Studi Mengenai Public Key Infrastructure dan Impementasinya pada Federal Public Key Infrastructure

Ronny – NIM : 13506092

Program Studi Teknik Informatika, Institut Teknologi Bandung

Jl. Ganesha 10, Bandung

E-mail : if16092@students.if.itb.ac.id

Abstrak

Adanya kunci public yang digunakan oleh institusi, bank, dan lain-lain merupakan faktor pendukung untuk menunjang bisnis proses mereka. Namun kunci public juga bisa menjadi bumerang bagi unit atau organisasi tersebut karena bisa banyak pihak yang menyalahgunakan kunci publik yang bukan miliknya tersebut untuk keperluan pribadi. Infrastruktur Kunci Publik(IKP) diperlukan untuk mengatasi masalah tersebut. IKP ini memiliki peran yang sangat penting dalam menyediakan pelayanan keamanan tersebut, seperti integritas, autentikasi, dan tanda tangan digital.

Dengan aspek teknologi informasi saat ini, mengenalkan dan mengaplikasikan IKP pada organisasi tersebut memerlukan perencanaan yang sangat baik dan melalui pemahaman pada relasinya dengan sistem "otomata" lain. Pada tulisan ini, akan dibahas mengenai basis teknologi dari IKP , otoritas sertifikasi, serta isu dan masalah terkait pengaplikasian InfraStruktur Kunci Publik Federal pada departemen/agen di pemerintah. Hal ini juga termasuk keuntungan dan kerugian dari implementasi dan pengoperasian implementasi tersebut pada *federal government* tersebut.

Diharapkan tulisan ini akan mampu membantu organisasi pemerintah di Indonesia bagaimana Infrastruktur Kunci Publik dapat dimanfaatkan pada dan dipasang pada agen pemerintah.

Kata kunci : Infrastruktur Kunci Pulbik,federal,agen pemerintah.

1. Pendahuluan

Infrastruktur Kunci Publik (IKP) adalah suatu sistem yang memungkinkan terjadinya integritas dan keaslian data melalui penggunaan digital signature dan mengamankan data penawaran melalui proses enkripsi.

- Kunci Privat (Privat Key)

Kunci privat adalah suatu kunci berupa data/kode yang sifatnya rahasia sehingga hanya boleh diketahui oleh masing-masing individu.

a. Bagi pengirim informasi (sender), dia menggunakan kunci privatnya untuk meng-enkripsi suatu pesan yang akan dia kirimkan, sehingga menjadi sebuah digital signature.
b. Bagi penerima informasi (receiver), dia menggunakan kunci privatnya untuk melakukan dekripsi terhadap digital envelope2 dari sender.

Kedua kunci tersebut mempunyai hubungan secara matematis sehingga suatu pesan yang di-enkripsi dengan suatu kunci hanya dapat di-dekripsi dengan kunci pasangannya.

- Kunci Public(Public key)

Kunci public adalah suatu kunci berupa data/kode yang sifatnya untuk diketahui oleh orang lain (umum).

a. Bagi pengirim informasi (sender), dia membutuhkan kunci publik receiver untuk melakukan enkripsi terhadap data yang akan dikirimkannya menjadi suatu digital envelope.
b. Bagi penerima informasi (receiver), dia membutuhkan kunci publik sender agar dapat melakukan dekripsi terhadap digital signature sender.

IKP bersifat mengikat kunci publik pada entitas entitas, memungkinkan entitas lain untuke memverifikasi ikatan kunci publik itu, dan juga menyediakan pelayanan yang diperlukan untuk melakukan manajemen kunci yang sedang digunakan pada sistem terdistribusi. Pada umumnya, tujuan dari arsitektur keamanan modern adalah melindungi dan menyebarkan informasi yang diperlukan pada lingkunga sistem terdistribusi yang rentan terhadap serangan, di mana user dan resource semuanya berada pada waktu dan tempat yang berbeda. Adanya infrastruktur kunci publik akan menjamin hal-hal sebagai berikut :

- Orang yang membuat pesan/mengirim pesan/sender tersebut adalah originator/asli
- Orang atau proses yang menerima transaksi adalah penerima yang dimaksudkan
- Integritas data dijamin, yang berarti data tersebut masih tetap utuh

