Implementasi *Registration Authority* dan Sistem *Personal Security Environment* menggunakan *Smart card*

Implementation of Registration Authority and Personal Security Environment System using Smart card

Gladhi Guarddin[1], Jundi Ahmad Alwan[2]
[1,2]Fakultas Ilmu Komputer, Universitas Indonesia
E-mail: [1]adin@ui.ac.id, [2]jundi.ahmad@ui.ac.id

Abstrak

Penelitian ini bertujuan untuk menghasilkan analisis, rancangan, dan prototipe *Personal Security Environment (PSE)* menggunakan *smart card*. Analisis dan rancangan dilakukan dengan berdasarkan peraturan perundangan tentang infrastruktur kunci publik (IKP) dan sertifikat elektronik, dokumen peraturan PSrE Induk, spesifikasi Konsorsium *Smart card* Indonesia (KSCI). Analisis dan rancangan tersebut kemudian diimplementasikan menjadi sebuah prototipe sistem *Registration Authority* (RA) yang bertugas untuk melakukan pendaftaran sertifikat elektronik bagi pengguna dan melakukan penyimpanan ke dalam PSE berupa *smart card* berbasis *chipset Xirka* yang merupakan Kartu Tanda Mahasiswa (KTM) Universitas Indonesia. Hasil implementasi menunjukkan bahwa seluruh skenario pengujian berhasil dilaksanakan dengan catatan kunci privat dan sertifikat elektronik masih diimplementasikan di dalam *field chipset Xirka* yang diperuntukkan sebagai penyimpanan foto dan *fingerprint.*

Kata kunci: PSrE, Xirka, *Personal Security Environment* (PSE), kartu pintar, KSCI

Abstract

The aim of this research is to produce analysis, design, and prototype of Personal Security Environment (PSE) using smart cards. The analysis and design is carried out based on the laws and regulations regarding public key infrastructure (IKP) and electronic certificates, the PSrE Induk regulatory documents, specifications of the Indonesian Smart card Consortium (KSCI). The analysis and design is then implemented into a prototype of the Registration Authority (RA) system which is in charge of registering electronic certificates for users and storing them into the PSE in the form of a smart card based on the Xirka chipset which is the University of Indonesia Student Identity Card (KTM). The results of the implementation show that all test scenarios were successfully carried out with private key records and electronic certificates still being implemented in the Xirka chipset field which is intended as photo and fingerprint storage.

Keywords: PSrE, Xirka, Personal Security Environment (PSE), Smart card, KSCI

1. PENDAHULUAN

Pemerintah Indonesia telah menerbitkan berbagai peraturan sebagai dasar hukum penyelenggaraan transaksi elektronik dan Infrastruktur Kunci Publik (IKP). Dua buah dasar hukum yang dapat dijadikan acuan penyelenggaraan transaksi elektronik adalah Peraturan Pemerintah nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Republik Indonesia nomor 11 tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik. Penyelenggaraan sertifikasi elektronik diperjelas juga dalam dokumen *Certificate Policy* dan *Certificate Practice Statement Root CA* Indonesia [1] disebutkan bahwa untuk menyelenggarakan sertifikasi elektronik dan IKP, sebuah lembaga, baik instansi pemerintah maupun non-instansi pemerintah, perlu terdaftar dan tersertifikasi oleh

menteri. Lembaga yang telah tersertifikasi tersebut disebut Penyelenggara Sertifikasi Elektronik (PSrE) Berinduk. Sebuah lembaga non-instansi pemerintah dapat mendaftarkan diri menjadi lembaga PSrE sesuai dengan peraturan yang berlaku.

Pada penelitian ini dilakukan analisis, rancangan, dan implementasi prototipe sistem PSrE Berinduk sesuai dengan peraturan yang diterbitkan oleh pemerintah dan dilakukan analisis, rancangan, dan implementasi untuk memanfaatkan *smart card* sebagai PSE untuk menyimpan kunci publik, kunci privat, dan sertifikat elektronik sebagai identitas digital sebagai persiapan penyelenggaraan sertifikasi elektronik dengan infrastruktur PSrE sebagai IKP.

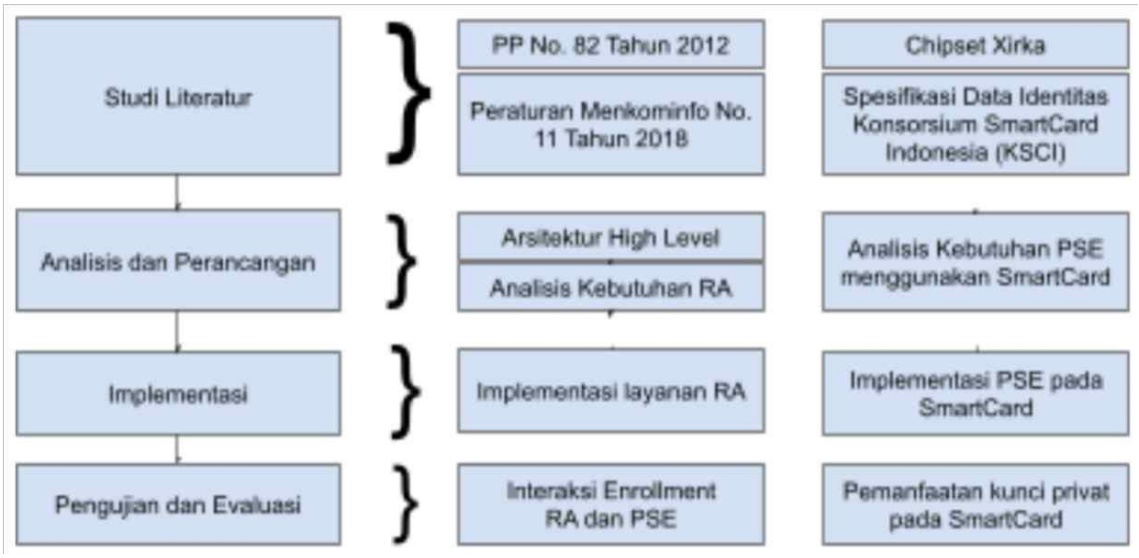
Personal Security Environment (PSE) merupakan sebuah environment, baik hardware maupun *software*, yang berfungsi untuk menyimpan kunci privat milik pengguna dengan aman. Di dalam proses penerbitan kunci privat pengguna menurut Klaus Schmeh [2], proses penerbitan sertifikat elektronik yang sering dikenal dengan istilah *enrollment* dapat dilakukan dengan beberapa cara yaitu:

