

## IMPLEMENTASI *ROLE-BASED ACCESS CONTROL (RBAC)* PADA PEMANFAATAN DATA KEPENDUDUKAN DITINGKAT KABUPATEN

Rubiyanto<sup>1\*</sup>, Selo<sup>2</sup>; Widyawan<sup>3</sup>

<sup>\*123</sup>Departemen Teknik Elektro, Teknologi Informasi, Fakultas Teknik,  
Universitas Gadjah Mada, Yogyakarta  
Jl. Grafika No.2, Sleman, Yogyakarta, Kode pos  
\*E-mail : mas.rubi@mail.ugm.ac.id.

### ABSTRAK

Kontrol akses dengan menggunakan *Role-Based Access Control (RBAC)* dapat dimanfaatkan untuk pengamanan pemanfaatan data kependudukan dalam proses otorisasi hak aksesnya. Hak akses sistem pemanfaatan data kependudukan ditingkat kabupaten merupakan syarat untuk dapat mengakses data kependudukan level kabupaten, yang diberikan berdasarkan mekanisme peraturan yang berlaku. Penentuan kewenangan yang berbeda harus dilakukan karena adanya perbedaan kebutuhan data dan peran berbagai sistem informasi yang membutuhkan data kependudukan. Penentuan kewenangan dalam mengakses data tersebut perlu dipetakan untuk mengetahui kebutuhan data setiap sistem pengakses, yang kemudian dijadikan sebagai pedoman dalam penyusunan pemberian hak akses dan kewenangannya.

Pendekatan analisis deskriptif dilakukan dengan kajian pustaka terkait penggunaan *RBAC*, ketersediaan dan pemanfaatan data kependudukan ditingkat kabupaten, otorisasi akses data kependudukan dan analisa kondisi aktual terkait keamanan sistem terutama kontrol akses yang dibutuhkan untuk mengetahui masalah yang ada.

Penelitian ini membahas mengenai otorisasi dalam pemanfaatan data kependudukan ditingkat kabupaten dengan pendekatan *Role-Based Access Control (RBAC)* sebagai salah satu upaya meningkatkan keamanan sistem *web service* yang digunakan. Pemetaan kebutuhan data kependudukan dilakukan dengan mengelompokkan sistem informasi pengakses berdasarkan jenis dan kelompok data yang dibutuhkan. Kebutuhan data sistem pengakses dipetakan berdasarkan fungsi bisnis dari sistem tersebut. Pemetaan yang dilakukan menghasilkan tiga kelompok kewenangan berbeda, dalam pengaksesan data identitas maupun data agregat kependudukan. Hasil penelitian ini diharapkan menjadi bahan masukan dalam pembuatan PKS sebagai dasar pemberian hak akses pada pelayanan data kependudukan oleh berbagai sistem pelayanan publik khususnya di tingkat Kabupaten Wonosobo

**Kata kunci:** *RBAC*, Hak Akses, Keamanan Sistem, Pemanfaatan Data Kependudukan

### ABSTRACT

*Access control using Role-Based Access Control (RBAC) can be utilized for securing the use of demographic data in the process of authorization of access rights. Utilization system permissions population data at the district level is a requirement to be able to access the district-level population data, which are awarded based on the mechanism of regulation. Determination of different powers to be done because of differences in data requirements and the role of Information systems requiring demographic data. Determining authority to access that data needs to be mapped to determine the needs of each system accessed the data, which is then used as a guide in the preparation of granting access rights and authority. Descriptive analysis approach performed by literature review related to the use of RBAC, the availability and utilization of population data at the district level, data access authorization of residence and the analysis of actual conditions associated security access control systems primarily needed to know the problem exists. This study discusses the authorization of the use of population data at the district level with the approach of Role-Based Access Control (RBAC) as an*

*effort to improve the security systems that use web service. Mapping needs population data is done by grouping the access of information systems based on the type and the required data group. The access system mapped data needs based on the business functions of the system. Scans taken produces three different authority groups, in accessing identity data and aggregate data on population. Results of this research are expected to be input in the manufacture of the Cooperation Agreement as the basis for granting access rights to service the population data by a variety of public services, especially at the level of Wonosobo regency*

**Keywords :** RBAC, Permissions, System Security, Data Utilization Population

## PENDAHULUAN

*Role-Based Access Control (RBAC)* adalah sebuah mekanisme pengelolaan sejumlah hak akses yang lebih fleksibel dibandingkan dengan model kontrol akses *Mandatory Access Control (MAC)* maupun *Discretionary Access Control (DAC)* (Habib, 2011). Hak akses tidak harus diberikan kepada subjek yang sama dalam waktu yang bersamaan dalam *RBAC* untuk menjaga keamanan sistem dari pihak yang tidak diinginkan (Strembeck M, 2004).

Data Kependudukan merupakan salah satu data yang paling banyak digunakan dalam proses pelayanan publik. *Database* Kependudukan dalam *SIK* menggunakan *NIK* untuk mengidentifikasi setiap *record* pada seluruh komponennya, mempunyai item data yang lengkap tentang identitas, pencatatan sipil, dan *biometric* memungkinkan untuk dimanfaatkan berbagai sistem informasi di Pemkab/ Pemkot (Sutanta & Ashari, 2012).

