PEMANFAATAN INFRASTRUKTUR KUNCI PUBLIK DALAM *SINGLE MEDICAL RECORD ONLINE* NASIONAL

Frizka Ferina[1] , Ummu Fauziah Fitri[2]

[1,2]Deputi Bidang Pengkajian Persandian, Lembaga Sandi Negara, Jakarta
[1]frizka.ferina@lemsaneg.go.id , [2]ummu.fauziah@lemsaneg.go.id

Abstrak

Rekam medis secara umum adalah dokumen rahasia yang dilindungi oleh kode etik kedokteran. Fakta di lapangan menyatakan bahwa rekam medis di Indonesia dikelola mandiri oleh masing-masing rumah sakit. Permasalahan data rekam medis yang belum terintegrasi pada seluruh Rumah Sakit di Indonesia menjadi isu utama berkembangnya wacana pengembangan sistem rekam medis terintegrasi secara online (single medical record online). Pengembangan sistem tersebut harus didukung oleh jaminan keamanan data karena rekam medis merupakan data rahasia. Solusi yang dapat digunakan adalah dengan menerapkan Public Key Infrastructure (Infrastruktur Kunci Publik) untuk proses otentikasi, tanda tangan digital, dan enkripsi dokumen. Dalam implementasi IKP perlu mempertimbangkan beberapa faktor, yaitu interoperabilitas dan kompatibilitas, kemudahan pengembangan dan kegunaan, fleksibilitas, keamanan CA (Certificate Authority), serta skalabilitas dan adaptibilitas.

Kata Kunci **:** *Infrastruktur Kunci Publik, Public Key Infrastructure, Rekam Medis Terintegrasi*

1. Pendahuluan

Setiap masyarakat Indonesia memiliki hak asasi untuk mencapai tingkat kesehatan yang optimal. Pencapaian tersebut dapat terlaksana salah satunya dengan dukungan layanan kesehatan yang diselenggarakan dalam sistem yang baik, mudah, serta terjangkau. Namun, saat ini layanan kesehatan di Indonesia masih bersifat sektoral serta belum ada integrasi. Masing-masing penyelenggara pelayanan kesehatan membangun sistem sendiri dan tidak saling terintegrasi dengan penyelenggra pelayanan kesehatan yang lain, sehingga pada saat masyarakat memeriksakan diri ke pusat pelayanan kesehatan yang berbeda maka proses yang dilalui baik secara administrasi maupun rekam medis menjadi membutuhkan waktu yang lebih lama.

Rekam medis menurut PERMENKES Nomor: 269/MENKES/PER/III/2008 adalah berkas yang berisi catatan dan dokumen antara lain identitas pasien, hasil pemeriksaan, pengobatan yang telah diberikan, serta tindakan dan pelayanan lain yang telah diberikan kepada pasien. Catatan merupakan tulisan-tulisan yang dibuat oleh dokter atau dokter gigi mengenai tindakan-tindakan yang dilakukan kepada pasien dalam rangka pelayanan kesehatan. Telah diketahui umum bahwa segala informasi yang ada pada rekam medis adalah rahasia dan dilindungi oleh kode etik kedokteran serta peraturan perundangan yang berlaku. Peraturan yang mengatur masalah kerahasiaan ini juga diatur oleh PERMENKES Nomor: 269/MENKES/PER/III/2008 khususnya pada pasal 10 dan pasal 11. Bentuk Rekam Medis dapat berbentuk manual maupun berbentuk elektronik.