1. *Enrollment* dengan inisialisasi secara *offline*, dan pembangkitan kunci dilakukan oleh pengguna (decentralized key generation). Kelemahan cara ini adalah pengguna harus mencari cara sendiri untuk membangkitkan pasangan kunci. Tidak ada jaminan juga bahwa kunci privat disimpan oleh pengguna dengan aman.
2. *Enrollment* dengan inisialisasi secara *online*, dan pembangkitan kunci dilakukan oleh pengguna *(decentralized key generation).* Kelemahan cara ini sama dengan cara sebelumnya ditambah jika koneksi tidak aman maka *man-in-the-middle attack* dapat terjadi dan proses *enrollment* menjadi tidak aman. Selain itu diperlukan mekanisme registrasi yang tidak memungkinkan seseorang menggunakan identitas orang lain.
3. *Enrollment* dengan inisialisasi secara *offline*, dan pembangkitan kunci dilakukan oleh *CA (centralized key generation).* Dengan cara ini, pembangkitan kunci dilakukan oleh CA. CA kemudian menerbitkan sertifikat elektronik berdasarkan kunci publik pengguna. Kemudian sertifikat elektronik dan kunci privat dari pengguna diberikan kepada *RA (Registration Authority).* RA membungkus sertifikat elektronik dan kunci privat dengan PSE pengguna. Kemudian PSE yang telah berisi kunci privat dan sertifikat elektronik dikembalikan kepada pengguna. Cara ini memungkinkan CA untuk melakukan *key recovery* di masa depan karena CA menyimpan dengan aman kunci privat pengguna.

Pada penelitian sebelumnya yang berkaitan dengan PSrE [4] dilakukan studi yang berfokus pada standardisasi dan manajemen penyelenggaraan PSrE di Indonesia, begitu pula beberapa penelitian tentang pemanfaatan *smart card* dalam transaksi elektronik [5][6] dan penerapan pada *IoT dan Blockchain* [7][8][9][10]. Fokus pada penelitian ini adalah melakukan implementasi PSE mengikuti mekanisme sesuai dengan alur *key enrollment* no 3 yang diterapkan pada *smart card* sebagai media penyimpanan kunci privat. Berdasarkan fokus tersebut, penelitian ini menghasilkan prototipe sistem *Registration Authority (RA)* yang dapat diintegrasikan dengan PSE menggunakan *smart card.* Manfaat dari penelitian ini adalah agar kunci privat yang sudah dibangkitkan langsung dapat dimasukkan kedalam PSE sehingga pengguna tidak dapat mengakses secara langsung dan menjamin kerahasiaan kunci. Selain itu juga diharapkan dapat menjadi literatur pendukung penerapan sistem PSrE Berinduk, RA dan PSE sesuai peraturan perundangan di Indonesia.

2. METODE PENELITIAN

Penelitian ini dilakukan dalam 4 (empat) tahap besar dengan rincian yang dapat dilihat pada Gambar 1 berikut ini:



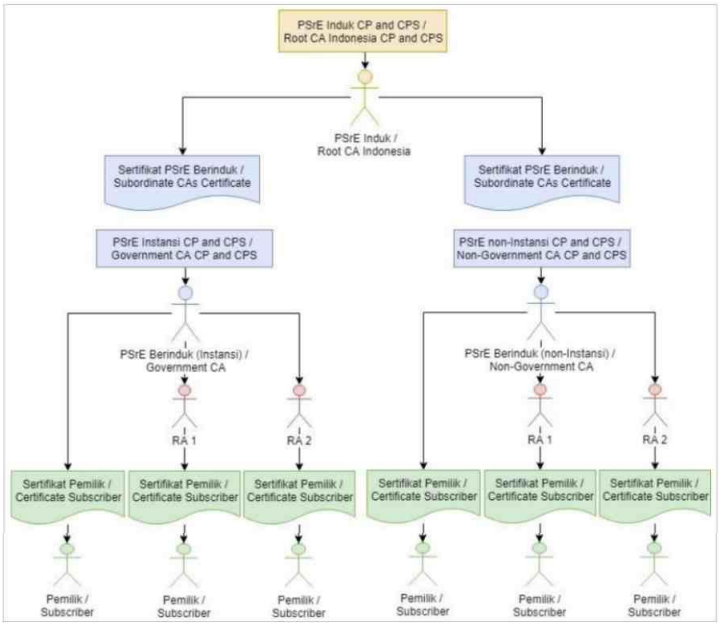
Gambar 1 Tahapan Metode Penelitian

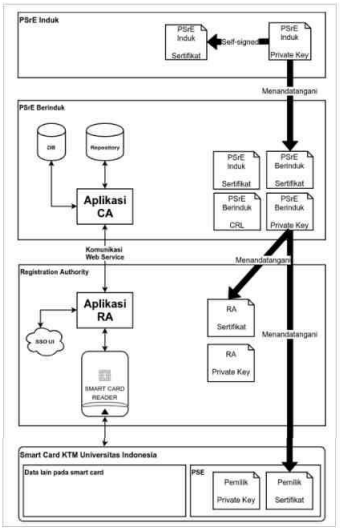
Pada tahap studi literatur, dilakukan beberapa studi meliputi PP No. 82 Tahun 2012 mengenai sistem dan transaksi elektronik secara umum termasuk didalamnya pembahasan tentang sistem penyelenggara sertifikat elektronik, Permenteri Kominfo No. 11 tahun 2018 mengenai penyelenggaraan sertifikat elektronik dan penyelenggara sertifikat elektronik, Pemanfaatan *chipset Xirka* dengan *interface contact standard ISO/IEC 7816-3* transmisi protokol tipe T=0 (*byte-oriented*) dengan struktur *file tree MF, DF, dan EF* yang menentukan cara pengaksesan data untuk aktivitas baca dan tulis kedalam *smart card.* Dilanjutkan dengan studi literatur atas spesifikasi Konsorsium *Smart card* Indonesia [3] untuk pemetaan data yang dipergunakan dalam penyimpanan kunci privat dan sertifikat elektronik di dalam *smart card.*

Tahap analisis dan perancangan dilakukan berdasarkan literatur yang seluruhnya berkaitan dengan penerapan *smart card* sebagai *Personal Secure Environment (PSE).* Secara *high level*, arsitektur IKP mengikuti hirarki IKP PSrE di Indonesia yang juga selaras dengan beberapa referensi penelitian di negara lain dalam hal penerapan PKI berbasis sertifikat digital [11][12]. Hirarki rancangan implementasi pada penelitian ini dapat dilihat pada Gambar 2.a. PSrE Induk Indonesia merupakan *root CA* dari IKP di Indonesia. PSrE Induk hanya bertugas untuk mengelola sertifikat elektronik milik PSrE Berinduk dan tidak menerbitkan sertifikat elektronik langsung kepada pemilik. PSrE Berinduk merupakan PSrE pada tingkatan kedua di bawah PSrE Induk. Pada dasarnya tanggung jawab dari PSrE Berinduk sama dengan tanggung jawab dari PSrE Induk karena keduanya merupakan PSrE. Yang membedakan adalah jenis sertifikat elektronik yang dikelola. PSrE Induk mengelola sertifikat elektronik PSrE Berinduk sementara PSrE Berinduk mengelola sertifikat elektronik pemilik. Kemudian proses *enrollment* dan transmisi kunci privat diinisialisasi secara *offline* ke dalam PSE berupa *Smart card* pemilik/*subscriber.*

