 ISSN: 1411-3201

STUDI KASUS PENGGUNAAN TinyCA SEBAGAI APLIKASI CERTIFICATE AUTHORIZATION (CA) YANG MUDAH DAN SEDERHANA PADA SISTEM OPERASI UBUNTU

Nila Feby Puspitasari
STMIK AMIKOM Yogyakarta
nilafeby@amikom.ac.id

ABSTRAKSI

Penggunaan sertifikat digital merupakan sebuah pembuktian yang sangat penting untuk mengamankan komunikasi. Sertifikat digital adalah surat atau lembaran yang umum digunakan untuk melengkapi sarana pembuktian identitas. Ada sebuah organisasi atau Certificate Authorization (CA) yang sudah dipercaya untuk memberikan sertifikat pada seseorang atau publik yang berhubungan dengan kunci publik ataupun kunci pribadi. Pada umumnya organisasi tersebut berbayar dan berlisensi.

TinyCA merupakan aplikasi sederhana berbasis ubuntu yang digunakan untuk membuat Certificate Autorization (CA) dengan mudah. Aplikasi tersebut menggunakan Secure Socket Layer (SSL) untuk mengenerate CA dan lebih mudah dalam pembuatannya karena menggunakan Graphical User Interface (GUI). TinyCA mengelola otoritas sertifikat berskala kecil dengan layanan otentikasi berstandar X.509 yang digunakan secara luas di internet misalnya dalam S/MIME, IP Security, SSL/TLS dan SET. Standar ini tidak memaksakan penggunaan dari algoritma tertentu tetapi menganjurkan RSA. Algoritma kunci publik yang dibuat oleh (Ron Rivest, Shamir dan Leonard Adleman).

Kata Kunci : *Certificate Authorization, TinyCA, Secure Socket Layer*

PENDAHULUAN

Latar Belakang Masalah

Penerapan kriptografi kunci publik membutuhkan pendukung yang dinamakan Infrastruktur kunci publik *(Public Key Infrastructure)*. *IKP* adalah sebuah pengaturan yang menjamin penggunaan kunci publik bagi pihak-pihak yang terlibat dalam sistem penggunaan sistem keamanan. *IKP* mengikat kunci publik dengan identitas pengguna, dan setiap pengguna dapat mengotentikasi satu sama lain. Informasi didalam sertifikat yang dikeluarkan oleh IKP digunakan untuk enkripsi dan deksripsi pesan antara pihak-pihak yang berkomunikasi.

Serangan yang umum terjadi pada kunci publik tanpa identitas merupakan bentuk dari penyamaran *(impersonation attack)*. Seseorang yang memiliki kunci publik orang lain dapat menyamar seolah-olah dia adalah pemilik kunci itu. Serangan tersebut adalah masalah yang muncul dari penggunaan kriptografi kunci publik. Contohnya dalam teknologi *e-commerce* maupun *e-busines*, terjadi pembayaran transaksi yang dilakukan dengan menggunakan kartu kredit dan pelanggan mengirimkan informasi kartu kreditnya melalui *website* pedagang online. Selama pengiriman, informasi kartu kredit tersebut dilindungi yaitu dengan cara melakukan enkripsi dengan kunci publik pedagang *online*. Bagaimana pelanggan itu memastikan bahwa website pedagang *online* tersebut memang benar milik pedagang *online* dan bukan *website* pihak lain yang menyamar sebagai *website* pedagang asli dengan tujuan untuk mencuri informasi kartu kredit.

