Jurnal J-MENDIKKOM 1 (2) (2024), ISSN: 3046-5893 (Online)
Jurnal J-MendiKKom (Jurnal Manajemen, Pendidikan dan Ilmu Komputer)
Journal homepage: https://jmendikkom.org

Tinjauan Keamanan Informasi Terhadap Sistem Integrasi EKTP pada Kota Cerdas

Rafiqa Dewi
Program Studi Manajemen Informatika, STIKOM Tunas Bangsa, Indonesia

Article Info

Article history:

Received Jul 09, 2024
Revised Jul 25, 2024
Accepted Jul 29, 2024

Kata Kunci:

Integrasi
Keamanan data
E-KTP
E-Government
Kota cerdas

Keywords:

Integration
Data security
Electronic id card
Electronic Government
Smart city

ABSTRAK

Dalam mendukung terwujudnya *E-Government* cerdas dimana warga sudah menggunakan Kartu Tanda Penduduk Elektronik (EKTP), pemerintah mulai mengintegrasikan EKTP dengan beberapa pusat layanan. Sehingga sistem akan dapat mengetahui riwayat perjalanan dan layanan yang digunakan oleh warga. Hal ini tentu saja akan bertentangan dengan hak privasi penghuninya. Sedangkan proses integrasi EKTP dengan sejumlah pusat layanan tentunya memiliki celah yang dapat dimanfaatkan oleh pihak yang tidak berkepentingan sehingga dapat disalahgunakan. Artikel ini akan mengulas bagaimana keamanan informasi pada sistem integrasi EKTP, artikel ini meninjau mekanisme apa saja yang dilakukan untuk mencegah aktivitas ilegal terhadap informasi yang dihasilkan.

ABSTRACT

In supporting the realization of an eGovernment where residents already use electronic identification cards (EKTP), the government has begun to integrate EKTP with several service centers. So the system will be able to find out the travel history and services that used by residents. This, of course, will conflict with the residents' right to privacy. While the integration process of EKTP with a number of service centers, of course, has loopholes that can be exploited by unauthorized parties so that it can be misused. This article will review how information security is on the EKTP integration system, what mechanisms have been taken to prevent illegal activities against the information produced.

Corresponding Author:
Rafiqa Dewi,
Manajemen Informatika, STIKOM Tunas Bangsa
Jalan Sudirman Blok A No. 1/2/3, Pematang Siantar, Sumatera Utara, 21111, Indonesia.
Email: rafiqa@amiktunasbangsa.ac.id

1. PENDAHULUAN

Integrasi EKTP dengan sejumlah pusat layanan telah banyak dilakukan pemerintah untuk menghadirkan pelayanan yang lebih optimal. Namun sistem EKTP, khususnya yang berbasis sistem identifikasi nasional, merupakan salah satu dari beberapa sistem penting perdebatan kontemporer seputar kewarganegaraan, pengawasan negara, keamanan, privasi, dan pemerintahan. KTP elektronik, memiliki beberapa karakteristik unik. Pada umumnya EKTP berjejaring dengan sistem informasi pribadi lainnya oleh karena itu, mereka biasanya berfungsi sebagai kartu multiguna dalam kerangka *E-Government* dan *E-Commerce* [1]. Melalui tata kelola yang transparan dan data terbuka, masyarakat mempunyai peluang untuk terlibat dalam keputusan pemerintah. Penerapan tata kelola yang transparan dan data terbuka dengan menggunakan dua faktor, yaitu sifat informasi seperti klasifikasi keterbukaan informasi, dan alat untuk mengakses informasi atau hak informasi diatur dalam konstitusi dan undang-undang sektoral seperti UU No. 14/2008 tentang publik.

