PENENTUAN MODEL KEPERCAYAAN INFRASTRUKTUR KUNCI PUBLIK DI INDONESIA DENGAN PENDEKATAN *ANALYTIC HIERARCHY PROCESS*

Eko Yon Handri[1)], Frizka Ferina[2)]
Puskaji Palsan, Lemsaneg
Jl. Harsono RM No.70 Ragunan
E-mail : yon.handri@lemsaneg.go.id[1)],frizka.ferina@lemsaneg.go.id[2)]

Abstrak

Infrastruktur Kunci Publik (IKP) dibutuhkan dalam menyediakan keamanan informasi pada layanan egovernment dimana CA menjadi inti pelaksanaan sistemnya. Permasalahan dalam implementasi IKP adalah bagaimana menentukan model kepercayaan yang tepat agar layanan e-government tidak terhambat akibat komunikasi antara pemerintah dan masyarakat yang tidak berjalan dengan baik. Makalah ini menggunakan pendekatan Analytic Hierarchy Process (AHP) dengan tujuan untuk mengevaluasi secara akurat dari pengaruh kriteria pada lima dasar pertimbangan penentuan model kepercayaan IKP dan sub-kriteria pada empat alternatif desain n-tier CA. Hasil analisis menunjukkan bahwa aspek keamanan menjadi priotitas utama sebagai kriteria dasar pertimbangan penentuan model kepercayaan, diikuti dengan aspek fleksibilitas, interoperabilitas dan kompatibilitas, skalibilitas dan adaptibilitas, dan yang terakhir adalah aspek kemudahan pengembangan dan kegunaan. Sedangkan pada sub-kriteria, model 3-tier CA merupakan pilihan utama untuk implementasi IKP di Indonesia, alternatif lainnya secara berurutan adalah model 2-tier CA, 3-tier CA modifikasi dan pilihan akhir adalah 1-tier CA.

Kata kunci: *Infrastruktur Kunci Publik, Analytic Hierarchy Process, AHP, CA, e-government*

1. LATAR BELAKANG

Penyelenggaraan *e-government* yang semakin berkembang saat ini tidak bisa lepas dari masalah keamanan informasi untuk melindungi data pribadi milik masyarakat yang telah memanfaatkan layanan pemerintah. Keamanan informasi yang dimaksud adalah menjaga keutuhan data (integritas), menjamin keaslian data (autentikasi) dan nir-sangkal terhadap penggunaan data. Dalam memenuhi kebutuhan keamanan informasi pada *e-government*, bentuk pengamanan yang bisa diterapkan adalah melalui Infrastruktur Kunci Publik [1]. Melalui UU Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Indonesia telah memiliki dasar yang kuat untuk mengimplementasikan Infrastruktur Kunci Publik (IKP). Dan melalui PP Nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), diatur lebih detail tentang mekanisme implementasi IKP khusunya dalam penyelenggaraan sertifikat digital. Pada pasal 61 PP PSTE disebutkan bahwa terdapat 3 (tiga) tingkatan pengakuan penyelenggara sertifikasi elektronik, atau yang biasa dikenal dengan *Certificate Authority*/CA, yaitu terdaftar, tersertifikasi dan berinduk [2]. Tingkatan berinduk merujuk pada pihak penyelenggara sertifikasi elektronik induk sebagai *Root CA* yang dikelola oleh pemerintah dengan model kepercayaan hirarki. Model hirarki memiliki beberapa alternatif desain n-tier yang didasarkan pada tingkatan peran CA. Penentuan desain n-tier perlu mempertimbangkan beberapa hal yaitu dengan melihat aspek bisnis proses, operasional, kebijakan dan kondisi demografik Indonesia.

