

# Analisis Penerapan *Digital Signature* Sebagai Pengamanan Pada Fitur *Workflow* - *DMS* (*Document Management System*)

Lyc0 Adhy Purwoko / 13508027  
Program Studi Teknik Informatika  
Sekolah Teknik Elektro dan Informatika  
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia  
lf18027@students.if.itb.ac.id

**Abstract** – transformasi pengelolaan dokumen atau data dan informasi secara manual berubah seiring dengan perkembangan teknologi informasi, dikenallah era digitalisasi. Pengelolaan dokumen yang sebelumnya berwujudkan bentuk fisik yang memiliki dimensi tertentu, sekarang hanya berupa sebuah data digital yang bentuk fisiknya tidak dapat dilihat secara kasat mata. Perkembangan isu pengelolaan dokumen digital inipun langsung merambah begitu pesat, baik di dunia bisnis maupun di dunia korporasi pemerintahan. Dengan karakteriknya, dokumen digital memiliki beberapa keunggulan dibandingkan pengelolaan dokumen fisik. Namun, dengan perkembangan pesat tersebut terdapat pula ancaman celah keamanan yang dapat dimanfaatkan oleh orang tak bertanggung jawab. Muncullah sebuah metode yang mampu mengenali untuk melakukan proses autentifikasi. Proses tersebut dilakukan untuk melakukan pengecekan status keaslian dari dokumen digital tersebut. Metode tersebut adalah *digital signature*. Pada pengimplementasiannya, *digital signature* ini menerapkan beberapa algoritma untuk meningkatkan keamanan proses autentifikasi. Pada makalah ini akan dibahas secara detail konsep dari pengelolaan dokumen digital saat ini (*Document Management System*) serta salah satu proses fatal (*workflow*) yang perlu dilakukan pengamanan berupa proses autentifikasi untuk mencegah adanya kegiatan yang tidak dapat dipertanggung jawabkan dan dapat memberikan dampak negatif lainnya.

**Key word** : *digital signature, document managemen system, workflow, rsa, sha*

## 1. PENDAHULUAN

Perkembangan dan kemajuan teknologi saat ini begitu berkembang sangat pesat dan cepat. Berbagai dampak ditimbulkan oleh perkembangan dunia teknologi informasi ini. Perubahan yang terjadi pun terjadi di berbagai aspek kehidupan manusia dalam menjalankan kegiatan sehari-harinya. Perkembangan ini memunculkan era baru yaitu era digitalisasi.

Data-data ataupun dokumen yang sebelumnya mempunyai bentuk fisik dengan dimensi tertentu mengalami tranformasi bentuk menjadi sebuah data digital yang tersimpan dalam sebuah repository tertentu.

Berbagai organisasi perusahaan atau lembaga pemerintahan adalah entitas yang terkena dampak begitu besar atas perkembangan era digitalisasi ini. Entitas-entitas tersebut sangat erat kaitannya dengan pengelolaan dan pengaturan data dan dokumen dalam keberjalanannya. Perkembangan teknologi informasi yang begitu pesat menuntut organisasi tersebut mampu beradaptasi akan perkembangan teknologi agar dapat memanfaatkannya, sehingga pengelolaan dan pengaturan dokumen pun dapat dilakukan lebih efektif dan efisien. Teknologi untuk pengelolaan dan pengaturan dokumen seiring disebut *Document Management System (DMS)*.

Namun dalam keberjalanannya, penerapan teknologi DMS dengan tujuan untuk mempermudah pengelolaan dokumen bukan berarti tidak memiliki celah kelemahan dan keamanan. Salah satu fitur dari sebuah DMS yang menonjol adalah fitur *workflow* yang mampu mengatur dan melakukan pemantauan terhadap dokumen yang berputar dalam sebuah organisasi dengan alur kepentingan tertentu. Pada proses tersebut terdapat sebuah mekanisme *approval* yang memiliki peranan penting dalam keberjalanan *workflow* secara menyeluruh. Terdapat beberapa ancaman serangan keamanan yang dapat memberikan dampak negatif bagi organisasi tersebut.

