PENGGUNAAN DAN PERBANDINGAN *BLIND RSA SIGNATURE* PADA *DIGITAL CREDENTIAL*

Raden Prana A. – NIM : 13506105

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16105@students.if.itb.ac.id

Abstrak

Salah satu protokol kriptografi adalah *blind signature*. *Blind signature* adalah sebuah bentuk tanda tangan digital dimana isi pesan disembunyikan sebelum ditanda-tangani. Hasil penandatanganan seperti ini bisa diverifikasi secara publik terhadap pesan asli yang tidak disembunyikan seperti pada halnya tanda tangan digital biasa. *Blind signature* umumnya digunakan untuk protokol yang terkait privasi dimana penandatangan pesan dan penulis pesan berasal dari pihak yang berbeda. Salah satu wilayah penggunaannya adalah pada *digital credential*, atau bentuk digital dari kartu identitas yang dimiliki seseorang. *Digital credential* ini diperlukan saat seseorang ingin agar informasi tertentu tentang diri mereka dapat diakses tanpa harus menunjukkan informasi penting lainnya yang tidak perlu diketahui pihak yang terkait.
Blind signature dapat diimplementasikan menggunakan teknik seperti pada halnya *digital signature* biasa, salah satunya menggunakan teknik *RSA*. Perbedaan yang cukup mendasar pada protokol *blind signature* dengan *digital signature* biasa ada pada penyembunyian pesan yang ditanda-tangani.
Penggunaan *digital credential* cukup luas dan mencakup berbagai aspek kehidupan. Di Indonesia sendiri, penggunaan *digital credential* sendiri sebenarnya memiliki prospek yang cerah, hanya saja masih memiliki beberapa kendala tertentu.

Kata kunci: *blind signature*, protokol kriptografi, *digital signature*, *RSA*, *digital credential*, penyembunyian pesan, tanda-tangan digital, perbandingan, penggunaan

1. Pendahuluan

1.1 Protokol Kriptografi

Protokol kriptografi adalah sebuah protokol konkrit atau abstrak yang melakukan sebuah fungsi terkait pengamanan dan mengaplikasikan metode kriptografi. Sebuah protokol mendeskripsikan bagaimana sebuah algoritma digunakan. Sebuah protokol yang cukup detil memasukan detil-detil penting berupa struktur dan representasi data, dimana selanjutnya dapat digunakan untuk mengimplementasikan berbagai *interoperabel* versi program.

Protokol kriptografi banyak digunakan untuk transport data secara aman pada level aplikasi. Sebuah protokol kriptografi umumnya terdiri dari beberapa aspek berikut:

1. Perjanjian sebuah kunci.
2. Autentikasi entitas.
3. Enkripsi simetrik.
4. Transport data pada level aplikasi yang sudah diamankan.
5. Metode non-repudiasi.

Beberapa protokol kriptografi sudah melebihi tujuan tradisional berupa konfidensialitas, integritas, dan autentikasi data. Protokol-protokol tersebut juga menjamin beberapa karakteristik yang diinginkan dari kolaborasi yang bermediakan komputer. Salah satu protokol itu adalah *blind signature*.

1.2 *Blind Signature*

Blind signature adalah sebuah bentuk tanda-tangan digital dimana isi pesan disembunyikan sebelum ditanda-tangani. Teknik ini diperkenalkan oleh David Chaum. Hasil *blind signature* dapat diverifikasi secara publik terhadap pesan asli yang tidak disembunyikan, seperti pada halnya tanda-tangan digital biasa. *Blind signature* umumnya digunakan untuk protokol yang terkait privasi dimana penandatangan dan penulis pesan berasal dari pihak yang berbeda dan tidak terkait satu sama lain.

Analogi yang biasa digunakan untuk *blind signature* adalah sebuah tindakan menutup pesan dengan sebuah amplop, kemudian disegel dan ditanda-tangani oleh seorang pihak penandatangan. Oleh karena itu, penandatangan tidak tahu isi pesan, tapi nanti pihak ketiga dapat memverifikasi tanda-tangan tersebut dan mengetahui bahwa tanda-tangan tersebut valid dengan batasan dari skema tanda-tangan yang berkaitan.