Implementasi IKP memiliki karakteristik tertentu pada suatu organisasi pemerintahan sehingga dapat mengakibatkan kegagalan atau menghasilkan kesuksesan pada pelaksanaaanya [3]. Kegagalan implementasi IKP dapat terjadi karena pembangunan infrastruktur yang terlalu kompleks dan mahal, infrastruktur belum tersedia atau kebutuhan teknis dan proses bisnis yang tidak siap. Akibat kegagalan tersebut layanan pemerintah dapat terhampat untuk berkomunikasi dengan masyarakat, swasta atau pun pihak lainnya. Namun sebaliknya apabila implementasi IKP berhasil dilaksanakan maka banyak manfaat yang diperoleh yaitu dapat meningkatkan layanan publik antara pemerintah dan masyarakat ataupun pihak swasta disertai dengan jaminan keamanan transaksi dan perlindungan dokumen sensitif.

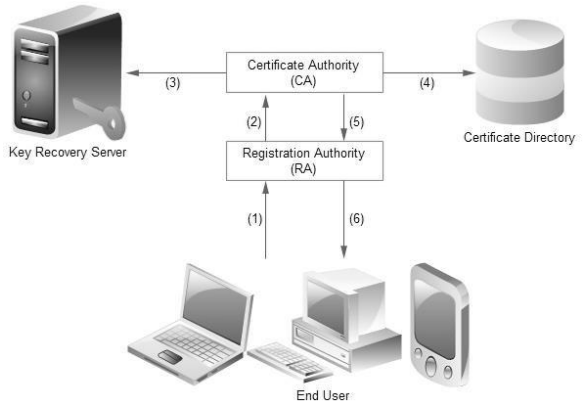
Berdasarkan hal tersebut di atas, maka implementasi IKP di Indonesia harus mampu mengakomodir segala permasalahan yang ada agar dapat diselenggarakan dengan baik. Langkah awal yang dapat dilakukan adalah dengan menentukan model kepercayaan hirarki yang tepat dengan melihat pertimbangan yang ada. Ada 5 (lima) pertimbangan dalam menentukan model kepercayaan IKP yaitu interoperabilitas dan kompatibilitas, kemudahan pengembangan dan kegunaan, fleksibilitas, keamanan CA serta skalabilitas dan adaptibilitas [4]. Makalah ini akan menjelaskan bagaimana menentukan prioritas desain n-tier CA dari model hirarki berdasarkan kelima pertimbangan tersebut yang diharapkan menjadi pilihan yang tepat dalam mengimplementasikan IKP di Indonesia.

2. INFRASTRUKTUR KUNCI PUBLIK (IKP)

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 [5]. 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.

2.1 Komponen IKP

IKP dapat diimplementasikan dengan baik melalui interaksi antar komponen dasarnya. Adapun komponen dasar IKP terdiri dari CA, *Registration Auhtority* (RA), Pengguna, *Key Recovery Server/Archive* dan *Certificate Directory/Repository* [6]. 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).



Gambar 1. Interaksi Antar Komponen Dasar IKP [6]

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) [7].

2.2 Model Kepercayaan Hirarki

Setiap IKP memiliki model kepercayaan yang dipilih berdasarkan pertimbangan matang oleh suatu organisasi. Model kepercayaan IKP yang dapat dipilih antara lain *web-of-trust*, *single CA*, hirarki, *browser trust-list*, *crosscertificate* dan *bridge CA* (*hybrid CA*). Dari beberapa model kepercayaan tersebut model hirarki merupakan bentuk arsitektur IKP yang paling umum digunakan karena semua CA saling mempercayai satu sama lain [4]. Hal ini menjadi salah satu kelebihan dibandingkan dengan model kepercayaan lainnya.

Konsep dari model hirarki adalah dibutuhkan adanya *Root CA* sebagai pusat kepercayaan bagi komponen di bawahnya. Kebijakan dan standar infrastruktur yang ditetapkan oleh *Root CA* harus dijalankan oleh komponen CA yang berada di bawah hirarkinya. Berdasarkan konsep tersebut di atas, maka model hirarki dapat dibagi menjadi beberapa alternatif desain infrastruktur dalam bentuk n-tier dimana n merupakan jumlah tingkat CA yang berperan. Pada umumnya, model hirarki yang banyak digunakan adalah antara 2-tier, 3-tier dan 4-tier, namun 1-tier (*single tier*) dapat juga diterapkan untuk organisasi yang kecil [8]. Berikut penjelasan model hirarki n-tier.