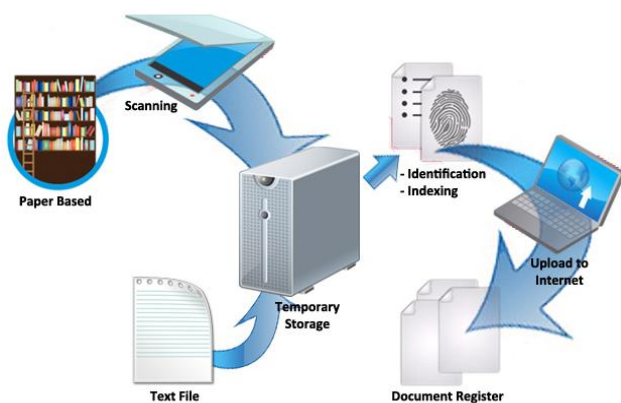
## 2. LANDASAN TEORI dan STUDI KASUS

### 2.1. *Document Management System*

*Document Managemen System* atau sistem manajemen dokuman adalah proses

pengorganisasian segala bentuk dokumen dalam bentuk digital mulai dari transformasi bentuk dokumen, pengelolaan, hingga penyimpanan atau pengarsipan. DMS melakukan penyimpanan versi elektronik dari semua dokumen baik yang sebelumnya berupa bentuk fisik maupun yang sudah dalam bentuk digital. Dokumen berupa bentuk fisik akan dilakukan penyalinan melalui proses scan. Setelah itu dokumen diatur untuk disimpan dalam sistem file atau folder dengan tujuan untuk memudahkan dalam pengelolaan file dan pencarian dokumen apabila sewaktu-waktu dibutuhkan oleh user.

Manajemen dokumen merupakan nama yang merepresentasikan beragam solusi yang terkait dengan efisiensi pengelolaan dokumen di dalam organisasi. Melalui penerapan DMS dalam sebuah institusi baik perusahaan maupun organisasi atau lembaga pemerintahan mampu mendidik organisasi tentang manajemen pengorganisasian yang baik, efektif, dan efisien. Secara teknis memanfaatkan repository terpusat sebagai media penyimpanan dokumen-dokumen yang ada mampu untuk memudahkan pengelolaan dan pembacaan dokumen tersebut tanpa terbatas oleh waktu dan tempat tertentu. Secara garis besar, mekanisme dari DMS dapat dilihat pada gambar 1.



gambar 1: Skema Proses DMS

Dilihat dari aspek manfaat yang mampu diberikan oleh DMS, diantaranya adalah:

- Mampu meningkatkan produktivitas proses bisnis, khususnya yang berhubungan dengan pengelolaan dokumen baik penyimpanan maupun pencarian dokumen.
- Dapat mempercepat *response time* dari proses

bisnis suatu organisasi.

- Dengan pengelolaan secara digital, mampu mengurangi total biaya dokumen dan meningkatkan efisiensi ruang penyimpanan.
- Mengurangi resiko kerusakan ataupun kehilangan dokumen.
- Berbagi dokumen secara mudah, efektif, dan efisien.
- Mekanisme keamanan dokumen yang lebih dapat diandalkan.
- Dapat memudahkan dalam mengontrol keberjalanan *workflow* suatu dokumen.

### 2.1.1. Fitur Utama DMS

Dalam penerapannya, DMS memiliki fitur-fitur standart atau utama untuk menjalankan mekanisme pengelolaan dokumen digital. Fitur-fitur utama dari DMS, diantaranya adalah:

- Penyimpanan dokumen, melakukan penyimpanan dokumen ke dalam repository terpusat (database server). Jenis dokumen yang dapat disimpan pada dasarnya terdapat dua jenis dokumen, yaitu dokumen yang berasal dari dokumen fisik (paper-based) dan dokumen non-fisik dengan tipe dokumen tertentu.
- Metadata dokumen, melakukan identifikasi dan penyimpanan data utama dari sebuah dokumen.
- Versioning dan indexing, identitas unik untuk memudahkan dan mempercepat dalam melakukan pencarian suatu dokumen.
- *Document sharing*, berbagi hak akses sebuah dokumen yang dapat diakses oleh beberapa user dari tempat yang berbeda.
- Pengaturan dokumen, melakukan pengelolaan dokumen dengan pengelompokan dokumen sesuai dengan kategori-kategori yang didefinisikan sebelumnya.
- Pencarian dokumen (*searching*), melakukan pencarian dokumen untuk dilihat kembali (retrieve) sesuai hak akses. Dan pencarian tidak hanya terbatas dari metadata-nya saja, tetapi pencarian sampai ke dalam isi file teks. Dikembangkan pula untuk metode pencarian dengan kata dasar (*stemming*).