Dalam melakukan implementasi di UI, rancangan dapat dilihat pada Gambar 2.b. Rancangan ini disusun berdasarkan kebutuhan bahwa *Smart card* yang dipergunakan adalah KTM (Kartu Tanda Mahasiswa) dengan *chipset Xirka* yang berinteraksi secara offline dengan *RA (Registration Authority)* yang mendukung 6 aspek pengukuran tingkat kepercayaan terhadap sistem CA [12]. Interaksi antara *Smart card* dengan RA menggunakan *Contact card Reader* untuk pengiriman data berupa APDU yang berisi kunci privat dan sertifikat elektronik yang sudah ditandatangani oleh PSrE Berinduk. Komunikasi antara RA dengan PSrE Berinduk adalah

menggunakan *webservice* yang dienkripsi menggunakan sertifikat elektronik digital RA yang terdaftar pada PSrE Berinduk. Antara PSrE Berinduk dengan PSrE Induk, yang merupakan *Root CA*, berlangsung secara *offline* yang dilakukan di luar lingkup penelitian ini.

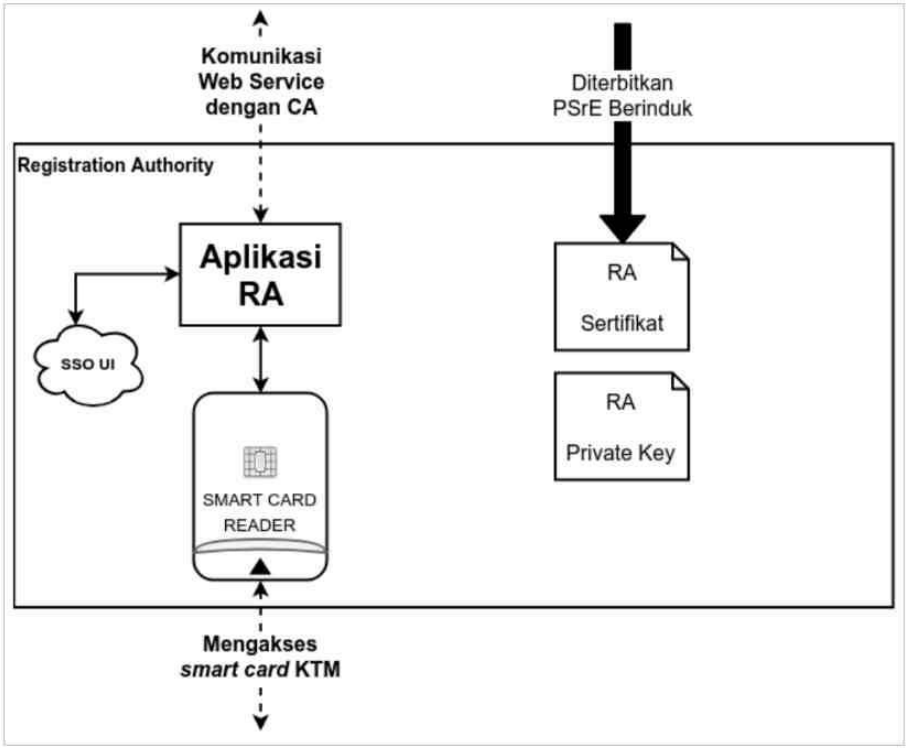




2.a. Hirarki IKP PSrE [1] 2.b. Rancangan implementasi di UI

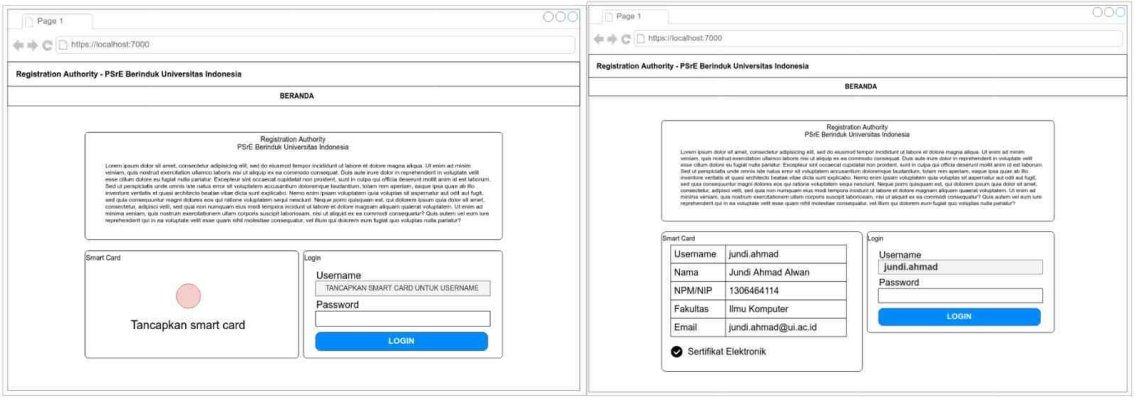
Gambar 2 Arsitektur High Level penerapan IKP

Interaksi antara PSrE Induk dan PSrE Berinduk berupa penerbitan sertifikat elektronik PSrE Berinduk dilakukan secara offline karena dalam penelitian ini PSrE Induk tidak difungsikan seperti PSrE melainkan sebagai sebatas penerbit sertifikat elektronik PSrE Berinduk. Sementara itu CA PSrE Berinduk dan RA berinteraksi menggunakan interface web service REST API untuk menjalankan fungsi-fungsi pelayanan PSrE Berinduk seperti menerbitkan, mencabut, dan memperbarui sertifikat elektronik, dan juga memperbarui kunci. Interaksi antara pemilik dengan sistem RA dilakukan melalui interface aplikasi dari RA agar pemohon atau pemilik menginisiasi permintaan kepada PSrE Berinduk untuk menerbitkan, mencabut, dan memperbarui sertifikat elektronik, dan juga memperbarui kunci milik pemohon. Pada Gambar 3 dijelaskan alur interaksi antara RA dengan PSE yang membutuhkan kontak fisik berupa pemilik perlu menancapkan *smart card* KTM miliknya pada card reader yang terhubung dengan aplikasi RA. *Smart card* ini berfungsi sebagai PSE untuk menyimpan kunci privat dan sertifikat elektronik.