Dua pihak yang akan melakukan transaksi bisnis secara aman mungkin dipisahkan oleh jarak yang jauh, atau bahkan mungkin pula keduanya tidak pernah bertemu secara langsung. Untuk itu, mereka dapat menggunakan IKP ini yang memanfaatkan penggunaan kunci publik untuk untuk mengautentikasi identitas pihak lain. Hal ini tidak akan menjadi persoalan khusu jika transaksi terjadi antar banyak pihak. Dalam kasus seperti ini mereka perlu untuk memanfaatkan pihak ketiga yang dapat dipercaya untuk mendistribusikan kunci publik dan melakukan asosiasi antara kunci publik dengan pihak yang bersangkutan.

Contohnya adalah pada e-commerece atau penjualan berbasis online. Pada proses itu, customer dan merchant terpisah pada jarak sangat jauh sehingga bentuk otentikasi diperlukan karena informasi keuangan dan kartu kredit dari customer tersebut perlu untuk dilindungi saat transmisi melalui jaringan internet. Merchant juga harus menjamin bahwa informasi tersebut aman saat ditransmisikan. Keduanya memerlukan metode enkripsi yang menggunakan kunci publik dan disediakan oleh IKP.

Komponen penting pada infrastruktur kunci publik

- *Certification Authority*(CA); merupakan komponen yang digunakan untuk melakukan identifikasi pada pihak yang melakukan pengiriman dan penerimaan. CA ini merupakan bentuk komunikasi formal yang diperlukan.
- *Registration Authority*(RA); komponen yang digunakan oleh CA untuk melakukan registrai dari user.
- *Repository;* merupakan database untuk sertifikat digital untuk sistem dari CA. Repositorydigunakan untuk menyediakan user data yang diperlukan untuk melakukan konfirmasi terhadap status dari pesan yang ditandatangani.
- *Archive;* merupakan database yang digunakan untuk menyimpan informasi yang akan digunakan ke depannya seperti apakah digital signature dari dokumen lama layak untuk dipercaya.
- *Certificate Holders*: Orang, mesin atau software agent yang telah memiliki sertifikat
- *Clients*: Memvalidasi digital signature dan sertifikat dari CA public key terpercaya.
- *Certification Revocation Lists*(CRL); Digunakan untuk mengecek status atau validitas dari suatu sertifikat.
- *Online Certificate Status Protocol*(OCSP); suatu protokol pengecekan status dari suatu sertifikat secara otomatis.

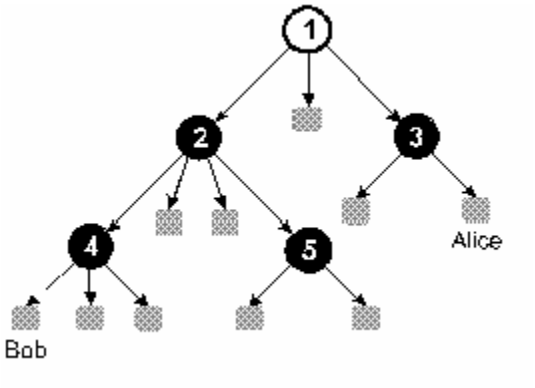
2. Arsitektur IKP

Certificate Holders(CH) akan memegang sertifikat yang berasal dari CA ayng berbeda. IKP biasanya terdiri dari banyak CA yang dihubungkan oleh *trust path*. *trust path* ini menghubungkan satu pihak dengan satu atau lebih pihak ketiga sehingga pihak terebut mendapat kepercayaan pada validitas dari sertifikat yang dikeluarkan. Begitu juga dengan penerima dari pesan yang tidak berhubungan dengan CA yang mengeluarkan sertifikat tersebut dapat melakukan validasi terhadap pengirimnya melalui link pada *trust path* ini.