### 2.1.2. Fitur Workflow

Salah satu pengembangan yang menarik dari konsep DMS adalah mekanisme *workflow*. Fitur ini memberikan kesempatan kepada user untuk membuat *workflow* suatu pendistribusian atau persetujuan suatu dokumen yang mengalir dari beberapa bagian atau bidang yang sesuai dengan

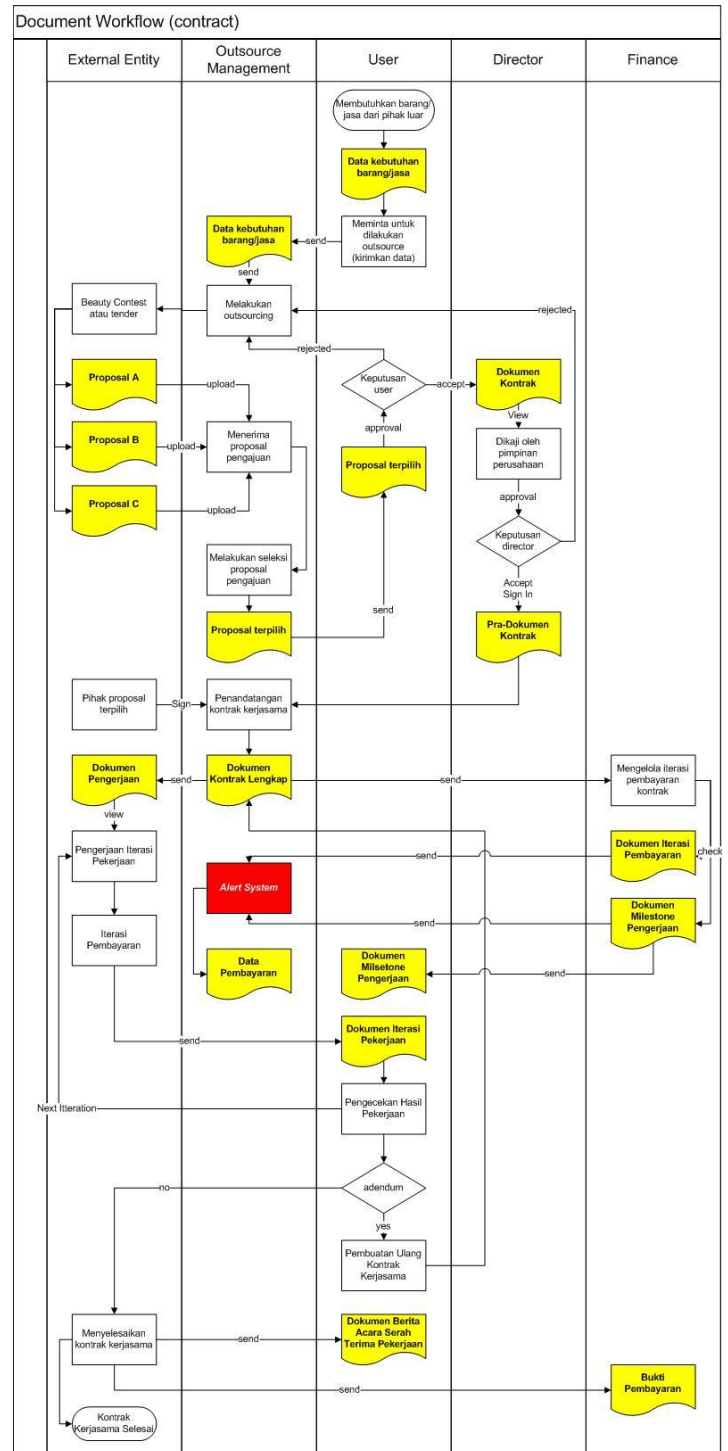
flow atau alur dokumen yang telah didefinisikan oleh user sebelumnya. Masing-masing bidang atau bagian mempunyai hak akses sistem yang berbeda pula sesuai dengan pendefinisian alur sistem sebelumnya. Kasus *workflow* yang ada pun bermacam-macam tergantung kebutuhan dari user itu sendiri.

