	Diasumsikan bahwa TOE terhubung pada jaringan terpercaya
A. SAM	Berupa *secure Integrated Circuit* (IC) yang digunakan untuk meningkatkan keamanan dan performa kriptografi untuk melindungi data dengan melakukan transaksi yang aman antara aplikasi dan *smart card* [6]. Diasumsikan SAM terhubung ke TOE dengan aman dan SAM yang digunakan telah memenuhi spesifikasi dan dievaluasi serta disertifikasi sesuai dengan persyaratan pada Permendagri 76 Tahun 2020.
A. LINGKUNGAN	Diasumsikan TOE beroperasi di lingkungan yang aman secara fisik dan dikelola dengan baik
A. TIMESTAMP	Diasumsikan lingkungan operasional TOE menyediakan *timestamp* yang dapat dipercaya
A. MANAJEMEN_ KUNCI	Diasumsikan TOE telah menerapkan manajemen dan pelindungan kunci yang digunakan untuk autentikasi cip KTP-el dan perangkat pembaca KTP-

Asumsi	Pernyataan
	el sesuai dengan standar nasional dan/atau internasional yang berlaku
A. PROSEDUR	Diasumsikan pihak yang berwenang telah menyusun dan mengesahkan prosedur-prosedur yang dibutuhkan untuk operasional TOE

3.2. Pengidentifikasian Tujuan Keamanan

Tujuan keamanan didefinisikan untuk menangani permasalahan keamanan yang telah didefinisikan sebagaimana dalam subbab 3.1. Adapun tujuan keamanan dibagi dalam 2 (dua) jenis yaitu tujuan keamanan TOE dan tujuan keamanan untuk lingkungan operasional TOE.

a. Tujuan Keamanan TOE

Pendefinisian tujuan keamanan TOE dilakukan berdasarkan daftar ancaman dan/ atau kebijakan yang berlaku yang ditetapkan terhadap fungsional TOE. Tabel 5 mendefinisikan tujuan keamanan TOE yang mana deskripsi setiap tujuan keamanan TOE tersebut menjelaskan bagaimana TOE menyediakan mekanisme untuk melindungi TOE terhadap ancaman yang telah diidentifikasi pada tabel 2 ataupun mendukung pelaksanaan kebijakan keamanan organisasi yang telah diidentifikasi pada tabel 3.

Tabel 5. Tujuan Keamanan TOE

Tujuan Keamanan TOE	Penjelasan
O. PENGGUNA_ AUTENTIK	TOE mengidentifikasi pengguna dan mengautentikasi pengguna sebelum mengizinkan akses ke fungsi manajemen dan objek TOE
O. ADMIN	TOE menyediakan mekanisme bahwa admin dapat mengelola dan membatasi peran untuk pengelolaan sistem TOE dengan aman dan menjalankan mekanisme pada kondisi tertentu
O. VERIFIKASI	TOE mengidentifikasi dan mengautentikasi cip dan pemilik KTP-el sebelum mengizinkan akses ke pembacaan data KTP-el
O. RAHASIA	TOE menyediakan mekanisme untuk mengamankan informasi privasi yang harus dilindungi sesuai dengan kebijakan keamanan dari pengungkapan yang tidak sah
O. AUDIT	TOE menyediakan mekanisme untuk membuat data log untuk memastikan akuntabilitas dengan mereviu data audit sebagai data balikan
O.UPDATE	TOE melakukan verifikasi terhadap pembaruan *firmware* dengan melakukan integritas data dan akan memunculkan notifikasi jika pembaruan data dilakukan terhadap versi yang lebih lama ataupun versi yang sama
O. KONDISI	TOE akan mempertahankan keadaan aman ketika terjadi kegagalan fungsi keamanan.
O. PROTEKSI _FISIK	TOE menyediakan perlindungan fisik yang memadai untuk melindungi aset yang disimpan dan memastikan bahwa gangguan fisik dapat dideteksi oleh pengguna

b. Tujuan Keamanan Lingkungan Operasional TOE

Tujuan keamanan lingkungan operasional TOE disusun berdasarkan asumsi yang digunakan untuk mendukung operasional TOE. Dalam hal ini, sasaran keamanan untuk lingkungan operasional TOE mencakup penetapan dan penerapan prosedur untuk memastikan bahwa TOE akan digunakan dengan cara yang aman, serta kompetensi personil dalam pengoperasionalan TOE. Tabel 6 mendefinisikan tujuan keamanan lingkungan operasional TOE sebagai berikut.