Tabel 1. Alternatif n-Tier CA [8]

No.	*n-Tier*	Penjelasan
1.	*1-tier (single*	Model hirarki ini biasanya memiliki pengguna kurang dari 300 orang yang membutuhkan sertifikat digital sehingga cukup membutuhkan 1(satu) CA. Kelebihannya adalah mudah dikelola sedangkan
	tier)	kelemahannya adalah apabila CA mengalami serangan, maka semua infrastruktur juga tidak dapat beroperasi.
2.	*2-tier*	Model hirarki ini membutuhkan 2 (dua) tingkatan CA. Satu tingkatan CA berperan sebagai *Root CA* yang offline dan tingkatan di bawahnya berperan sebagai sub-CA yang menerbitkan sertifikat digital kepada pengguna. Kelebihannya adalah apabila salah satu sub-CA mengalami serangan maka subCA lainnya atau *Root CA* tidak terpengaruh sehingga infrastruktur masih terjaga.
3.	*3-tier*	Model hirarki ini membutuhkan 3 (tiga) tingkatan CA. Satu tingkatan CA sebagai *Root CA*, tingkatan kedua CA sebagai intermedia-CA untuk penentuan kebijakan dan tingkatan ketiga CA sebagai sub-CA penerbit sertifikat digital pengguna. Kelebihannya adalah lebih fleksibel dan lebih aman dalam implementasi infrastruktur karena diatur oleh kebijakan berbeda dari intermediate CA.
4.	*4-tier*	Model hirarki ini membutuhkan 4 (empat) tingkatan CA. Konsepnya sama seperti 3-tier namun di bagian sub-CA masih dapat diturunkan menjadi sub-CA yang lebih spesifik fungsinya. Kelebihannya adalah paling fleksibel dibandingkan dengan n-tier lainnya.

Beberapa negara yang memilih model hiraki dalam implementasi IKP memiliki bentuk n-tier yang berbedabeda. Negara Qatar menggunakan 2-tier CA [9]. Negara Filipina menggunakan 3-tier CA [10]. Negara India melakukan modifikasi 2-tier CA dimana terdapat sub-CA yang memiliki sub-CA lagi di bawahnya [11].

2.3 Dasar Pertimbangan

Pelaksanaan implementasi IKP perlu mempertimbangkan beberapa kriteria agar sesuai dengan kebutuhan operasional, bisnis proses dan kondisi demografik Indonesia dalam membangun infrastrukturnya. Menurut Choudhury, ada 5 (lima) kriteria yang dapat dijadikan pertimbangan untuk menentukan solusi yang tepat pada implementasi IKP seperti dijelaskan pada tabel 2 berikut.

Tabel 2. Kriteria Dasar Implementasi IKP [4]

No.	Kriteria	Penjelasan
1.	Interoperabilitas dan Kompatibilitas	Desain IKP yang akan diimplementasikan harus dapat mengikuti perkembangan teknologi sehingga tetap dapat berhubungan dengan perangkat dan aplikasi terbaru, komponen IKP lainnya serta sesuai standar
2.	Kemudahan Pengembangan dan Kegunaan	Pengembangan IKP tidak hanya berkaitan dengan sertifikat digital, algoritma kriptografi, dan kunci-kunci kriptografi tetapi hasil implementasi harus mendukung penggunaan aplikasi yang *user friendly.*
3.	Fleksibilitas	Desain IKP yang dipilih untuk diimplementasikan tidak perlu terlalu kompleks dan memiliki ruang lingkup yang memungkinkan untuk dikembangkan sesuai dengan kebutuhan pengguna.
4.	Keamanan CA	CA yang merupakan inti dari seluruh sistem IKP membutuhkan pengamanan dengan tingkat maksimal karena apabila terdapat bagian CA yang lemah keamanannya maka akan melemahkan keseluruhan sistem IKP.

5.	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.