Komisi Informasi Publik (KIP) merupakan pengawal keterbukaan informasi publik, namun pada kenyataannya hal-hal tersebut menjadi permasalahan mendasar dalam penegakan peraturan tersebut, misalnya: infrastruktur internet, sumber daya manusia, kesiapan teknologi, dan perilaku budaya. Terlepas dari permasalahan tersebut, belum ada bukti empiris yang tepat untuk membenarkan efektivitas undang-undang keterbukaan informasi publik, dan untuk membuktikan bahwa data terbuka bermanfaat bagi kondisi publik di tingkat pemerintah daerah. Sementara itu, pengguna Internet di Indonesia meningkat secara signifikan sebesar 34,9% dari tahun 2014 hingga 2016, dengan perkiraan pengguna Internet saat ini lebih dari 132,7 juta atau lebih dari separuh populasi penduduk [2][3].

2. TINJAUAN PUSTAKA

a. Kartu Identitas Elektronik

Fungsi utama kartu identitas elektronik atau EKTP di antaranya adalah untuk mengefektifkan fungsi pemerintahan dan pelayanan publik, meningkatkan keamanan negara, mempermudah mendeteksi pelaku teror, serta memudahkan aplikasi perpajakan elektronik [4]. Implementasi EKTP sangat strategis untuk sistem pelayanan publik yang integratif serta menjadi sumber daya informasi utama bagi pemerintah dalam rangka penyediaan informasi bagi masyarakat [5]. Dari segi keamanan definisi EKTP dapat dilihat sebagai tiga bentuk fungsionalitas keamanan informasi yakni: Identifikasi (*Identification*) yaitu A dapat membuktikan kepada B bahwa dia adalah A, tetapi orang lain tidak dapat membuktikan kepada B bahwa dia adalah A. Otentikasi (*Authentication*) yaitu A dapat membuktikan kepada B bahwa dia adalah A, tetapi B tidak dapat membuktikan kepada orang lain bahwa dia adalah A. Tanda tangan (*Signature*) yaitu A dapat membuktikan kepada B bahwa dia adalah A, tetapi B tidak dapat membuktikan kepada dirinya sendiri bahwa dia adalah A [6].

b. Kota Cerdas (*Smart City*)

Menurut Washburn, D., dkk [7] bahwa *smart city* di definisikan sebagai penggunaan teknologi komputasi cerdas untuk mengintegrasikan komponen-komponen penting dari infrastruktur dan layanan kota, seperti administrasi kota, pendidikan, kesehatan, keselamatan publik, *real estate*, transportasi dan keperluan kota lainnya, dimana penggunaan keseluruhannya harus dilakukan secara cerdas, saling berhubungan dan efisien. Sedangkan menurut Hall, R. E. [8], *Smart City* adalah sebuah kota yang memonitor dan mengintegrasikan kondisi semua infrastrukturnya, termasuk jalan, jembatan, terowongan, rel, kereta bawah tanah, bandara, pelabuhan, komunikasi, air, listrik, bahkan seluruh bangunan pemerintahan sehingga dapat digunakan untuk mengoptimalkan sumber daya, rencana kegiatan dan memantau keamanan sekaligus memaksimalkan pelayanan kepada warganya.

c. Integrasi Data

Integrasi data meliputi kombinasi data yang berada pada sumber yang berbeda dan menyediakan *user* dengan tampilan terpadu untuk data-data tersebut. Proses ini mencakup dua instansi yang berbeda dengan model pengolahan data yang sama. Dalam lingkaran manajemen, hal ini sering merujuk kepada integrasi data sebagai ”*Enterprise Information Integration*” (EII). Sistem integrasi data biasanya secara formal disebut sebagai triple GSM dimana G diartikan sebagai global schema, S diartikan sebagai set dari skema yang bersumber dari *heterogen*, dan M diartikan sebagai *mapping* (pemetaan) antara *query* dari sumber dan skema global. Smart city memiliki tiga karakteristik yaitu *Intrumented*, *Interconnected*, dan *Intelligent*. *Instrumented* mencakup pengukuran dan pengendalian dari sebuah kota meliputi transportasi, air, udara, sosial dan ekonomi melalui penyebaran berbagai macam sensor. Interconnected artinya integrasi data menjadi sebuah *platform* perusahaan layanan komputer dan komunikasi informasi diantara berbagai layanan kota. Intelligent berarti adanya analisis komplek, pemodelan, optimasi, dalam proses bisnis operasional untuk membuat keputusan operasional yang lebih baik [9].

