Penggunaan *Digital Signature* untuk Autentikasi pada Kartu Tanda Penduduk

Igor Bonny Tua Panggabean [1)]
1) Jurusan Teknik Informatika ITB, Bandung 40132, email: if14022@students.if.itb.ac.id

Abstraksi *- Kartu Tanda Penduduk (KTP) adalah sebuah penanda identitas bagi warga negara Indonesia yang sudah berumur 17 tahun ke atas. Idealnya, setiap orang hanya memiliki satu buah KTP saja. Namun seringkali KTP dipalsukan oleh pihak-pihak tertentu dengan maksud untuk tindak kejahatan dan merugikan pemilik KTP yang sah.*
Digital signature pada KTP digunakan dengan memanfaatkan Nomor Induk Kependudukan (N.I.K) yang terdapat pada KTP. Untuk setiap KTP, terdapat satu NIK yang unik. Dengan melihat NIK yang ada pada KTP, pelaku pemalsuan dapat dengan mudah melakukan pemalsuan KTP sekaligus mengganti NIK pada KTP tanpa dicurigai. Oleh alasan inilah, penggunaan Digital signature diharapkan dapat membantu peran otentikasi NIK dan mempersulit pemalsuan pada NIK KTP.
Algoritma digital signature yang akan digunakan pada makalah ini adalah algoritma Digital Signature Algorithm (DSA) dengan menggunakan fungsi hash MD5 menggantikan fungsi Secure Hash Algorithm (SHA) untuk mengubah pesan menjadi message diggest.
Dengan adanya digital signature pada KTP, pengguna tinggal melakukan otentikasi dengan mendapatkan message diggest dari NIK untuk kemudian dibandingkan dengan message diggest hasil dekripsi dari digital signature yang ada pada KTP.
Pada makalah ini juga akan dibahas tentang kelebihan, kekurangan dan contoh kasus pemalsuan KTP yang sudah diperlengkapi dengan digital signature.

Kata Kunci: *Tanda tangan digital, DSA, MD5, keamanan kriptografi.*

1. PENDAHULUAN

Kemajuan dalam bidang teknologi informasi telah berkembang pesat. Terutama dalam bidang kemananan data. Tidak seperti jaman dahulu, ketika data yang bersifat rahasia masih sangat mudah untuk dibongkar. Sejak adanya ilmu kriptografi, kerahasiaan data menjadi sangat kuat dan semakin lama semakin sulit untuk ditembus.
Selain dipergunakan untuk merahasiakan data, ilmu kriptografi juga dipergunakan untuk konfirmasi keaslian data. Salah satunya dengan menggunakan cara pemberian tanda tangan digital.
Di Indonesia, dipergunakan sebuah kartu identitas yang digunakan untuk identifikasi kependudukan, yaitu Kartu Tanda Penduduk (KTP). Setiap warga negara Indonesia yang telah berumur 17 tahun wajib hanya memiliki satu buah Kartu Tanda Penduduk, dan untuk setiap Kartu Tanda Penduduk hanya dimiliki oleh satu orang penduduk (tidak ada kepemilikan ganda).
Namun seiring dengan perkembangan teknologi, kejahatan dalam bentuk penipuan sering terjadi. Semakin lama kejahatan ini pun semakin canggih. Hal ini pun tidak terlepas dari kejahatan yang dilakukan dengan memalsukan Kartu Tanda Penduduk yang pada akhirnya dipergunakan untuk tindakan yang tidak baik. Baik itu dengan membuat cetak ganda dari KTP seseorang maupun dengan melakukan usaha pencetakan KTP sendiri dengan identitas yang dipalsukan.
Maka pada makalah ini akan dibahas tentang penggunaan tanda tangan digital (*digital signature*) untuk menghindari tindak kejahatan ini, beserta keuntungan dan kerugiannya.
Algoritma yang akan digunakan untuk menambahkan tanda tangan digital adalah *Digital Signature Algorithm* namun menggunakan fungsi *hash* MD5 untuk menggantikan fungsi *Secure Hash Algorithm* sebagai fungsi standar pada Standar Tanda Tangan Digital.