Skema *blind signature* dapat diimplementasikan menggunakan sejumlah skema penandatangan kunci publik, seperti *RSA* dan *DSA*. Untuk melakukan penandatanganan tersebut, pertama-tama pesan disembunyikan, umumnya dengan suatu cara penyembunyian acak. Pesan yang sudah disembunyikan diteruskan kepada penandatangan yang akan menandatangani pesan tersebut dengan dengan algoritma penandatanganan standar. Pesan yang dihasilkan, beserta faktor penyembunyiannya, selanjutnya dapat diverifikasi terhadap kunci publik milik penandatangan. Pada beberapa skema *blind signature*, seperti *RSA*, dimungkinkan bagi kita untuk menghapus faktor penyembunyian (*blinding*) dari tanda-tangan sebelum diverifikasi. Pada skema-skema ini, keluaran terakhir dari skema *blind signature* identik dengan protokol tanda-tangan biasa.

1.3 *Digital Credential*

Digital credential dimaksudkan untuk menjadi bentuk digital ekivalen dari tanda identitas diri yang *paper-based*. *Digital credential* membuktikan sesuatu tentang pemiliknya, yaitu informasi personal seperti nama, tempat dan tanggal lahir, atau informasi biometrik seperti foto atau sidik jari.

Digital credential memungkinkan seseorang untuk hanya menunjukkan sebagian informasi tentang dirinya. Hal ini diperlukan terutama apabila informasi pada *digital credential* tersebut hanya diperlukan sebagian, dan sang pemilik tidak ingin data-data lainnya dilihat begitu saja.

Digital credential menjaga properti kunci privasi dari dokumen *paper-based* dan *plastic tokens*, tapi juga menawarkan keamanan dan fungsionalitas lebih:

1. *Digital credential* hanya berupa sekuens 0 dan 1, sehingga dapat ditransfer secara elektronis dan dapat diverifikasi dengan akurasi 100 persen oleh komputer.
2. Pemilik *digital credential* dapat memilih secara selektif untuk menutup sebuah properti dari data yang dimasukan pembuat ke dalamnya, tanpa menunjukkan informasi lainnya.
3. Peminjaman *digital credential* dapat dihambat dengan memasukkan data konfidensial ke dalamnya, layaknya nomor kartu kredit sang pemilik. Meskipun pemilik dapat menyembunyikan data konfidensial ketika menggunakan *digital credential*, tidaklah mungkin untuk menggunakan *digital credential* tersebut tanpa mengetahui secara aktual data konfidensial tersebut.
4. *Digital credential* yang bersifat terbatas dapat menyimpan sebuah identifikasi *built-in* yang dapat diperlihatkan pada pihak sentral hanya jika *digital credential* tersebut ditunjukkan lebih dari sejumlah angka yang sudah ditentukan sebelumnya.
5. *Digital credential* dapat dimasukkan ke dalam kartu chip yang berbiaya rendah atau peralatan tahan-banting lainnya. Hal ini memberikan lapisan perlindungan tambahan terhadap kehilangan, pencurian, peminjaman, penggandaan, dan dapat mencegah bentuk lain dari tindakan yang tidak dibolehkan.

Untuk memungkinkan hal ini, digunakanlah beberapa protokol kriptografi, dan salah satu yang pling sering digunakan adalah *blind signature*.

2. Aplikasi Metode

2.1 Skema *Blind Signature*

Blind signature bekerja dengan skema sebagai berikut, dan untuk kasus ini kita akan menggunakan skema yang didasarkan pada algoritma *RSA*:
Sebuah tanda-tangan *RSA* tradisional dihitung dengan memuat pesan *m* ke eksponen rahasia *d* modulo modulus publik *N*. Versi *blind* menggunakan nilai acak *r* dimana *r* bersifat prima secara relatif terhadap *N*. *r* dimuat ke eksponen publik *e* modulo *N*, dan nilai yang dihasilkan, $r^e \bmod N$, digunakan sebagai faktor *blinding*. Penulis pesan menghitung nilai dari pesan dan faktor *blinding*

$$m' \equiv mr^e \pmod{N}$$

Dan mengirim nilai hasil *m'* pada pihak penanda-tangan. Karena *r* adalah nilai acak dan pemetaan $r \rightarrow r^e \bmod N$ adalah permutasi maka dapat disimpulkan bahwa $r^e \bmod N$ bernilai acak juga. Hal ini membuktikan bahwa *m'* tidak membocorkan informasi apapun tentang *m*. Pihak penanda-tangan kemudian menghitung tanda-tangan yang sudah disembunyikan *s'* sebagai