d. Keamanan Informasi

Dengan adanya integrasi sistem informasi, data-data dan informasi baik yang ada di departemen maupun data-data masyarakat menjadi data sentral yang bisa dipakai antar departemen. Masalah data yang tersentralisasi merupakan satu isu tersendiri yang perlu diperhatikan. Sentralisasi data tidak hanya berhubungan dengan bagaimana prosedur pengumpulan data itu sendiri , tetapi akan terkait dengan masalah infrastruktur, kapasitas penyimpanan, dan juga faktor keamanan data. Unsur privasi harus pula diperhatikan dalam arti kata para pengguna website merasa yakin bahwa tidak ada hal -hal yang akan merugikan dirinya terkait dengan isu keamanan berinteraksi secara digital ketika mengakses website pemerintah [10].

Dalam hal ini penerapan prinsip otentifikasi dengan memberikan password dan *Personal Identification Number* (PIN) sebagai alat transaksi bagi penduduk menjadi satu hal yang sangat penting dalam integrasi sistem data kependudukan. Apabila sebuah kota telah memiliki proses mengolahan data dan informasi dengan menggunakan keamanan yang baik, sehingga setiap data yang terakses tetap terjaga nilai kepentingan yang ada di dalam data dan informasinya, maka menurut I Putu Agus (2014) kota tersebut telah sampai pada level 4 dalam merealisasikan *smart city*.

e. Arsitektur Keamanan EKTP

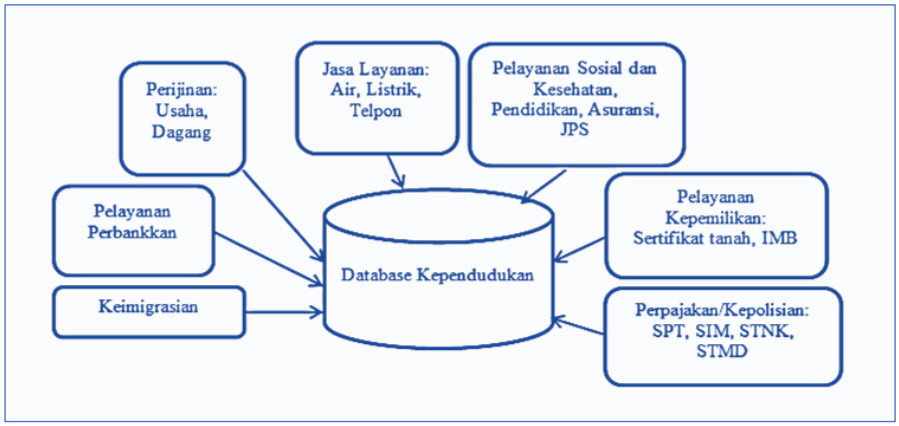
Dari arsitektur sistem keamanan, sistem keamanan EKTP memiliki arsitektur semua dimensi, multilevel dan multi aspek. Secara umum, risiko keamanan sistem dapat dibagi menjadi dua aspek yakni:

1. Keamanan tautan: Ini berarti keamanan tautan antara terminal akses dan batas jaringan akses harus melebihi tautan pribadi atau mengadopsi teknologi enkripsi untuk memastikan integritas informasi.
2. Keamanan jaringan: Artinya kerahasiaan dan integral dari transmisi informasi harus terjamin, dan langkah-langkah harus diambil seperti enkripsi, isolasi, dan kuda perlindungan, juga otentikasi keamanan, hak istimewa, dan promosi keamanan lainnya harus disediakan dengan terminal akses dan pengguna untuk mempertahankan risiko keamanan jaringan.

Keamanan *hosting*: Artinya soliditas keamanan dengan *hosting* termasuk terminal dan *server* harus disediakan terhadap keamanan operasi *host* [11].