Permasalahan rekam medis yang tidak terintegrasi serta kerahasiaan dari rekam medis menjadi masalah yang harus diperhatikan. Salah satu solusi atas permasalahan tersebut adalah dengan menerapkan *single medical record online* di mana seluruh data rekam medis terintegrasi dalam sistem *online*. Berdasarkan UU No. 29 Tahun 2004 tentang praktik kedokteran, Permenkes No. 269 Tahun 2008 tentang rekam medis, UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), serta Permenkes No. 1171 Tahun 2011 tentang Sistem Informasi

Rumah Sakit (SIRS), terdapat beberapa syarat untuk menjaga keamanan data rekam medis pasien dikarenakan data tersebut merupakan data rahasia. Persyaratan keamanan yang harus dipenuhi apabila *medical record* akan dikembangkan secara *online* serta terintegrasi adalah sebagai berikut dengan mengacu pada *Handbook of Applied Cryptography* (Menezes, 1997):

a. *Confidentiality,* dalam melakukan pencatatan rekam medis harus dijaga keamanan data tersebut dalam suatu tempat yang aman serta sesuai dengan standar karena data rekam medis merupakan data privasi pasien;
b. *Integrity,* data milik pasien yang berupa rekam medis tersebut harus dapat dijamin integritas atau keutuhan datanya;
c. *Authentication,* setiap entitas yang mengakses rekam medis pasien adalah pihak-pihak berwenang yang telah terotentikasi;
d. *Availability,* data yang berada di sistem harus dapat diakses kapan pun sesuai dengan kebutuhan;
e. *Non-repudiation,* bahwa sistem dapat menjamin anti penyangkalan terhadap pihak-pihak yang sebenarnya mengakses data tersebut.

Dengan mengacu syarat keamanan tersebut, maka solusi keamanan yang ditawarkan dalam *single medical record online* adalah dengan menerapkan *Public Key Infrastructure* (Infrastruktur Kunci Publik).

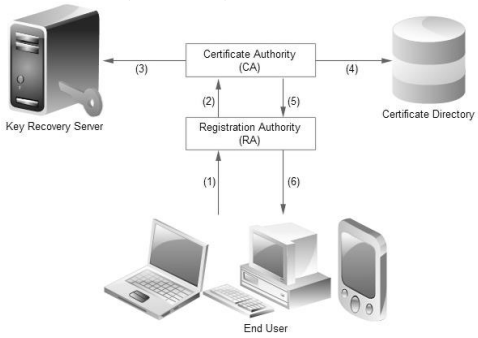
2. Infrastruktur Kunci Publik (IKP)

2.1. Gambaran Umum

Infrastruktur Kunci Publik (IKP) adalah suatu sistem yang terintegrasi dari perangkat lunak, metodologi enkripsi, protokol, perjanjian legal dan layanan pihak ketiga yang memungkinan pengguna untuk dapat berkomunikasi secara aman (M.Whitman, 2012). Sistem IKP mengkombinasikan penggunaan sertifikat digital, algoritma kriptografi kunci publik dan *Certificate Authority* (CA) ke dalam suatu jaringan keamanan informasi. Aspek keamanan yang disediakan oleh IKP adalah autentikasi, integritas data, kerahasiaan, otorisasi dan nir-sangkal.

2.2. Komponen IKP

IKP dapat diimplementasikan dengan baik melalui interaksi antar komponen dasarnya. Adapun komponen dasar IKP terdiri dari CA, *Registration Authority* (RA), Pengguna, *Key Recovery Server/Archive* dan *Certificate Directory/Repository* (S. Burnett, 2004). Komponen lainnya dapat terlibat seiring dengan semakin kompleksnya kebutuhan keamanan IKP antara lain *Time Stamping Service* (TSS), *Certificate Management Protocol* (CMP) dan *Certificate Policy/Certification Practice Statement* (CP/CPS).



Gambar1. Interaksi antar komponen dasar IKP (S. Burnett, 2004)

Gambar 1 di atas menggambarkan alur interaksi komponen dasar IKP. Interaksi diawali dengan pendaftaran pengguna melalui RA untuk memperoleh sertifikat digital. RA melakukan verifikasi data pengguna kemudian dapat membuatkan *Certificate Signing Request* (CSR) atau meneruskan CSR yang telah dibuat oleh pengguna kepada CA apabila data hasil verifikasi adalah valid. CA menandatangani CSR menjadi sertifikat digital dan menyimpannya di *Key Recovery Server* jika diperlukan. CA juga menyimpan sertifikat digital yang sudah ditandatangani ke dalam *Certificate Directory*. Sertifikat digital selanjutnya disampaikan ke RA. Pada interaksi terakhir, RA menyampaikan sertifikat digital yang sudah ditandatangani oleh CA kepada pengguna. Sertifikat digital yang diterima pengguna dapat digunakan untuk kebutuhan *email encryption*, HTTPS, *Virtual Private Network* (VPN), *File Encryption, Single Sign-On* (SSO), tanda tangan digital, *code signing, online banking* dan *Secure Electronic Transaction* (SET) (K.Schmeh, 2003).