Dalam makalah ini akan dibahas lebih lanjut dan detail pada fitur *workflow*. Pendefinisian *workflow* pada makalah ini digambarkan dalam sebuah studi kasus *workflow* tertentu yaitu aliran pengelolaan suatu dokumen kontrak dalam proses outsourcing project sebuah perusahaan. Pada aliran kerja di sini melibatkan empat stakeholder atau aktor yaitu entitas luar, outsource management, user, director, dan finance management. Pada awal mula muncul kebutuhan dari user (bagian/divisi tertentu dari perusahaan tersebut) yang membutuhkan barang/jasa dari pihak luar (proyek kerjasama).

Data awal dibuat dan di-upload ke sistem oleh pihak user yang kemudian disampaikan ke pihak outsource management (view document) untuk dilakukan proses outsourcing. Beberapa pihak luar akan mengirimkan (upload ke dalam sistem) proposal pengajuan yang akan diseleksi oleh pihak outsource management. Proposal yang terpilih akan dikirimkan (send document) via sistem ke pihak user untuk di-review (view document) apakah diterima atau ditolak, bila diterima (accept document via sistem) proposal pengajuan akan dikirim ke pimpinan perusahaan untuk di-review dan disetujui atau tidaknya pengajuan proyek tersebut. Setelah disetujui oleh pimpinan perusahaan (approval document via sistem), dokumen kontrak dibuat dan ditandatangani bersama oleh pihak pengelola proyek dengan outsource management (dokumen kontrak di-upload ke sistem).

Kontrak telah disetujui dengan tahap iterasi pengerjaan dan pembayaran yang sudah disepakati bersama (pihak luar dan user dapat melihat dokumen iterasi yang telah disepakati via sistem). Pengecekan dokumen pembayaran akan diawasi oleh pihak finance management dan pengecekan dokumen hasil pekerjaan akan di-review oleh user. Setiap review iterasi pekerjaan, user akan memberikan keputusan, apabila berjalan lancar pekerjaan dilanjutkan tetapi apabila ada masalah atau perubahan akan dilakukan addendum (perubahan isi dokumen kontrak kerjasama). Hal

tersebut akan terus ter-iterasi hingga pekerjaan proyek selesai sesuai kesepakatan. Sistem juga akan memberikan peringatan kepada user apabila sudah jatuh tempo iterasi pengerjaan ataupun pembayaran. Setelah hasil pekerjaan selesai, pihak luar akan mengirimkan (upload) dokumen berita acara serah terima pekerjaan dan bukti pembayaran. Proses keseluruhan ini dapat dilihat pada ilustrasi gambar 2.



gambar 2: contoh *workflow* dokumen kontrak

## 2.2. Digital Signature

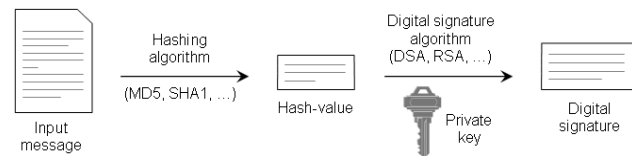
*Digital signature* atau tanda tangan digital merupakan sebuah skema matematis untuk melakukan proses autentifikasi dari suatu pesan atau dokumen digital. Dilihat dari arti harfiahnya, tanda tangan digital bukan berarti tanda tangan seseorang yang dilakukan proses digitalisasi dengan sebuah alat scanner tertentu untuk menjadi sebuah tanda tangan digital pada dokumen digital. *Digital signature* ini merupakan sebuah nilai kriptografis yang bergantung pada pesan dan pengirim pesan. Secara umum, teknis yang digunakan dalam membentuk sebuah tanda tangan digital adalah dengan memanfaatkan kombinasi antara algoritma fungsi *hash* dengan algoritma kriptografi kunci publik.