Tabel 6. Tujuan Keamanan Lingkungan Operasional TOE

Tujuan Keamanan Lingkungan Operasional	Penjelasan
OE. PENGGUNA	Pengguna TOE tidak ceroboh, bertanggung jawab atas pengoperasian TOE yang aman dan patuh pada kebijakan penggunaan TOE
OE. KONEKSI	TOE terhubung pada jaringan terpercaya
OE. VERIFIKASI_ VISUAL	Pengguna yang berwenang dan terpercaya dapat mengoperasionalkan TOE untuk melakukan verifikasi visual melalui foto wajah yang diakses perangkat pembaca secara aman dari dalam cip KTP-el dalam kondisi operasional lapangan terkait dengan kebutuhan pelayanan publik secara masal yang membutuhkan waktu yang cepat pada kondisi khusus tertentu.
OE. SAM	TOE terhubung dengan SAM yang aman dan telah dievaluasi dan disertifikasi sesuai dengan persyaratan pada Permendagri 76 Tahun 2020
OE. LINGKUNGAN	TOE dioperasionalkan pada lingkungan yang aman dengan pengelolaan yang baik
OE. TIMESTAMP	Lingkungan operasional TOE menyediakan *timestamp* yang dapat dipercaya
OE. MANAJEMEN_ KUNCI	TOE telah menerapkan manajemen dan pelindungan kunci untuk autentikasi cip KTP-el dan perangkat pembaca KTP-el sesuai dengan standar nasional dan/atau internasional yang berlaku
OE. PROSEDUR	Pihak yang berwenang menyusun dan menerbitkan prosedur-prosedur yang dibutuhkan untuk pengoperasionalan TOE

3.3. Penentuan Spesifikasi Keamanan

Pada tahap ini akan dilakukan penyusunan matriks rasional yang menghubungkan antara permasalahan keamanan dan tujuan keamanan untuk memastikan bahwa setiap permasalahan keamanan akan terjawab oleh tujuan keamanan TOE ataupun lingkungan operasional TOE sebagaimana ditunjukkan pada tabel 7.

Tabel 7. Korespondensi Permasalahan Keamanan terhadap Tujuan Keamanan

FUNGSI KEAMANAN	TUJUAN KEAMANAN															
	O. PENGGUNA_AUTENTIK	O. ADMIN	O. VERIFIKASI	O. RAHASIA	O. AUDIT	O. UPDATE	O. KONDISI	O. PROTEKSI_FISIK	OE. PENGGUNA	OE. KONEKSI	OE. VERIFIKASI_VISUAL	OE. SAM	OE. LINGKUNGAN	OE. TIMESTAMP	OE. MANAJEMEN_KUNCI	OE. PROSEDUR
T. TEBAK_PASSWORD	✓															
T. COBA_VERIFIKASI			✓													
T. PENGUNGKAPAN				✓												
T. BACALOG		✓			✓				✓							
T. GAGAL_MEMBUAT_LOG					✓											
T. MALWARE						✓										
T. MALAFUNGSI							✓									
T. TAMPERING								✓								
P. PENGGUNA	✓								✓							✓
P. PASSWORD																✓
P. VERIFIKASI_VISUAL		✓									✓					✓
P. SAM												✓				✓
P. PENGGUNAAN																✓
P. MANAJEMEN_KUNCI															✓	✓
A. PENGGUNA									✓							
A. KONEKSI										✓						
A. SAM												✓				
A. LINGKUNGAN													✓			
A. TIMESTAMP														✓		
A. MANAJEMEN_KUNCI															✓	
A. PROSEDUR																✓

Pada tabel 7 maka dapat diketahui korespondensi antara permasalahan dan tujuan keamanan melalui penggunaan tanda (✓). Justifikasi tersebut menunjukkan bahwa tujuan keamanan dapat mengatasi permasalahan keamanan yang berkaitan dengan tepat. Berdasarkan tabel 7, maka dapat diketahui sebagai berikut:

a. O.PENGGUNA_AUTENTIK dapat memitigasi T.BACA_LOG dan mendukung P.PENGGUNA malalui penyediaan mekanisme identifikasi dan autentikasi pengguna
b. O.ADMIN dapat memitigasi T.BACALOG dan mendukung P. VERIFIKASI_VISUAL dengan menyediakan kebijakan hanya admin yang dapat mengubah mode untuk mendukung operasional layanan masal sesuai Permendagri 76 Tahun 2020
c. O.VERIFIKASI dapat memitigasi T.COBA_VERIFIKASI melalui melalui perenapan mekanisme untuk menjamin pemilik KTP-el yang sah.
d. O.RAHASIA dapat memitigasi P.PENGUNGKAPAN melalui penyediaan meknisme untuk mengamankan informasi yang ditransmisikan
e. O.AUDIT dapat memitigasi T.BACALOG dan T.GAGAL_MEMBUAT_LOG melalui menyediakan mekanisme untuk membuat log dan persedianya log aktivitas pengguna.
f. O.UPDATE dapat memitigasi T.MALWARE melalui mekanisme untuk mendeteksi kesalahan integritas.
g. O.KONDISI dapat memitigasi T.MALAFUNGSI melalui mekanisme pemulihan terhadap fungsi tertentu sehingga kegagalan fungsi dapat dikembalikan pada keadaan aman.
h. O.PROTEKSI_FISIK dapat memitigasi T.TAMPERING melalui penyediaan fitur deteksi serangan fisik.
i. OE.PENGGUNA mendukung P.PENGGUNAAN melalui tersedianya kebijakan petunjuk operasional TOE dan A.PENGGUNA yang mana pengguna TOE telah sesuai dengan asumsi keamanan sehingga dapat memitigasi T.BACALOG.

j. OE.KONEKSI mendukung A.KONEKSI dengan mensyaratakan bahwa TOE terhubung dengan jaringan terpercaya
k. OE.VERIFIKASI_VISUAL mendukung P.VERIFIKASI_VISUAL dengan menyediakan kebijakan untuk mengoperasionalkan TOE ketika melakukan verifikasi visual
l. OE.SAM mendukung P.SAM dan A.SAM dengan menerapkan SAM yang aman sesuai dengan spesifikasi pada Permendagri 76 Tahun 2020
m. OE.LINGKUNGAN mendukung A.LING-KUNGAN dengan mensyaratkan TOE dioperasional pada lingkungan yang aman dengan pengelolaan yang baik
n. OE.TIMESTAMP mendukung A.TIME-STAMP dengan menyediakan *timestamp* yang dapat dipercaya
o. OE.MANAJEMEN_KUNCI mendukung P.MANAJEMEN_KUNCI dan A.MANA-JEMEN_KUNCI dengan menerapkan manajemen dan pelindungan kunci yang aman untuk autentikasi cip sesuai dengan standar nasional dan/atau internasional yang berlaku.
p. OE.PROSEDUR mendukung P.PENGGUNA, P.PASSWORD, P.VERIFIKASI_VISUAL, P.SAM, P.PENGGUNAAN, P.MANAJEMEN _KUNCI dan A.PROSEDUR untuk mensyaratkan pihak yang berwenang menyusun dan menerbitkan prosedur-prosedur yang dibutuhkan untuk operasionalan TOE.

3.4. Pengidentifikasian Tujuan Keamanan

Persyaratan fungsi keamanan disusun dengan menentukan kelas fungsi keamanan berdasarkan ISO/IEC 15408-2:2022 dan ISO/IEC TS 19608:2018. Pemilihan kelas fungsi keamanan ini mempertimbangkan 8 (delapan) tujuan keamanan TOE. Tabel 8 menunjukkan pemetaan fungsi keamanan terhadap setiap tujuan keamanan TOE. Sedangkan tujuan keamanan untuk lingkungan operasional TOE telah terpenuhi dengan mendukung kebijakan keamanan organisasi dan pemenuhan asumsi untuk mendukung operasional TOE.

