Pembangunan ***Public Key Infrastructure*** di Indonesia

I Nyoman Winardi, Dian Drikusuma, Sandy Eggi

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if11040@students.if.itb.ac.id, if11046@students.if.itb.ac.id, if11082@students.if.itb.ac.id

Abstrak

Perkembangan transaksi dan komunikasi berbasis digital semakin meluas. Hal ini mendorong kebutuhan penggunaan sistem kriptografi kunci publik untuk mengatasi serangan *eavesdropping* dan modifikasi. Kunci publik perlu dijaga integritasnya selama penyimpanan dan pendistribusian. Mekanisme ini dilakukan dengan cara memberikan sertifikasi pada kunci publik sehingga pengguna kunci publik akan dapat meyakini kunci publik yang digunakan benar. Sertifikasi diperoleh *Certification Authorities* (CAs). CA, pengguna aplikasi kunci publik, dan manajemen kunci publik membentuk suatu infrastruktur yang disebut *Public Key Infrastructure* (PKI).

Memasuki era globalisasi dan semakin berkembangnya *e-commerce*, Indonesia perlu mengimplementasikan PKI. Masih banyaknya kelemahan baik dari infrastruktur, budaya, keamanan, dan hukum di Indonesia, memang diperlukan persiapan yang lebih banyak sebelum menuju ke pembangunan PKI di Indonesia. Apalagi Indonesia selama ini hanya bergantung pada CA yang ada di luar negeri. Dengan mempertimbangkan berbagai faktor, diusulkan model/struktur PKI yang cocok untuk diimplementasikan di Indonesia.

***Kata kunci**: public key infrastructure (PKI), Certification Authorities (CA), model*

1. Pendahuluan

Penggunaan *electronic messaging* dan transaksi *e-commerce* semakin meluas seiring dengan kemajuan telekomunikasi dan teknologi informasi. Hal ini mendorong peningkatan interkoneksi *user* dan penggunaan komunikasi secara digital, yang berarti semakin banyak informasi yang dikirim secara elektronik, sehingga menjadi rentan terhadap serangan *eavesdropping* dan modifikasi. Sistem kriptografi kunci publik dan *digital signature* memegang peranan penting dalam mengatasi serangan dengan menyediakan *end-to-end security* yang dapat menjaga *confidentiality*, *integrity*, *non-repudiation*, *authentication*, *access control*, dan *availability*.

Pada sistem kriptografi kunci publik konvensional, kunci publik disimpan dan dapat diakses oleh pihak umum. *Enemy/bad guy* dapat berpura-pura menyediakan kunci publik yang asli untuk digunakan pihak lain yang memerlukan. Dengan berpura-pura sebagai penyedia kunci publik maka *bad guy* dapat mengakses informasi penting yang akan digunakan selama transaksi yang menggunakan pengamanan sistem kunci publik.

Masalah tersebut memerlukan solusi untuk melindungi *confidentiality* kunci privat dan menjaga integritas kunci publik selama penyimpanan dan pendistribusian. Mekanisme ini dilakukan dengan cara memberikan sertifikasi pada kunci publik sehingga pengguna kunci publik akan dapat meyakini kunci publik yang digunakan adalah kunci yang benar. Sertifikasi diperoleh dari pihak yang bernama *Certification Authorities* (CAs). CA, pengguna aplikasi, dan manajemen kunci publik membentuk suatu infrastruktur yang disebut *Public Key Infrastructure* (PKI).

Definisi PKI :

The policies and procedures for establishing a secure method for exchanging information within an organization, an industry, a nation or worldwide. It includes the use of certification authorities (CAs) and digital signatures as well as all the hardware and software used to manage the process. [4]

Di Indonesia perkembangan *e-commerce* memang belum maju. Menurut suatu survei oleh AC Nielsen, masyarakat Indonesia menggunakan internet untuk email(42%), membaca berita(39%), mencari informasi produk atau layanan(29%), membaca majalah(27%), chatting(23%), dan kurang dari 10% dari pengguna internet yang memiliki keinginan untuk bertransaksi lewat internet. Sehingga dapat dikatakan *e-commerce awareness* masih rendah di kalangan pengguna internet Indonesia. Hal ini juga dipengaruhi tingginya tingkat *cyber crime* di Indonesia. Indonesia menempati urutan pertama dalam jumlah transaksi dan peringkat tiga dalam volume transaksi untuk kasus penipuan/penggelapan.