Gambar 3 Arsitektur dasar RA

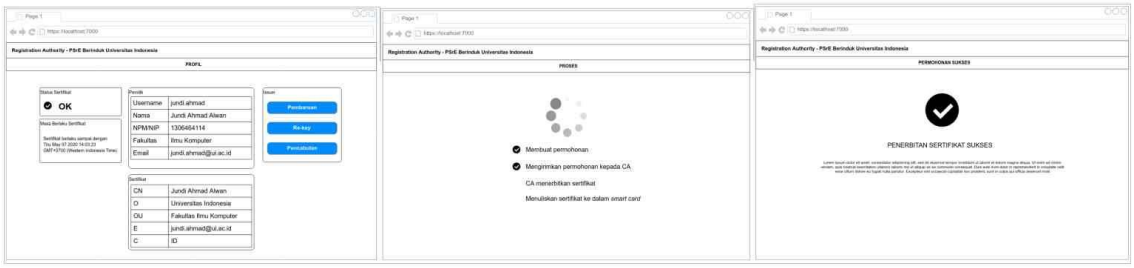
Sebuah RA tidak perlu ditanam pada sebuah server sentral melainkan dapat dijalankan pada komputer lokal dan menggunakan kunci privat dan sertifikat elektronik yang ditandatangani oleh PSrE Berinduk untuk berkomunikasi secara aman dengan CA PSrE Berinduk. Ketika RA dapat terhubung dengan PSrE maka fungsi RA sudah dapat dipergunakan dengan rancangan interaksi berupa tampilan web interface pada Gambar 4.



4.a. Ketika *smart card* tidak tertancap 4.a. Ketika *smart card* tertancap

Gambar 4 Rancangan Interaksi RA dengan *smart card*

Rancangan *web interface* untuk melayani fungsi penerbitan, pembaruan, penggantian *passphrase* pada kunci privat, dan pencabutan *(revoke) key* dapat dilihat pada Gambar 5. Seluruh fungsi yang disediakan oleh RA (Gambar 5.a) terhubung secara *centralized* pada PSrE Berinduk untuk mendapatkan validasi *certificate* terhadap data *Certificate Revocation Table* (CRT) [13]. Ketika proses sedang berlangsung, RA menampilkan kemajuan atas tahapan-tahapan fungsi yang dapat dilihat pada Gambar 5.b. Apabila proses sudah selesai, RA menampilkan status akhir yang dapat dilihat pada Gambar 5.c.



5.a. Tampilan layanan RA 5.b. Tampilan progress 5.c. Tampilan hasil proses

Gambar 5 Rancangan Web Interface RA

Implementasi aplikasi RA dibagi menjadi dua bagian besar, yaitu implementasi backend dan implementasi frontend. Implementasi dari backend aplikasi RA akan dibagi menjadi beberapa komponen besar. Komponen-komponen backend tersebut antara lain yaitu:

1. Fungsi enkripsi dan verifikasi otentikasi dari CA
2. Fungsi otentikasi pemilik
3. *Event handler smart card reader*
4. Socket server untuk berkomunikasi *real-time* dengan *frontend* RA
5. *Event handler* halaman *home*
6. *Event handler login*
7. *Event handler* halaman profil
8. *Event handler* penerbitan sertifikat
9. *Event handler* pencabutan sertifikat
10. *Event handler* pembaharuan sertifikat
11. *Event handler re-key* sertifikat

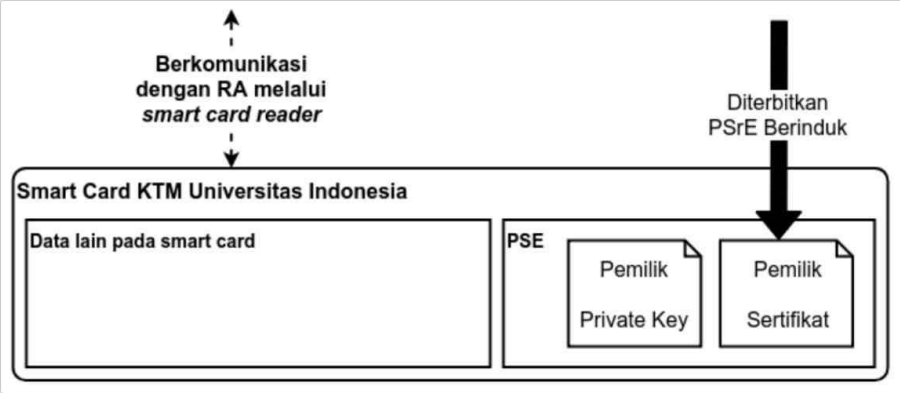
Sementara itu komponen-komponen *frontend* antara lain:

1. *User interface* halaman *home*
2. *User interface* halaman profil
3. *User interface* halaman proses permohonan
4. *User interface* halaman sukses/gagal
5. *Socket client* untuk berkomunikasi *real-time* dengan *backend* RA

Berkas-berkas penting yang perlu disimpan pada PSE antara lain kunci privat dan sertifikat elektronik yang telah diterbitkan, rancangan arsitektur PSE dapat dilihat pada Gambar 6. Walaupun sertifikat elektronik bukan merupakan berkas yang wajib disimpan pada PSE namun dengan menyimpan sertifikat elektronik pada PSE di dalam KTM, terdapat banyak potensi pemanfaatan KTM untuk keperluan lain di masa mendatang yang membutuhkan sertifikat elektronik, dan kunci publik yang terkandung di dalamnya. Dengan adanya sertifikat elektronik, maka aplikasi pengguna PSE akan memiliki kemudahan dengan tidak perlu lagi mengakses *repository* PSrE Berinduk untuk mendapatkan sertifikat elektronik pemilik dan dapat beroperasi secara *offline*.