3. METODOLOGI PENELITIAN

Penentuan model kepercayaan IKP memiliki beberapa dasar pertimbangan dan alternatif desain n-tier CA yang menyebabkan pengambilan keputusan menjadi cukup kompleks. Salah satu pendekatan yang dapat digunakan untuk menyelesaikan masalah tersebut adalah *Analytic Hierarchy Process* (AHP). AHP merupakan suatu pendekatan yang digunakan untuk melakukan pengambilan keputusan dari banyak kriteria yang mengkombinasikan analisis kuantitatif dengan analisis kualitatif berdasarkan model struktur [12]. Pendekatan AHP menyelesaikan masalah dengan memilih beberapa kriteria dan sub-kriteria sebagai masukan-masukan pertimbangan untuk mencapai tujuan akhir yang diinginkan dalam bentuk skala prioritas.

Langkah-langkah dalam penelitian yang menggunakan pendekatan AHP ini, dimulai dengan melakukan studi literatur dan identifikasi masalah. Selanjutnya dilakukan pengumpulan data baik data primer maupun data sekunder. Data primer didapatkan melalui kuisioner dan hasil wawancara dari informan-informan yang memiliki kompetensi di bidang keamanan informasi dan teknologi informasi khususnya di bidang kriptografi. Sedangkan data sekunder diperoleh dari dokumen *Certificate Policy* dan *Certificate Practice Statement* (CPCPS) beberapa negara yang telah mengimplementasikan IKP dan *best-practice* implementasi IKP dari referensi. Langkah selanjutnya adalah menyusun struktur hirarki berdasarkan kriteria dan sub-kriteria dari data-data yang dikumpulkan, melakukan analisis pembobotan, dan langkah terakhir adalah menentukan urutan prioritas model kepercayaan sesuai dengan pendekatan AHP.

4. *ANALYTIC HIERARCHY PROCESS*S

Analytic Hierarchy Process (AHP) merupakan metode analisis yang dikembangkan oleh Thomas L. Saaty sebagai solusi untuk menyederhanakan permasalahan yang kompleks menjadi variabel dalam tingkatan hirarki [12].Untuk memperoleh data primer, metode AHP mensyaratkan penilaian tingkat kepentingan menurut responden terhadap pernyataan yang diajukan. Tingkat kepentingan tersebut menggunakan skala perbandingan 1 sampai 9 dengan keterangan sebagai berikut :

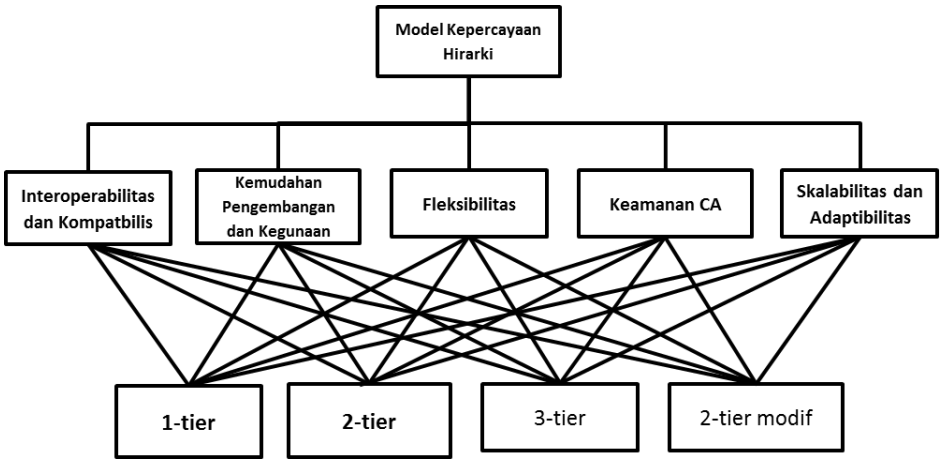
Tabel 3. Skala Penilaian Perbandingan Berpasangan [12]