Top Countries by of Fraudulent	Total Volume Transaction	Top Countries by of Fraudulent	Percentage Transactions
Country	Ranking	Country	Ranking
USA	1	**Indonesia**	1
Canada	2	Nigeria	2
Indonesia	3	Pakistan	3
Israel	4	Ghana	4
United Kingdom	5	Israel	5
India	6	Egypt	6
Turkey	7	Turkey	7
Nigeria	8	Lebanon	8
Germany	9	Bulgaria	9
Malaysia	10	India	10

Tabel 1Daftar prosentase Cyber Crime

Sumber : *January 2004 edition of US VeriSign's "Internet Security Intelligence Briefing" report*

Kepastian hukum (*cyber law*) terhadap kasus penipuan di dunia *cyber* di Indonesia memang belum ada. Sampai saat ini hanya ada beberapa istilah dari "*cyber law*" yang digunakan, misalnya, Hukum Sistem Informasi, Hukum Informasi, dan Hukum Telematika (Telekomunikasi dan Informatika). Di dalam hukum tersebut seharusnya memuat atau membicarakan mengenai aspek-aspek hukum yang berkaitan dengan aktivitas manusia di Internet. Dengan adanya hukum ini maka pihak luar juga akan merasa nyaman bertransaksi dengan Indonesia.

Melihat banyaknya kelemahan baik dari infrastruktur, budaya, keamanan, dan hukum di Indonesia, memang diperlukan persiapan yang lebih banyak sebelum menuju ke pembangunan PKI di Indonesia. Apalagi Indonesia selama ini hanya bergantung pada CA yang ada di luar negeri. Memasuki era globalisasi dengan semakin berkembangnya aktifitas yang memerlukan pengamanan

kunci publik, Indonesia harus tetap bersiap mengimplementasikan PKI.

2. Pihak-pihak PKI

Sesuai dengan definisi dari [4] maka pihak-pihak yang terlibat dalam PKI adalah :
1. Organisasi
2. Industri
3. Negara
4. Dunia

3. Komponen PKI

Komponen utama dalam PKI adalah [*2*] dan [*5*] :

1. *Certification Authorities* (CAs)

   Suatu badan yang berwenang untuk memberikan validasi atau sertifikat digital pada kunci publik dalam suatu negara.

2. *Repository kunci*, sertifikat dan *Certificate Revocation Lists* (CRLs)

   Basis data untuk menyimpan semua data tentang kunci publik dan sertifikat kunci publik tersebut. Disamping itu terdapat *list expiry time* untuk managemen kunci bagi para pemilik kunci. CRL merupakan daftar kunci yang harus ditarik dan diganti dengan kunci yang baru.

   CA secara periodik mengeluarkan *CRL* (*Certificate Revocation List*) yang berisi nomor seri sertifikat digital yang ditarik. Sertifikat digital yang sudah kadaluarsa otomatis dianggap sudah tidak sah lagi dan dimasukkan ke dalam *CRL*. Dengan cara ini, maka *CA* tidak perlu memberitahu perubahan sertifikat digital kepada setiap orang.

3. *Management Function*

   Suatu prosedur yang digunakan untuk menjadi *guideline* dari keseluruhan proses yang ada dalam PKI.

4. *Policy Approving Authority* (PAA)

   Memberikan *guideline* untuk keseluruhan PKI dan melakukan sertifikasi kunci publik dari PCA

5. *Policy Certification Authority* (PCA)

   Memberikan *policy* untuk semua CA dan *user* yang ada pada domainnya dan melakukan sertifikasi kunci publik dari CA

6. *Organizational Registration Authority* (ORA)

   Entitas yang berperan sebagai perantara antara CA dan *user*.

4. Fungsi yang dilakukan PKI

PKI melindungi keamanan informasi yang dikirimkan selama transmisi atau transaksi dilakukan dalam berbagai cara sebagai berikut [*6*]:

1. Mengautentikasi identitas. Dengan sertifikasi digital yang dikeluarkan oleh PKI maka tiap pihak dapat mengautentikasi pihak lawan dalam melakukan transaksi sehingga pihak dapat meyakini bahwa pihak yang melakukan transaksi adalah pihak yang berhak.