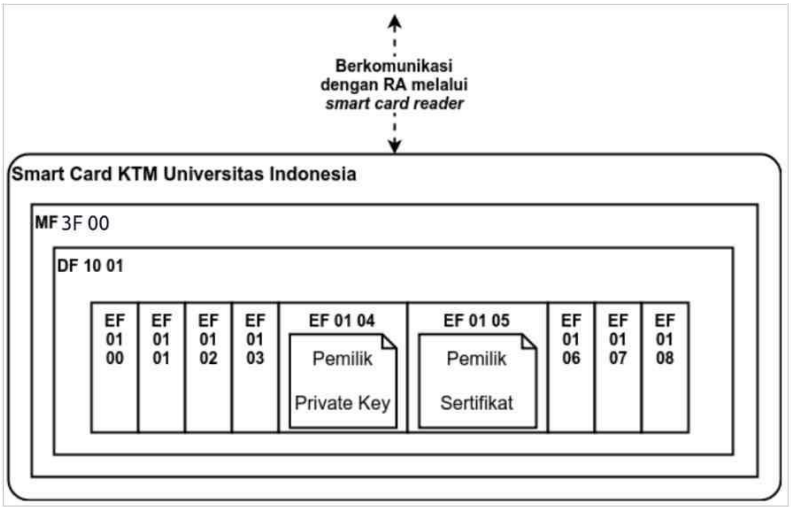
Untuk dapat melakukan akses baca/tulis kunci privat dan sertifikat elektronik ke dalam *smart card* dengan spesifikasi KSCI perlu dilakukan *data chunker*. Hal ini diperlukan untuk mengakomodasi limitasi dari protokol komunikasi T=0 yang hanya dapat melakukan transmisi, baik baca atau tulis, maksimal sebesar 255 *byte*. Untuk kasus penulisan, *data chunker* akan digunakan untuk memecah *command* APDU per pemanggilan 255 *byte* data secara berurutan. *Data chunking* dibagi menjadi beberapa tahapan yaitu 1) Melakukan *chunking* panjang data *Method* menerima *input* yaitu sebuah nilai integer merepresentasikan panjang dari data yang ingin ditulis dan memberikan *output* berupa *array of integer* yang berisi deretan angka merepresentasikan panjang data yang sudah dilakukan *chunking*, menghasilkan *chunked length*. Contoh *input* 300 *byte*s maka *output* [255, 45]; *input* 265 *byte*s maka *output* [255, 10]; *input* 1000 *byte*s maka *output* [255, 255, 255, 235]. 2) Melakukan *chunking* data berdasarkan *chunked length*.

Tahapan ini hanya diperlukan untuk penulisan data. Pada tahapan ini data yang dimasukkan dalam bentuk HEX *string* dengan *output* berupa *array* of data yang telah dilakukan *chunk* berdasarkan *chunked length*, menghasilkan *chunked data*. 3) Membuat daftar pemanggilan APDU *command*. Jika *command* merupakan pembacaan maka APDU *command* yang dihasilkan merupakan kombinasi *chunked length* dengan CLA, INS, P1, P2. Contoh untuk data dengan panjang 300 maka *output*nya yaitu [00B00000FF, 00B000FF2D].



Gambar 6 Arsitektur dasar PSE pada *smart card*

Input berupa jenis data yang akan dibaca berdasarkan struktur data spesifikasi KSCI. Kemudian APDU *command* generator memberikan *output* satu atau lebih *command* APDU yang siap ditransmisikan secara berurutan berdasarkan hasil data chunker sebelumnya. Berdasarkan hasil analisis atas spesifikasi KSCI, kunci privat akan diletakkan pada *field* foto. *Field* foto dapat diakses pada alamat MF '3F 00', DF '10 01', dan EF '01 04'.



Gambar 7 Alamat penyimpanan kunci privat dan sertifikat digital di dalam *smart card*

Pembacaan akan dilakukan dengan template *command* APDU dengan langkah pengaksesan dan pembacaan data kunci privat pada *field* foto sebagai berikut:

1. Mengakses MF, APDU: '00 A4 00 00 02 3F 00'
2. Mengakses direktori DF, APDU: '00 A4 00 00 02 10 01'
3. Mengakses direktori EF Foto, APDU: '00 A4 00 00 02 01 04'
4. Mendapatkan panjang data pada EF Foto dari hasil pemanggilan APDU *Field* dan *Length Map* . Panjang data pada suatu *field* diwakili oleh sebuah variabel yang perlu dicek setiap kali dilakukan pembacaan data. Pengambilan *Field* dan *Length Map* dapat dilakukan sesuai instruksi yang dijelaskan dalam spesifikasi KSCI.

5. Membaca data pada EF Foto sesuai dengan panjang data, dengan susunan APDU: '00 B0 [offset P1] [offset P2] [partial *length*]'. Offset P1, offset P2, dan partial *length* merupakan variabel bebas yang perlu dikalkulasi setiap kali melakukan pemanggilan per chunk data dengan ukuran maksimal 255 *byte*.
6. Menggabungkan semua response data menjadi satu sesuai dengan urutan pemanggilan.
7. Menerjemahkan data kunci privat dari bentuk HEX ke bentuk ASCII dari data yang telah digabungkan.

Penulisan akan dilakukan dengan template *command* APDU dengan langkah-langkah pengaksesan dan penulisan data kunci privat pada *field* foto sebagai berikut.

1. Mengakses MF, APDU: '00 A4 00 00 02 3F 00'
2. Mengakses direktori DF, APDU: '00 A4 00 00 02 10 01'
3. Mengakses direktori EF Foto, APDU: '00 A4 00 00 02 01 04'
4. Menulis data ke dalam EF Foto, APDU: '00 D0 [offset P1] [offset P2] [data *length*] [data]'. Offset P1, offset P2, data *length*, dan data merupakan variabel yang perlu dikalkulasi setiap kali melakukan penulisan per-chunk dengan ukuran maksimal 255 *byte*. Setiap kali penulisan berhasil didapatkan response APDU '90 00'.
5. Memperbarui informasi panjang data foto pada *Field* dan *Length Map* sesuai instruksi yang dijelaskan dalam spesifikasi KSCI.

Mengikut spesifikasi KSCI, dalam penelitian ini *field* foto dengan alamat EF Foto APDU '01 04' dapat dipergunakan untuk penyimpanan kunci privat, sedangkan *field fingerprint* dengan alamat EF *Fingerprint* APDU '01 05' dipergunakan untuk penyimpanan sertifikat elektronik pengguna. Dengan cara yang sama seperti kunci privat, sertifikat elektronik dapat dibaca dan ditulis dari dalam *smart card*.

Smart card kartu tanda mahasiswa (KTM) Universitas Indonesia mengadopsi spesifikasi KSCI dengan basis kartu merupakan *chipset Xirka* yang kompatibel dengan standar ISO7816-3. Namun pada spesifikasi data identitas KSCI [3] tidak ditemukan *field* yang spesifik diperuntukkan menyimpan kunci privat dan sertifikat elektronik. Dari spesifikasi dapat dijumlahkan dari seluruh *field* bahwa total kapasitas memori yang tersedia adalah 9061 *byte*. Panjang konten kunci privat dengan modulus 4096 bit memiliki ukuran 3000-3500 *byte*s. Sementara itu sertifikat elektronik bervariasi tergantung dengan konten yang tersimpan di dalamnya, namun dapat diperkirakan jika menggunakan konfigurasi PSrE maka panjang konten sertifikat elektronik yang dihasilkan memiliki ukuran 2000-2500 *byte*. Total dibutuhkan sekitar 5000-6000 *byte* untuk menyimpan kunci privat dan sertifikat elektronik.

