Analisis Fitur Keamanan Dokumen dengan Format PDF pada Kakas Adobe Acrobat Professional

Shinta Marino [1)]

1) Program Studi Teknik Informatika ITB,Bandung 40132, email: if14130@students.if.itb.ac.id

Abstract – *Format PDF yang dibuat oleh Adobe Systems pada tahun 1993, sesuai namanya, telah banyak digunakan untuk kebutuhan pertukaran dokumen. Oleh karena itu, Adobe Acrobat Professional menyediakan sejumlah fitur keamanan untuk dokumen elektronik untuk mendukung fungsi portable dari format PDF. Fitur tersebut antara lain enkripsi dokumen, restriksi akses, dan tanda tangan digital. Ketiga fitur tersebut telah tergolong cukup lengkap untuk aplikasi sejenis. Akan tetapi disamping kelengkapan fitur tersebut, masih terdapat sejumlah kekurangan dalam hal penggunaan fitur-fitur keamanan Adobe Acrobat Professional*

Kata Kunci*: Adobe Acrobat, PDF, kemanan dokumen*

1. PENDAHULUAN

Dokumen PDF (*Portable Dokumen Format*) merupakan format file yang dibuat oleh Adobe Systems pada tahun 1993. Sesuai dengan namanya, dokumen ini ditujukan untuk fungsi pertukaran dokumen (bersifat *portable*). PDF digunakan untuk merepresentasikan dokumen 2 dimensi yang independen dari segi resolusi tampilan. Dokumen PDF dapat menyimpan data yang terdiri dari teks, gambar dan vector grafis 2 dimensi.

Pengiriman dalam bentuk digital seringkali terpaksa dilakukan melalui saluran komunikasi umum seperti internet yang keamanannya tidak terjamin. Untuk menjamin keamanan dokumen penting tersebut terdapat beberapa cara antara lain dengan melakukan enkripsi terhadap dokumen untuk menjaga kerahasiaannya atau dengan memberikan tanda tangan digital untuk menjaga keaslian dokumen. Disamping itu dapat pula dilakukan pembatasan akses untuk menghindari penyalahgunaan dokumen tersebut.

Adobe Acrobat Professional, salah satu kakas yang digunakan untuk membuat dokumen PDF telah menyediakan sejumlah sarana pengaman untuk dokumen PDF.

2. PENGAMANAN DOKUMEN

Seperti telah disebutkan sebelumnya, ada beberapa cara yang dapat digunakan untuk mengamankan sebuah dokumen. Beberapa diantaranya adalah enkripsi dokumen, pemberian tanda tangan digital (*digital signature*), dan pembatasan akses terhadap dokumen.

2.1. Enkripsi / Dekripsi

Konsep enkripsi-dekripsi telah dikenal sejak lama mulai dari algoritma sederhana yang melakukan substitusi dan transposisi terhadap setiap karakter dari dokumen sampai dengan algoritma yang saat ini digunakan untuk dokumen digital (algoritma kriptografi modern) yaitu algoritma berbasis bit.

Secara umum ada dua kelompok besar algoritma kriptografi modern yaitu algoritma kriptografi kunci simetri (*symmetric key algorithm*) dan algoritma kriptografi kunci nirsimetri (*asymmetric key algorithm*). Algoritma kriptografi kunci simetri menggunakan satu kunci yang sama untuk melakukan enkripsi dan dekripsi. Sedangkan algoritma kriptografi kunci nirsimetri menggunakan sepasang kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Salah satu golongan dari algoritma kunci nirsimetri yang disebut algoritma kunci publik merupakan algoritma kriptografi yang sangat populer saat ini.

Dalam pengiriman dokumen digital, proses enkripsi-dekripsi akan memastikan kerahasiaan dokumen dan keaslian dokumen. Perubahan yang dilakukan pada cipherteks akan menghasilkan dokumen hasil dekripsi yang rusak sehingga gangguan terhadap dokumen dalam perjalanan akan terdeteksi dengan mudah.

2.2. Tanda tangan digital (*digital signature*)

Konsep tanda tangan digital kurang lebih berusaha untuk menirukan fungsi tanda tangan pada dokumen konvensional yaitu untuk menjamin otentikasi dokumen baik keaslian isinya maupun memastikan orang yang membuat dokumen tersebut.

Saat ini, fungsi dari tanda tangan digital sebenarnya lebih dari sekedar menggantikan tanda tangan konvensional. Dengan memberikan tanda tangan digital pada dokumen maka integritas (keaslian) dan otentikasi dokumen terjamin serta penyangkalan dari penulis dokumen dapat dihindari.