2. Verifikasi integritas dokumen. Dengan adanya sertifikasi digital maka dokumen dapat diyakini tidak mengalami perubahan selama pengiriman.

3. Jaminan privasi. Dengan protokol yang digunakan selama transmisi menggunakan sertifikat digital maka jalur yang digunakan dalam transmisi dipastikan aman dan tidak dapat diakses oleh pihak lain yang tidak berhak.

4. Sertifikat digital dari PKI dapat menggantikan peranan proses autentikasi *user* dalam sebuah sistem.

5. Dengan menggunakan sertifikat digital dari PKI maka suatu pihak dapat menentukan transaksi yang aman dengan menggunakan validasi kunci publik.

6. Dukungan anti penyangkalan. Dengan adanya validasi pada sertifikat digital maka tidak mungkin untuk melakukan penyangkalan pada suatu transaksi yang telah dilakukan.

5. Aktivitas PKI

Fungsi PKI pada bahasan sebelumnya diimplementasikan dalam aktifitas berikut [2]:

1. Pembangkitan, pemberian sertifikat, dan pendistribusian kunci
2. Pemberian tanda tangan dan verifikasi tanda tangan
3. Perolehan sertifikat
4. Verifikasi sertifikat
5. Penyimpanan sertifikat untuk penggunaan lebih lanjut
6. Perolehan sertifikat yang sudah disimpan
7. Laporan kehilangan kunci
8. Pembangkitan ulang kunci yang hilang
9. Perolehan CRL
10. Pemberian ulang kunci dan pemberian sertifikat ulang
11. Pelaksanaan audit terhadap kejadian, seperti permintaan pasangan kunci dan sertifikat.
12. Pengarsipan kunci.

6. Faktor–faktor dalam Implementasi PKI

Berikut merupakan faktor-faktor yang harus dipertimbangkan dalam membangun suatu PKI [2] :

1. Robustness

Dalam membangun suatu struktur PKI harus dipertimbangkan kecepatan dalam pengiriman dan tidak mengganggu proses transmisi dari transaksi sendiri. Faktor ini dipengaruhi oleh kondisi negara, keadaan wilayah beserta dengan tipe transaksi yang dominan yang ada pada suatu negara. Pembangunan PKI yang tepat harus mempertimbangkan faktor tersebut.

2. Scalability

Dengan struktur yang ada maka PKI harus dapat mendukung semua aktifitas yang ada pada daerah yang dijangkaunya. Sehingga dalam membangun struktur maka harus dipertimbangkan jangkauan antar komponen PKI agar dapat beroperasi sesuai wilayah jangkauan.

3. Flexibility

Struktur implementasi PKI harus dapat menyesuaikan dengan kondisi negara atau daerah yang jangkauannya. Apabila kondisi negara dan transaksi

yang berubah-ubah maka struktur harus dapat menyesuaikan sendiri dan tidak mengalami perubahan yang besar.

4. *Easy of use*

Struktur yang ada dalam PKI harus memiliki abstraksi aksi yang jelas terhadap *user*. *User* dalam memanfaatkan suatu implementasi PKI secara teknis cukup dengan menekan tombol dalam *browser* merupakan salah satu contoh kemudahan dalam pengimplementasian PKI pada level *end user*.

5. *Trust*

Sesuai dengan fungsinya maka PKI yang dibangun harus memiliki sistem yang handal sehingga dipercaya oleh seluruh *user* yang memanfaatkannya.

6. *Interoperation*

Pemilihan struktur dan pihak yang menjadi komponen dalam PKI harus mempertimbangkan kemampuan masing-masing komponen untuk bekerja sama secara kooperatif dan menjalankan fungsinya. Struktur yang dibangun harus tetap dapat bekerja dengan struktur pada area yang lain dan area yang lebih besar.

7. *Implementation Timeframe*

Waktu pembentukan dari struktur berpengaruh pada kerja PKI sendiri. *Timeframe* ini meliputi waktu perolehan *user*, penentuan CA dan PCA yang baru.