Pada spesifikasi KSCI tidak ada blok *field* yang memiliki panjang blok yang cukup untuk menampung konten sebanyak 5000-6000 *byte* sekaligus. Namun jika diperhatikan terdapat *field* foto dan *field fingerprint* yang memiliki kapasitas masing-masing 4096 *byte*, total 8192 *byte*. *Field* foto dapat ditemukan pada alamat MF '3F 00', DF '10 01', dan EF '01 04'. Sementara *field fingerprint* dapat ditemukan pada alamat Akses ke MF '3F 00', DF '10 01', dan EF '01 05'. Kedua *field* ini dapat dimanfaatkan untuk menyimpan kunci privat dan sertifikat elektronik pada KTM. Oleh karena itu ditetapkan bahwa implementasi pada *smart card* KTM Universitas Indonesia akan digunakan *field* foto untuk menyimpan kunci privat dan *field fingerprint* untuk menyimpan sertifikat elektronik dengan asumsi kedua *field* tersebut kosong dan tidak dipergunakan.

3. HASIL DAN PEMBAHASAN

Sistem RA yang berinteraksi dengan *smart card* PSE diimplementasikan menggunakan platform NodeJs dengan bahasa pemrograman JavaScript. Pemanggilan perintah APDU ke dalam *smart card* dilakukan dengan memanfaatkan pustaka node.js "pscslite" sebagai *application-level interface* yang dapat diprogram sesuai dengan pola APDU yang sudah dijelaskan pada bagian analisis, khususnya ketika penulisan dan pembacaan kunci privat maupun sertifikat elektronik. Sebelum sebuah RA dapat berfungsi dan melayani pengguna, perlu dilakukan inisialisasi pasangan kunci yang dapat diterima ketika berkomunikasi dengan PSrE. Dapat dilihat pada Gambar 8 di bawah ini, sebuah RA diinisiasi dengan kunci modulus 4096 dan diberi *commonName*, *organizationName*, dan *countryName* yang disesuaikan dengan kaidah yang diperkenalkan oleh Root CA Indonesia (2018).

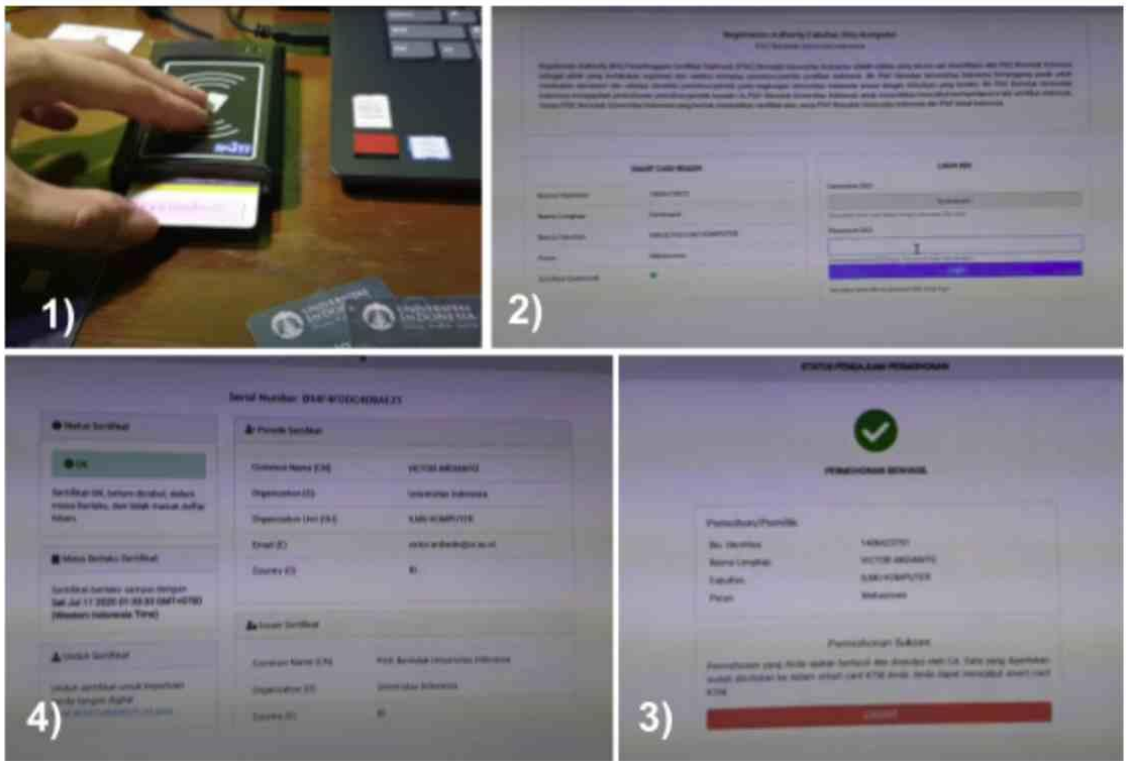
```
jundialwan@jundi-bahasa-ai:~/dev/ra-psre-berinduk$ . ./init.sh
Generating RSA private key, 4096 bit long modulus
.....................................................................................++
.....................................................................++
e is 65537 (0x10001)
Using configuration from openssl.conf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 13352979234085711371 (0xb94f4fddc4d8ae0b)
        Validity
            Not Before: Jun 10 13:14:06 2019 GMT
            Not After : Jun 19 13:14:06 2020 GMT
        Subject:
            countryName               = ID
            organizationName          = Universitas Indonesia
            organizationalUnitName    = Registration Authority PSrE Berinduk Universitas Indonesia
            commonName                = RA001 PSrE Berinduk Universitas Indonesia
            emailAddress              = ra001@ui.ac.id
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                0B:E4:08:DA:BC:8F:CF:85:85:5A:57:5E:E5:68:ED:C3:71:C6:BB:89
            X509v3 Authority Key Identifier:
                keyid:7A:F5:3D:CA:55:96:5D:99:A9:14:87:CA:B6:D7:8F:16:8B:91:2A:EE

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            Authority Information Access:
                OCSP - URI:http://localhost:6277

Certificate is to be certified until Jun 19 13:14:06 2020 GMT (375 days)

Write out database with 1 new entries
Data Base Updated
```

Gambar 8 Inisialisasi sertifikat digital RA

Pada Gambar 9 dapat dilihat hasil implementasi dan pengujian skenario pembuatan sertifikat baru seorang pengguna yang telah ditandatangani oleh RA. Proses dimulai dari 1) menancapkan *smart card* di card reader, kemudian 2) pada browser akan tampil status bahwa kartu sudah tertancap dan informasi identitas sudah terbaca. Ketika pengguna mengajukan sertifikat baru 3) ditampilkan status hasil pembuatan sertifikat, kemudian untuk memvalidasi bahwa sertifikat masih berlaku pengguna dapat melihat pada 4) dengan menggunakan serial number dari sertifikat elektronik yang dimiliki pengguna.