3. HASIL DAN PEMBAHASAN

Berdasarkan beberapa tinjauan literatur yang mengulas *smart city*, *E-Government*, integrasi EKTP dan keamanan informasi maka skema integrasi EKTP dengan berbagai pusat layanan dalam sebuah pemerintahan kota dapat digambarkan pada gambar 1.

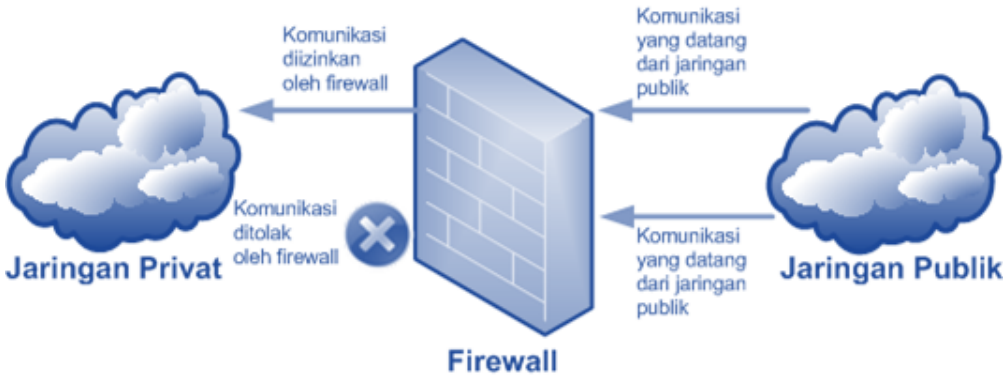


Gambar 1. Skema integrasi data kependudukan melalui EKTP dengan beberapa pusat layanan

Pada skema di atas tidak dijelaskan bagaimana keamanan informasi dan privasi masyarakat terjamin perlindungannya. Padahal isu keamanan data merupakan yang paling sensitif yang mana jika pemerintah tidak dapat menjamin keamanan informasi masyarakat maka akan menjadi bumerang yang justru dapat menghambat integrasi sistem EKTP. Karena penerapan *E-Government* membutuhkan dukungan dari berbagai pihak, pelaksanaannya memerlukan strategi yang terkelola dengan baik. Keamanan informasi pada *E-Government* dapat berbentuk jaminan pemerintah terhadap privasi data penduduk, terkendali dan terlindungi dari penyalahgunaan dengan menghadirkan teknologi sekuriti yang handal dan undang-undang perlindungan privasi yang mapan. Beberapa strategi keamanan informasi yang dapat diterapkan oleh pemerintah adalah sebagai berikut:

a. Yang diterapkan oleh Dinas Perpajakan California (FTB) dalam memberikan jaminan keamanan informasi adalah sebagai berikut :
   1. Privasi dari pembayar pajak dijaga secara ketat. Penggunaan informasi yang berhubungan dengan mereka diatur dalam aturan yang pasti. Penyalahgunaan terhadap privasi akan mendapatkan hukuman yang berat.
   2. Aspek kedua yang erat hubungannya adalah masalah keamanan data. Tidak bisa dipungkiri , keamanan data menjadi isu yang paling sensitif dalam hal ini. Dalam hal keamanan data, dibuat berbagai aplikasi berlapis agar tidak terjadi kebocoran.

Prinsip otentifikasi dengan memberikan password dan Personal Identification Number (PIN) sebagai alat transaksi [10].