8. *Management Structure*

Pengimplementasian dari PKI harus mempertimbangkan struktur. Penentuan pihak dan lembaga untuk menempati posisi suatu komponen dalam PKI merupakan hal utama dalam faktor ini.

9. *Exposure to Liability*

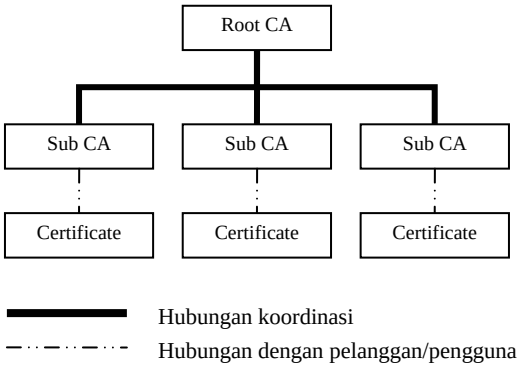
Pemilihan struktur tergantung oleh kewajiban finansial dari *user* dan CA masing-masing. Ukuran dari kewajiban finansial dari *user* dan CA yang besar pada suatu struktur akan mempengaruhi *trust* dari *user*.

7. Struktur/Model PKI

Berikut merupakan model yang telah diimplementasikan di beberapa negara. Diagram digambarkan hanya berupa entitas CA , root CA dan user pengguna sertifikat dan keterhubungan antar entitas untuk mempermudah pemahaman [2].

7.1 Hierarchical model

Hierarchical model dapat digambarkan pada diagram berikut ini :



Gambar 1. *Hierarchical model*

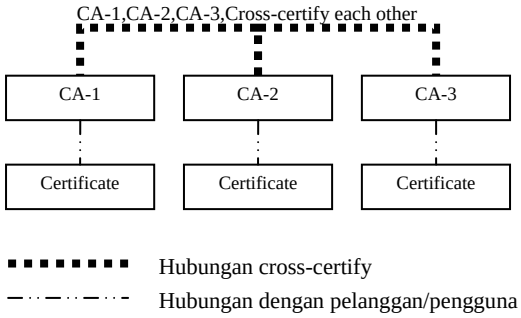
Dalam *hierarchical model*, CA pusat yang ada pada PKI dibagi menjadi Sub-sub CA yang lebih kecil. Pembagian CA menjadi sub-CA didasarkan pada bisnis

yang ditangani. Sehingga tiap sub-CA akan menangani pelanggan/pengguna yang berbeda bisnisnya.

Karena pembagian CA menjadi sub-CA yang spesifik pada bisnis tertentu maka model ini cocok digunakan untuk negara yang memiliki cukup banyak bisnis tipe dan dan masing-masing bisnis telah berkembang.

7.2 Cross certification model (*Peer-to-peer model*)

Cross certification model dapat digambarkan pada diagram berikut ini :



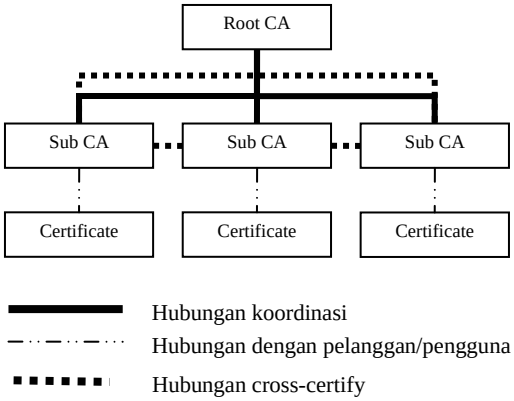
Gambar 2. *Cross certification model*

Dalam *cross certification model* peran *root* CA dilakukan oleh masing-masing CA. Sehingga *root* CA dapat dihilangkan. Proses di *root* CA digantikan dengan saling memvalidasi sertifikat dari CA yang lain (*shared trust*). Struktur ini cocok digunakan untuk negara yang mempunyai tipe bisnis yang banyak dan berkembang dan masing-masing tipe bisnis sangat berbeda dengan *load* yang tinggi.

