PENERAPAN DIGITAL SIGNATURE UNTUK VALIDASI SURAT BERHARGA DIGITAL DAN NON DIGITAL

Okharyadi Saputra (13510072)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
okharyadi@gmail.com

***Abstrak*—Surat berharga seperti akte kelahiran, ijazah, dan berbagai surat lainnya merupakan sebuah surat yang sangat penting untuk diketahui kevalidan dan akurasinya. Sebuah surat berharga seperti ijazah sering dianggap sebagai sebuah modal yang sangat penting. Sayangnya, seperti yang kita ketahui saat ini, banyak beredar surat berharga palsu, seperti ijazah palsu dan KTP palsu. Maraknya proses pemalsuan surat berharga mungkin dipicu salah satunya oleh sulitnya proses validasi kebenaran surat berharga yang harus dilakukan oleh golongan yang berkepentingan. Hingga saat ini, proses valdasi surat berharga masih dilakukan secara manual, dimana pengecekan harus dilakukan dengan membandingkan surat berharga dengan arsip yang dimiliki oleh penerbit surat tersebut secara langsung. Proses ini tentu saja membutuhkan banyak waktu dan biaya, terutama jika penerbit surat berada di tempat yang jauh. Terkadang proses validasi juga sulit dilakukan karena arsip yang dibutuhkan sering kali sudah hilang atau rusak karena termakan usia. Dengan perkembangan teknologi informasi, sebenarnya hal ini dapat diperbaiki. Dalam tulisan ini penulis mencoba untuk menerapkan konsep *digital signature* untuk proses validasi surat berharga.**

***Kata Kunci*—Surat berharga, pemalsuan, validasi, digital signature**

I. PENDAHULUAN

Surat berharga, seperti ijazah, akte kelahiran, akte tanah dan berbagai jenis surat lainnya merupakan sebuah surat yang sangat penting untuk diketahui akurasi dan validasi datanya. Seperti yang kita ketahui, saat ini banyak terjadi kasus yang terkait dengan pemalsuan data dalam surat berharga, seperti ijazah palsu, akte palsu ataupun KTP palsu.

Untuk dapat memeriksa validasi dari suatu surat berharga, dibutuhkan pengecekan secara manual dengan membandingkan berkas asli serta arsip yang dimiliki oleh lembaga penerbit surat berharga tersebut. Sayangnya metode tersebut dinilai tidak efektif dan efisien karena dibutuhkan *effort* yang cukup besar untuk melakukan penyocokan data secara fisik tersebut. Selain itu, seiring dengan bertambahnya jumlah arsip yang harus disimpan, menyebabkan semakin sulit dilakukannya pengelolaan data dan semakin berdampak kepada ketidak efektif dan efisienan. Seperti yang kita ketahui sering terjadi kasus dimana arsip yang disimpan oleh lembaga penerbit surat berharga tersebut hilang ataupun rusak, sehingga ketika seseorang ingin melakukan validasi surat hal tersebut menjadi sulit untuk dilakukan, bahkan mungkin menjadi tidak dapat dilakukan.

Dalam proposal ini penulis mengajukan usul untuk melakukan penerapan *digital signature* pada surat berharga baik dalam bentuk digital ataupun non digital. Dengan mekanisme ini, setiap surat berharga yang diterbitkan oleh setiap lembaga akan diberi *digital signature*. Setiap *digital signature* yang diterbitkan akan disimpan dalam suatu sistem terpusat. Hal ini memungkinkan dilakukannya pengecekan/validasi surat tanpa perlu dilakukannya pengecekan secara fisik. Selain itu, karena data yang perlu disimpan cukuplah *digital signature*-nya, maka hal tersebut akan membuat penyimpanan data menjadi jauh lebih efektif dan efisien serta tidak memakan tempat. Dengan adanya sistem terpusat, hal ini akan menyebabkan autentikasi data dapat dilakukan dimana saja dan kapan saja, tanpa ada biaya tambahan untuk ongkos secara fisik.

Diharapkan dengan mekanisme seperti ini, pengecekan untuk validasi suatu surat berharga dapat dilakukan dengan lebih mudah serta tidak membutuhkan media penyimpanan yang besar untuk menyimpan seluruh arsip yang ada.

II. SURAT BERHARGA

Surat berharga adalah surat yang memiliki nilai dan makna lebih. Surat berharga dikaitkan sebagai sebuah surat atau berkas formal yang dikeluarkan secara resmi dari suatu lembaga yang berwenang. Surat berharga yang diakui di Indonesia ada berbagai macam jenis, seperti KTP, akte kelahiran, ijazah, dan berbagai surat lainnya.

Kevalidan dan akurasi dari suatu surat berharga sangatlah penting, karena sering kali sebuah surat berharga digunakan sebagai acuan formal dalam berbagai kegiatan atau tindakan yang dilakukan. Misalkan saja seperti penggunaan passport untuk proses izin masuk ke dalam suatu negara atau penggunaan ijazah untuk proses pelamaran kerja atau melanjutkan ke jenjang pendidikan yang lebih tinggi.