Untuk menjawab permasalahan diatas, solusinya adalah dengan memberikan sertifikat digital pada kunci publik. Sertifikat digital adalah kunci publik dan informasi penting mengenai jati diri pemilik kunci publik, seperti misalnya nama, alamat, pekerjaan, jabatan, perusahaan dan bahkan hash dari suatu informasi rahasia yang ditandatangani oleh suatu pihak terpercaya. Sertifikat ini biasa digunakan oleh pihak ketiga yang berfungsi untuk meyakinkan (trusted parties) dalam bertransaksi dan berkomunikasi. Sertifikat digital tersebut ditandatangani oleh sebuah pihak yang dipercaya yaitu Certificate Authority atau pemegang otoritas sertifikat. CA adalah institusi keuangan (seperti Bank) atau institusi terpercaya lainnya. Contoh CA yang terkemuka adalah Verisign (verisign.com), Cybertrust, Thawte (www.thawte.com). Ketiga CA tersebut berbayar dan berlisensi. Namun apabila pengguna hanya sekedar ingin belajar untuk mengetahui cara kerja atau konsep pemberian sertifikat digital dan untuk keperluan intranet, ada sebuah *tools* bernama TinyCA yang merupakan aplikasi berbasis ubuntu yang sederhana dan dapat digunakan dengan mudah.

 ISSN: 1411-3201

Batasan Masalah

Beberapa parameter yang digunakan dalam permasalahan ini adalah "Bagaimana menggunakan aplikasi TinyCA sebagai aplikasi Certificate Authorization (CA) yang mudah dan sederhana pada sistem operasi ubuntu meliputi proses instalasi, konfigurasi dan cara kerja".

Tujuan dan Manfaat Penelitian

Tujuan dari penelitian ini adalah untuk membuktikan bahwa ada aplikasi yang berbasis ubuntu, sederhana yang mudah digunakan dan memiliki layanan otentikasi standar X.509 dan dapat digunakan untuk pembelajaran bagi pengguna yang ingin mengetahui cara kerja atau konsep pemberian sertifikat digital.

Adapun manfaat yang bisa diperoleh dari penelitian ini yaitu hasil penelitian ini bisa di jadikan sebagai acuan dan referensi tentang kemudahan penggunaan aplikasi TinyCA sebagai aplikasi CA berbasis ubuntu yang sederhana dan mudah digunakan.

Dasar Teori

Kriptografi

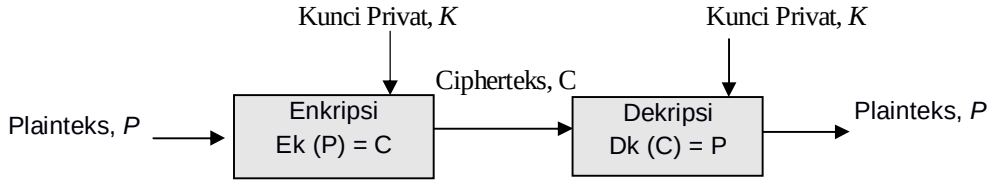
Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga *message-message* agar tetap aman (secure).

Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

a. *Confidelity* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
b. *Data integrity* (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
c. *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
d. *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Secara global teknik enkripsi dan dekripsi data terdiri dari dua metoda, yaitu metode kunci publik dan metode kunci simetri. Metode kunci simetri menggunakan password atau kata kunci yang sama untuk melakukan enkripsi juga dekripsi data. Karena itu metode ini sering juga disebut dengan metode Secret Key Criptography. Contoh-contoh metode ini adalah DES (Data Encryption Standard) dan IDEA (International Data Encryption Algorithm), RC5, Blowfish, AES (Advanced Encryption Standard) dan FEAL. Cara kerja metode enkripsi ini terlihat pada gambar 1 dibawah ini.



Gambar 1. Kriptografi Kunci Simetri

Masalah utama bagi penggunaan metode pengamanan data dengan kunci simetris adalah bagaimana mengirimkan kunci simetris tersebut dari pengirim kepada penerima. Tentunya metode pengamanan ini tidak akan berguna apabila kunci sampai jatuh ke tangan orang yang tidak berhak. Untuk itu dikembangkan metode kunci asimetris yang dikenal juga sebagai kunci publik.