Tabel 8. Pemetaan Fungsi Keamanan untuk Tujuan Keamanan TOE

Tujuan Keamanan TOE	Fungsi Keamanan
O. PENGGUNA _AUTENTIK	FCS_COP.1 Operasi kriptografi (password hashing)
	FIA_ATD.1 Definisi atribut pengguna
	FIA_UAU.2 Autentikasi pengguna sebelum melakukan tindakan
	FIA_UID.2 Identifikasi pengguna sebelum melakukan tindakan
O.ADMIN	FDP_ACC.1 Kontrol akses subset
	FMT_MOF.1 Manajemen perilaku fungsi keamanan
	FMT_SMF.1 Spesifikasi fungsi manajemen
	FMT_SMR.1 Peran keamanan
O.VERIFIKASI	FDP_ACC.1 Kontrol akses subset
	FIA_AFL.1 Penanganan kegagalan autentikasi
	FIA_UAU.2 Autentikasi pengguna sebelum melakukan tindakan
	FIA_UAU.7 Umpan balik autentikasi yang dilindungi
	FIA_UID.2 Identifikasi pengguna sebelum melakukan tindakan
O.RAHASIA	FPT_ITC.1 Kerahasiaan antar fungsi keamanan selama transmisi
O.AUDIT	FAU_GEN.1 Pembangkitan data audit
	FAU_GEN.2 Asosiasi identitas pengguna
	FAU_SAR.1 Reviu audit
	FAU_STG.2 Penyimpanan data audit yang dilindungi
	FAU_STG.4 Tindakan jika terjadi kemungkinan kehilangan data audit
	FDP_DAU.1 Autentikasi basic data
	FPFW_COI.1 Presentasi pilihan
	FPFW_CON.1 Memperoleh persetujuan
	FPFW_DEL.1 Penghapusan dan pengarsipan
O.UPDATE	FPT_FLS.1 Kegagalan dengan preservasi kondisi aman
	FPT_TST.1 Pengujian mandiri fungsi keamanan
O.KONDISI	FPT_RCV.1 Pemulihan manual
	FPT_TST.1 Pengujian mandiri fungsi keamanan
O. PROTEKSI _FISIK	FPT_PHP.1 Deteksi pasif serangan fisik
	FPT_PHP.3 Perlawanan terhadap serangan fisik

Berdasarkan tabel 8, terdapat 25 (dua puluh lima) fungsi keamanan yang terdiri dari 7 (tujuh) kelas keamanan berdasarkan ISO/IEC 15408-2 dan ISO/IEC TS 19608 untuk memenuhi 8 (delapan) tujuan keamanan TOE. Adapun kelas fungsi keamanan tersebut meliputi: fungsi kriptografi, fungsi identifikasi dan autentikasi, fungsi audit, fungsi proteksi data pengguna, fungsi manajemen keamanan, fungsi proteksi fungsional keamanan, dan fungsi persyaratan privasi berdasarkan *framework* privasi berdasarkan ISO/IEC 29100.

Persyaratan jaminan keamanan TOE yang ditentukan merupakan perangkat yang digunakan untuk memverifikasi data penduduk dan kepemilikan kartu identitas penduduk yang mana termasuk dalam data pribadi. Sedangkan kategori ancaman yang mungkin terjadi adalah penyerang yang canggih dengan sumber daya yang melimpah yang bersedia mengambil sedikit risiko. Hal ini karena penyerang berusaha untuk mendapatkan informasi tanpa ada risiko diketahui oleh pihak yang berwenang. Atas pertimbangan tersebut, maka pengguna perangkat pembaca KTP-el membutuhkan tingkat keamanan yang menjamin level menengah hingga tinggi dan sesuai. Berdasarkan matriks *degree of robustness* [19], maka jaminan keamanan yang dipilih adalah EAL 4 dengan jaminan paket berdasarkan ISO/IEC

15408-5:2022 untuk jaminan keamanan pada EAL 4 [14]. Hasil dari penelitian ini berupa dokumen *Protection Profile* Perangkat Pembaca KTP-el Tingkat Kedua.

3.5. Pengujian kelas APE

Berdasarkan hasil rancangan dokumen PP yang telah disusun, peneliti melakukan pengujian secara manual dengan melakukan penilaian kesesuaian pada kelas *Assurance Protection Profile Evaluation* (APE) berdasarkan ISO/IEC 18045:2022. Adapun pengujian tersebut tediri dari 6 (enam) komponen, meliputi pendahulan PP, klaim kesesuaian, definisi permasalahan keamanan, tujuan keamanan, definisi komponen tambahan, dan persyaratan keamanan. Tabel 9 berikut merupakan rekapitulasi hasil pengujian kelas APE berdasarkan ISO/IEC 18045:2022.