Tingkat Kepentingan	Definisi	Keterangan
1	Sama pentingnya	Kedua elemen mempunyai pengaruh yang sama
3	Sedikit lebih penting	Pengalaman dan penilaian sangat memihak satu elemen dibandingkan dengan pasangannya
5	Lebih penting	Satu elemen sangat disukai dan secara praktis dominasinya sangat nyata, dibandingkan dengan elemen pasangannya
7	Sangat penting	Satu elemen terbukti sangat disukai dan secara praktis dominasinya sangat nyata, dibandingkan dengan elemen pasangannya
9	Mutlak lebih penting	Satu elemen mutlak lebih disukai dibandingkan dengan pasangannya, pada tingkat keyakinan tertinggi
2, 4, 6, 8	Nilai-nilai tengah diantara dua pendapat yang berdampingan	Nilai-nilai ini diperlukan suatu kompromi

Langkah-langkah yang dilakukan dengan metode AHP diawali dengan mendefinisikan masalah dan solusi seperti yang telah dijelaskan di latar belakang. Langkah selanjutnya adalah menentukan struktur hirarki yang dibentuk dari dasar pertimbangan implementasi IKP sebagai kriteria utama dan desain n-tier sebagai kriteria alternatif. Struktur hirarki yang telah dibuat menjadi dasar penyusunan matriks perbandingan berpasangan sehingga dapat ditentukan nilai *eigen vector* dan *eigen value*. Langkah terakhir dari metode AHP adalah melakukan uji konsistensi indeks dan rasio.

4.1 Penyusunan Struktur Hirarki

Permasalahan yang dihadapi adalah desain n-tier manakah dari model kepercayaan hirarki yang tepat untuk mengimplementasikan IKP di Indonesia. Berdasarkan teori dan contoh implementasi yang telah dilakukan oleh beberapa negara seperti Qatar, India dan Filipina maka dapat diambil 4 (empat) alternatif solusi yaitu 1-tier, 2tier, 3-tier dan 2-tier modifikasi. Secara berturut-turut diberi kode kriteria 1T, 2T, 3T dan 2TM. Penentuan prioritas keempat alternatif tersebut dipengaruhi oleh 5 (lima) kriteria dasar dalam mengimplementasikan IKP menurut Choudbhury et al. Secara berturut-turut diberi kode kriteria IK, KPK, F, KCA dan SA. Dengan demikian, struktur hirarki AHP model kepercayaan IKP dapat disusun seperti gambar 2 di bawah ini.



Gambar 2. Struktur Hirarki AHP Model Kepercayaan IKP

4.1 Penyusunan Matriks Perbandingan

Matriks perbandingan berpasangan disusun berdasarkan perhitungan data hasil kuisioner dari para informan. Ada 2 (dua) matriks perbandingan yang disusun yaitu matriks kriteria dari dasar-dasar pertimbangan dan matriks sub-kriteria dari alternatif desain n-tier CA. Model skala perbandingan berpasangan yang digunakan dapat dilihat seperti tabel 3 di bawah ini. Kriteria berpasangan (Kriteria 1 dengan Kriteria 2) untuk dasar perbandingan memiliki 10 pilihan. Sedangkan Sub-kriteria berpasangan untuk alternatif desain n-tier CA memiliki 30 pilihan.

Tabel 4. Model Skala Perbandingan Berpasangan

Kriteria 1	Bobot Nilai Faktor																Kriteria 2
	Lebih Penting Daripada								Sama	Kurang Penting Daripada							
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9

Berdasarkan skala perbandingan berpasangan tersebut di atas, maka dapat dibuat matriks perbandingan berpasangan dengan cara seperti tabel 5. Bobot perbandingan berpasangan dapat dihitung dengan formula:

$$C(ij) = \frac{Ci}{Cj}, \text{ dimana } i \text{ (baris)}, j \text{ (kolom)} = 1,2,3,...n \quad (1)$$

Tabel 5. Matriks Perbandingan Berpasangan Bobot Kriteria

	C1	**C2**	**....**	**Cn**
C1	C11	C12	....	C1n
C2	C21	C22	....	C2n
....	....	....	....	....
Cn	C1	C1	....	Cnn

4.2 Penentuan Eigen Vektor dan Nilai Eigen

Penentuan eigen vektor dan nilai eigen dapat dihitung dengan menyusun matriks perbandingan berpasangan intensitas kepentingan seperti pada tabel 6.