Implementasi dari metode teknologi tanda tangan digital ini adalah dengan memanfaatkan algoritma kunci publik. Sepasang kunci publik-privat dibuat untuk keperluan seseorang. Kunci privat disimpan oleh pemiliknya, dan dipergunakan untuk membuat tanda tangan digital, sedangkan kunci publik doberikan atau diserahkan kepada siapa saja yang ingin memeriksa tanda tangan digital yang bersangkutan pada suatu dokumen.

Sebuah tanda tangan atau *signature* mempunyai karakteristik khusus sebagai berikut:

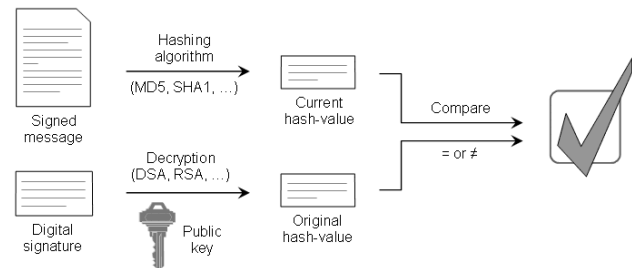
- Tanda tangan merupakan sebuah bukti otentik, sehingga tidak bisa/sulit ditulis/ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti, sehingga penandatanganan tak bisa menyangkal bahwa dulu ia tidak pernah menandatangani.
- Tanda tangan merupakan sebuah hal yang sukar untuk dilupakan oleh pemiliknya.
- Tanda tangan tidak dapat dipindahkan begitu saja untuk digunakan kembali.
- Dapat diperiksa dengan mudah, termasuk oleh pihak-pihak yang belum pernah bertatap muka langsung dengan penandatanganan
- Sebagai tanda otentik sebuah dokumen, dokumen yang telah ditanda tangani tidak dapat dilakukan perubahan.
- Tanda tangan tidak dapat disangkal akan keberadaan dan keunikannya masing-masing.

Pada gambar 3 berikut ini merupakan ilustrasi proses penyisipan tanda tangan digital ke dalam suatu pesan atau dokumen tertentu.



gambar 3: Penyisipan tanda tangan digital

sedangkan dalam proses autentifikasi suatu pesan atau dokumen yang memiliki tanda tangan digital digambarkan pada langkah yang diilustrasikan pada gambar 4.



gambar 4: Proses autentifikasi *digital signature*

### 2.2.1. Algoritma RSA

Algoritma RSA merupakan sebuah algoritma dengan karakteristik kunci public yang paling terkenal dari segi keamanannya, sehingga algoritma ini paling sering untuk diaplikasikan dalam beberapa kasus keamanan. Keunikan dari algoritma RSA adalah tingginya tingkat keamanan algoritma karena sukarnya memfaktorkan bilangan yang besar menjadi faktor-faktor yang prima. Algoritma ini ditemukan oleh Ron Rivest, Adi Shamir, dan Len Adleman pada tahun 1976, ketiganya merupakan peneliti dari MIT (*Massachusetts Institute of Technology*)

Algoritma RSA memiliki beberapa property yang digunakan untuk proses enkripsinya, yaitu sebagai berikut

1.  $p$  dan  $q$  bilangan prima (rahasia)
  2.  $n = p \cdot q$  (tidak rahasia)
  3.  $\phi(n) = (p - 1)(q - 1)$  (rahasia)
  4.  $e$  (kunci enkripsi) (tidak rahasia)
- Syarat:  $PBB(e, \phi(n)) = 1$
5.  $d$  (kunci dekripsi) (rahasia)
  6.  $d$  dihitung dari  $d \equiv e^{-1} \pmod{\phi(n)}$
  7.  $m$  (plainteks) (rahasia)
  8.  $c$  (cipherteks) (tidak rahasia)

### 2.2.2. Algoritma SHA

SHA merupakan algoritma *hash* satu arah yang dibuat oleh NIST dan digunakan bersama DSS (*Digital Signature Standards*). Algoritma *SHA*