Pemanfaatan data kependudukan di tingkat kabupaten untuk sistem informasi pelayanan publik, bisa diwujudkan dengan pelayanan data kependudukan menggunakan teknologi *web service* (Istiyanto & Sutanta, 2012) (Sutanta, 2011) (Wardana & Rahman, 2016). Pada implementasinya, sistem informasi pelayanan publik sebagai pengakses, harus mempunyai hak akses yang di tuangkan dalam Perjanjian Kerja Sama, yang didalamnya harus memuat tentang kewenangan sistem informasi Pengakses. Belum adanya standar baku yang mengatur tentang jenis dan kelompok data apa saja dalam pemanfaatan data kependudukan, menyebabkan penentuan pemberian hak akses untuk jenis dan kelompok data dimungkinkan mengalami kesulitan atau bahkan menghambat proses pemberian hak akses tersebut.

Pemberian hak akses sistem pelayanan data kependudukan, diwujudkan melalui

perjanjian kerja sama (PKS) antara Instansi yang mempunyai sistem informasi Pengakses dengan Dinas Kependudukan dan Pencatatan Sipil sebagai pemilik data Kependudukan. Informasi mengenai kebutuhan data apa saja yang perlu diakses, bagaimana hal tersebut dapat terlayani, pengaturan apa saja yang diperlukan serta sistem seperti apa yang dibutuhkan merupakan beberapa hal yang harus ada dalam PKS. PKS tersebut berlaku secara individu bukan kelompok sistem, sehingga tiap sistem informasi wajib mempunyai PKS sendiri untuk dapat mengakses data kependudukan.

Ditingkat kabupaten Wonosobo, terdapat beberapa sistem informasi yang membutuhkan data kependudukan dengan jenis yang berbeda. Oleh karena itu dibutuhkan pemetaan kebutuhan data untuk mengetahui data apa saja yang sebenarnya digunakan dalam sistem informasi mereka. Selain itu, pemetaan ini digunakan untuk memfilter data-data yang tidak perlu di ekspos, tidak di keluarkan dalam pelayanan data tersebut. Hal ini akan menghemat resource baik dalam ekspose dari data master hingga transmisi data yang dilakukan.

Penelitian ini bertujuan untuk memberikan usulan mengenai kewenangan sistem informasi atau kelompok sistem informasi dalam akses data kependudukan yang disediakan berdasarkan sensitifitas data dan jenis data. Dengan menggunakan metode *role-based access control (RBAC)*, pemetaan kebutuhan data dilakukan pada berbagai sistem informasi pelayanan publik yang membutuhkan data kependudukan. Kewenangan yang terpetakan dapat dijadikan sebagai masukan dalam penyusunan Perjanjian Kerja Sama (PKS), sebagai dasar pemberian hak akses dalam pemanfaatan data kependudukan sesuai dengan Permendagri

nomor 61 Tahun 2015(Menteri Dalam Negeri Republik Indonesia, 2015).

## METODE

Penelitian ini bertujuan untuk mengusulkan model pengamanan akses sistem *web service* pelayanan data kependudukan dengan pendekatan *Role-Based Access Control (RBAC)* yang disesuaikan dengan Permendagri nomor 61 tahun 2015 tentang Persyaratan, Ruang Lingkup Dan Tata Cara Pemberian Hak Akses Serta Pemanfaatan Nomor Induk Kependudukan, Data Kependudukan Dan Kartu Tanda Penduduk Elektronik(Menteri Dalam Negeri Republik Indonesia, 2015). Pendekatan yang dilakukan dalam penelitian ini merupakan pendekatan analisis deskriptif dengan cara melakukan kajian pustaka terkait *RBAC*, ketersediaan *Database* kependudukan, pemanfaatan data kependudukan oleh sistem informasi pelayanan publik di tingkat kabupaten, otorisasi dalam akses data kependudukan, dan dilanjutkan analisa kondisi aktual terkait dengan keamanan sistem terutama dalam kontrol akses yang dibutuhkan untuk mengetahui masalah yang ada. Selanjutnya disampaikan usulan konsep model keamanan sistem *web service* untuk pelayanan data kependudukan bagi sistem informasi di tingkat kabupaten dengan pendekatan *RBAC*, kemungkinan masalah yang akan timbul serta alternatif solusinya.

## HASIL DAN PEMBAHASAN

Penelitian mengenai implementasi *RBAC* yang telah dilakukan para peneliti sebelumnya diantaranya Asrianda yang menyimpulkan bahwa hak akses pengguna dapat dibatasi dengan *mutually exclusive permission (MEP)*(Asrianda, 2016). Pengguna yang sama tidak dapat mengaktifkan dua *role* yang berbeda meskipun *session*nya berbeda.

Siregar dalam penelitiannya menyimpulkan bahwa pemberian kewenangan kepada setiap user, dilakukan untuk mencegah kebocoran data dengan memisahkan kewenangan berdasarkan tugas dan tanggungjawabnya. Pemisahan kewenangan tersebut dilakukan untuk mencegah terjadinya konflik dari tugas antar *user* (Siregar et al., 2017).