2.3. Kriteria Penerapan IKP

Pelaksanaan implementasi IKP perlu mempertimbangkan beberapa kriteria agar sesuai dengan kebutuhan operasional, bisnis proses dan kondisi demografik Indonesia dalam membangun infrastrukturnya. Terdapat 5 kriteria yang dapat dijadikan pertimbangan untuk menentukan solusi yang tepat pada implementasi IKP (S. Choudhury, 2002) sebagai berikut:

a. Interoperabilitas dan kompatibilitas

Desain IKP yang akan diimplementasikan harus dapat mengikuti perkembangan teknologi sehingga tetap dapat berhubungan dengan perangkat dan aplikasi yang sedang berjalan, yang akan dikembangkan, komponen IKP lainnya serta sesuai standar. Interoperabilitas IKP dapat dievaluasi dengan mengikuti dua faktor, yaitu standar-standar IKP dan produk-produk dari berbagai vendor. Beberapa standar IKP yang umum diimplementasikan adalah PKIX, X.509 Versi 3, PKCS #10, PKCS #7, dan S/MIME. Sedangkan interoperabilitas produk-produk pada implementasi IKP mengikuti tiga kategori, yaitu interoperabilitas antar aplikasi, antar komponen, dan antar perusahaan.

b. Kemudahan pengembangan dan kegunaan

Pengembangan IKP harus mempertimbangkan faktor kemudahan sehingga para pengguna dapat menggunakannya. Walaupun pengembangan IKP melalui tahapan sangat kompleks yang terdiri atas sertifikat digital, algoritma kriptografi, dan kunci-kunci kriptografi, tetapi hasil implementasi harus mendukung penggunaan GUI yang *user friendly.*

c. Fleksibilitas

Solusi IKP yang dipilih untuk diimplementasikan tidak perlu terlalu rigid dan memiliki ruang lingkup yang memungkinkan untuk dikembangkan sesuai dengan kebutuhan pengguna.

d. Keamanan CA

CA merupakan inti dari seluruh sistem IKP, termasuk di dalamnya adalah fungsi-fungsi penting dari IKP. Oleh karena itu, CA membutuhkan pengamanan dengan tingkat maksimal karena apabila terdapat bagian CA yang lemah keamanannya maka akan melemahkan keseluruhan sistem IKP. Beberapa langkah yang dapat dilakukan untuk menjaga keamanan CA antara lain dengan membatasi akses ke CA, menjaga keamanan kunci privat CA dengan cara menyimpannya pada lokasi penyimpanan yang aman dari pihak-pihak yang tidak terotorisasi, melakukan tanda tangan digital pada seluruh permintaan sertifikat, dan memastikan bahwa CA yang digunakan telah diverifikasi oleh entitas luar.

e. Skalabilitas dan adaptibilitas

IKP yang diimplementasikan harus mendukung penambahan atau perubahan sistem menyesuaikan dengan sistem yang sedang berjalan dan kebutuhan yang direncanakan untuk implementasi kedepannya. Hal ini sebagai solusi terhadap perubahan lingkungan bisnis suatu organisasi, baik yang berkaitan dengan kebijakan maupun infrastruktur.