Tabel 9. Hasil Pengujian Kelas APE terhadap Dokumen PP Perangkat Pembaca KTP -el Tingkat Kedua V.1.0

Komponen	Hasil Evaluasi
APE_INT.1	Memenuhi Dokumen PP telah mengidentifikasi referensi dengan unik dan gambaran umum TOE dijelaskan secara konsisten. Dokumen PP telah mendekripsikan fungsi dan kegunaan TOE, tipe TOE dan kebutuhan perangkat
APE_CCL.1	Memenuhi Dokumen PP telah mengidentifikasi ISO/IEC 15408 yang diklaim dan konsisten terhadap klaim kesesuaian tambahan dari ISO/IEC 15408.
APE_SPD.1	Memenuhi Dokumen PP telah mendefinisikan 8 (delapan) permasalahan keamanan beserta aset yang dituju, 6 (enam) kebijakan keamanan organisasi untuk mendukung operasional, dan 7 (tujuh) asumsi untuk mendukung operasional TOE.
APE_OBJ.2	Memenuhi Dokumen PP telah menentukan 8 (delapan) tujuan keamanan TOE dan 8 (delapan) tujuan keamanan untuk lingkungan operasional TOE. Adapun setiap tujuan keamanan telah menjawab seluruh definisi permasalahan keamanan. Dokumen PP telah menjelaskan bagaimana tujuan keamanan TOE mampu memitigasi ancaman dan bagaimana tujuan keamanan untuk lingkungan operasional TOE mampu mendukung kebijakan keamanan organisasi dan asumsi.
APE_ECD.1	Memenuhi Dokumen PP telah mendefinisikan dan menjelaskan komponen tambahan terhadap ISO/IEC 15408-2 dan tidak terdapat komponen tambahan terhadap ISO/IEC 15408-3. Adapun komponen tambahan terhadap ISO/IEC 15408-2:2022 yaitu penerapan komponen keamanan FPFW_COI.1, FPFW CON.1 dan FPFW_DEL.1 berdasarkan ISO/IEC TS 19608:2018 untuk pemenuhan fungsional keamanan yang berkaitan dengan pelindungan privasi.
APE-REQ.2	Memenuhi Dokumen PP telah menentukan persyaratan fungsional dan jaminan keamanan dengan jelas, tidak ambigu dan setiap persyaratan fungsional keamanan memenuhi tujuan keamanan TOE.

Berdasarkan tabel 9 di atas, maka evaluasi terhadap *Protection Profile* Perangkat Pembaca KTP-el tingkat kedua memperoleh hasil memenuhi uji untuk seluruh komponen (enam komponen) pada kelas APE berdasarkan ISO/IEC 18045:2022. Atas hal tersebut, maka hasil pengujian terhadap dokumen yang disusun dinyatakan memenuhi kriteria berdasarkan seri ISO/IEC 15408.

4. DISKUSI

Terdapat beberapa penelitian yang telah melakukan penyusunan persyaratan fungsional keamanan berdasarkan ISO/IEC 15408 baik itu pada aplikasi enkripsi file [20] [21], sistem informasi kompetensi personil [22] dan penyelenggaraan sertifikasi [23], sistem absensi biometrik [24] serta kontrol akses aplikasi layanan informasi [25]. Namun pada penelitian tersebut TOE bersifat spesifik terhadap versi tertentu dan tidak berkorelasi secara langsung dengan fungsional keamanan perangkat pembaca KTP-el

Selain itu, juga terdapat penelitian yang telah melakukan pengembangan *Protection Profile* baik itu pada untuk *standalone file encryption* [26], sistem keamanan informasi personal [10], perangkat pembaca kartu cerdas pada bidang kesehatan [9] dan perangkat pembaca KTP-el [11]. Keterbaruan pada penelitian ini dibandingkan dengan penelitian sebelumnya yaitu penelitian ini disusun dengan mempertimbangkan fungsi keamanan sebagaimana yang menjadi amanat dalam Permendagri 76 Tahun 2020 dan mempertimbangkan pelindungan privasi sehingga penyusunan fungsional keamanan yang disusun berdasarkan ISO/IEC 15408-2: 2022 dan ISO/IEC TS 19608:2018. Adapun beberapa komponen fungsional tambahan hasil penelitian yaitu FPFW_COI, FPFW_CON dan FPFW_DEL untuk memberikan pelindungan privasi, FAU_STG untuk penjaminan penyimpanan data audit, dan FPT_RCV untuk pemulihan jika terjadi malafungsi.