Tabel 6. Matriks Perbandingan Berpasangan Intensitas Kepentingan

	W1	**W2**	**....**	**Wn**
W1	W11	W12	....	W1n
W2	W21	W22	....	W2n
....	....	....	....	....
Wn	W1	W1	....	Wnn

Nilai Wi dan Wj pada matriks dihasilkan dengan formula 2.

$W(i) = \sqrt[n]{(Ci1 \times Ci2 \times ... \times Cin)}$, *i = 1,2,3,...n* (2)

Secara berturut-turut, Eigen Vektor (Xi) dapat dihitung dengan formula 3 dan nilai eigen terbesar (λ_{maks}) dihitung dengan formula 4.

$$X(i) = \frac{Wi}{\sum Wj} \quad (3) \qquad \lambda_{maks} = \sum Cij \times Xj \quad (4)$$

4.3 Uji Konsistensi dan Rasio Konsistensi

Uji konsistensi dilakukan untuk mengetahui apakah ada penyimpangan terhadap konsistensi data. Adapun cara pengujiannya dimulai dengan mengitung indeks konsistensi (CI) dengan formula sebagai berikut :

$\lambda_{maks} = \pi$ (5)

$CI = n - 1$

Tabel 7. Tabel Indeks Keacakan

Ordo Matriks	1	2	3	4	5	6	7	8	9	10
RI	**0**	**0**	**0,58**	**0,9**	**1,12**	**1,24**	**1,32**	**1,41**	**1,45**	**1,49**

Dengan diketahui Indeks Keacakan (RI) yang telah ditentukan seperti pada tabel 7, maka Rasio Konsistensi (CR) dapat dihitung dengan formula sebagai berikut:

$$CR = \frac{CI}{RI} \leq 0,1 \quad (6)$$

Nilai CR dapat diterima apabila nilai yang dihasilkan kurang dari 0,1 atau sama dengan 0,1.

5. ANALISIS DATA

Berdasarkan pengolahan data dengan pendekatan AHP dari penyusunan matriks perbandingan berpasangan hingga penentuan nilai eigen, dilakukan analisis data dengan hasil seperti dijelaskan di bawah ini.

5.1 Kriteria Dasar

Berdasarkan hasil perhitungan yang telah dilakukan dengan mengikuti langkah-langkah metode AHP, matriks perbandingan berpasangan dan nilai eigen vector untuk kriteria dasar implementasi IKP ditunjukkan pada tabel 8. Tabel tersebut menunjukkan bahwa prioritas paling tertinggi dalam menentukan mode kepercayaan IKP adalah pertimbangan pada aspek Keamanan CA dengan nilai 0,363. Prioritas selanjutnya secara berturut-turut adalah pertimbangan pada aspek Fleksibilitas (0,225), Skalabilitas dan Adaptibilitas (0,168), Interopebailitas dan Kompatibilitas (0,156), dan prioritas paling rendah adalah Kemudahan Pengembangan dan Kegunaan(0,088).

Tabel 8. Matriks Perbandingan Berpasangan Kriteria Dasar

Kriteria Dasar	**IK**	**KPK**	**F**	**KCA**	**SA**	**Eigen Vector**
IK	**1.000**	2.117	0.356	0.377	1.708	0.156
KPK	0.472	**1.000**	0.494	0.286	0.423	0.088
F	2.806	2.024	**1.000**	0.363	1.500	0.225

KCA	2.654	3.500	2.757	**1.000**	1.299	0.363
SA	0.585	2.367	0.667	0.770	**1.000**	0.168
Total	7.517	11.007	5.274	2.795	5.930	**1.000**