2. DASAR TEORI

2.1. Tanda Tangan Digital

Tanda tangan sudah sering dipergunakan untuk membuktikan keotentikan sebuah dokumen. Sehingga, dengan dokumen yang ditandatangani, dokumen menjadi sulit untuk diubah oleh pihak lain. Tidak hanya pada dokumen, namun juga pada dokumen digital. Tanda tangan pada dokumen digital disebut *digital signature*.
Tanda tangan digital tidak pernah sama antara satu dokumen dengan dokumen yang lainnya.
Ada 2 tahap utama dalam melakukan pemberian tanda tangan digital. Tahap pertama yaitu mendapatkan *message diggest* dari pesan dengan menggunakan fungsi *hash* satu arah. Tahap kedua yaitu melakukan enkripsi terhadap *message diggest* yang telah didapatkan dengan menggunakan kunci privat pemilik dokumen. Dari hasil tahap kedua, didapatkan tanda tangan digital dari dokumen. Maka pengirim akan melakukan pengiriman dokumen serta tanda tangannya.
Juga terdapat 2 tahap utama dalam melakukan verifikasi tanda tangan digital. Tahap pertama yaitu melakukan dekripsi terhadap tanda tangan digital dengan menggunakan kunci publik pengirim untuk

mendapatkan *message diggest* yang tersembunyi di dalamnya. Tahap kedua yaitu menggunakan fungsi hash satu arah terhadap pesan yang dikirim untuk mendapatkan *message diggest*. Maka verifikasi dilakukan dengan membandingkan kedua *message diggest* yang didapatkan. Bila keduanya ternyata sama, maka dapat dipastikan bahwa dokumen masih otentik (asli). Sebaliknya, bila hasilnya ternyata berbeda, berarti pesan sudah tidak asli lagi.

Terdapat 2 algoritma yang umum dipergunakan untuk melakukan tanda tangan digital. Yaitu algoritma ElGamal, dan *Digital Signature Algorithm* (*DSA*). Algoritma DSA adalah hasil pengembangan dari algoritma ElGamal dan sudah ditetapkan secara internasional sebagai standar algoritma untuk tanda tangan digital (*Digital Signature Standard*).

2.2. *Digital Signature Algorithm* (*DSA*)

DSA adalah algoritma kriptografi kunci publik. DSA adalah algoritma yang dispesifikasikan khusus untuk tanda tangan digital. Sehingga DSA tidak dapat dipergunakan untuk melakukan enkripsi. Dalam DSA, terdapat dua fungsi utama yaitu pembentukan tanda tangan (*signature generation*) dan pemeriksaan keabsahan tanda tangan (*signature verification*).

DSA membutuhkan dua buah kunci, yaitu kunci privat dan kunci publik. Untuk pembentukan tanda tangan, digunakan kunci privat. Sedangkan untuk pemeriksaan keabsahan tanda tangan, digunakan kunci publik.

DSA memiliki 6 buah parameter yaitu.

1. p, merupakan bilang prima dimana $2^{L-1} < p < 2^L$ dengan $512 \leq L \leq 1024$ dan L adalah kelipatan dari 64. p bersifat publik
2. q, yaitu bilangan prima 160 bit sedemikian sehingga $(p\text{-}1) \bmod q = 0$ dimana $2^{159} < q < 2^{160}$. q bersifat publik.
3. $g = h^{(p-1)/q} \bmod p$ dengan $1 < h < p - 1$ sedemikian sehingga $h^{(p-1)/q} \bmod p > 1$. g bersifat publik.
4. x, adalah bilangan bulat kurang dari q. x adalah kunci privat.
5. $y = g^x \bmod p$, adalah kunci publik.
6. m, pesan yang akan diberi tanda-tangan.

Pemberian tanda tangan dilakukan dengan cara berikut.

1. Ubah pesan m menjadi *message digest* dengan fungsi *hash SHA*, H.
2. Tentukan bilangan acak k dengan $k < q$.
3. Tanda-tangan dari pesan m adalah bilangan r dan s. Hitung r dan s sebagai berikut:
   $r = (g^k \bmod p) \bmod q$
   $s = (k^{-1} (H(m) + x * r)) \bmod q$
4. Kirim pesan m beserta tanda-tangan r dan s.

Sedangkan untuk melakukan verifikasi pada tanda tangan digital dilakukan dengan cara berikut.