Pada penelitian ini dilakukan pengujian terhadap dokumen *Protection Profile* yang disusun pada kelas APE berdasarkan ISO/IEC 18045:2022 untuk pemastian terpenuhinya persyaratan PP sebagaimana ditentukan dalam ISO/IEC 15408-3:2022. Berdasarkan hasil penelitian yang telah dilakukan, dokumen *Protection Profile* yang tersusun telah memenuhi seluruh komponen persyaratan yang ditentukan dalam ISO/IEC 15408-3:2022. Adapun yang menjadi penilaian kesesuaian dalam dokumen *Protection Profile* yang disusun adalah bagian identitas dan pendahuluan *Protection Profile*, klaim kesesuaian, pendefinisian permasalahan keamanan, tujuan keamanan, pendefinisiain komponen tambahan, dan persyaratan fungsional keamanan. Sedangkan pada penelitian sebelumnya tidak

dilakukan pengujian terhadap dokumen *Protection Profile* yang telah disusun.

5. KESIMPULAN

Telah dilakukan pengembangan *Protection Profile* Perangkat Pembaca KTP-el tingkat kedua berdasarkan ISO/IEC 15408:2022 dan ISO/IEC TS 19608:2022. Pendefinisian permasalahan keamanan meliputi 8 (delapan) jenis ancaman, 6 (enam) jenis kebijakan keamanan organisasi dan 7 (tujuh) asumsi. Sedangkan tujuan keamanan TOE yang didefinisikan sebanyak 8 (delapan), sedangkan tujuan keamanan lingkungan operasional yang didefinisikan sebanyak 8 (delapan). Berdasarkan tujuan keamanan TOE, maka spesifikasi keamanan yang telah dirancang terdiri dari 25 (dua puluh lima) komponen persyaratan keamanan untuk memenuhi fungsi keamanan perangkat pembaca KTP-el tingkat kedua sesuai dengan Permendagri 76 Tahun 2020 dan dengan mempertimbangan pelindungan data pribadi dalam kegiatan pemrosesan dan/atau pengendalian data pribadi dengan jaminan keamanan yang ditentukan yaitu EAL 4. Dokumen *Protection Profile* yang telah disusun telah diuji pada kelas APE berdasarkan ISO/IEC 18045:2022 dan dinyatakan memenuhi seluruh persyaratan sebagaimana ditentukan dalam ISO/IEC 15408-3:2022. Adapun penelitian lebih lanjut yang dapat dikembangkan dari penelitian ini yaitu pengembangan *protection profile* perangkat pembaca KTP-el untuk jenis lainnya, misalkan untuk tingkat pertama dan ketiga, serta penyesuian arsitektur perangkat sehingga mendukung integrasi sistem.

DAFTAR PUSTAKA

[1] Kementerian Sekretariat Negara Republik Indonesia, Undang-Undang Nomor 20 Tahun 2014 tentang Standardisasi dan Penilaiain Kesesuaian, Jakarta, 2014.

[2] Kementerian Sekretariat Negara Republik Indonesia, Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara, Jakarta, 2021.

[3] Badan Siber dan Sandi Negara, Peraturan Badan SIber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara, Jakarta, 2021.

[4] Badan Siber dan Sandi Negara, Peraturan Badan Siber dan Sandi Negara Nomor 15 Tahun 2019 tentang Penyelenggaraan Skema Common Criteria Indonesia, Jakarta, 2019.

[5] ISO/IEC, ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model, Switzerland: ISO/IEC, 2022.

[6] Kementerian Dalam Negeri Republik Indonesia, Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 76 Tahun 2020 tentang Perangkat Pembaca dan Penulis seta Perangkat Pembaca Kartu Tanda Penduduk Elektronik, Jakarta: Kementerian Dalam Negeri Republik Indonesia, 2020.

[7] Kementerian Sekretariat Negara Republik Indonesia, Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Jakarta: Kementerian Sekretariat Negara Republik Indonesia, 2022.

[8] D. Priyasa, "Perangkat Pembaca KTP Elektronik Mandiri Untuk Industri Nasional," in *Seminar Nasional Insentif Riset Sinas* , Bandung, 2012.

[9] Y. A. Setyoko and R. Yasirandi, "Security Protection Profile on Smart Card System Using ISO 15408 Case Study: Indonesia Health Insurance Agency," in *2018 6th International Conference on Information and Communication Technology (ICoICT)*, Bandung, Indonesia, 2018

[10] H.-J. Lee, K. Lee and D. Won, "Protection Profile of Personal Information Security System," in *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, Changsha, China, 2011.