Data urutan prioritas pertimbangan dalam menentukan model kepercayaan IKP di atas sesuai dengan kondisi dan perkembangan implementasi IKP di Indonesia saat ini, karena masih belum banyak CA yang beroperasi di Indonesia. Tercatat ada 2 (dua) CA yang sudah beroperasi di lingkungan instansi pemerintah yaitu Otoritas Sertifikat Digital (OSD) milik Lemsaneg dan iOtentik milik BPPT. Kriteria aspek keamanan CA menjadi prioritas tertinggi untuk memberikan jaminan bahwa operasional CA tahan terhadap berbagai serangan sehingga layanan sertifikasi elektronik tetap berjalan dengan baik. Beberapa kegiatan yang dapat dilakukan untuk menjaga keamanan CA antara lain dengan membatasi akses ke CA, menjaga keamanan kunci privat CA 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. Selama keamanan CA tetap terjaga maka aspek pertimbangan lainnya dapat diakomodir dengan baik guna mendukung keberhasilan implementasi IKP di Indonesia.

Kriteria yang memiliki nilai cukup besar adalah Fleksibilitas menjadi perhatian di sini karena seiring dengan kebutuhan akan keamanan informasi pada layanan *e-government* maka dibutuhkan ruang yang lebih luas untuk meningkatkan infrastruktur ke arah yang lebih kompleks. Sedangkan untuk prioritas terendah yaitu aspek kemudahan pengembangan dan kegunaan dapat dipahami bahwa saat ini teknologi IKP masih sedikit diterapkan untuk mendukung layanan *e-government* sehingga belum menjadi perhatian khusus.

5.2 Model Kepercayaan

Pembahasan selanjutnya adalah hasil akhir perhitungan metode AHP untuk menentukan prioritas kriteria alternatif desain n-tier CA yang ditunjukkan pada tabel 5. Tabel tersebut menunjukkan bahwa prioritas tertinggi yang dapat diambil untuk menentukan model keperacayaan hirarki IKP di Indonesia adalah model hirarki 3-tier dengan nilai bobot 0,320. Dan secara berturut-turut, prioritas yang dapat dipilih adalah 2-tier (0,257), 2-tier modifikasi (0,216) dan yang paling rendah adalah 1-tier (0,207).

Tabel 9. Hasil Akhir

Kriteria Alternatif	**IK**	**KPK**	**F**	**KCA**	**SA**	**Bobot Prioritas**
	0.156	0.088	0.225	0.363	0.168	
1T	0.393	0.060	0.074	0.286	0.113	**0.207**
2T	0.232	0.222	0.257	0.274	0.264	**0.257**
3T	0.244	0.462	0.347	0.278	0.375	**0.320**
2TM	0.130	0.255	0.322	0.162	0.248	**0.216**

Nilai bobot prioritas dari hasil akhir menunjukkan dengan jelas bahwa model kepercayaan hirarki yang sebaiknya dipilih adalah 3-tier dimana ada 3 tingkatan CA yaitu sebagai *Root CA*, Intermediate CA dan sub-CA penerbit sertifikat pengguna. Seperti pada data pada tabel 4 untuk kriteria dasar, hal ini juga sesuai dengan kondisi dan perkembangan IKP di Indonesia saat ini dilihat dari banyaknya organisasi pemerintahan maupun non-pemerintahan serta wilayah demografik. Model 3-tier CA memungkinkan pemerintah dalam mengoptimalkan implementasi IKP yang semakin kompleks seiring dengan banyaknya layanan *e-government* di berbagai bidang dan wilayahnya melalui intermediate CA. Namun untuk mewujudkan hal tersebut membutuhkan persiapan dan kesiapan infrastruktur yang lebih matang.
Prioritas selanjutnya adalah 2-tier CA yang lebih sederhana dibandingkan 3-tier. Model hirarki 2-tier CA dapat dipilih dengan beberapa pertimbangan antara lain memanfaatkan infrastruktur IKP dan CA yang telah siap untuk mendukung layanan *e-government* dan sebagai pemicu munculnya CA baru sehingga implementasi IKP menjadi lebih maksmimal. Dan prioritas terakhir adalah model 1-tier CA. Hal ini membuktikan teori bahwa implementasi IKP untuk skala besar tidak cocok menggunakan model 1-tier CA karena tidak mampu mengakomodir kebutuhan pengguna yang semakin banyak.