$$s' \equiv (m')^d \pmod{N}.$$

Nilai *s'* dikirim kembali kepada penulis pesan, yang kemudian akan menghapus faktor *blinding* untuk memunculkan *s*, tanda-tangan yang valid dari *m*

$$s \equiv s' \cdot r^{-1} \pmod{N}$$

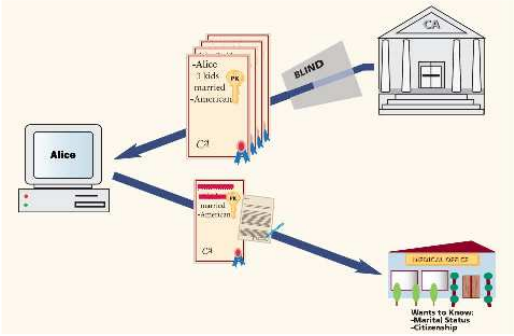
Rumus diatas bekerja karena kunci *RSA* memenuhi persamaan $r^{ed} \equiv r \pmod{N}$ dan oleh karena itu

$$s \equiv s' \cdot r^{-1} \equiv \left(m'\right)^d r^{-1} \equiv m^d r^{ed} r^{-1} \equiv m^d r r^{-1} \equiv m^d \pmod{N},$$

Yang berarti *s* adalah benar tanda-tangan dari *m*.

2.2 Skema *Digital Credential*

Model standar dari *digital credential* bekerja seperti gambar dibawah:



Gambar 1 Model *Digital Credential* Standar

Dari basis data kependudukan, data dari Alice di-*blind* (disembunyikan) dan ditanda-tangan dengan menggunakan skema *blind signature*, yang kemudian hanya memunculkan data status perkawinan dan status kependudukan yang akan digunakan oleh rumah sakit yang membutuhkan data tersebut dari Alice, tanpa Alice perlu menunjukkan data lainnya. Untuk lebih teknisnya, berikut penjelasan cara memasukkan atribut-atribut identitas Alice $(x_1,...,x_l)$ pada sebuah *digital credential*:

Tuple $(x_1, ..., x_l, \alpha)$ adalah kunci rahasia Alice untuk *digital credential* miliknya. Alice membangkitkan nilai α secara acak dari Z_q pada saat terjadinya protokol pembuatan. Meskipun Alice mungkin menutup sebagian atau semua atribut pada Bob ketika protokol penunjukan, Alice menjaga α tetap rahasia setiap saat. Hal ini untuk memastikan bahwa hanya Alice yang mengetahui seluruh kunci rahasia tersebut.

Kunci publik *digital credential* sama dengan produk dari

$$g_1^{x_1} \cdots g_l^{x_l} h_0^{\alpha}.$$

Elemen $g_1, ..., g_l, h_0$ telah dibangkitkan oleh otoritas kredensial (*CA*, atau *Credential Authority*) secara acak dari grup G_q dari orde prima *q*; mereka adalah bagian dari kunci publik. Untuk alasan teknis, h_0 tidak boleh sama dengan 1, untuk bisa mejadi pembangkit nilai G_q.

Kunci publik dari *digital credential* tidak memberikan informasi tentang $x_1,...,x_l$ karena banyak kunci rahasia yang berkoresponden dengan kunci publik yang sama. Secara spesifik, untuk kunci publik $h \in G_q$ apapun dan atribut tuple $(x_1,...,x_l)$ apapun, terdapat sebuah $\alpha \in Z_q$ yang cocok, dengan α adalah sebuah logaritma diskrit $h/(g_1^{x1},..., g_l^{xl})$ dengan pembangkit h_0. Karena Alice membangkitkan α secara acak dan menjaganya agar tetap rahasia, *h* tidak memberikan informasi tentang $x_1,...,x_l$. Untuk alasan ini, α disebut faktor *blinding*.

Ada dua properti keamanan yang terjadi di skema ini, yaitu:

1. Apapun pilihan nilai *l*, anggap bahwa tidaklah layak untuk menghitung logaritma diskrit pada G_q, Alice tidak dapat mengkomputasikan sebuah kunci publik dari *digital credential* dimana dia mengetahui lebih dari satu kunci rahasia.
2. Anggap bahwa tidaklah layak untuk menghitung logaritma diskrit pada G_q, Bob tidak dapat mengkomputasikan kunci rahasia apapun ketika diberikan kunci publik dari *digital credential* Alice, tidak bergantung pada atribut $(x_1,...,x_l)$ apapun yang ditutup oleh Alice terhadap Bob.