Gambar 2. Skema sistem keamanan informasi pada kota cerdas

Tanpa adanya keamanan data yang memadai, partisipasi penduduk tidak bisa diharapkan terlalu besar. Secara fisik *Electronic Identity Card* (EID)didesain tidak menunjukkan data-data lengkap seseorang, sehingga jika hilang atau digunakan orang lain tidak bisa dipakai secara lebih luas. Data-data itu tersimpan di dalam bank data pemerintah yang hanya bisa diakses oleh yang berwenang. Hal lain yang juga membantu adalah teknologi keamanan pada sertifikat digital yang cukup canggih sehingga memungkinkan penduduk merasa aman dan nyaman dalam proses pemakaian kartu tersebut.

b. Penggunaan Sertifikat Digital

Proses penerbitan terutama mencakup: pertama, pasangan kunci publik/pribadi dibuat dengan aman di kartu EID; pengguna mengajukan permintaan yang berisi kunci publik dan informasi identitasnya ke infrastruktur manajemen EID yang juga disebut infrastruktur kunci publik. Setelah memeriksa kebenaran dan keunikan pengguna, infrastruktur kunci publik mengeluarkan sertifikat digital yang berisi kunci publik dan EID pengguna yang terkait dengan identitas yang sebenarnya. Dengan demikian, sertifikat digital yang dienkapsulasi sebagai amplop digital akan dikirim kembali ke pengguna dan ditulis ke dalam kartu EID. Penyedia layanan juga memerlukan sertifikat servernya dari infrastruktur kunci publik. Kedua, pendaftaran dan validasi EID pengguna akan diselesaikan antara pengguna dan penyedia layanan [12].

c. Penggunaan PIN dan Token

Algoritma pertukaran kunci merekonstruksi rahasia individu dari sejumlah besar yang disimpan pada token perangkat keras dan PIN. Adalah penting bahwa rahasia individu yang benar tidak dapat dideteksi dari formatnya dan itu hanya angka, dan angka apa pun memiliki kemungkinan untuk ditebak. Pada dasarnya hubungan itu linier dan dalam bentuk:

$$D = N + PIN$$

di mana D adalah rahasia individu, dan N adalah nomor pada token.

Otoritas tepercaya mengetahui nomor rahasia utama. Identitas pengguna dipetakan menggunakan fungsi hash yang sesuai ke titik-titik pada kurva eliptik tertentu. Pengguna Alice memiliki identitasnya di-hash dan dipetakan ke titik A dengan orde prima besar pada kurva, dan memilih nomor PIN yang diinginkan. Setelah mengautentikasi dirinya ke otoritas tepercaya, dia menerima A dan sA, menghitung A, mengurangi keduanya, menyimpan A dan $(s - \alpha)A$, dan merekam. Seperti dalam skema pembagian rahasia sederhana, kedua bagian ini perlu disatukan kembali untuk merekonstruksi nilai sA yang benar. Jelas Alice tidak dapat menentukan s tanpa memecahkan masalah logaritma diskrit yang sulit. Kami memiliki hubungan linier sederhana $sA = (s\alpha)A + A$ [13].

d. Membangun *Trusted Platform Module* (TPM)

Ide dasar dari TPM adalah untuk melindungi dari identifikasi pencurian dengan autentikasi, dan menghubungkannya dengan keyakinan tinggi ke identitas pengguna. Kami pertama-tama akan menyajikan Pengesahan Jarak Jauh sebagai alat untuk memverifikasi integritas sistem. Sebuah diskusi tentang lingkungan eksekusi yang dapat dipercaya dan cocok yang berbeda berikut. Akhirnya diperkenalkanlah protokol untuk membangun kepercayaan dalam otentikasi TPM dengan EKTP. Yaitu dengan menerapkan tahapan:

1. Pengesahan jarak jauh
2. Lingkungan eksekusi tepercaya
3. Protokol untuk menetapkan identitas terverifikasi [14].

4. KESIMPULAN

Artikel ini meninjau keamanan informasi yang ditimbulkan oleh integrasi EKTP dengan pusat-pusat layanan dalam ruang lingkup *E-Government*. Terdapat banyak elemen yang terlibat dalam menciptakan sistem keamanan informasi yang menggabungkan keahlian, pengalaman dan keterampilan mitra dengan kompetensi multidisiplin yang saling melengkapi. Menghadirkan platform terpercaya untuk menjamin keamanan informasi yang bersifat privasi menjadi tantangan tersendiri dalam mewujudkan integrasi ini.