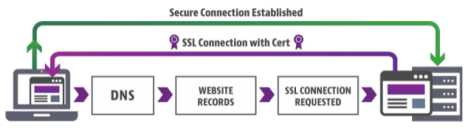
3. Disain Sistem

3.1. *Web Authentication*

Pada sistem rekam medis *online,* dapat dijamin keabsahan bahwa sistem yang diakses benar adalah dengan mengimplementasikan IKP dalam bentuk *digital certificate* (sertifikat digital) untuk protokol SSL. Penerapan sertifikat digital untuk *web authentication* pada *single medical record online* berdasarkan pada dokumen analisis kebutuhan yang mempertimbangkan mekanisme otentikasi, yaitu *single authentication* atau *mutual authentication.*

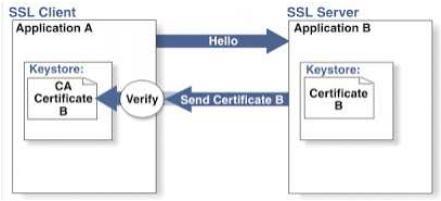
a. *Single authentication*

Mekanisme *single authentication* atau *one way authentication* merupakan mekanisme dimana pengguna mengakses halaman web *single medical record online* yang benar dengan cara memverifikasi sertifikat digital miliki *web server.* Mekanisme *one way authentication* secara umum ditunjukkan dalam gambar 2.



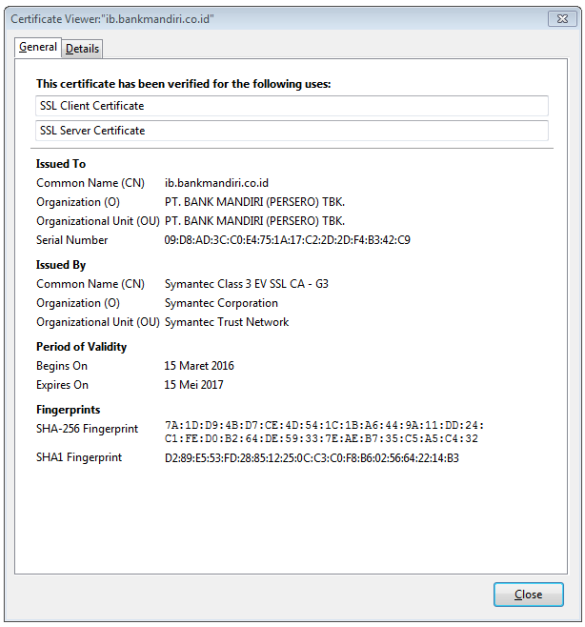
*Gambar2***.** Mekanisme *single authentication* (https://www.entrust.com)

Berdasarkan gambar 2, pengguna melakukan akses terhadap alamat DNS kemudian *website* akan melakukan pencatatan dan permintaan koneksi SSL ke *web server*. *Web server* selanjutnya membalas melakukan koneksi SSL dengan sertifikat digitalnya. Sisi pengguna akan melakukan proses verifikasi terhadap sertifikat digital yang dikirimkan oleh *web server*. Verifikasi dilakukan oleh *Certificate Authority* (CA) yang tersimpan dalam *keystore* pengguna seperti yang ditunjukkan dalam Gambar 3 di bawah ini.



Gambar 3. Proses *request* koneksi SSL (https://www.entrust.com)

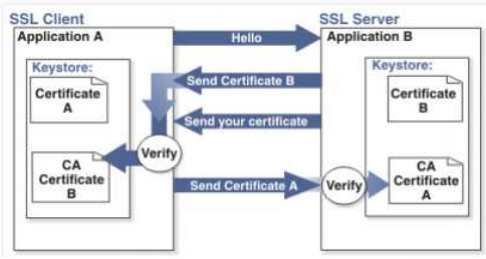
Dalam implementasi sertifikat digital, terdapat beberapa informasi di dalamnya yang dapat dijadikan informasi untuk proses otentikasi. Sertifikat digital berisi informasi entitas pemilik, penerbit sertifikat digital, periode, dan kunci. Gambar 4 di bawah ini merupakan salah satu contoh sertifikat digital yang digunakan untuk *one way authentication.*



Gambar 4. Contoh sertifikat digital

b. *Mutual authentication*

Mekanisme *mutual authentication* atau yang bisa disebut dengan *two-ways authentication*, merupakan proses otentikasi dua arah antara *client* dan *server*. Pada mekanisme ini, *client* melakukan akses ke sebuah *web server* kemudian akan dibalas dengan pengiriman serifikat digital milik *web server*. *Client* selanjutnya akan memverifikasi sertifikat *web server* dengan CA sertifikat milik *web server* yang tersimpan di dalam *keystore client.* Sisi *client* juga mengirimkan sertifikat digitalnya ke *web server* untuk selanjutnya diverifikasi dengan CA milik *client* yang tersimpan di *web server.* Mekanisme *two-ways authentication* ditunjukkan oleh gambar 5 di bawah ini.