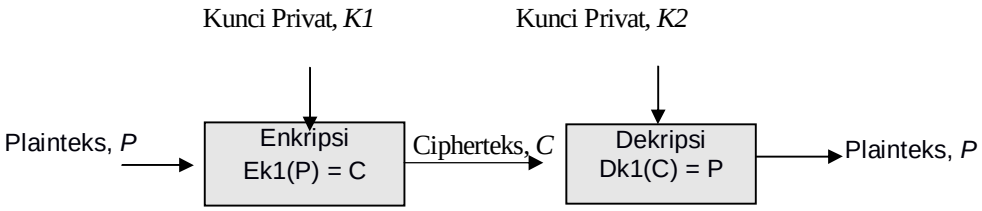
 ISSN: 1411-3201

Kriptografi Kunci Publik

Masalah ini dipecahkan oleh Diffie dan Hellman dengan mengusulkan kriptografi nirsimetri(asymetric cryptosystem) yang memungkinkan pengguna berkomunikasi secara aman tanpa perlu berbagi kunci rahasia. Nama lainnya adalah kriptografi kunci publik*(public-key cryptography)*, sebab kunci untuk enkripsi diumumkan kepada publik sehingga dapat diketahui oleh siapapun, sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan (karena itu rahasia). Siapapun dapat mengirim pesan yang dienkripsi dengan kunci publik tersebut, tetapi hanya penerima pesan yang dapat mendekripsi pesan karena hanya ia yang mengetahui kunci privatnya sendiri. Ini berlawanan dengan kriptografi kunci simetri yang hanya mempunyai satu kunci. Kriptografi kunci publik dibuat sepasang, satu kunci untuk enkripsi dan satu kunci untuk dekripsi (Gambar 2).

1. Kunci untuk enkripsi diumumkan kepada publik oleh karena itu tidak rahasia sehingga dinamakan kunci publik (public-key).
2. Kunci untuk dekripsi bersifat rahasia sehingga dinamakan kunci privat (private key).

Karena ada kunci enkripsi ≠ kunci dekripsi, maka sistem kriptografi kunci-publik kadang-kadang disebut juga sistem kriptografi asimetri.



Gambar 2. Kriptografi Kunci Publik

Infrastruktur Kunci Publik

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)**
  Suatu kunci berupa data/kode yang sifatnya rahasia sehingga hanya boleh diketahui oleh masing-masing individu.
  1. Bagi pengirim informasi (sender), dia menggunakan kunci privatnya untuk meng enkripsi suatu pesan yang akan dia kirimkan, sehingga menjadi sebuah digital signature.
  2. Bagi penerima informasi (receiver), dia menggunakan kunci privatnya untuk melakukan dekripsi terhadap digital envelope2 dari sender.
- **Kunci Publik (Public Key)**
  Suatu kunci berupa data/kode yang sifatnya untuk diketahui oleh orang lain (umum).
  1. Bagi pengirim informasi (sender), dia membutuhkan kunci publik receiver untuk melakukan enkripsi terhadap data yang akan dikirimkannya menjadi suatu digital envelope.
  2. Bagi penerima informasi (receiver), dia membutuhkan kunci publik sender agar dapat melakukan dekripsi terhadap digital signature sender.

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

Konsep Infrastruktur Kunci Publik

Komponen Infrastruktur Kunci Publik adalah sebagai berikut:

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

 ISSN: 1411-3201

memberitahu perubahan sertifikat digital kepada setiap orang.

3. **Management Function**
   Suatu prosedur yang digunakan untuk menjadi guideline dari keseluruhan proses yang ada dalam IKP.
4. **Policy Approving Authority (PAA)**
   Memberikan guideline untuk keseluruhan IKP 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.

Fungsi yang dilakukan IKP adalah sebagai berikut :

1. Mengautentikasi identitas. Dengan sertifikasi digital yang dikeluarkan oleh IKP 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 IKP dapat menggantikan peranan proses autentikasi user dalam sebuah sistem.
5. Dengan menggunakan sertifikat digital dari IKP 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.