REFERENCES

[1] A. Çavlin Bozbeyoğlu, "Citizenship rights in a surveillance society: The case of the electronic ID card in Turkey," *Surveill. Soc.*, vol. 9, no. 1–2, pp. 64–79, 2011, doi: 10.24908/ss.v9i1/2.4095.

[2] M. Razaghi and M. Finger, "Smart Governance for Smart Cities," *Proc. IEEE*, vol. 106, no. 4, pp. 680–689, 2018, doi: 10.1109/JPROC.2018.2807784.

[3] T. APJII, "Saatnya jadi Pokok Perhatian Pemerintah dan Industri," *Bul. APJII*, vol. 1, 2016.

[4] . A., . T., and A. Latif, "Rekayasa Perangkat Lunak Sistem e-KTP Terintegrasi Birokrasi Umum Di Kota Batam," *J. Nas. Teknol. dan Sist. Inf.*, vol. 2, no. 2, pp. 97–108, 2016, doi: 10.25077/teknosi.v2i2.2016.97-108.

[5] D. Septiyarini and R. N. Pranaka, "Implementasi Program Dan Pemanfaatan E-Ktp Yang Terintegrasi Di Kabupaten Sambas," *Publikauma J. Adm. Publik Univ. Medan Area*, vol. 7, no. 1, p. 30, 2019, doi: 10.31289/publika.v7i1.2173.

[6] S. Arora, "National e-ID card schemes: A European overview," *Inf. Secur. Tech. Rep.*, vol. 13, no. 2, pp. 46–53, 2008, doi: 10.1016/j.istr.2008.08.002.

[7] D. Washburn and U. Sindhu, "Helping CIOs Understand 'Smart City' Initiatives," *Growth*, p. 17, 2009, [Online]. Available: http://c3328005.r5.cf0.rackcdn.com/73efa931-0fac-4e28-ae77-8e58ebf74aa6.pdf.

[8] R. E. Hall, B. Bowerman, J. Braverman, J. Taylor, and H. Todosow, "The vision of a smart city," *2nd Int. Life …*, vol. 28, p. 7, 2000, [Online]. Available: ftp://24.139.223.85/Public/Tesis_2011/Paper_Correction_4-15-09/smartycitypaperpdf.pdf.

[9] A. Ichwani, "Perancangan metode architecture smart city," *Ilmu Komput.*, vol. 3, no. 1, pp. 44–53, 2018, [Online]. Available: https://www.esaunggul.ac.id/wp-content/uploads/2018/02/4.-PERANCANGAN-METODE-ARCHITECTURE-SMART-CITY.pdf.

[10] R. E. Indrajit, A. Zainudin, and D. Rudianto, "Electronic government in action," *Yogyakarta Andi Yogyakarta*, pp. 1–272, 2004, [Online]. Available: https://www.academia.edu/download/50613264/Preinexus-TeknikSearchingEfektifDuniaPendidikan.pdf.

[11] R. E. Indrajit, "Ict pura," *Seri 999 E-Artikel Sist. dan Teknol. Inf.*, pp. 1–4, 2012.

[12] B. Chen, Y. Dai, B. Jin, X. Zou, and L. Zhou, "The RFID-based electronic identity security platform of the Internet of Things," *Proc. 2011 Int. Conf. Mechatron. Sci. Electr. Eng. Comput. MEC 2011*, pp. 246–249, 2011, doi: 10.1109/MEC.2011.6025447.

[13] M. Scott, "Authenticated ID-based Key Exchange and remote log-in with simple token and PIN number," *IACR Cryptol. ePrint Arch.*, vol. 2002, p. 164, 2002.

[14] A. Klenk, H. Kinkelin, C. Eunicke, and G. Carle, "Preventing identity theft with electronic identity cards and the Trusted Platform Module," *Proc. 2nd Eur. Work. Syst. Secur. EUROSEC'09*, pp. 44–51, 2009, doi: 10.1145/1519144.1519151.