Komunikasi antara *smart card* dengan card reader menggunakan standard APDU ISO 7816-3 yang kemudian masuk ke sistem operasi melalui driver PCSC. Pustaka node.js "pcsclite" menjadi jembatan antara driver PCSC dengan perintah di tingkat aplikasi yang antara kartu dengan pengguna maupun *event* yang dibangkitkan dari interaksi pengguna terhadap aplikasi. Untuk menciptakan interaksi pengguna yang bersifat interaktif menggunakan browser, digunakan framework node.js yang memungkinkan penerapan langsung komunikasi *asynchronous* antara

aplikasi *frontend* web dengan *backend* yang terkoneksi secara fisik dengan perangkat card reader.



Gambar 9 Tampilan halaman web proses inisialisasi sertifikat elektronik

Pada Tabel 1 di bawah ini dapat dilihat seluruh skenario dan hasil pengujian fungsionalitas pada halaman web frontend Registration Authority (RA).

Tabel 1 Skenario dan hasil pengujian *frontend* RA

No	Skenario	Ekspektasi	Hasil
1	Mengakses halaman "/"	Ditampilkan halaman home dan form login	Berhasil.
2	Login tanpa menancapkan kartu	Ditampilkan error tidak boleh login tanpa menancapkan kartu	Berhasil. Ditampilkan pesan error tidak boleh login.
3	Login dengan menancapkan kartu	Dialihkan ke halaman profil pengguna	Berhasil. Login sukses dan dialihkan ke halaman profil pengguna.
4	Mengakses halaman "/user" setelah login	Ditampilkan halaman profil dengan konten akun SSO UI dan rincian sertifikat, jika ada	Berhasil. Ditampilkan halaman profil
5	Mengakses halaman "/user" tanpa login	Ditampilkan error tidak boleh mengakses halaman. 403 Forbidden.	Berhasil. Ditampilkan error 403 Forbidden.
6	Mengakses halaman proses penerbitan sertifikat; belum pernah membuat sertifikat/sertifikat telah dicabut	Ditampilkan halaman proses penerbitan sertifikat dengan indikator proses permohonan.	Berhasil.Ditampilkan halaman proses penerbitan sertifikat.
7	Mengakses halaman proses penerbitan sertifikat; sertifikat masih aktif	Ditampilkan error tidak boleh mengakses halaman. 403 Forbidden.	Berhasil. Ditampilkan error 403 Forbidden.

8	Mengakses halaman proses pencabutan sertifikat; sertifikat aktif	Ditampilkan halaman proses pencabutan sertifikat dengan indikator proses permohonan.	Berhasil. Ditampilkan halaman proses pencabutan sertifikat.
9	Mengakses halaman proses pencabutan sertifikat; sertifikat telah dicabut/belum pernah membuat sertifikat	Ditampilkan error tidak boleh mengakses halaman. 403 Forbidden.	Berhasil. Ditampilkan error 403 Forbidden.
10	Mengakses halaman proses pembaruan sertifikat; pernah membuat sertifikat	Ditampilkan halaman proses pembaruan sertifikat dengan indikator proses permohonan.	Berhasil. Ditampilkan halaman proses pembaruan sertifikat.
11	Mengakses halaman proses pembaruan sertifikat; belum pernah membuat sertifikat	Ditampilkan error tidak boleh mengakses halaman. 403 Forbidden.	Berhasil. Ditampilkan error 403 Forbidden.
12	Mengakses halaman proses re-key sertifikat; pernah membuat sertifikat	Ditampilkan halaman proses re-key sertifikat dengan indikator proses permohonan.	Berhasil. Ditampilkan halaman proses re-key sertifikat.
13	Mengakses halaman proses re-key sertifikat; belum pernah membuat sertifikat	Ditampilkan error tidak boleh mengakses halaman. 403 Forbidden.	Berhasil. Ditampilkan error 403 Forbidden.
14	CA mengembalikan response gagal	Ditampilkan halaman status permohonan dengan indikator permohonan gagal.	Berhasil.Ditampilkan status dan indikator permohonan gagal.
15	CA mengembalikan response sukses	Ditampilkan halaman status permohonan dengan indikator permohonan sukses.	Berhasil.Ditampilkan status dan indikator permohonan sukses.

Pada Tabel 2 di bawah ini dapat dilihat seluruh skenario dan hasil pengujian fungsionalitas pada backend Registration Authority (RA).

Tabel 2 Skenario dan hasil pengujian *backend* RA

No	Skenario	Ekspektasi	Hasil
1	*Smart card* ditancapkan ke dalam reader	Event terpicu. Object reader terbentuk dan siap untuk dilakukan pembacaan/penulisan.	Berhasil. Event terpicu dan object reader terbentuk.
2	*Smart card* dicabut dari dalam reader	Event terpicu. Object reader dihancurkan.	Berhasil. Event terpicu dan object reader dihancurkan.
3	Mengakses MF	Mendapatkan response APDU 61 xx	Berhasil, Mendapatkan response APDU 61 XX.
4	Mengakses DF	Mendapatkan response APDU 61 xx	Berhasil, Mendapatkan response APDU 61 XX.
5	Mengakses EF 0100 untuk *Field + Length Map*	Mendapatkan response APDU 61 xx	Berhasil, Mendapatkan response APDU 61 XX.
6	Membaca file pada EF 0100 berisi *Field + Length Map* pada kartu	Mendapatkan data dalam bentuk hexadecimal dengan panjang 51 *byte*	Berhasil, Mendapatkan response data sepanjang 51 *byte* dalam format HEX
7	Mengakses EF 0104 untuk *field* Foto (kunci privat)	Mendapatkan response APDU 61 xx	Berhasil, Mendapatkan response APDU 61 XX.
8	Menulis file pada EF 0104 berisi kunci privat	Mendapatkan response APDU 61 xx	Berhasil, Mendapatkan response APDU 61 XX.
9	Membaca ulang EF 0104 untuk *field* Foto (kunci privat)	Mendapatkan response data kunci privat dalam bentuk hexadecimal	Berhasil, Mendapatkan response data kunci privat dalam format HEX.

10	Mengakses EF 0105 untuk *field Fingerprint* (sertifikat elektronik)	Mendapatkan response APDU 61 xx	Berhasil, Mendapatkan response APDU 61 XX.
11	Menulis file pada EF 0105 berisi sertifikat elektronik	Mendapatkan response APDU 61 xx	Berhasil, Mendapatkan response APDU 61 XX.
12	Membaca ulang EF 0105 untuk *field Fingerprint* (sertifikat elektronik)	Mendapatkan response data sertifikat elektronik dalam bentuk hexadecimal	Berhasil, Mendapatkan response data sertifikat elektronik dalam format HEX.

Lalu, untuk membuktikan bahwa kunci privat dan sertifikat elektronik yang tersimpan di dalam PSE dapat dipergunakan, telah dilakukan pengujian yang dilampirkan pada Tabel 3.