Beberapa penelitian tersebut mengimplementasikan *RBAC* pada user manusia

sebagai subjeknya. Selain itu implementasi *RBAC* digunakan pada sistem informasi.

Implementasi *RBAC* pada penelitian ini berbeda dari sisi penggunaannya yaitu berupa sistem informasi yang akan mengakses layanan *web service* data kependudukan. Sehingga implementasi pada pemberian kewenangan (*role*) adalah kewenangan untuk sistem informasi dalam mengakses layanan yang disediakan berdasarkan tugas dan perannya dalam melakukan pelayanan publik.

### *Role Based Access Control (RBAC)*

*RBAC (Role Based Access Control)* adalah kontrol akses yang merupakan perpaduan *mandatory access control (MAC)* dan *discretionary access control (DAC)*(Osborn, Sandhu, & Munawer, 2000). *RBAC* mengacu pada *role based security* yang bersifat netral(Rajkumar & Sandhu, 2016) dan merupakan teknologi kontrol akses yang fleksibel untuk simulasi *DAC* dan *MAC*(Osborn et al., 2000). *RBAC* sebenarnya adalah bentuk *MAC*, tetapi tidak didasarkan pada persyaratan keamanan yang bertingkat seperti diterapkan pada aplikasi militer(Ferraiolo & Kuhn, 1992).

Kebijakan akses yang dilakukan oleh *MAC* berdasarkan ketentuan yang ditentukan oleh otoritas pusat (Samarati & Vimercati, 2001), bukan dilakukan oleh para pemilik individu dari objek tersebut, dan pemilik tidak dapat mengubah hak akses yang telah dibuat(Pfleeger, 1997). *MAC* memperlakukan kontrol akses berdasarkan keamanan informasi yang melekat pada pengguna dan objek.

Berbeda dengan *MAC*, *Discretionary Access Control (DAC)* adalah model akses sumber daya berdasarkan identitas pengguna. Pengguna dapat memberikan izin ke pengguna lain atau kelompok lain dalam model *DAC* (Strembeck, 2004). Akses dibatasi berdasarkan otorisasi yang diberikan pada pengguna, sehingga subjek diizinkan untuk menentukan tipe akses apa yang dapat terjadi pada objek yang mereka miliki. Kebijakan dari kontrol akses yang dapat diubah oleh pemiliknya sendiri serta secara optional dapat melimpahkan kewenangan yang mereka miliki sehingga akan menimbulkan kesulitan untuk mengontrol informasi secara efisien (Na & Cheon, 2000).

*RBAC* memberikan hak akses untuk *roles* bukan menerapkan hak akses pelaku atau subjek. Pengguna tidak bisa mengambil hak

akses pengguna lain merupakan dasar perbedaan antara *RBAC* dan *DAC* (Ferraiolo & Kuhn, 1992). Dalam organisasi, *roles* dibuat untuk fungsi kerja yang berbeda sesuai dengan peran keanggotaan yang didasarkan pada kompetensi, tugas, dan kewenangan. Tugas keamanan *RBAC* diberikan pada kontrol akses sebagai prioritas tertinggi untuk mengontrol akses ke sumber daya.

Administrator sangat berperan dalam memberikan hak kepada pengguna, sehingga subjek akan mendapatkan akses ke objek melalui *role* yang telah diberikan oleh *administrator* (Khayat & Abdallah, 2003).

Struktur *RBAC* meliputi *roles*, *permission*, *user*, dan *session* (Chen & Sandhu, 1996).

*RBAC* memerlukan penugasan hak akses untuk *role* pada setiap subjek (Khayat & Abdallah, 2003), dengan cara menghubungkan subjek dengan *role*. Hak akses yang ditugaskan ke *roles* akan digunakan oleh pengguna untuk membuat sebuah *session*, dan *session* akan mendapatkan izin (*permission*) dari *role* yang didapatkan oleh pengguna untuk mengaktifkan perannya (*roles*).

Dalam *RBAC*, *role* didefinisikan sebagai suatu gagasan yang merupakan dasar dari kebijakan kontrol akses (Sandhu & Bhamidipati, 1999). *Role* didefinisikan dalam ilmu perilaku sebagai pola yang ditentukan sesuai perilaku seseorang dalam situasi tertentu berdasarkan posisi orang.

*Permission* merupakan wewenang diberikan kepada pengguna atau subjek melakukan beberapa operasi atau tindakan yang dilakukan kepada objek (Ferraiolo & Kuhn, 1992). Objek dalam konteks kontrol akses dianggap sebagai sumber daya yang oleh pengguna dapat melakukan beberapa kegiatan. Objek dapat berupa file, folder, *directory*, *record*, atau *table* dan lain-lain. Tipe objek tergantung dengan sifat pada sistem yang dibuat.

Subjek merupakan proses untuk menjalankan tugas atau aktivitas atas nama pengguna. Dalam sebuah *role*, untuk menjalankan tugas tertentu dilakukan dengan melibatkan beberapa subjek yang aktif. Subjek pada setiap proses akan melakukan jalur aksesnya, sehingga akan diketahui proses tersebut dipanggil oleh pengguna yang resmi atau tidak. Hal ini dilakukan pengguna dengan memasukkan identitasnya dalam melakukan

*login* ke sistem. Program utama yang beroperasi atas nama pengguna untuk *login* didefinisikan sebagai subjek (Ferraiolo & Kuhn, 1992).