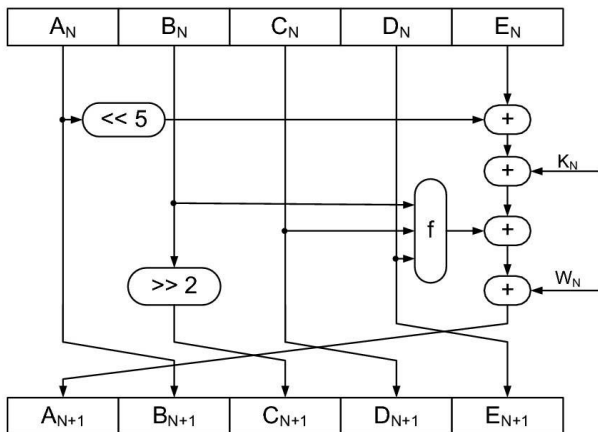
menerima masukan berupa pesan dengan ukuran maksimum 264 bit (2.147.483.648 *gigabyte*) dan menghasilkan *message digest* yang panjangnya 160 bit, lebih panjang dari *message digest* yang dihasilkan oleh MD5.

Enam varian dari SHA yaitu SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, dan SHA-512. Adapun SHA-0 sering diacu sebagai SHA saja. Pada gambar 5 menunjukkan perbandingan karakteristik dari SHA\_0, SHA-1, dan SHA-2.

|       | Output size (bits) | Internal state size (bits) | Block size (bits) | Max message size (bits) | Word size (bits) | Rounds | Operations           | Collision found?                               |    |
|-------|--------------------|----------------------------|-------------------|-------------------------|------------------|--------|----------------------|--|----|
| SHA-0 |                    |                            |                   |                         |                  |        |                      | Yes  |    |
| SHA-1 | 160                | 160                        | 512               | $2^{64} - 1$            | 32               | 80     | +, and, or, xor, rot | Theoretical attack ( $2^{51}$ ) <sup>[2]</sup> |    |
| SHA-2 | SHA-256/224        | 256/224                    | 256               | 512                     | $2^{64} - 1$     | 32     | 64                   | +, and, or, xor, shr, rot                      | No |
|       | SHA-512/384        | 512/384                    | 512               | 1024                    | $2^{128} - 1$    | 64     | 80                   |  |    |

gambar 5: Perbandingan beberapa algoritma SHA

Pada gambar 6 menggambarkan skema proses operasi pada algoritma SHA-1.



gambar 6: Skema proses SHA-1

### 3. ANALISIS

#### 3.1. Ancaman Serangan Keamanan

Berdasarkan hasil analisis penulis terhadap ancaman keamanan pada proses *approval workflow* ini adalah kemungkinan perubahan atau pemalsuan hasil keputusan *approval* yang mungkin berbeda dengan hasil keputusan sebenarnya dan kemungkinan munculnya pihak yang tidak bertanggung jawab untuk mengeluarkan hasil keputusan *approval* yang tidak dapat dipertanggung

jawabkan dan dapat menimbulkan dampak negative secara keseluruhan terhadap proses *workflow* dokumen dari hulu hingga hilir.

#### 3.2. Digital Signature pada workflow-DMS

Dalam konsep DMS khususnya pada fitur *workflow* yang sudah dijelaskan secara medetail pada bahasan sebelumnya, kunci keberhasilan akan proses *workflow* tersebut terletak pada mekanisme *approval* dari suatu actor terhadap actor lainnya.

Pada studi kasus *workflow* dokumen kontrak yang diapaparkan sebelumnya, serta ancaman-ancaman yang dapat terjadi pada proses *approval* ini, maka dibutuhkan sebuah sistem yang mampu menjami bahwa *approval* yang dilakukan dalam suatu tahap memang berasal dari stakeholder terkait yang memang bertanggung jawa terhadap keputusan tersebut serta sebagai bukti atas keputusan yang telah dibuat. Status dari hasil mekanisme *approval* yang bersifat *confidential* menuntut agar hasil tersebut bukan sebagai konsumsi umum, sehingga dapat terjamin keamanan atau kerahasiaan hasil keputusan beserta penjaminan bahwa hasil keputusan tersebut berasal dari stakeholder terkait dan mampu dipertanggung jawabkan. Hal tersebut untuk mencegah timbulnya kecurangan dan permainan birokrasi pada pengelolaan *workflow* dokumen digital.