Banyak pembentukan dari G_q diketahui tidak layak untuk menghitung logaritma diskrit. Salah satu pilihan untuk G_q adalah subgrup dari Z_p^*, dimana *p* adalah bilangan prima sehingga *q* membagi $(p - 1)$ secara genap. Dalam kasus apapun, direkomendasikan bahwa *q* paling sedikit sepanjang 160 bit.

Lihat bahwa $x_1,...,x_l$ semuanya harus berupa angka dalam Z_q, karena *q* adalah urutan dari G_q. Cara pemetaan informasi atribut yang bermakna menjadi angka dalam Z_q tergantung pada *CA*.

Bisa saja menjelaskan pemetaan efisien pada daftar publik (misal, jenis kelamin Alice dapat digambarkan dengan bit satuan, dan kewarganegaraannya dengan angka antara 0-266) atau menggunakan *encoding* yang memungkinkan siapapun untuk mengambil arti dari x_i dari x_i itu sendiri (misal, kewarganegaraan Alice direpresentasikan dalam ASCII). Interpretasi dari tiap x_i tergantung pada penggunaan pada saat tersebut. Contohnya:

1. Pada uang elektronis, x_1 dapat menggambarkan mata uang, dan x_2 dapat menggambarkan jumlah nilai yang bisa dinegosiasikan Alice kepada Bob dengan harapan mendapat diskon.
2. Pada kartu identitas nasional, x_1 dapat merepresentasikan nama, x_2 = tempat dan tanggal lahit, x_3 = jenis kelamin, x_4 = status perkawinan, x_5 = umur, dan sebagainya.

CA dapat membuat nilai *hash* dari atribut yang tidak dapat direpresentasikan oleh angka dalam Z_q dengan menggunakan fungsi *hash collision-intractable*. Untuk menutup atribut-atribut tersebut, Alice harus menutup prekondisi dari x_i yang berkoresponden. Namun, jumlan nilai yang dapat ditampung dalam satu atribut harus dibatasi (kecuali Alice dapat menyembunyikan atribut tersebut ketika menunjukkan *digital credential*) , selain itu *CA* dapat mengidentifikasi Alice dalam protokol penunjukan dengan melakukan *encoding* sebuah nilai atribut unik ke dalam *digital credential* miliknya. Dalam konteks ini, pendekatan untuk mempublikasikan daftar pemetaan publik lebih dianjurkan, dan *CA* dapat mempublikasikan daftar ini beserta dengan kunci publik, dan menanda-tanganinya dengan kunci rahasia yang terkait.

3. Perbandingan Metode

Blind signature yang digunakan dibandingkan dengan teknik tanda-tangan digital biasa tanpa penyembunyian pesan. Dari situ dapat diambil beberapa perbedaan seperti:

1. Pesan tidak tersembunyikan pada penanda-tanganan pesan dengan tanda-tangan digital biasa, sehingga kemungkinan informasi yang tidak perlu diperlihatkan dapat dilihat pihak lain, sedangkan pada pesan yang menggunakan *blind signature* isi berhasil disembunyikan sehingga hanya informasi yang dibutuhkan yang dapat dilihat pihak lain disebabkan penggunaan faktor *blinding*.
2. *Digital credential* membutuhkan kerahasiaan isi pesan, sehingga *blind signature* dapat menjamin hal tersebut.
3. *Digital credential* dengan *blind signature* menjamin anonimitas.
4. Teknik *blind signature* rawan terhadap serangan seperi *RSA blinding attack*, dimana kita dapat ditipu untuk mendekripsi pesan dengan melakukan *blind signing* pada pesan lain. Tindakan ini dapat menyebabkan pihak penyerang mendapatkan isi pesan yang asli karena ketika pesan yang sudah tersembunyi ditanda-tangan kembali, maka pesan yang asli dapat terlihat. Pada skema tanda-tangan digital biasa, penand-tangan hanya perlu menerapkan sebuah skema *padding* pada pesan untuk mengatasi serangan diatas.