Merujuk pada definisi *role* yang ambigu (Zhu, 2003), karenanya kolaborasi dengan kontrol akses masih disesuaikan dengan kebutuhan sehingga dalam implementasi pada penelitian ini *role* di definisikan sebagai peran pengguna terkait kebutuhan data kependudukan nya.

#### **Database SIAK dan pemanfaatannya.**

Sistem Informasi Administrasi Kependudukan (SIAK), yang terdiri dari Aplikasi, *Database* dan jaringan SIAK, terhubung dari pemerintah pusat, pemerintah provinsi dan pemerintah kabupaten yang dijalankan oleh pengelolanya masing-masing (Indonesia, 2013). *Database* kependudukan pada SIAK di kabupaten memiliki muatan yang kompleks dan seragam. *Database* kependudukan di Kabupaten menggunakan platform *Database* yang memuat data-data wilayah; keluarga; biodata; pencatatan sipil; serta foto, sidik jari tangan, dan tanda tangan. Data wilayah, terdiri atas nama dan kode provinsi; nama dan kode kabupaten/kota; nama dan kode kecamatan/lainnya; serta nama dan kode desa/kelurahan/lainnya, sedangkan data keluarga terdiri atas: nomor kartu keluarga; nama kepala keluarga; alamat; RT; RW; dusun; kode pos; dan nomor telepon.

Pemanfaatan data kependudukan telah diatur oleh pemerintah dalam UU nomor 24 tahun 2013 (Indonesia, 2013) dan lebih rinci dalam Permendagri nomor 61 tahun 2015 (Menteri Dalam Negeri Republik Indonesia, 2015). Pemanfaatan data kependudukan oleh lembaga negara, kementerian/lembaga pemerintah non kementerian atau badan hukum Indonesia adalah data kependudukan yang sudah dikonsolidasikan dan dibersihkan oleh Kementerian Dalam Negeri. Data Kependudukan diterbitkan secara berkala, untuk skala Nasional, skala Provinsi dan Kabupaten/Kota diterbitkan per semester yaitu semester pertama diterbitkan tiap tanggal 30 Juni dan semester kedua diterbitkan tanggal 31 Desember setiap tahun kalender (Indonesia, 2013) yang akan di olah untuk menjadi pelayanan data agregat untuk digunakan dalam perencanaan dan pelaporan.

Instansi pelayanan publik di tingkat kabupaten merupakan ujung tombak pelayanan pemerintah kepada masyarakat. Mereka membutuhkan data identitas mutakhir sesuai dengan administrasi kependudukan agar lebih efektif dan efisien dalam pelayanan, mengurangi redundansi data, serta mengurangi munculnya banyak versi hasil olahan data akibat inkonsistensi data kependudukan (Sutanta, 2011) pada sistem informasi pelayanan publik yang dimilikinya. Namun sampai saat ini, berbagai sistem informasi tersebut belum dapat mengakses layanan data yang disediakan oleh pemerintah pusat (Fakrulloh, 2015). Oleh karena itu, untuk memenuhi kebutuhan tersebut diperlukan sebuah sistem pelayanan data kependudukan yang aman ditingkat kabupaten berbasis data pelayanan. Sedangkan untuk mendapatkan pelayanan data tersebut, terlebih dahulu harus mendapatkan hak akses yang dituangkan dalam perjanjian kerja sama (PKS) dengan Disdukcapil Kabupaten (Menteri Dalam Negeri Republik Indonesia, 2015). Hak akses terhadap data kependudukan akan diberikan sesuai dengan kewenangan yang tercantum dalam PKS tersebut.

### **Penggunaan web service dalam pemanfaatan data kependudukan oleh sistem lain.**

Ketersediaan *Database* kependudukan berbasis NIK yang saat ini semakin baik akan memberikan manfaat yang maksimal di Pemkab/Pemkot (Sutanta & Ashari, 2012), melalui pengembangan ragam aplikasi sistem informasi yang terintegrasi dengan memanfaatkan *Database* kependudukan, terutama aplikasi pelayanan publik. Integrasi pada level data, middleware, dan aplikasi dikembangkan dengan teknologi *web service* (Istiyanto & Sutanta, 2012), yang disertai dengan evaluasi atas kinerja sistem secara terus-menerus sebagai bagian proses dalam siklus hidup sistem informasi (Sutanta & Ashari, 2012).