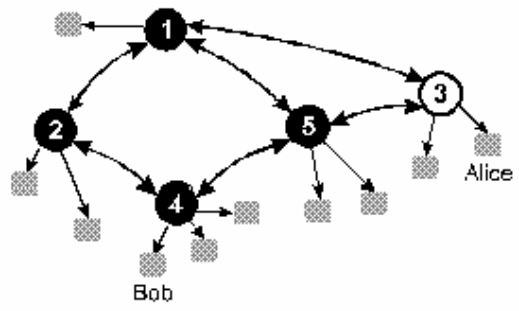
Untuk mengaplikasikannya, IKP perlu dibangun melalui sebuah skema enterprise. Untuk mencapai tujuan ini, pada umumnya terdapat 2 jenis arsitektur, yaitu *hierarchical* dan *mesh*. Belakangan muncul juga jenis arsitektur *bridge CA*, yang digunakan untuk memudahkan para enterprise tersebut

menghubungkan IKP milik mereka dengan milik rekan bisnis mereka.

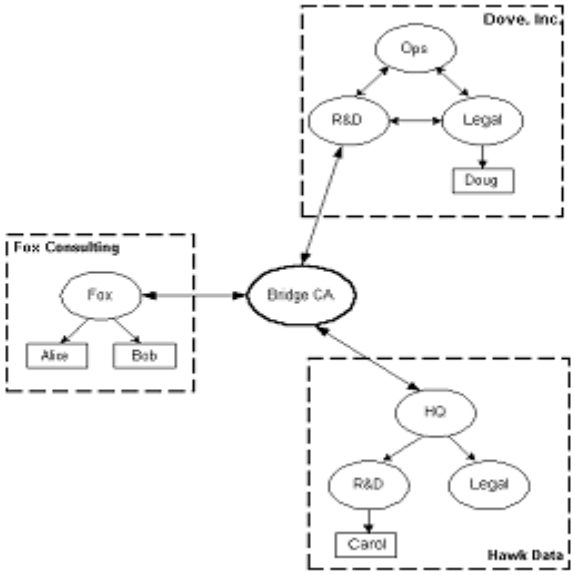
- *Hierarchical*; semua otoritas disusun oleh root CA yang akan mengeluarkan sertifikat untuk subordinatnya. CA yang ini juga akan mengeluarkan sertifikat untuk CA di bawahnya (seperti pohon). Semua sertifikat dapat dilakukan dengan melakukan verifikasi pada root CA. misalnya untuk melakukan verifikasi pada CA3 dilakukan melalui CA2(yang mengeluarkan sertifikat untuk CA3), kemudian ke CA (yang mengeluarkan sertifikat untuk CA2) yang kunci oubliknya diketahui. Berikut ini adalah contoh skema arsitektur *hierarchical* :



- *Mesh*; setiap pasang CA saling mengeluarkan sertifikat masing-masing sehingga keduanya dapat saling mengetahui sertifikatnya. Biasanya setiap pihak dapat kunci publik dari pihak yang ada di sekelilingnya. Arsitektur ini tidak berbentuk pohon, namun leih seperti graf yang lebih acak. Berikut ini adalah contoh skemanya :



- *Bridge CA*; dibangun untuk membangun relasi dengan IKP milik enterprise. Dengan membangun peer to peer relationship dengan IKP enterprise, jembatan kepercayaan dapat dibangun. [ada gambar berikut terlihat bahwa jembatan CA menghubungkan 3 buah IKP enterprise, yaitu CA bob dan Alice, IKP *hierarchical* milik Carol dan IKP *mesh* milik Doug. Alice dan Bob memepercayai bridge CA yang mengeluarkan sertifikat untuk mereka. Carol memepercayai bridge CA sebab root dari IKP hierarchical miliknya memiliki sertifikat untuk bridge CA. Dan Doug juga mempercayai CA sebab ada path dari CA yang memberikan sertifikat padanya ke bridge CA. Berikut ini gambarnya :



3. IKP FEDERAL

Banyak agen pemerintah telah memulai usaha untuk membangun sebuah CA independen untuk mendukung aplikasi seperti pembelanjaan, perjalanan, atau fungsi lain yang digunakan untuk mendukung misi-msi mereka. Untuk melakukannya, teknologi kunci publik dapat digunakan untuk memberi keuntungan langsung pada suatu aplikasi milik pemerintah. Cara lain yang mungkin adalah menggunakan penyedia layanan CA komersial untuk mengeluarkan sertifikat dan memfasilitasi pengiriman; kemudian tentunya mereka pun perlu dibayar.