Gambar 5. Mekanisme *two-ways authentication* (https://www.entrust.com)

Implementasi *two-ways authentication* pada sistem *single medical record online* dapat dengan memanfaatkan *token* sebagai penambahan keamanan otentikasi berdasarkan konsep *"what you have"* dalam *multifactor authentication.* Penentuan tersebut harus mengacu pada kajian lebih lanjut untuk menentukan analisis kebutuhan yang dalam makalah ini tidak dibahas. *Two-ways authentication* pada *single medical record online* ditunjukkan pada gambar 6, gambar 7, dan gambar 8 di bawah ini.

Gambar 6. Akses web *single medical record* tanpa token

Gambar 6 menunjukkan bahwa pada saat *client* mengakses halaman web tanpa menggunakan *token* maka *web server* akan menampilkan halaman bahwa koneksi ke web gagal. *Client* atau pengguna harus memasang *token* yang didalamnya berisi sertifikat digitalnya ke port USB kemudian melakukan akses kembali ke halaman web. Pada tahap ini, *client* telah melakukan verifikasi sertifikat digital miliki *web server* yang ditandai dengan alamat web yang telah berubah menjadi https, tetapi *web server* belum memverifikasi sertifikat digital *client.* Selanjutnya *client* harus memasukkan *password* yang ditunjukkan oleh Gambar 7.

Gambar 7. Kotak dialog *input password*

Apabila *password* yang dimasukkan benar, maka *web server* akan memverifikasi sertifikat digital *client.* Selanjutnya jika sertifikat digital tersebut terotentikasi, maka *web server* akan menampilkan halaman *login web* seperti yang ditunjukkan dalam gambar 8.

Gambar 8. Halaman *login web*

Mekanisme *two-ways authentication* pada *single medical record online* merupakan pengamanan pertama di sisi akses *web server.*

3.2. *Document Signing*

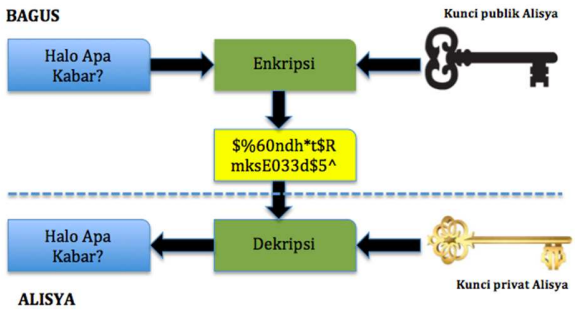
Pengelolaan data dalam rekam medis pasien harus menjamin adanya integritas data. Solusi yang dapat digunakan adalah dengan menerapkan IKP dalam bentuk *digital signature* (tanda tangan digital) untuk proses tanda tangan dokumen. Tanda tangan digital dalam sistem *single medical record online* digunakan untuk proses tanda tangan dokumen rekam medis sehingga dapat dijamin integritas atas data tersebut.

Menurut UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), tanda tangan elektronik (tanda tangan digital) adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi, atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Merujuk pada UU tersebut, maka tanda tangan digital merupakan alat sah untuk menandatangani dokumen elektronik yang dapat dijadikan sebagai jaminan keutuhan data serta dapat dipertanggungjawabkan secara legal. Dengan menerapkan tanda tangan digital pada *single medical record online*, maka dapat diketahui pihak-pihak mana saja yang telah merubah data rekam medis pasien.