[11] M. E. Aminanto and S. Sutikno, "Development of Protection Profile and Security Target for Indonesia Electronic ID Card's (KTP-el) Card Reader Based on Common Criteria V3.1:2012/ SNI ISO/IEC 15408:2014," in *International Conferenceof Advanced Informatics: Concept, Theory and Application (ICAICTA)*, Bandung, 2014.

[12] ISO/IEC, ISO/IEC 15446:2017 Information technology - Security techniques - Guidance for the production of Protection Profiles and Security Targets, Switzerland: ISO/IEC, 2017.

[13] ISO/IEC, ISO/IEC 15408-2 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part: 2 Security functional components, Switzerland: ISO/IEC, 2022.

[14] ISO/IEC, ISO/IEC 15408-5 Information security, cybersecurity and privacy protection - Evaluation criteria dor IT security - Part 5: Pre-defined packages of security requirements, Switzerland: ISO/IEC, 2022.

[15] ISO/IEC, ISO/IEC TS 19608:2018 Guidance for developing security andprivacy functional requirements based on ISO/IEC 15408, Switzerland: ISO/IEC, 2018.

[16] ISO/IEC, ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection

- Evaluation criteria for IT security - Methodology for IT security evaluation, Switzerlan: ISO/IEC, 2022.

[17] W. Caesar and F. Wigunanto, "Perancangan Emulator KTP Elektronik Berbasis Java Card untuk Mendukung Pengujian Fungsionalitas Pembaca KTP Elektronik Industri Nasional," *Jurnal Teknik Elektro*, vol. 8, no. 2, pp. 31-38, 2016.

[18] D. Priyasta and W. Cesar, "Pengembangan Alat Uji Kesesuaian Perilaku Kartu Cerdas terhadap KTP Elektronik," in *Seminar Nasional Sains dan Teknologi*, Jakarta, 2018.

[19] National Security Agency , Information Assurance Technical Framework Release 3.1, Maryland: National Security Agency , 2002.

[20] Y. S. Gustiviana and E. R. Agustina, "Perancangan Spesifikasi Fungsi Keamanan Aplikasi File Encryption (Filtion) Versi 1.0.0 berdasarkan SNI ISO/IEC 15408:2014," in *Seminar Nasional Sains dan Teknologi Informasi*, Medan, 2021.

[21] A. Saut, F. Achmad and E. R. Agustina, "Perancangan Spesifikasi Keamanan pada SIFER berdasarkan SNI ISO/IEC 15408:2014 - Teknologi informasi - Teknik keamanan - Kriteria evaluasi keamanan teknologi informasi," in *The 11th National Conference on Information Technology and Electrical Engineering*, Jogja, 2019.

[22] E. R. Agustina, A. Saut, M. Christine and I. Fitriani, "Perancangan Spesifikasi Keamanan Aplikasi Sistem Kompetensi Personil LSPro BSSN (SIKOMPRONAS) versi 1.0.0 berdasarkan SNI ISO/IEC 15408:2014," in *Seminar Nasional Teknologi Informasi, Komunikasi dan Administrasi*, Balikpapan, 2019.

[23] M. Yudhistira, E. R. Agustina and A. Saut, "Perancangan Spesifikasi Keamanan pada Aplikasi Persiapan Penyelenggaraan Sertifikasi Keamanan Perangkat Teknologi Informasi (SIAGASIKAT) Versi 1.0.0 berdasarkan SNI ISO/IEC 15408:2014," in *The 12th National Conference on Information Technology and Electrical Engineering (CITEE)*, Yogyakarta, 2020.

[24] R. S. P. Yasirandi, A. MHD and E. Fefyosa, "Security Functional Requirements for the Development of a Biometrics Attendance System," in *8th International Conference on Information and Communication Technology (ICoICT)*, Yogyakarta, 2020.

[25] F. Achmad and E. R. Agustina, "Perancangan Spesifikasi KeamananKontrol Akses pada Aplikasi Layanan Informasi di Lingkungan Instansi Pemerintah," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 6, no. 2, pp. 195-200, 2019.

[26] E. R. Agustina and Y. S. Gustiviana, "Perancangan Protection Profile untuk Standalone File Encryption berdasarkan SNI ISO/IEC 15408:2014," in *Seminar Nasional Sains dan Teknologi Informasi*, Medan, 2021.