1. Hitung
   $w = s^{-1} \bmod q$
   $u_1 = (H(m) * w) \bmod q$
   $u_2 = (r * w) \bmod q$
   $v = ((g^{u1} * y^{u2}) \bmod p) \bmod q$
2. Jika $v = r$, maka tanda-tangan sah, yang berarti bahwa pesan masih asli dan dikirim oleh pengirim yang benar.

2.3. Fungsi Hash *MD5*

MD5 adalah fungsi *hash* satu arah. Fungsi ini diciptakan oleh Ronald R Rivest dari MIT. Algoritma *MD5* ini adalah hasil pengembangan dari algoritma *MD4* yang juga diciptakan oleh orang yang sama, setelah algoritma *MD4* berhasil diserang oleh kriptanalis. Algoritma ini mampu menerima pesan dengan berbagai ukuran dan menghasilkan pesan *message diggest* yang berukuran 128 bit.

Lagkah-langkah pembuatan *message diggest*.

1. Penambahan bit bit pengganjal
   Pada tahap pertama ini, pesan yang akan diproses ditambahkan dahulu dengan bit-bit pengganjal sehingga panjang pesan kongruen dengan 448 modulo 512. Sehingga, jika pesan memiliki panjang 448 bit, ditambahkan dengan 512 bit pengganjal, maka pesan tersebut menjadi 960 bit. Pada pesan ini, panjang bit pengganjal adalah antara 1 hingga 512. Bit pengganjal diawali dari bit 1, kemudian sisanya adalah bit 0.

2. Penambahan nilai panjang pesan awal
   Setelah ditambahkan bit pengganjal, pesan juga ditambahkan dengan 64 bit yang berisi panjang pesan semula. Jika ternyata panjang pesan lebih dari 2^{64}, maka panjang pesan dinyatakan dalam modulo 2^{64}. Setelah ditambahkan dengan 64 bit, maka panjang pesan sekarang menjadi kelipatan 512 bit.

3. Inisialisasi penyangga (*buffer*)
   Penyangga yang dibutuhkan dalam *MD5* terdiri dari 4 buah penyangga. Masing-masing penyangga memiliki panjang 32 bit. Sehingga total panjang untuk keseluruhan penyangga adalah 128 bit. Penyangga ini akan menampung hasil antara dalam proses pengolahan, dan juga hasil akhir dari fungsi *MD5*. Keempat penyangga yang diberi nama A, B, C, dan D kemudian diinisialisasi sebagai berikut:
   ```
   A = 01234567
   B = 89ABCDEF
   C = FEDCBA98
   D = 76543210
   ```

4. Pengolahan pesan dalam blok
   Pada awalnya, pesan dibagi ke dalam beberapa bagian (blok) dengan panjang tiap blok adalah 512 bit. Setiap blok 512 bit ini diproses dengan penyangga dan menghasilkan keluaran 128 bit. Proses ini disebut H_{MD5}. Pada awal proses, penyangga ini berisi nilai inisialisasi penyangga. Namun untuk proses berikutnya, penyangga berisi nilai dari proses pengolahan H_{MD5}.

Proses H_{MD5} terdiri dari 4 buah putaran, dengan masing-masing putaran melakukan.
Keluaran akhir dari algoritma *MD5* adalah hasil penyambungan dari bit-bit di A, B, C, dan D.

3. PEMBAHASAN

Dalam setiap Kartu Tanda Penduduk, pasti terdapat sebuah Nomor Induk Kependudukan (NIK) yang hanya bisa dimiliki oleh satu orang saja. Nomor induk inilah yang akan diproses untuk diberikan tanda tangan digital.
Tanda tangan digital yang telah didapatkan bisa ditambahkan di bagian bawah KTP.
Pada pembahasan ini akan dilakukan contoh pengujian langsung dengan NIK KTP yang asli. NIK yang akan digunakan pada bagian ini adalah

`10.1633.251086.0006`

3.1. Pemberian Tanda Tangan Digital

Tahap pertama yang dilakukan adalah menghitung nilai *message diggest* dari NIK yang ada pada KTP dengan menggunakan fungsi *hash MD5*.
Hasil *message diggest* dari