*Web service* diusulkan sebagai sarana untuk melakukan integrasi secara horizontal antara pemilik data kependudukan dengan sistem informasi lain yang membutuhkan. ditingkat kabupaten. Integrasi horizontal ditingkat lokal, ditingkat regional dan tingkat pusat, serta integrasi vertikal di semua tingkatan akan dapat dilakukan jika masing-

masing instansi sudah terelasi dengan baik (Informasi, 2012)

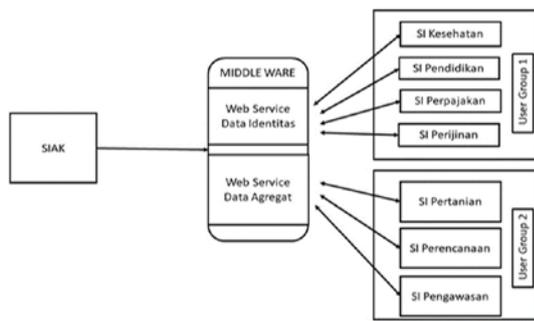
### **Pengamanan sistem berdasarkan otorisasi pengguna**

Pengamanan sistem integrasi, berkaitan dengan pemanfaatan data kependudukan menjadi suatu hal yang harus dilakukan untuk mendapatkan manfaat dari integrasi sistem. Beberapa hal yang menjadi pertimbangan dalam mengembangkan keamanan sistem tersebut antara lain kebutuhan untuk menjamin *confidentiality*, *integrity*, dan *availability* data penduduk yang disediakan oleh sistem, serta berbagai kemungkinan kerentanan baik yang disebabkan oleh tindakan sengaja (penyerangan) maupun karena kelalaian.

Salah satu cara dalam pengamanan sistem adalah dengan otorisasi. *Authorization* merupakan proses mengizinkan atau penolakan untuk mengakses sumber daya dari service yang disediakan. Proses tersebut dilakukan dengan menyediakan *access control* terhadap *resource* atau operasi yang dapat dilakukan oleh *user*.

Dalam konteks *web service* pemanfaatan data kependudukan, proses otorisasi diawali dengan memberikan hak akses bagi *user /user group*, sesuai dengan kebutuhan datanya. Pembagian *user group* didasarkan pada perjanjian kerja sama (PKS) yang di dasarkan pada Permendagri nomor 61 tahun 2015 yang dibuat oleh masing-masing instansi dengan pihak dukcapil. Jenis data agregat ataupun data detail yang dibutuhkan oleh sistem informasi *requester* akan dilayani jika sesuai dengan hak akses yang terdaftar.

Berdasarkan pada peran masing-masing sistem informasi milik berbagai dinas di tingkat kabupaten dalam pelayanan publik, didapatkan gambaran mengenai kebutuhan data kependudukan berbagai sistem informasi tersebut. Kebutuhan data secara garis besar dipetakan menjadi 2 kelompok (grup). Kebutuhan data tersebut dibedakan menjadi kebutuhan data identitas dan kebutuhan data agregat kependudukan. Kebutuhan data dimaksud digambarkan pada Gambar 1 :



Gambar 1. Model pemetaan *kebutuhan data kependudukan* berdasarkan PKA

Pemetaan kebutuhan data oleh sistem informasi berdasarkan jenis data antara lain:

1. Identitas : yang dimaksud dengan identitas adalah data pribadi yang merupakan data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta

- dilindungi kerahasiaannya , (pasal 1 point 22 UU No 24 tahun 2013)
2. Agregat Penduduk: Data kependudukan yang dihimpun dari pendaftaran penduduk dan pencatatan sipil menjadi data agregat penduduk yang meliputi himpunan data perseorangan berupa data kuantitatif dan data kualitatif. Data Kependudukan tersebut digunakan untuk semua keperluan berasal dari Kementerian Dalam Negeri (pasal 58 UU No. 24 Tahun 2013)

Dalam implementasi pemetaan kebutuhan data berdasarkan fungsi dan peran sistem informasi dikabupaten Wonosobo, jenis data yang dibutuhkan di gambarkan dalam Tabel 1:.

Tabel 1 : Kebutuhan data penduduk berdasarkan data identitas dan agregat oleh sistem informasi di tingkat Kabupaten Wonosobo

	SINTA/ PATEN SIS NAKER	SIK	SIMRS	RENDA	APRIZ (Perijinan)	Dapodik mas DIK PORA	Perke bunan Diper tan	SIGA	BPH TB	PBB	SIM KAH	SIM MIG RASI	Penerbitan SKCK	Penbita SIM	SIM WAS	BPS
NIK	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		
Nama Lengkap	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		
Blok Alamat	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		
Blok Data Kelahiran		✓	✓	✓		✓		✓			✓	✓	✓	✓		
Jenis Klmin		✓	✓	✓		✓		✓			✓	✓	✓	✓		
Gol Darah			✓	✓		✓		✓			✓	✓	✓	✓		
Agama						✓					✓					
Jenis Pekerjaan		✓			✓							✓	✓	✓		
Blok Status Kawin											✓	✓	✓	✓		
Pendidikan akhir		✓				✓		✓								
Blok No Kk			✓	✓		✓		✓			✓	✓	✓	✓		
Nama Lgkp Ibu			✓	✓		✓		✓			✓	✓	✓	✓		
Nama Lgkp Ayah			✓	✓		✓		✓			✓	✓				

Data Agregat Penduduk	✓	✓	✓	✓	✓	✓	✓	✓	✓
-----------------------	---	---	---	---	---	---	---	---	---

Pada Tabel 1, beberapa data dimasukkan kedalam blok data, dikarenakan elemen data tersebut tidak bisa dipisahkan dari yang lain. Blok-blok data tersebut antara lain :

1. Blok alamat : nama prop, no prop, nama kab, no kab, nama kec, no kec, nama kel, nama kel, alamat, no rw, no rt
2. Blok data kelahiran : tempat lahir, tanggal lahir, umur, status akta kelahiran, no akta kelahiran
3. Blok pendidikan: status pendidikan, no ijazah, tanggal lulus
4. Blok status kawin : status kawin, no akta kawin/buku nikah, no akta cerai
5. Blok kk : no kk, nama kepala keluarga, alamat kk, status hub dalam keluarga.