Salah satu isu penting dalam IKP federal adalah bagaimana cara membuat path sertifikat antara agen pemerintah yang akan menghasilkan penyaluran yang reliable. Untuk itu, sebuah bridge CA digunakan untuk membangun sebuah path sertifikasi yang sistematis antara CA di dalam agen dan luar agen. CA yang memenuhi kriteria standar tertentu

akan diijinkan untuk melakukan pengecekan silang dengan Federal Bridge CA(FBCA). Melalui proses tersebut, agen penerintah dapat saling memperoleh sertifikat masing-masing.

Operasi pada FBCA harus selalu dipantau oleh federal policy management authority (FPMA). FPMA ini juga akan melakukan seleksi untuk melakukan sertifikasi dengan FBCA sehingga tidak sembarang pihak dapat melakukan sertifikasi. Untuk memberikan fleksibilitas maksimum pada agen pemerintah dan tidak mengganggu hak prerogatif mereka, agen tersebut tidak perlu mengadopsi aturan dari FBCA. Mereka bahkan diijinkan untuk membangun kebijakannya sendiri atau memanfaatkan penyedia layanan IKP komersial. Berikut ini adalah komponen-komponen penting pada arsitektur KPI:

- *Federal Policy Management Authority* (FPMA); merupakan bagian yang mengatur seluruh kebijakan dari IKP federal dan prosedur untuk menetukan sertifikasi.
- *Trust Domains*; bagian dari IKP federal yang beroperasi pada otoritas manajemen kebijakan tunggal. Pada setiap *Trust Domain* terdapat satu atau lebih CA.
- *Domain Policy Management Authority* (DPMA); bagian yang menyetujui sertifikasi dari CA yang terdapat di dalam sebuah *Trust Domain*. Bagian ini juga mengawasi dan menjalankan domain repository.
- *Federal Bridge CA* (FBCA); bagian doperaikan oleh FPMA an berfungsi menjadi jembatan antara trust domain baik di dalam IKP federal maupun dengan trust domain non-federal. Konsepnya adalah sebagai berikut : FPMA melakukan approval pada *principal CA* yang ada di *Trust Domain* yang telah di *cross-certify* dengan FCBA.
- *Principal CA*; merupakan CA utama yang ada pada sebuah trust domain yang akan di cross-certify oleh FCBA. Pada domain dengan arsitektur *hierarchical* principal CA ini akan menjadi rootnya.
- *Peer CA*; sebuah CA yang terdapat pada domain yang berbentuk *mesh*. *Peer CA* ini memiliki sertifikat yang ditandatangani sendiri dan didistribusikan pada *certificate holder* dan digunakan oleh mereka untuk menginisiasikan path sertifikasi.
- *Root CA*; merupakan root yang melakukan inisisasi dan berada di level paling atas dalam *trust domain* berbentuk *hierarchical*.
- *Subordinate CA*; merupakan CA yang menerima sertifikasi dari CA di level atas nyadalam *trust domain* berbentuk *hierarchical.*

Certification Revocation List(CRL) pada IKP federal

IKP federal menspesifikasikan 2 buah profil CRL, satu untuk FBCA dan yang lainnya untuk semua CA lain pada IKP federal. Profil yang kedua ini meliputi 2 buah tipe ekstensi yang berbeda.

Tipe pertama adalah CRL entry extension, yang mengandung informasi tambahan mengenai sertifikat yang direvoked. CRL entry extension ini adalah bagian yang mengeluarkan sertifikat. *Defaultnya*, sertifikat yang ada di CRL dibentuk oleh CA yang membangun CRL tersebut. Jika terjadi kesalahan, CRL akan melakukan pengecekan terhadap CA yang mengeluarkan sertifikat tersebut.

Tipe kedua adalah CRL extension yang menyediakan informasi tambahan mengenai semua CRL. Tipe ini berperan sebagai pengidentifikasi kunci atau juga penghasil nama alternatif dan distributing point.