`m="10.1633.251086.0006"`

adalah

`H(m)="5B92CEA800BE7A38951877D153B3651A"`

Setelah menemukan *message diggest*, proses berikutnya adalah membangkitkan sepasang kunci untuk kunci privat dan kunci publik. Prosedurnya adalah sebagai berikut:

1. Pilih bilangan prima p dan q sembarang yang memenuhi syarat $(p\text{-}1) \bmod q = 0$
   $p = 59419$
   $q = 3301$
2. Hitung g yang memenuhi $g = h^{(p-1)/q} \bmod p$ dengan $1 < h < p - 1$
   $h = 100$
   $g = 18870$
3. Tentukan nilai x sebagai kunci privat
   $x = 3223$
4. Hitung nilai kunci publik y yang memenuhi $y = g^x \bmod p$
   $y = 29245$
5. Tentukan bilangan k yang memenuhi $k < q$
   $k = 997$
6. Hitung nilai r dan nilai s.
   $r = (g^k \bmod p) \bmod q = 848$
   $s = (k^{-1} (H(m) + x * r)) \bmod q$
   $= 417$
7. Masukkan nilai r dan nilai s sebagai nilai untuk tanda tangan pada KTP.

3.2. Pengujian Tanda Tangan Digital

Prosedur untuk pengujian tanda tangan digital oleh pihak kedua yang membutuhkan autentikasi data pada KTP adalah sebagai berikut

1. Hitung
   $w = s^{-1} \bmod q$
   $= 1132 \bmod 3301$
   $= 1132$
   $u1 = (H(m) * w) \bmod q$
   $= 1878$
   $u_2 = (r * w) \bmod q$
   $= 959936 \bmod 3301$
   $= 2646$
   $v = ((g^{u1} * y^{u2}) \bmod p) \bmod q)$
   $= 848$
2. Karena $v = r$, maka tanda tangan lolos uji.

3.3. Keuntungan

Beberapa keuntungan yang dapat diperoleh setelah menggunakan tanda tangan digital dalam KTP adalah

1. Autentikasi integritas data dan pemilik data
   Bila dalam suatu proses yang membutuhkan KTP, pihak yang membutuhkan KTP melakukan pengujian pada tanda tangan digital dan melihat bahwa hasil pengujian menunjukkan ketidak sesuaian, maka dapat diambil kesimpulan bahwa NIK pada KTP tersebut telah berubah, yang berarti juga bahwa KTP tersebut telah dipalsukan, atau bahwa kunci publik yang digunakan tidak sesuai, yang berarti bahwa proses pemberian tanda tangan tidak dilakukan oleh pemilik yang datanya tertulis pada KTP tersebut.

2. Autentikasi kepemilikan data
   Dengan menguji tanda tangan digital, bila didapatkan hasil yang benar, dapat dijamin bahwa tanda tangan digital tersebut diuji dengan kunci publik yang benar. Dari sini bisa didapatkan data mengenai pemilik kunci publik tersebut. Bila data pemilik kunci dibandingkan dengan data yang terdapat pada KTP ternyata memiliki perbedaan, dapat dipastikan bahwa yang memberi tanda tangan pada KTP berbeda dengan pemilik KTP. Hal ini dapat terjadi bila si pemalsu KTP memalsukan KTP si A namun agar tanda tangan terlihat asli, pelaku pemalsuan mengambil NIK acak dan memberi tanda tangan berdasarkan NIK tersebut dengan kunci privat si pemalsu.

3. Minimalisasi pemalsuan.
   Karena algoritma tanda tangan digital ini menggunakan pasangan kunci yaitu kunci publik dan kunci privat, maka keberadaan kunci privat akan menurunkan niat para pemalsu KTP untuk melakukan pemalsuan. Dengan adanya kunci privat ini, tidak menjadi mudah untuk memalsukan NIK atau membuat tanda tangan palsu karena kriptanalis pada kunci privat akan

membutuhkan usaha yang jauh lebih berat dan merepotkan dari pada pemalsuan KTP tanpa tanda tangan digital. Dengan demikian usaha untuk pemalsuan pun dapat dikurangi.