Pemberian tanda tangan digital pada dokumen dapat dilakukan dengan beberapa cara, yaitu :

a. Melakukan enkripsi dengan algoritma kunci simetri pada dokumen. Otentikasi dokumen dapat dilakukan jika dokumen di enkripsi dengan menggunakan algoritma kriptografi kunci simetri.

Hanya saja metode enkripsi tidak dapat mengatasi masalah penyangkalan dari pengirim bahwa ia telah membuat dan mengirimkan pesan tersebut. Untuk mengatasi masalah ini, diperlukan mekanisme yang lebih rumit yaitu dengan menggunakan bantuan pihak ketiga yaitu arbitrase.

b. Melakukan enkripsi dengan algoritma kunci publik pada dokumen. Penggunaan algoritma kunci publik untuk tanda tangan digital dilakukan dengan menggunakan pasangan kunci privat dan kunci publik secara terbalik. Kunci privat digunakan untuk me-enkripsi pesan dan secara otomatis kunci publik digunakan untuk melakukan dekripsi terhadap cipherteks.
c. Menggunakan fungsi hash. Fungsi hash merupakan sebuah fungsi satu arah yang menerima masukan berupa string dengan panjang sembarang dan memberikan keluaran berupa string baru yang panjang tertentu. Fungsi hash akan memberikan keluaran yang berbeda untuk setiap string masukan yang berbeda. Cara memberikan tanda tangan digital pada dokumen dengan fungsi hash secara umum adalah dengan memberikan pesan sebagai masukan fungsi hash dan menyimpan keluaran fungsi hash tersebut bersama pesan dalam sebuah dokumen. Dengan demikian, jika di kemudian hari hasil penghitungan nilai hash dari dokumen berbeda, berarti dokumen telah mengalami perubahan setelah dokumen tersebut ditandatangani oleh pembuatnya.

2.2. Pembatasan Akses (*Restriction*)

Jika metode enkripsi menghalangi akses dokumen dari pihak-pihak yang tidak berhak dan tanda tangan digital memastikan integritas dan keotentikan dokumen, maka pembatasan akses dimaksudkan untuk menghindari penyalahgunaan dokumen seperti penggunaan dokumen, baik sebagian maupun secara keseluruhan secara komersil oleh orang yang tidak berhak.

Pembatasan akses biasanya dilakukan dalam bentuk pembatasan pada *editing*, *printing*, dan penyalinan dokumen. Pembatasan dapat dilakukan dengan melarang sama sekali akses terhadap ketiga hal di atas ataupun membatasi pengubahan, pencetakan maupun penyalinan pada beberapa bagian tertentu dalam dokumen.

3. FITUR KEAMANAN PADA ADOBE ACROBAT

Kakas Adobe Acrobat menyediakan sejumlah fitur keamanan untuk dokumen yang cukup mampu memenuhi kebutuhan keamanan dokumen yang ada saat ini. Fitur-fitur tersebut berupa enkripsi, Restriksi (pembatasan akses) dan tanda tangan digital. Berikut dijelaskan masing-masing fitur tersebut.

3.1. Enkripsi

Dalam melakukan enkripsi dokumen, adobe acrobat menggunakan konsep *Hybrid Encryption* untuk meningkatkan level keamanan dokumen enkripsi.

Hybrid encryption merupakan proses enkripsi dokumen dengan menggunakan algoritma kunci simetri dan kemudian menggunakan algoritma kunci nirsimetri untuk melakukan enkripsi terhadap kunci enkripsi dokumen. File hasil enkripsi dan kunci yang telah dienkripsi disatukan dalam sebuah file pdf.

Adobe acrobat juga memungkinkan sebuah dokumen untuk diamankan untuk sejumlah penerima dimana masing-masing mempunyai pasangan kunci yang berbeda. Dengan demikian personalisasi enkripsi dapat dilakukan sehingga dokumen tersebut benar-benar jelas ditujukan kepada siapa dan siapa pengirim dokumen tersebut.

Dalam proses enkripsi/dekripsi dokumen, yang digunakan sebagai kunci adalah *Digital ID* dari pembuat dokumen dan penerima dokumen. Jika *digital ID* penerima tidak cocok dengan dokumen, dokumen tidak dapat diakses.