Berdasarkan kelompok data, data kependudukan dibagi menjadi dua kelompok yaitu :

1. Data Umum ; Merupakan data kependudukan baik data identitas maupun data aggregate yang bersifat umum atau tidak dirahasiakan sesuai dengan aturan kependudukan menurut UU nomor 24 tahun 2013 yang di perjelas dengan Permendagri no 61 tahun 2015.
2. Data sensitif/ rahasia; Merupakan data yang di rahasiakan berdasarkan peraturan perundangan yang berlaku. Data ini meliputi keterangan tentang cacat fisik dan/atau mental, sidik jari, iris mata, tanda tangan, dan elemen data lainnya yang merupakan aib seseorang.

Berkaitan dengan data sensitif tersebut, dalam pengaksesan untuk data-data dimaksud memerlukan peraturan khusus. Bagi sistem-informasi yang membutuhkan data-data sensitif misalnya sistem informasi dinas sosial, membutuhkan hak akses khusus yang harus di kaji terlebih dahulu oleh kementerian dalam negeri. Sehingga tidak dibahas dalam penelitian ini.

Pada implementasi di *web service* pelayanan data kependudukan, misalkan *user* sistem informasi Kesehatan mendapatkan hak

akses sesuai kewenangannya, maka dapat mengakses data yang digambarkan dengan perintah seperti pada Gambar 2 :

```
http://adminduk.wonosobokab.go.id:8311/index.html?akses=nik&user=lintas_siak_sik_wns&pa swd=siak_sik_3307_mr&nomor_nik=33070617 07800001
```

Gambar 2. Perintah untuk mendapatkan data sesuai kewenangannya

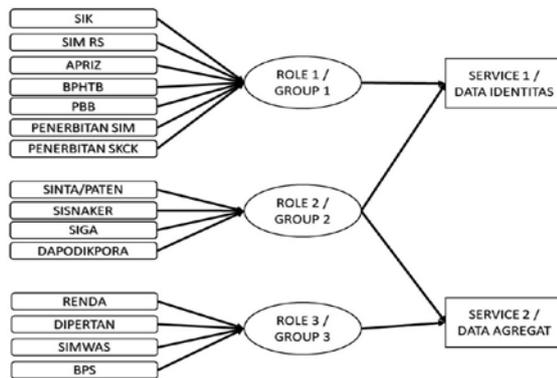
*User* lintas\_siak\_sik\_wns serta *password* siak\_sik\_3307\_mr , merupakan hak akses berdasarkan *role* pada kelompok pengakses data identitas. Dengan perintah tersebut *web service* akan memberikan respon yang isinya menyesuaikan dengan kebutuhan data yang tercantum dalam PKS yang telah disepakati bersama, yang diantaranya dapat digambarkan pada Gambar 3:

```
{"siak2sik":{"nomor_nik":"3307061707800001","nama_lengka p":"RUBIYANTO","nama_prop":"JAWA TENGAH","no_prop":"33","nama_kab":"WONOSOBO","no_k ab":"7","nama_kec":"SELOMERTO","no_kec":"6","nama_kel": "SELOMERTO","no_kel":"1008","alamat":"JAGALAN","rt":"5 ","rw":"8","tempat_lahir":"WONOSOBO","tanggal_lahir":"17- 07-1980","kelamin":"LAKI-LAKI","gol_darah":"O","nama_ibu":"KINASIH","nama_ayah "DARMAJI"}}
```

Gambar 3. Respon yang didapatkan dari *middleware* sesuai dengan kewenangan hak akses.

Berdasarkan hasil pemetaan kebutuhan data dalam tabel 1, didapatkan bahwa sistem informasi yang membutuhkan data identitas merupakan sistem informasi yang melayani publik secara langsung. Artinya SI-sistem informasi tersebut digunakan untuk bertransaksi dengan masyarakat. Sedangkan sistem informasi yang membutuhkan data agregat adalah jenis sistem informasi yang digunakan untuk memberikan laporan atau tidak digunakan untuk transaksi dengan masyarakat secara langsung. Namun beberapa sistem informasi juga membutuhkan kedua jenis data, baik detail maupun agregat, karena fungsi sistem informasi nya selain memberikan laporan juga digunakan untuk transaksi. Data identitas minimal yang dibutuhkan oleh kelompok pengguna, meliputi data NIK; Nama

Lengkap dan Blok Alamat. Pengelompokan



kebutuhan data yang didapatkan digambarkan pada Gambar 4:

Gambar 4. Pengelompokan *user group* berdasarkan kebutuhan data.