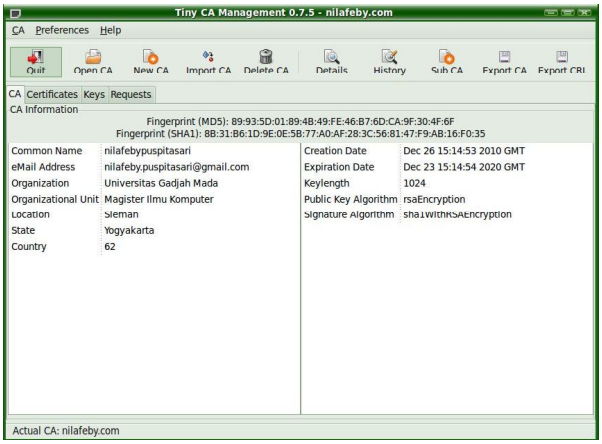
Aktifitas yang dilakukan IKP :

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.

Sertifikat Digital

Sertifikat digital adalah kunci publik dan informasi penting mengenai jati diri pemilik kunci publik, seperti misalnya nama, alamat, pekerjaan, jabatan, perusahaan dan bahkan hash dari suatu informasi rahasia yang ditandatangani oleh suatu pihak terpercaya. Sertifikat ini biasa digunakan oleh pihak ketiga yang berfungsi untuk meyakinkan (trusted parties) dalam bertransaksi dan berkomunikasi. Contoh sebuah sertifikat digital: Bob membawa kunci n publiknya dan mendatangi CA untuk meminta sertifikat digital. CA mengeluarkan sertifikat digital dan menandatangani sertifikat tersebut dengan cara mengenkripsi nilai hash dari kunci publik Bob (atau nilai hash dari sertifikat digital keseluruhan) dengan menggunakan kunci privat CA. Contoh isi sertifikat digital dari CA kira-kira seperti Gambar 3.

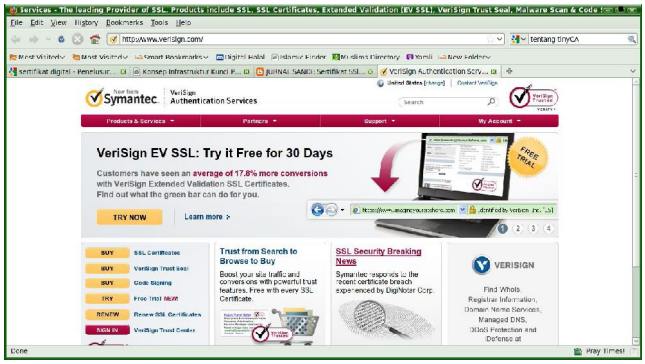
 ISSN: 1411-3201



Gambar 3. Contoh Sertifikat Digital

Sertifikat digital tersebut ditandatangani oleh sebuah pihak yang dipercaya yaitu Certificate Authority atau pemegang otoritas sertifikat. CA membangkitkan nilai hash dari sertifikat digital tersebut (misalnya dengan fungsi hash satu-arah MD5 atau SHA), lalu menandatangani nilai hash tersebut dengan menggunakan kunci privat CA. Supaya sertifikat digital itu dapat diverifikasi (dicek kebenarannya), maka kunci publik CA harus diketahui secara luas. Seseorang yang memiliki kunci publik CA dapat memverifikasi bahwa tanda tangan di dalam suatu sertifikat itu sah dan karena itu mendapat jaminan bahwa kunci publik di dalam sertifikat itu memang benar.