6. SIMPULAN DAN SARAN

Metode AHP dapat digunakan untuk membantu pengambil keputusan dalam menentukan model kepercayaan IKP di Indonesia. Makalah ini memberikan masukan kepada pengambil keputusan mengenai prioritas model hirarki yang dapat dipilih sehingga sesuai dengan kondisi dan perkembangan impelementasi IKP saat ini.

6.1 Simpulan

Prioritas tertinggi dalam menentukan model kepercayaan IKP adalah pertimbangan terhadap aspek keamanan CA karena hal ini memberikan jaminan bahwa operasional CA tahan terhadap berbagai serangan sehingga layanan sertifikasi elektronik tetap berjalan dengan baik. Ketahanan terhadap serangan seperti hacker atau pembobolan sistem menjadi jaminan keberhasilan penerapan keamanan informasi untuk mendukung layanan *egovernment*. Kriteria dasar fleksibilitas juga menjadi bahan pertimbangan yang sangat penting karena ke depan kebutuhan pengguna akan semakin kompleks sehingga dibutuhkan ruang yang cukup luas dalam menyesuaikan kebutuhan tersebut. Berdasarkan pertimbangan kriteria dasar implementasi IKP yang didapatkan, maka prioritas model kepercayaan hirarki yang tepat untuk diterapkan di Indonesia saat ini adalah model 3-tier CA. Model 3tier CA memungkinkan untuk mengakomodir permasalahan implementasi IKP dari sisi struktur organisasi dan wilayah demografi yang luas. Pemilihan model 3-tier CA ini juga dihadapkan proyeksi ke depan dimana implementasi IKP akan semakin kompleks seiring dengan banyaknya layanan *e-government* di berbagai bidang dan wilayahnya. Alternatif lain yang dapat dipilih adalah model 2-tier CA dengan pertimbangan pemanfaatan infrastruktur yang telah siap.

6.2 Saran

Makalah ini memberikan gambaran tentang model kepercayaan IKP yang tepat untuk kondisi implementasi IKP saat ini. Seiring dengan perkembangan teknologi dan kebutuhan pengguna, impelementasi IKP di Indonesia akan semakin kompleks. Oleh karena itu, perlu dilakukan penelitian lebih lanjut untuk menentukan apakah model kepercayaan IKP saat ini masih tepat atau perlu dilakukan perubahan sesuai kondisi nanti.

7. DAFTAR RUJUKAN

[1] J. T. Jaafar, N. Hamza dan B. E. M. Hassan, "Security Model in E-government With Biometric Based on PKI," *International Journal of Computer Application,* vol. 93, 2014.

[2] R. Indonesia, *Peraturan Pemerintah RI Nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik,* Republik Indonesia, 2012.

[3] P. D'Angio, P. Vassilliadas dan P. Kaklamanis, "PKI - Crawling Out of the Grave & Into the Arms of Government," dalam *ISSE 2009 Securing Electronic Business Process*, Vieweg+Teubner, 2009, pp. 108115.

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

[5] M. Whitman dan H. Mattord, Principles of Information Security, Boston: Course Technology, 2012, p. 376.

[6] S. Burnett dan S. Paine, RSA Security's Official Guide to Cryptography, California: McGraw-Hill, 2004. [7] K. Schmeh, Cryptography and Public Key Infrastructure on the Internet, Sussex: Wiley & Sons Ltd, 2003.

[8] B. Komar, Windows Server 2008 : PKI and Certificate Security, Washington: Microsoft Press, 2008. [9] MoI Policy Authority, *Public Key Infrastructure Certificate Policy*, Doha: Qatar Ministry of Interior, 2014.

[10] Integrated Government Phliphines Project, *Philippine National Public Key Infrastructure Certification Practice Statement,* Quezon City: Department of Science and Technology, 2013.

[11] Controller of Certiying Authorities, *X.509 Certificate Policy for India PKI,* Ministry of Communication and Information Technology, 2015.

[12] T. L. Saaty, "Decision Making With the Analytic Hierarchy Process," *Int. J. Services Sciences,* vol. 1, p. 83, 2008.