**Kemungkinan masalah dan solusinya.**

Masalah yang berpotensi terjadi dalam upaya pengamanan sistem *web service* pemanfaatan data kependudukan melalui pendekatan *RBAC* antara lain : kemungkinan berubahnya bisnis yang ditangani oleh Instansi pengguna *web service* sebagai akibat pemecahan atau penggabungan organisasi yang lazim terjadi di Pemkab. Karenanya perlu dilakukan evaluasi secara periodik terhadap kebutuhan data tersebut minimal satu tahun sekali dengan pertimbangan bahwa jangka waktu tersebut di anggap cukup untuk melakukan evaluasi berkaitan hak akses.

Masalah lain yang mungkin muncul adalah keinginan untuk mendapatkan hak akses yang melebihi kebutuhannya. Hal ini bisa terjadi dikarenakan pengelola sistem informasi yang berkeinginan untuk mengetahui atau mengekspos data kependudukan lebih banyak tetapi sebenarnya hal tersebut tidak dibutuhkan oleh sistem informasi nya.. tersebut membuat proses untuk mendapatkan hak akses tersebut tidak mudah. Untuk mengatasi permasalahan tersebut, dibutuhkan komitmen baik para pimpinan maupun pengelola sistem informasi yang membutuhkan data kependudukan untuk mempelajari berbagai persyaratan legal (Menteri Dalam Negeri Republik Indonesia, 2015) dibutuhkan untuk mendapatkan hak. Selain itu, baik pihak *provider* maupun *requester* harus benar-benar memahami kewenangannya masing-masing.

Berbagai upaya pengamanan sistem termasuk kontrol akses meelalui implementasi *RBAC* harus diimbangi dengan peningkatan kualitas sumberdaya manusia pengelola dan pemakainya. Hal ini bertujuan agar sistem yang sudah terbangun dapat memberikan manfaat yang optimal.

**SIMPULAN DAN SARAN**

Upaya pengamanan sistem *web service* pelayanan data kependudukan, salah satunya dapat dilakukan dengan implementasi *RBAC*. Untuk menentukan kewenangan dalam hak akses berbagai sistem pelayanan di tingkat kabupaten, dibutuhkan untuk mengetahui kebutuhan data kependudukan bagi setiap sistem atau kelompok sistem. Pemetaan kebutuhan data kependudukan pada sistem pelayanan publik, dilakukan dengan mengelompokkan kebutuhan berdasarkan jenis data dan sensitifitas data. Hasil yang didapatkan dari pengelompokkan tersebut bahwa beberapa sistem informasi membutuhkan data agregat untuk memberikan informasi, perencanaan dan pelaporan, sedangkan untuk sistem informasi pelayanan publik membutuhkan data identitas, dengan beberapa variasi berkaitan dengan data yang digunakan.

Pemetaan yang sudah dilakukan berdasarkan estimasi kebutuhan, dapat dijadikan sebagai masukan dalam penyusunan PKS, terutama berkaitan dengan pemberian hak akses. Namun, karena berdasarkan estimasi kebutuhan, maka kebutuhan *real* yang di butuhkan oleh sistem informasi terkait tersebut dimungkinkan akan ada perbedaan dengan penelitian ini. Oleh karena itu, perlu dilakukan kajian mendalam mengenai berbagai kebutuhan data kependudukan khususnya oleh sistem pelayanan publik dengan melibatkan para pemangku kepentingan di berbagai instansi yang mengampunya.

**UCAPAN TERIMAKASIH**

Ucapan terimakasih setinggi-tingginya ditujukan kepada Dosen pengajar, dosen pembimbing, pegawai dan staf Departemen Teknik Elektro dan Teknologi Informasi Universitas Gadjah Mada, terutaman Bapak Selo, S.T., M.T., M.Sc., Ph.D, sebagai pembimbing utama serta Bapak Widyawan, S.T., M.Sc., Ph.D, sebagai pembimbing kedua yang telah meluangkan waktu ditengah

kesibukan beliau berdua untuk memberikan bimbingan dalam penelitian ini.