Digital ID merupakan data dari seorang pengguna yang berfungsi kurang lebih sebagai tanda pengenal digital. Ada beberapa cara yang dapat dilakukan untuk mendapatkan *digital ID*, yaitu :

a. Melalui penyedia CDS (*Certified Document Services*). Sebuah penyedia CDS akan memberikan sejumlah persyaratan untuk memastikan identitas seseorang sebelum mereka menyetujui untuk menerbitkan *digital ID*. Salah satu contoh penyedia CDS adalah GeoTrust.
b. Melalui penyedia *Certificate Authority* (CA). Berbeda dengan CDS, penyedia CA bervariasi dalam hal jumlah informasi yang diminta untuk memperoleh sebuah *digital ID*. Contoh penyedia CA antara lain GeoTrust, VeriSign, dan Entrust.
c. Melalui IT *group* sebuah perusahaan. Jika seorang pengguna bekerja pada sebuah perusahaan yang menjadi anggota dari suatu IT *group*, maka pengguna dapat mengajukan permintaan *digital ID* padakelompok tersebut. Sejumlah IT *groups* menyebut *digital ID* sebagai *signing certificate*, *e-mail certificate*, atau *identity certificate.*
d. Membuat *self-signed digital ID* dengan menggunakan adobe acrobat.

Untuk melakukan enkripsi, pengguna terlebih dahulu harus mempunyai *digital ID*. Dokumen di-enkripsi dengan menggunakan *digital ID* pengirim dan penerima. Jika pasangan ID ini tidak cocok, maka akses terhadap dokumen akan dilarang, tapi jika

pasangan ID cocok, dokumen dapat digunakan seperti biasa.

Metode enkripsi seperti tersebut diatas secara otomatis memberikan otentikasi pengirim kepada penerima sehingga sampai batas tertentu sudah menggantikan fungsi dari tanda tangan digital.

Pada Adobe Acrobat Professional, algoritma yang diimplementasikan untuk fitur ini adalah AES (128 dan 256 bit), RC4 (128 bit) dan 3DES untuk algoritma kunci simetri serta RSA (1024 dan 2048 bit) untuk algoritma kunci publik (nirsimetri).

Saat dokumen yang telah dienkripsi hendak dibuka, adobe acrobat akan mendekripsi dokumen dengan menggunakan *digital ID* yang dimiliki pengguna. Jika *digital ID* tersebut sesuai, maka dokumen akan dapat dibuka seperti biasa.

3.2. Restriksi

Restriksi memberikan batasan akses bagi penerima seperti pembatasan dalam pencetakan dan penyalinan isi dokumen, menambahkan komentar, menambahkan atau menghapus halaman dan sejumlah batasan lainnya

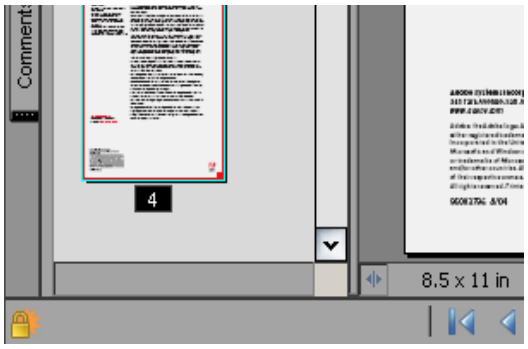
Selain memberi batasan akses, Restriksi juga mencakup control dinamis terhadap dokumen. Control dinamis ini menyangkut hak akses terhadap dokumen setelah dokumen tersebut dipublikasikan. Dengan adanya fitur ini, penulis dokumen dapat melakukan hal-hal berikut :

a. Memberikan tanggal kadaluwarsa dokumen sehingga dokumen hanya dapat di akses sampai batas waktu tertentu.
b. Memungkinkan *update* otomatis jika terdapat versi lebih baru dari dokumen yang dibuat oleh penulis. Dengan demikian, penulis tidak perlu melakukan distribusi ulang secara manual untuk setiap perubahan yang ia buat pada dokumen.
c. Mengatur akses dokumen secara *off-line* seperti membatasi hak akses atau member batas waktu sebuah dokumen dapat diakses secara *offline* sehingga pengguna harus terhubung ke internet untuk mendapat akses lebih lanjut.
d. Mengontrol versi dokumen secara persisten. Dimana akses terhadap dokumen versi lama dapat diubah oleh penulis sementara versi lebih baru masih dalam persiapan untuk dirilis.