Tabel 3 Skenario dan hasil pengujian kunci privat dan sertifikat elektronik

No	Skenario	Ekspektasi	Hasil
1	Verifikasi signature kunci privat oleh kunci publik yang terdapat pada sertifikat	Signature terverifikasi benar	Berhasil.
2	Dekripsi data terenkripsi oleh kunci publik menggunakan kunci privat	Data terenkripsi data dibuka oleh kunci privat	Berhasil.
3	Komparasi hash dari modulus pada kunci privat dan kunci publik di dalam sertifikat	Hash harus bernilai sama, kunci privat dan kunci publik tersebut merupakan pasangan kunci yang sah.	Berhasil.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil dari 3 (tiga) kategori skenario pengujian dapat disimpulkan bahwa RA dan PSE yang telah dirancang dan diimplementasikan telah memenuhi semua skenario pengujian dengan baik sesuai ekspektasi dan tidak ditemukan kendala. Kunci privat dan sertifikat elektronik yang ditandatangani oleh PSrE melalui perantara RA juga sudah berhasil tersimpan ke dalam PSE berbasis *smart card*. Selain itu, oleh karena implementasi didasari peraturan pemerintah yang berlaku PSrE Induk, PSrE Berinduk, dan RA sudah memenuhi syarat yang layak sebagai sistem PSrE. Sementara itu, *smart card* dengan spesifikasi KSCI juga sudah dapat berfungsi sebagai PSE meskipun belum ada *field* khusus sebagai tempat penyimpanan kunci privat dan sertifikat elektronik. *Smart card* spesifikasi KSCI dengan *chipset Xirka* tetap dapat berfungsi sebagai PSE dengan menggunakan *field* EF data foto dan *fingerprint*.

Beberapa saran yang dapat dilakukan untuk pengembangan berikutnya adalah 1) untuk menghemat ruang memori pada *smart card* dapat dilakukan kompresi khusus pada konten kunci privat dan sertifikat elektronik sebelum dituliskan ke dalam *smart card*, 2) untuk meningkatkan keamanan pada *smart card*, pada lingkungan produksi disarankan untuk mengimplementasikan Secure Access Module (SAM) pada *smart card* sebagai otentikasi agar pembacaan dan penulisan hanya dapat dilakukan oleh pihak yang berwenang saja, 3) untuk meningkatkan keamanan kunci privat pemilik akan lebih baik jika kunci privat dapat dibangkitkan secara aman di dalam *smart card* dengan menggunakan applet khusus yang menjalankan fungsi pembangkitan kunci privat. Dengan demikian kunci privat dapat aman dan tidak perlu meninggalkan *smart card*, 4) sebuah infrastruktur kunci publik tidak akan bermanfaat apabila tidak dipergunakan oleh proses bisnis lain.

Beberapa contoh potensi pemanfaatan KTM-UI sebagai PSE dengan *chipset Xirka* yang bersifat *contact card* adalah sistem yang mendukung kegiatan tri dharma di lingkungan Universitas Indonesia, antara lain yang mendukung proses bisnis 1) Sistem Penerbitan Ijazah Digital, 2) Sistem Penerbitan Tanda Tangan Digital (Digital Signature), 3) Sistem Penandatanganan Naskah Skripsi/Tesis/Disertasi, dan 4) Identitas Digital Pemilik Kartu (Staf/Mahasiswa).

DAFTAR PUSTAKA

[1] Mariam F. Barata, 2019, *Certificate Policy (CP) Penyelenggaraan Sertifikasi Elektronik (PSrE) Induk Indonesia*, Certificate Policy Root CA Indonesia, Direktorat Pengendalian Aptika Kementerian Komunikasi dan Informatika Republik Indonesia

[2] Schmeh, K., 2006. *Cryptography and public key infrastructure on the internet*, Chichester, Wiley

[3] Konsorsium *Smart card* Indonesia, 2016, Spesifikasi Data *Map* ping & Interoperabilitas Berbasis *Smart card* untuk Fungsi Non-Finansial Antar Lembaga Pendidikan di Indonesia https://www.researchgate.net/publication/354872685_Spesifikasi_Data_*Map*ping_Interoperabilitas_Berbasis_SmartCard_Untuk_Fungsi_Non-Finansial_Antar_Lembaga_Pendidikan_Di_Indonesia, diakses tgl 20 Februari 2021.

[4] Hermawan, Wawan, 2019, Perancangan Manajemen Risiko Keamanan Informasi pada Penyelenggara Sertifikasi Elektronik (PSrE), InComTech: Jurnal Telekomunikasi dan Komputer Vol 9, No 2 (2019)

[5] Haris, M. A., Halomoan, J., Estananto, Hasudungan, F., 2018, Perancangan Surat Tanda Nomor Kendaraan Elektronik Menggunakan *Smart card* dan Secure Access Module, Jurnal Penelitian dan Pengembangan Telekomunikasi, Kendali, Komputer, Elektrik, dan Elektronika, Vol 3 No 2 (2018): TEKTRIKA Vol.3 No.2

[6] Gunardi, Chandra Winata, Wijayanti, Linda, 2018, Aplikasi *Smart card* Sebagai Dompet Elektronik dan Penyimpan Kupon Pada Alat Permainan, Jurnal Elektro, Unika Atma Jaya, Vol 11 No 1

[7] Geeta, S., Sheetal, K., 2018, A lightweight multi-factor secure *smart card* based remote user authentication scheme for cloud-IoT applications, Journal of Information Security and Applications Vol 42, October 2018, Pages 95-106

[8] B.B.Gupta, Megha Quamara, 2018, An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using *smart card*s, Procedia Computer Science Volume 132, 2018, Pages 189-197

[9] Neyire Deniz Sarier, 2021, Efficient biometric-based identity management on the Blockchain for smart industrial applications, Pervasive and Mobile Computing Vol 71, February 2021

[10] Gibson Barbosa, Patricia Takako Endo, Djamel Sadoka, 2019, An internet of things security system based on grouping of *smart card*s managed by *field* programmable gate *array*, Computers & Electrical Engineering Vol 74, March 2019, Pages 331-348

[11] Satoshi Uda, Mikifumi Shikida, 2016, Challenges of Deploying PKI based Client Digital Certification, SIGUCCS '16: Proceedings of the 2016 ACM SIGUCCS Annual ConferenceNovember 2016 Pages 55–60

[12] Michael P. Heinl, Alexander Giehl, Norbert Wiedermann, Sven Plaga, Frank Kargl, 2019, MERCAT: A Metric for the Evaluation and Reconsideration of Certificate Authority Trustworthiness, CCSW'19: Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop November 2019 Pages 1–15

[13] Luke Dickinson, Trevor Smith, Kent Seamons, 2019, Leveraging Locality of Reference for Certificate Revocation, ACSAC '19: Proceedings of the 35th Annual Computer Security Applications ConferenceDecember 2019 Pages 514–528