4. Kegunaan

4.1 Kegunaan *Blind Signature* Pada *Digital Credential* dan Penggunaan Pada Kehidupan Sehari-hari

Pada dasarnya, penggunaan *blind signature* pada *digital credential* diperlukan untuk hal-hal berikut ini:

1. Menjamin anonimitas.
2. Menjamin tersimpannya informasi pribadi pada saat-saat tertentu.

Pada kehidupan sehari-hari, *digital credential* dapat diaplikasikan pada beberapa aspek berikut, yaitu:

1. Sistem kontrol akses (misalnya untuk VPN, servis berbasis langganan, situs web, dll).
2. Kartu identitas nasional yang sudah ditingkatkan level privasinya.
3. Tiket transport publik.
4. Voting secara elektronis.
5. Sistem *e-health*.
6. Perdagangan sekuritas finansial.
7. Proteksi *copyright* digital.
8. *Road-toll pricing*.
9. Uang elektronis.

4.2 Penggunaan *Digital Credential* di Indonesia

Di Indonesia sendiri, penggunaan *digital credential* masih sangat minim. Saat ini bentuk identitas digital yang ada umumnya dalam bentuk kartu yang dikeluarkan perbankan.

Padahal untuk di Indonesia, penggunaan *digital credential* dapat dioptimalkan untuk beberapa sektor berikut:

1. Pendataan penduduk.
2. Proses pemilihan umum.
3. Pemudahan transaksi finansial masyarakat.

Kendala penggunaan *digital credential* di Indonesia sendiri terdiri dari beberapa hal berikut:

1. Kesulitan dalam pendataan.
2. SDM yang belum terlatih.
3. Sulitnya untuk merubah paradigma masyarkat dari *paper-based credential*.

5. Kesimpulan

Kesimplan yang didapat dari hasil studi perbandingan dan penggunaan *blind signature* pada *digital credential* adalah:

1. Protokol *blind signature* sangat tepat digunakan pada *digital credential*, dimana dibutuhkan penyembunyian informasi di dalam benda tersebut.
2. *Blind signature* dapat diimplementasikan dengan algoritma tanda-tangan digital biasa, sehingga memudahkan dalam implementasi.
3. Protokol *blind signature* menjamin tersembunyinya isi pesan, suatu hal yang tidak dijamin protokol tanda-tangan digital biasa. Namun, protokol *blind signature* lebih rawan terhadap serangan dibanding protokol tanda-tangan digital biasa.
4. Penggunaan *digital credential* sangat beragam, dan hal ini dapat memudahkan kehidupan masyarkat. Untuk di Indonesia, prospek pengembangannya cukup cerah, namun masih memiliki banyak kendala.

DAFTAR PUSTAKA

[1] Blind signature. http://en.wikipedia.org/Blind_signature. Tanggal akses: 5 Mei 2009 pukul 09.42.

[2] Brands, Stefan. (2002). Towards Digital Credentials. http://www.ercim.org/publication/Ercim_News/enw49/brands.html. Tanggal akses: 6 Mei 2009 pukul 17.46.

[3] What is a blind signature scheme?. http://www.rsa.com/rsalabs/node.asp?id=2339. Tanggal akses: 6 Mei 2009 pukul 16.35.

[4] Chaum, David. (1992). Achieving Electronoc Privacy. http://ntrg.cs.tcd.ie/mepeirce/Project/Chaum/sciam.html. Tanggal akses: 6 Mei 2009 pukul 16.33.

[5] Cryptographic protocol. http://en.wikipedia.org/wiki/Security_protocol. Tanggal akses: 5 Mei 2009 pukul 09.42.

[6] Silaghi, Marius C. & Kattmarui, Kishore R. (2005). Publicly Verifiable Private Credential. Florida Institute of Technology.

[7] Brands, Stefan. (2002). A Technical Overview of Digital Credential. Credentica.

[8] Brands, Stefan. (2004). Non-Intrusive Identity Management. McGill School of Computer Science & Credentica.

[9]Digital credential. http://www.wikipedia.org/wiki/Digital_credential. Tanggal akses: 6 Mei 2009 pukul 16:33.

[10] Bleumer, Gerrit. (2004). Blind Signature.

[11] Brands, Stefan & Legare, Frederic. Digital Identity Management Based On Digital Credentials. Credentica Inc.