3.3. Enkripsi Dokumen

Enkripsi dokumen rekam medis pasien dilakukan apabila data tersebut dikirimterimakan secara *online* tanpa melalui *web* resmi *single medical record online.* Enkripsi dokumen data

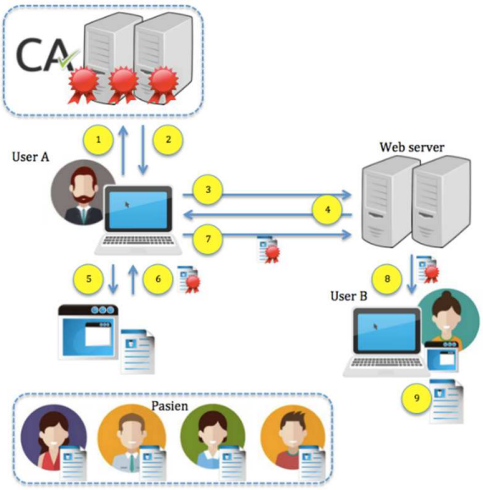
rekam medis dapat menjadi salah satu solusi yang dapat dipakai apabila sistem rekam medis terintegrasi belum berjalan secara optimal. Proses enkripsi dengan mekanisme kunci asimetrik ditunjukkan pada gambar 9 di bawah ini dengan mengacu pada penjelasan dari *Handbook of Applied Cryptography* (Menezes, 1997).



Gambar 9. Proses enkripsi dokumen

3.4. Arsitektur Sistem

Arsitektur yang diajukan Penulis untuk *single medical record online* yang dapat diimplementasikan di Indonesia ditunjukkan dalam gambar 10 di bawah ini.



Gambar 10. Arsitektur *single medical record online*

Berikut adalah penjelasan dari langkah-langkah penerapan IKP pada arsitektur *single medical record online* pada gambar10 :

1. User A sebagai pegawai rumah sakit yang memiliki wewenang terhadap rekam medis pasien melakukan permohonan sertifikat digital kepada CA.
2. CA menerbitkan sertifikat digital milik user A.
3. User A melakukan akses *single medical record online* ke *web server* yang secara otomatis merupakan tahap permintaan koneksi SSL.
4. Web server mengijinkan User A melakukan koneksi SSL apabila dongle dan password yang dimasukkan sesuai (dengan menggunakan metode *two ways authentication*).
5. User A membuka aplikasi enkripsi file dan melakukan enkripsi sekaligus menandatangani dokumen rekam medis secara elektronik.
6. User A telah mendapatkan dokumen rekam medis terenkripsi dan sudah ditandatangani secara elektronik.
7. User A mengupload dokumen rekam medis yang sudah ditandatangani serta dienkripsi ke *web server*.
8. User B atau sebagai pegawai rumah sakit lain yang memiliki wewenang terhadap akses dokumen rekam medis melakukan verifikasi dokumen dan melakukan dekripsi dokumen.
9. User B mendapatkan dokumen rekam medis terdekripsi dan terverifikasi milik pasien.

4. Penutup

4.1. Simpulan

Penerapan IKP pada *single medical record online* atau sistem rekam medis terintegrasi di Indonesia dapat menjadi solusi dalam menjamin keamanan informasi elektronik khususnya yang berupa dokumen rekam medis. Disain sistem yang dikembangkan harus memperhatikan analisis kebutuhan yang mencakup sistem otentikasi, tanda tangan digital pada dokumen, dan enkripsi dokumen. Sedangkan implementasi IKP harus mempertimbangkan beberapa kriteria yaitu, interoperabilitas dan kompatibilitas, kemudahan pengembangan dan kegunaan, fleksibilitas, keamanan CA, serta skalabilitas dan adaptibilitas.

4.2. Saran

Berdasarkan pembahasan di atas, berikut beberapa saran dari Penulis:

a. Perlu dibangun sistem rekam medis terintegrasi secara *online* di Indonesia dengan memperhatikan kaidah-kaidah keamanan informasi;
b. Perlu dilakukan penelitian lebih lanjut untuk menyusun analisis kebutuhan keamanan pada sistem yang akan diterapkan;
c. Investasi dalam pengembangan IKP untuk *single medical record online* dalam rumah sakit tidak hanya dapat digunakan untuk rekam medis saja, tetapi dapat juga dimanfaatkan untuk sistem elektonik lain dalam rumah sakit tersebut.