Berikut ini adlaah tabel yang mengidentifikasi ekstensi wajib dan pilihan untuk setiap jenis CRL baik extension maupun entry extension :

CRL Extension	Mandatory or Optional	Contents
CRL number	Appears in all CRLs	Monotonically increasing integer; may be used to detect emergency CRL generation
Authority key identifier	Appears in all CRLs	SHA-1 hash of the public key which verifies the signature on the CRL; used to select the right key
Issuer alternative name	optional	Can be used to specify the CA's email address
Issuing distribution point	Appears in all indirect and segmented CRLs	Contents must match the CRL distribution points extension in the certificates covered by the CRL

CRL entry extension	Mandatory or Optional	Contents
Reason code	Appears for every certificate, unless the CA has no information	Specifies if the certificate was revoked because th were compromised, the subject's affiliation chang was superseded by a newer certificate.
Certificate issuer	Appears in all indirect CRLs	Identifies the issuer for a subset of the certificates this CRL.

Untuk melakukan pemasangan/penggunaan IKP pada suatu agen pemerintah, ada beberapa hal yang harus diperhatikan, antara lain :

- Analisis data dan aplikasi pada departemen/agen tersebut
  IKP perlu dianalisis sesuai dengan kebutuhan dari bagian tersebut dengan memperhatikan prinsip manajemen resiko. Berkutnya adalaha analisis biaya yang mungkin dikeluarkan jika anda akan melakukan implementasinya. Selain itu data dan aplikasi yang digunakan pun perlu diperhatikan. Dampak yang akan terjadi dan juga tingkat resikonya perlu diperhatikan. Kadang diperlukan lebih dari satu policy jika ada banyak macam resiko berkaitan dengan aplikasi yang berbeda.
- Mengambil beberapa contoh kebijakan dan menentukan standard.
  Pengembangan IKP yang efisien memerlukan pengambilan contoh sampel dari kebijakan dan standard lain. Standard ini diperlukan agar keterhubungan antar agen pemerintah dapat berjalan dengan baik.
- Membuat *Draft Certificate Policy*
  Draft ini menggambarkan jenis aplikasi yang akan digunakan dan harus menjamin bahwa policy tersebut tidak akan sering diubah.
- Menentukan product IKP yang akan digunakan dan penyedia layanannya
  Ada beberapa hal yang perlu dipertimbangkan, antara lain : kompabilitas dengan IKP lain, kemudahan mengadopsi standard terbuka, mudah dideploy, fleksibilitas dari administrasi, juga scalability dan portability dari pemasangan (jika data akan diperbesar atau dipindahkan).
- Mengembangkan CPS (*Certification Practice Statement*)
  Merupakan pernyataan yang menggambarkan bagaimana agen tersebut akan mengimplementasikan IKPnya termsuk detail-detailnya. Cps juga berisi prinsip yag digunakan untuk melindungi private key dari CA dan hal-hal lain yang berhubungan dengan sekuriti.
- Melakukan pengecekan.pemeriksaan
  Hal ini dimaksudkan agar aplikasi yang menggunakan IKP tersebut akan berjalan dengan baik dalam segala situasi.
- Melakukan *cross-certify* dengan FBCA
- Ini merupakan langkah terakhir yang perlu dilakukan agar agenda tersebut dapat melakukan sertifikasi dengan pihak lain. Untuk melakukannya, diperlukan penentuan sebuah *principal* CA yang dapat ditentukan bergantung pada arsitekturnya (seperti dijelaskan di atas).

4. KESIMPULAN

- Infrastruktur kunci public (IKP) ini merupakan salah satu penerapan yang penting dari pengaplikasian keamanan data atau transaksi pada umumnya karena menggunakan prinsip Kriptografi Kunci Publik yang mengandung : *confidentiality, integrity, authentication, and digital signatures.*
- IKP biasanya terdiri dari banyak CA yang dihubungkan dengan path of trust dan dibangun dengan arsitektur tertentu seperti sudah dijelaskan
- Tulisan ini masih banyak kekurangannya, namun diharapkan saat bisa dikembangkan nanti, agen pemerintahan akan mampu memanfaatkannya untuk menentukan apakah IKP perlu dikembangkan di kegiatan mereka umumnya. Tulisan ini hanya bersifat sebagai starting point saja.

Daftar Pustaka

Burr, W., D. Dodson, N. Nazario, W.T. Polk. Minimum Interoperability Specification for PKI Components (MISPC) http://csrc.nist.gov/publications/nistpubs/800-15/SP800-15.PDF

Housley, R., and W.T. Polk. Planning for PKI: Best practices for PKI Deployment, Wiley & Sons, 2001