Proses Restriksi terhadap dokumen pdf dapat dilakukan pada saat pembuatan maupun dengan melakukan perubahan di kemudian hari. Pilihan teknologi Restriksi dokumen yang tersedia pada Adobe Acrobat Professional secara lengkap adalah :

a. Pengubahan (*editing*) : No *changes allowed / Any changes except extracting pages / Fill in form fields / Comment and annotate / Digitally sign / Insert, delete, and rotate pages / Copy text, images, and other content / Enable text access for screen reader devices for the visually impaired*
b. Pencetakan : *No printing allowed / Low-resolution printing only (150 dpi)/ High-resolution printing*
c. Izin akses : *Modify permissions after publication and distribution / Expire and revoke distributed documents / Manage offline access / Enforce content management system security policies outside system*

Sebuah dokumen yang telah diberi restriksi seperti dijelaskan di atas pada sudut kiri bawah layar Adobe Acrobat akan ditandai gambar gembok emas seperti diperlihatkan pada gambar 1.



Gambar 1 Simbol penanda dokumen yang direstriksi

3.3. Tanda tangan digital (*digital signature)*

Pemberian tanda tangan digital pada dokumen PDF, seperti halnya enkripsi dokumen, dilakukan dengan menggunakan *digital ID*. Jika pada fitur enkripsi dibutuhkan identitas pengirim dan penerima, maka pada pemberian tanda tangan digital hanya dibutuhkan *digital ID*.

Gambar 2 Contoh notifikasi tanda tangan digital

Metode yang digunakan pada Adobe Acrobat Professional untuk mengimplementasikan fitur digital signature melibatkan :

a. *Parity bits* atau fungsi *Cyclical redundancy*

checking (CRC) yang mampu mendeteksi perubahan pada dokumen sampai batas tertentu. Fungsi ini bisa dikelabui oleh pihak ketiga dengan cara tertentu.

b. *One way hash*. Seperti yang telah disebutkan dalam bagian sebelumnya, penggunaan fungsi hash merupakan salah satu cara untuk mengimplementasikan tanda tangan digital. Fungsi hash yang digunakan Adobe adalah algoritma SHA-1 dan SHA-256 yang diterima secara luas sebagai standar keamanan dokumen.
c. *Message Authentication Codes* (MAC). MAC memastikan bahwa sebuah dokumen tidak dapat diubah oleh pihak ketiga dan kemudian menambahkan tanda tangan digital baru (fungsi hash). Hal ini dilakukan dengan cara melewatkan sebuah kunci simetri yang telah dihubungkan dengan MAC kepada sebuah fungsi hash (disebut HMAC). Metode ini digunakan dalam Adobe Acrobat secara kondisional.
d. *Public Key Infrastructure* (PKI) yang menyediakan suatu bentuk sertifikat yang dapat digunakan penerima dokumen untuk mengetahui suatu kunci publik benar-benar milik dari individu tertentu.

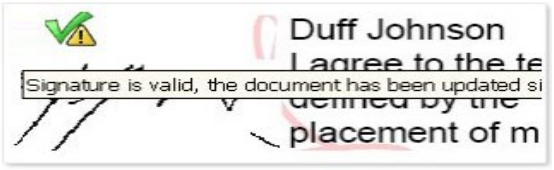
CRC, fungsi Hash, dan MAC akan memastikan keotentikan sebuah dokumen, sedang PKI berfungsi untuk menghindari penyangkalan dari pengirim dokumen.

Gambar 3 Pesan Validasi tanda tangan digital

Untuk membubuhkan tanda tangan digital pada sebuah dokumen pada adobe acrobat, pengguna akan diminta untuk membuat sebuah *signature field* atau pengguna dapat juga memilih untuk membuat sebuah *invisible signature.* Selanjutnya, pengguna cukup mengikuti langkah-langkah yang dibutuhkan untuk membubuhkan sebuah tanda tangan digital.

Gambar 4 Pesan Validasi untuk dokumen yang diubah

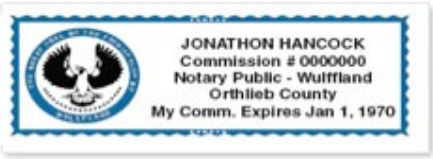
Sebuah dokumen yang dibubuhi tanda tangan digital akan menampilkan layar seperti pada gambar 2. Disamping itu, Adobe Acrobat juga memberikan keterangan mengenai status validasi tanda tangan digital. Keterangan tersebut ditampilkan dalam bentuk *prompt message* seperti tampak pada gambar 3 dan gambar 4.