3.4. Kesulitan

Kesulitan yang dihadapi dalam penggunaan tanda tangan digital pada KTP penduduk Indonesia adalah:

1. Penyimpanan Kunci Publik
   Di Indonesia masih mengalami kesulitan dalam menggunakan kunci privat dan kunci publik untuk kriptografi. Terutama dalam menggunakan tempat yang dapat menyimpan kunci publik bagi masyarakat Indonesia. Karena sesuai dengan sifatnya, kunci publik harus mudah untuk di akses dan terbuka bagi umum. Selain itu, masyarakat Indonesia masih belum terlalu peduli akan masalah keamanan bahkan cenderung merasakan bahwa penggunaan kriptografi kunci publik hanya merepotkan saja.

2. Kesadaran masyarakat akan penggunaan KTP
   Masyarakat Indonesia sendiri masih belum memiliki kesadaran yang tinggi akan penggunaan KTP sebagai kartu identitas pribadi. Bahkan KTP cenderung dianggap tidak penting dan jarang digunakan. Sebagian masyarakat Indonesia juga tidak terlalu merasakan bahaya yang dapat terjadi jika terjadi kasus pemalsuan KTP. Bahkan cenderung merasa bukan suatu masalah bila KTP jarang dibawa, bahkan bila tidak memiliki KTP sama sekali.

3. Transaksi dengan KTP
   Di Indonesia sendiri, transaksi dengan menggunakan KTP masih cukup jarang digunakan. Walaupun terjadi transaksi dengan menggunakan KTP, cenderung hanya sebagai pelengkap persyaratan saja. Penggunaan KTP di Indonesia paling banyak hanya sebagai kartu identitas yang dapat digunakan bila terlibat masalah hukum.

4. KESIMPULAN

KTP di Indonesia dipergunakan sebagai tanda identitas kependudukan bagi penduduk Indonesia yang sudah berumur 17 tahun ke atas. Dalam KTP terdapat Nomor Induk Kependudukan (NIK) yang berbeda untuk tiap penduduk. Namun kombinasi NIK dalam KTP sangat mudah untuk dipahami dan ditiru.

Tindakan pemalsuan KTP sangat mudah untuk dilakukan karena hanya tinggal memberikan data palsu dan merancang kombinasi NIK yang tidak tampak mencurigakan.

Penggunaan tanda tangan digital yang menggunakan pesan berupa NIK pada KTP diharapkan dapat meminimalisasi usaha pemalsuan melalui KTP sekaligus meningkatkan kesadaran masyarakat Indonesia terhadap faktor keamanan identitas.

Terdapat beberapa keuntungan yang bisa didapatkan dengan menggunakan tanda tangan digital pada KTP. Diantaranya adalah jaminan bahwa KTP tersebut masih berisi data yang sesuai, juga jaminan bahwa tanda tangan yang terdapat pada KTP ditanda tangani oleh pemilik yang datanya tertera pada KTP.

Namun pada masyarakat Indonesia sendiri, masih terdapat beberapa kesulitan yang harus dihadapi bila ingin menggunakan tanda tangan digital pada KTP. Diantaranya yaitu faktor keamanan identitas di Indonesia masih belum terlalu dianggap penting. Sehingga penggunaan tanda tangan digital cenderung dianggap sebagai usaha yang merepotkan, juga karena masyarakat Indonesia masih belum memiliki kesadaran yang tinggi akan kepemilikan KTP. Bahkan banyak yang jarang membawa KTP, bahkan tidak memilikinya. Selain itu karena transaksi dengan menggunakan KTP di Indonesia ini masih dianggap tidak terlalu penting, dan cenderung sebagai pelengkap persyaratan.

Berdasarkan hal ini, maka dapat diambil kesimpulan bahwa penggunaan tanda tangan digital pada KTP di Indonesia secara teori dapat dilaksanakan dan sangat menaikkan nilai keamanan dan integritas data pada KTP. Namun secara praktis, penggunaan tanda tangan digital pada KTP masih memerlukan waktu yang lama sebelum masyarakat Indonesia siap.

DAFTAR REFERENSI

[1] R. Munir, "*Digital Signature Standard (DSS)*", IF5054 Kriptografi, Program Studi Teknik Informatika Institut Teknologi Bandung.

[2] "*Digital Signature Standard*", National Institute of Standards and Technology, 2000.

[3] R. Munir, "*Diktat Kuliah IF5054 Kriptografi*", Program Studi Teknik Informatika Institut Teknologi Bandung, 2006.