DaftarPustaka

Menezes, Alfred J., Oorschot, Paul C.Van., Vanstone, Scott A. (1997). *Handbook of Applied Cryptography.* CRC press LLC : Boca Raton.

Schneier, Bruce .(1996). *Applied Cryptography: Protocol, Algorithms And Source Code in C, Second Edition*. John Willey & sons, inc.

M. Whitman, H. Mattord.(2012).*Principles of Information Security*. Boston: Course Technology.

S. Burnett dan S. Paine. (2004).RSA Security's Official Guide to Cryptography, California: McGraw-Hill.

K. Schmeh. (2003).Cryptography and Public Key Infrastructure on the Internet, Sussex: Wiley & Sons Ltd.

S. Choudhury, K. Bhatnagar, W. Haque dan NIIT.(2002).*Public Key Infrastructure Implementation and Design*, New York: M&T Books.

Yon Handri, Frizka Ferina. (2016). *Penentuan Model Kepercayaan Infrastruktur Kunci Publik di Indonesia dengan Pendekatan Analytic Hierarchy Process.* Seminar Nasional Sistem Informasi Indonesia.

Undang-Undang No. 29 Tahun 2004 tentang Praktik Kedokteran.

Peraturan Menteri Kesehatan No. 269 Tahun 2008 tentang Rekam Medik.

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan Menteri Kesehatan No. 1171 Tahun 2011 tentang Sistem Informasi Rumah Sakit.

https://www.entrust.com diakses terakhir pada tanggal 26 September 2016

BiodataPenulis

Frizka Ferina , memperoleh gelar Sarjana Sains Terapan di Sekolah Tinggi Sandi Negara setelah menyelesaikan pendidikan selama 4 tahun dengan jurusan Teknik Persandian dengan bidang minat Teknik Rancang Bangun Palsan. Penulis kemudian melanjutkan pendidikan Pasca Sarjana di Universitas Pembangunan Nasional Veteran Jakarta hingga memperoleh gelar S2. Saat ini Penulis menjadi karyawan di Lembaga Sandi Negara dan aktif dalam hal penelitian serta pengembangan persandian.

Ummu Fauziah Fitri, menyelesaikan pendidikan S1 selama 4 tahun di SekolahTinggi Sandi Negara. Jurusan yang diambil adalah Teknik Persandian bidang minat Teknik Kripto. Penulis kemudian melanjutkan ke jenjang pendidikan yang lebih tinggi dan berhasil memperoleh gelar S2 di STMIK Eresha Jakarta . Saat ini Penulis menjadi karyawan di Lembaga Sandi Negara dan aktif pada kegiatan penelitian serta pengembangan persandian.

BERITA ACARA PELAKSANAAN HASIL SEMINAR SESI PARALEL KNASTIK 2016

Judul	: Pemanfaatan Infrastruktur Kunci Publik Dalam Single Medical Record Online
Pemakalah	: Frizka Ferina, Ummu Fauziah Fitri
Moderator	: Halim Budi Santoso, S.Kom., MBA, M.T.
Notulis	: Maria Dina
Peserta	: 8 orang di ruang : B.3.2

Tanya Jawab :

1. Kemampuan setiap rumah sakit berbeda-beda baik dalam SDM maupun infrastruktur. Apakah dengan kondisi tersebut akan mempengaruhi dalam implementasi IKP?
   Seharusnya tidak mempengaruhi karena saat ini pemerintah sebagai heading sector implementasi IKP sangat mendukung implementasi tersebut dan akan memberikan pelayanan secara free.

Masukan Seminar :

Sistem ini cukup menarik untuk dikembangkan.

Yogyakarta, 19 November 2016

Moderator Kelas

knastik

Halim Budi Santoso, S.Kom., MBA, M.T.

Penyaji Makalah

Frizka Ferina