#### DAFTAR PUSTAKA

- Asrianda. 2016. Kontrol Akses dan Keamanan Data bagi Penduduk Miskin. Hal. 51–55 in *Proceeding Seminar Nasional Ilmu Komputer (SEMINASIK)*, vol. 1. Bireun, Aceh: Fakultas Ilmu Komputer Universitas Almuslim, 11 - 18 November 2016. Di akses 9 Juli 2017 ([http://www.academia.edu/34671943/KONTROL\\_AKSES\\_DAN\\_KEAMANA\\_N\\_DATA\\_BAGI\\_PENDUDUK\\_MISKI\\_N](http://www.academia.edu/34671943/KONTROL_AKSES_DAN_KEAMANA_N_DATA_BAGI_PENDUDUK_MISKI_N)).
- Chen, Fang dan Ravi S. Sandhu. 1996. Constraints for role-based access control. *Proceedings of the first ACM Workshop on Role-based access control - RBAC '95* (7):14–es. Di akses 18 Juli 2017 (<http://dl.acm.org/citation.cfm?id=270152.270177>).
- Fakrulloh, Zudan Arif. 2015. Pemanfaatan Data Kependudukan Untuk Mendukung Pelayanan Publik. 1–16. Di akses 9 Juli 2017 (<ftp://167.205.53.175/pub/ISO-IMAGES/linux/eii2015itb/dukcapil - ITB 2015.pdf>).
- Ferraiolo, David F. dan D.Richard Kuhn. 1992. Role-Based Access Controls. Hal. 554–63 in *15 th National Computer Security Conference*. Baltimore.
- Habib, M. A. 2011. Role inheritance with object-based DSD. *International Journal Internet Technology and Secured Transactions* 3(2):149–60.
- Istiyanto, Jazi Eko dan Edhy Sutanta. 2012. Model Interoperabilitas antar Aplikasi E-Government. *Jurnal Teknologi Technoscintia* 4(2):137–48.
- Kementrian Negara Komunikasi dan Informasi. 2012. *Sisfonas 2010: Sisfonas Sebagai Tulang Punggung Aplikasi E-Government*. Jakarta.
- Khayat, E. J. dan A. E. Abdallah. 2003. A formal model for flat role-based access control. Hal. 75 in *ACS/IEEE International Conference on Computer Systems and Applications, 2003. Book of Abstracts*. Tunis, Tunisia: IEEE. Di akses 4 Oktober 2017 (<http://ieeexplore.ieee.org/document/1227507/>).
- Menteri Dalam Negeri Republik Indonesia. 2015. Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 61 Tahun 2015 tentang Persyaratan, Ruang Lingkup Dan Tata Cara Pemberian Hak Akses Serta Pemanfaatan Nomor Induk Kependudukan, Data Kependudukan Dan Kartu Tanda Penduduk Elektronik. 1–6. Di akses 29 Juli 2017 ([http://www.dukcapil.kemendagri.go.id/zCFiles/uploads/downloads/PERMENDAGRI\\_NOMOR\\_61\\_THN\\_2015.pdf](http://www.dukcapil.kemendagri.go.id/zCFiles/uploads/downloads/PERMENDAGRI_NOMOR_61_THN_2015.pdf)).
- Na, Sang Yeob dan Suh Hyun Cheon. 2000. Role delegation in role-based access control. Hal. 39–44 in *RBAC'00 Proceedings of the fifth ACM workshop on Role-based access control*. Berlin, Germany: ACM New York.
- Osborn, Sylvia, Ravi Sandhu, dan Qamar Munawer. 2000. Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Transactions on Information and System Security* 3(2):85–106.
- Pfleeger, Charles P. 1997. *Security in Computing*. 2 ed. Upper Saddle River, New Jersey, US: Prentice Hall Professional Technical Reference.
- Presiden Republik Indonesia. 2013. Undang-undang Nomor 24 Tahun 2013 tentang perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. 1–43. Di akses 26 Juli 2017 ([http://www.dukcapil.kemendagri.go.id/zCFiles/uploads/downloads/UU\\_24\\_Thn\\_20132.pdf](http://www.dukcapil.kemendagri.go.id/zCFiles/uploads/downloads/UU_24_Thn_20132.pdf)).
- Rajkumar, P. V dan Ravi Sandhu. 2016. POSTER : Security Enhanced Administrative Role Based Access Control Models. Hal. 1802–4 in *CCS'16*. Viena, Austria.
- Samarati, P. dan S. C. de Vimercati. 2001. Access Control: Policies, Models, and Mechanisms. Hal. 137–96 in *FOSAD 2000: Foundation of Security Ananlysis and Design*. Berlin, Heidelberg: Springer.
- Sandhu, Ravi dan Venkata Bhamidipati. 1999. Role-based administration of user-role assignment: The URA97 model and its Oracle implementation. *Journal of Computer Security* 7(4):317–42.

- Siregar, Firman Hamonangan et al. 2017. Analisis Metode Role-Based Access Control Pada Sistem Pengamanan Basis Data Dengan Konsep CIA. 1–7. Di akses 8 Agustus 2017 ([http://journal.stth-medan.ac.id/mahasiswa/index.php/doc\\_download/373-v1254-analisis-metode-role-based-access-control-pada-sistem-pengamanan-basis-data-dengan-konsep-cia](http://journal.stth-medan.ac.id/mahasiswa/index.php/doc_download/373-v1254-analisis-metode-role-based-access-control-pada-sistem-pengamanan-basis-data-dengan-konsep-cia)).
- Strembeck, M. 2004. Conflict Cheking of Separation of Duty Constraints in RBAC Implementation Experiences. Hal. 1–6 in *In Proc. of the Conference on Software Engineering*.
- Sutanta, Edhy. 2011. Model Intregrasi Database Penduduk Indonesia Dengan Berbagai Sistem Informasi Berbasis Komputer. *Jurnal Informatika* 5(2):542–53.
- Sutanta, Edhy dan Ahmad Ashari. 2012. Pemanfaatan Database Kependudukan Terdistribusi pada Ragam Aplikasi Sistem Informasi di Pemerintah Kabupaten/Kota. *Jurnal Ilmiah Sisfotenika* 2(1):11–20.
- Wardana, Mohamad Ali dan Rahman. 2016. Interoperabilitas Sistem Terdistribusi Berbasis Protokol Soap. *Jurnal Ilmiah Ilkom* 8(1):57–62.
- Zhu, Haibin. 2003. A Role Agent Model for Collaborative Systems. *IKE* 438–44.