Untuk membangun suatu komunitas *trust* maka diperlukan suatu audit yang memvalidasi dan meyakinkan pengimplementasian tetap berada pada kesepakatan antar CA.

7.3 Hybrid model

Hybrid model dapat digambarkan pada diagram berikut ini :



Gambar 3. *Hybrid model*

Hybrid model merupakan penggabungan antara dua model sebelumnya. Masing-masing sertifikat sub-CA dapat divalidasi oleh *root* atau divalidasi oleh sub-CA yang lain sesuai dengan domain transaksi.

Model ini cocok diterapkan pada negara dengan tipe bisnis yang banyak dan masing-masing bisnis saling terkait dengan bisnis yang lain. Pada bisnis yang bersifat umum maka sertifikat dapat divalidasi oleh *root* tetapi pada bisnis yang spesifik dan terganting dengan bisnis yang lain maka sertifikat dapat divalidasi oleh sub-CA dengan tipe bisnis yang bersangkutan.

Dengan mempertimbangkan struktur/model yang ada, maka diusulkan model PKI yang diimplementasikan di Indonesia adalah *hierarchical model*.

Pemilihan ini didasarkan pertimbangan tipe bisnis di Indonesia yang menggunakan *publik key* belum banyak dan diharapkan bisa semakin berkembang dengan adanya banyaknya sektor bidang industri. Untuk *cross certification model* tidak mungkin diimplementasikan karena *load* untuk CA belum tinggi.

Lembaga yang perlu dibangun sebagai komponen root PKI untuk Indonesia adalah sebuah lembaga baru yang diberi nama Indonesian National CA. Secara nasional Indonesian National CA akan menjadi root dari sub-sub CA di bawahnya. Lembaga ini menjadi suatu sub-CA di bawah CA internasional. Organisasi-organisasi yang dapat menjadi CA di bawah Indonesian Nasional CA antara lain Indosat/Indosatcom, Pos/Wasantara, Telkom, Deprindag (MITI), dan lembaga pendidikan seperti ITB, UI.

7. Kesimpulan

Dari keseluruhan bahasan maka dapat disimpulkan sebagai berikut :

1. Indonesia masih memiliki *cyber awareness* yang rendah dan bisnis yang berkembang pada sektor digital masih sedikit.

2. Model/struktur PKI yang dapat dikembangkan terdiri dari *hierarchical model, cross-certified model* dan *hybrid model*.

3. Sesuai dengan kondisi Indonesia maka model yang paling cocok untuk diimplementasikan di Indonesian adalah *hierarchical model*. Struktur PKI yang dibangun akan memiliki satu *root* CA nasional (Indonesia National CA) yang membawahi CA-CA yang dapat dilakukan oleh lembaga-lembaga seperti Indosat/Indosatcom, Pos/Wasantara, Telkom, Deprindag (MITI), dan lembaga pendidikan seperti ITB, UI. Kedudukan PKI Indonesia berada di bawah root CA yang bersifat internasional.

[1] AICPA/CICA. WebTrust SM/TM.*Principles and Criteria for Certification Authorities*,Version 1.0.9 Februari 2000. American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. Exposure Draft. http://www.aicpa.org diakses tanggal 6 Januari 2005.

[2] S.Berkhovits,et all.1994. *Public Key Infrastructure Study*,*Final Report*. Gaithersburg : National Institute of Standards and Technology.

[3] FreeS/WAN. *Glossary for the Linux FreeS/WAN project*. Linux FreeS/WAN project, http://www.freeswan.org/freeswan_trees/freeswan-1.5/doc/glossary.html#PKI, diakses tanggal 6 Januari 2005.

[4] ITRMC. *IT Acronyms and Glossary of Terms*, Information Technology Resource Management Council, http://www2.state.id.us/itrmc/pubs&resources/acronyms.htm, diakses tanggal 6 Januari 2005.

[5] RSA Data Security, Inc. *Understanding Public Key Infrastructure (PKI). An RSA Data Security White Paper*, http://www.rsa.com, diakses tanggal 6 Januari 2005.

[6] VeriSign. *Understanding PKI*, http://verisign.netscape.com/security/pki/understanding.html, VeriSign-Netscape, diakses tanggal 6 Januari 2005.