CA adalah institusi keuangan (seperti Bank) atau institusi terpercaya lainnya. Contoh CA yang terkemuka adalah Verisign (verisign.com), Cybertrust, Thawte (www.thawte.com)

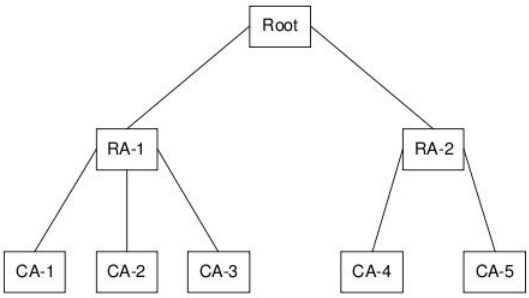


Gambar 4. Situs web Verisign.com

Mendapatkan Sertifikat

Sertifikat pengguna yang dikeluarkan oleh suatu CA mempunyai karakteristik bahwa seorang pengguna dengan akses ke public key dari CA dapat memeriksa public key pengguna tersebut bahwa tersertifikasi. Tidak ada pihak diluar dari otoritas sertifikasi dapat memodifikasi sertifikat tersebut tanpa ijin dari pemilik sertifikat. Karena sertifikat tidak dapat dipalsukan, maka dapat ditempatkan dalam suatu direktori tanpa perlu direktori tersebut dibuat usaha khusus untuk melindunginya. Adapun hirarki CA dapat dilihat dalam struktur pohon seperti gambar 5.

 ISSN: 1411-3201



Gambar 5. Struktur Hirarki CA

Keterangan dari gambar diatas adalah :

1. Aras ke-nol adalah root. Root merupakan root certificate authority, yang mana adalah Internet Policy Registration Authority (IPRA).
2. Root mensertifikasi CA aras satu dengan menggunakan privat root yang disebut root key.
3. CA aras satu disebut RA (Regional Authorities), yang bertindak sebagai policy creation authority, yaitu oganisasi yang membuat kebijakan untuk memperoleh sertifikat digital. Sebuah RA mungkin mencakup beberapa area geografis, seperti negara bagian, negara, atau benua.
4. RA menandatangai sertifikat digital untuk CA di bawahnya dengan menggunakan kunci privat RA.
5. CA menandatangani sertifikat digital untuk individu atau organisasi dengan mengguankan kunci privat CA.
6. CA bertanggung jawab untuk otentikasi sertifikat digital, sehingga CA harus memeriksa informasi secara hati-hati sebelum mengeluarkan sertifikat digital

.

Sekilas tentang TinyCA

TinyCA adalah sebuah aplikasi sederhana pada Ubuntu yang digunakan untuk membuat CA dengan mudah. sebenarnya tinyCA menggunakan SSL untuk mengenerate CA tetapi pembuatannya lebih mudah karena tinyCA menggunakan GUI. TinyCA juga menyediakan juga layanan untuk membuat SubCA, revoke CA dll. TinyCA mengelola otoritas sertifikat berskala kecil dengan layanan otentikasi berstandar X.509 yang digunakan secara luas di internet misalnya dalam S/MIME, IP Security, SSL/TLS dan SET. Standar ini tidak memaksakan penggunaan dari algoritma tertentu tetapi menganjurkan RSA. Algoritma kunci publik yang dibuat oleh *(Ron Rivest, Shamir dan Leonard Adleman).*

Layanan Otentikasi X.509

X.509 adalah bagian layanan CCITT X.500 (Rekomendasi x.500) yang mendefnisikan suatu layanan direktori berupa suatu server atau himpunan server yang merawat atau memelihara database informasi mengenai pengguna dan mendefinisikan (framework) kerangka kerja untuk layanan otentikasi dengan direktori x.500 kepada penggunanya. Direktori tersebut dapat melayani sebagai suatu repository dari sertifikat public-key. X.509 juga mendefinisikan protokol otentikasi alternatif berdasarkan pada penggunaan dari sertifikat public-key X.509 didasarkan pada penggunaan kriptigrafi public-key dan tanda tangan digital. Standard ini tidak memaksakan penggunaan dari suatu algoritma tertentu tetapi menganjurkan RSA. (Algoritma kriptografi kunci publik yang dibuat oleh *(Ron Rivest, Shamir dan Leonard Adleman).* Format sertifikat X.509 digunakan luas, misalnya dalam S/MIME, IP Security, SSL/TLS dan SET.

Layanan tersebut memiliki informasi seperti pada tabel 1.