Gambar 5 Tanda tangan digital dengan gambar serta identitas pengguna

Bentuk dari tanda tangan digital pada Adobe Acrobat bisa beragam. Pada gambar 5, 6 dan 7 diberikan beberapa contoh. Adobe Acrobat memungkinkan pengguna untuk membubuhkan tanda tangan digital dengan sekaligus mencantumkan gambar tanda tangan pengguna tersebut dalam dokumen.

Gambar 6 Tanda tangan digital dengan gambar



Gambar 7 Tanda tangan digital dengan lambang suatu instansi

Hasil dari validasi tanda tangan digital pada Adobe Acrobat dapat berupa tanda tangan valid, tanda tangan tidak dikenali, tanda tangan invalid dan tanda tangan valid tapi dokumen berubah. Keempat status tanda tangan digital itu dilambangkan dalam bentuk gambar seperti terlihat pada gambar 8.

Gambar 8 Simbol status validasi tanda tangan digital

4. KESIMPULAN

Secara umum, Adobe Acrobat telah berhasil memfasilitasi kebutuhan pengamanan dokumen dalam tiga bentuk yaitu enkripsi, otorissasi dan tanda tangan digital. Ketiga bentuk tersebut telah berhasil

menjalankan fungsi kerahasiaan, otorisasi, integritas, otentisitas, dan penyangkalan (non-repudiation).

Akan tetapi terdapat ditengah kelengkapan fitur tersebut, masih terdapat kekurangan pada fitur keamanan Adobe Acrobat tersebut,.diantaranya :

a. Sejumlah pihak telah berhasil menemukan cara untuk mengatasi restriksi dokumen pada adobe acrobat.
b. Penggunaan tanda tangan digital pada dokumen masih cukup rumit, terutama bagi pengguna yang masih awam. Menurut sejumlah pihak, Adobe Acrobat merupakan salah satu aplikasi yang berhasil memberikan fitur tanda tangan digital melalui proses yang sederhana. Akan tetapi, bahkan dengan proses tersebut pun konsep tanda tangan digital masih terkesan cukup rumit.
c. Pembubuhan tanda tangan digital dan enkripsi dokumen membutuhkan adanya sebuah *digital ID*. Konsep *digital ID* ini belum dikenal secara luas, bahkan bagi pihak-pihak yang sudah merasa cukup familiar dengan masalah keamanan internet. Untuk mendapatkan sebuah *digital ID*, pengguna harus menghubungi pihak ketiga yang mempunyai hak untuk menerbitkan *digital ID*. Cara ini tentu saja membutuhkan dana. Memang Adobe Acrobat memungkinkan pengguna untuk membuat sendiri *digital ID*-nya (*self-signed digial ID*), akan tetapi *digital ID* tersebut malah menimbulkan masalah baru. Proses validasi pada dokumen yang menggunakan *self-signed digital ID* menjadi lebih sulit. Jika pada dokumen yang menggunakan *digital ID* keluaran pihak ketiga pengguna cukup terhubung dengan internet dan adobe acrobat secara otomatis akan melakukan validasi, maka pada dokumen dengan *self-signed digital ID* pengguna harus mempunyai arsip *digital ID* pengirim agar dapat melakukan validasi.

Mengingat masih rumitnya proses penggunaan fitur keamanan pada Adobe Acrobat dan keberhasilan sejumlah pihak untuk mengatasi restriksi yang diberikan pada dokumen pdf, mungkin sebaiknya metode yang diimplementasikan untuk fitur keamanan tersebut diganti. Misalnya dengan menggunakan *Certificateless Public Key Cryptography* (CL-PKC). Metode ini diusulkan karenamenurut sejumlah penelitian level keamanan CL-PKC ini lebih tinggi dari penggunaan PKI. Disamping itu, metode ini tidak membutuhkan sertifikat (*digital ID*) yang diterbitkan otoritas tertentu. Tidak dibutuhkannya sertifikat ini tentu saja menyederhanakan proses penggunaan fitur keamanan tersebut.

DAFTAR REFERENSI

[1] Adobe System Incorporated “A primer on electronic document security, How document control and digital signatures protect electronic documents”, 2004.

[2] Adobe System Incorporated, “Acrobat Digital Signature Overview“,2001.

[3] Adobe System Incorporated ,“Adobe PDF Security Guide”, 2005.

[4] Adobe System Incorporated, “Sample signatures for use with Acrobat Digital Signature plug-ins”, 2005.

[5] Blanchette. Jean-Francois, “The Digital Signature Dilemma”, Annales des Terecommunications, 2006.

[6] Munir. Rinaldi, “Diktat Kuliah IF5054 Kriptigrafi”, STEI-ITB, Bandung, Indonesia 2006.