*Digital signature* dapat diterapkan pada mekanisme *approval* proses *workflow* dokumen digital untuk meningkatkan keamanan isi hasil *approval* (*confidentiality*) serta menjamin sumber hasil keputusan *approval* tersebut memang benar-benar berasal dari pihak yang berwenang dan mampu dipertanggung jawabkan, sehingga secara keseluruhan dapat dilakukan untuk mengotentifikasi hasil *approval workflow* dokumen tersebut.

Secara teknis, pengimplementasian *digital signature* pada proses *approval workflow* dokumen dapat dijelaskan sebagai berikut. Dapat dimisalkan A adalah hasil keputusan atau *approval* yang dikeluarkan oleh salah satu stakeholder untuk diberikan ke stakeholder berikutnya. Hasil *approval* A ditandatangani menjadi sebuah hasil keputusan terenkripsi S dengan menggunakan kunci privat yang dimiliki oleh stakeholder pemberi keputusan *approval* (SK)

$$S = \text{Esk}(A)$$

Dalam hal ini E adalah algoritma enkripsi dari algoritma kunci public. Selanjutnya S dikirim melalui fitur *workflow*. Aspek hasil keputusan yang melekat pada dokumen didapatkan karena sudah dienkripsi terlebih dahulu sebelum dikirimkan. Hal ini dapat memastikan informasi hasil keputusan *approval* tidak dapat diketahui oleh siapapun kecuali orang yang berwenang terhadap *approval* tersebut. Sementara aspek otentifikasi dari hasil keputusan *approval* tersebut dapat dijelaskan pada penjabaran sebagai berikut:

1. Apabila hasil keputusan *approval* yang diterima oleh stakeholder berikutnya sudah dipalsukan atau ditambahkan, maka  $AD'$  yang dihasilkan dari fungsi hash berbeda dengan  $AD$  (*Approval Digest*) semula.
2. Apabila hasil keputusan *approval* tidak berasal dari stakeholder sebelumnya yang berwenang terhadap pembuat keputusan tersebut maka *Approval Digest (AD)* yang dihasilkan sebelumnya berbeda dengan  $AD'$  yang dihasilkan dari proses verifikasi.
3. Apabila  $AD = AD'$ , menunjukkan bahwa hasil keputusan *approval* yang diterima oleh stakeholder berikutnya merupakan hasil keputusan *approval* yang asli dan stakeholder berwenang sebelumnya yang membuat hasil keputusan *approval* tersebut adalah stakeholder berwenang yang sebenarnya.

### KESIMPULAN

Berdasarkan hasil analisis yang dilakukan oleh penulis, dapat diambil beberapa kesimpulan sebagai berikut:

1. Penerapan dan pengimplementasian *digital signature* pada proses *approval workflow* sebuah dokumen dapat meningkatkan keamanan dokumen yang dikirimkan dari satu stakeholder ke stakeholder berikutnya.
2. Proteksi terhadap pengelolaan sebuah dokumen digital dapat dilakukan secara digital pula, sehingga relatif lebih aman dan mudah dalam penggunaannya.
3. Penggunaan *digital signature* juga dapat menghindari tindak kriminal yang dapat dilakukan oleh pihak-pihak yang tidak bertanggung jawab.

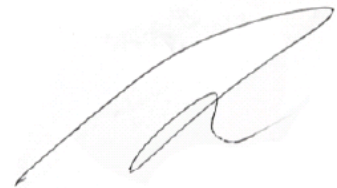
### REFERENCES

- Archscan LLC, "Electronic Document Management System", 143 Brightwater Drive Annapolis, MD 21401.  
Slide IF 3058, Kriptografi, Rinaldi Munir  
<http://www.informatika.org/~rinaldi/Kriptografi/kriptografi.htm> (waktu akses: 9 Mei 2012)

### PERNYATAAN

Dengan ini penulis menyatakan bahwa makalah yang penulis tulis ini adalah tulisan penulis sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 13 Mei 2012



Lyco Adhy Purwoko – 13508027