PENCATATAN SIPIL
(WARGA NEGARA INDONESIA)
KUTIPAN
AKTA KELAHIRAN

Gambar 1
Contoh Surat Berharga

Saat ini banyak terjadi kasus pemalsuan surat berharga, terutama ijazah. Hal ini dikarenakan banyak pihak yang tidak bertanggung jawab yang lebih memilih untuk menggunakan jalan pintas. Proses pembuatan ijazah palsu dapat dilakukan dengan sangat mudah, hanya bermodalkan beberapa ratus ribu rupiah saja, seseorang dapat memperoleh sebuah ijazah palsu seperti yang diinginkannya.

Seperti yang sudah dibahas sebelumnya, saat ini satu-satunya cara untuk melakukan validasi kebenaran dari suatu surat berharga hanya dapat dilakukan dengan proses validasi secara manual, dimana proses pencocokan surat berharga dilakukan dengan dibandingkan dengan arsip dari surat berharga yang ada. Sayangnya metode ini sangatlah tidak efisien serta memakan banyak biaya, termasuk biaya untuk menyimpan dan merawat arsip yang ada yang semakin hari akan semakin menumpuk.

III. DIGITAL SIGNATURE

Salah satu konsep yang ada di kriptografi adalah konsep *digital signature*. *Digital signature* adalah tanda tangan digital yang diberikan kepada suatu dokumen digital. *Digital signature* ini dibuat dengan menggunakan suatu algoritma khusus.

Pembubuhan *digital signature* ke sebuah data digital dapat berguna untuk melakukan validasi terhadap data tersebut karena sifat dari *digital signature* itu sendiri. Misalkan saja jika sebuah email dibubuhi dengan *digital signature*, maka sebenarnya *digital signature* itu diperoleh berdasarkan konten atau isi dari email itu tersendiri. Jika ada perubahan dari isi email, walau hanya satu karakter, akan berakibat proses validasi *digital signature* menjadi tidak berhasil alias gagal.

Sifat dari *digital signature* ini dapat dimanfaatkan untuk melakukan proses validasi surat berharga, tentunya dengan mekanisme yang disesuaikan.

Dalam implementasi kali ini, penulis menggunakan algoritma yang telah penulis gunakan dalam tugas besar sebelumnya. Implementasi *digital signature* dilakukan dengan menggunakan algoritma El Gamal serta SHA-256. Proses pembentukan *digital signature* akan dilakukan dengan mengecek nilai SHA dari suatu *plain teks* lalu kemudia nilai tersebut dienkripsi dengan menggunakan algoritma El Gamal. Proses enkripsi tersebut dilakukan dengan menggunakan kunci publik. Hasil dari enkripsi ini adalah *digital siganture* yang akan digunakan.

IV. PERANCANGAN DAN IMPLEMENTASI SISTEM

Sistem yang penulis kembangkan ini dibuat dengan menggunakan bahasa pemrograman PHP dan JAVA. Sistem ini dikembangkan dengan menggunakan webapp, sehingga dapat diakses dengan mudah dimana saja. Berikut konsep desain sistem yang penulis lakukan:

1. Prosedur Pendaftaran Lembaga

   Seperti yang diketahui, setiap surat berharga tentu saja diterbitkan oleh sebuah lembaga resmi yang diakui. Semakin tinggi nilai dari surat berharga tersebut, cenderung semakin tinggi juga lembaga yang menerbitkannya.

   Agar proses validasi terhadap suatu surat berharga dapat dilakukan, terlebih dahulu perlu dilakukan pendaftaran terhadap lembaga terkait yang akan menerbitkan surat berharga tersebut. Dengan kata lain, setiap lembaga yang ingin melibatkan diri dengan sistem ini haruslah melakukan pendaftaran melalui sistem.

   Dalam prosedur pendaftaran, lembaga yang terkait haruslah memasukkan berbagai data sebagai berikut:

   a. Nama Lembaga
      Merupakan data berupa nama resmi dari lembaga tersebut. Dalam satu sistem tidak dimungkinkan terdapat dua akun lembaga yang sama.
   b. Lokasi Lembaga
      Merupakan data berupa lokasi resmi lembaga tersebut.
   c. Contact Person Lembaga
      Merupakan data berupa penanggung jawab yang mewakili lembaga tersebut.
   d. Surat Berharga yang Diterbitkan
      Merupakan data berupa surat berharga apa saja yang diterbitkan oleh lembaga tersebut, seperti ijazah, akte, dan sebagainya.

   Segala data yang diberikan tersebut selanjutnya akan dicatat ke dalam sistem. Selain itu, setiap lembaga yang mendaftar ke dalam sistem akan mendapatkan sebuah kode khusus. Kode ini penulis sebut dengan kode lembaga. Kode lembaga ini akan dijadikan kode unik yang membedakan setiap lembaga yang ada.

   Misalkan sebuah lembaga A memiliki kode U-001 dan lembaga B memperoleh kode U-002. Kedua kode ini akan digunakan untuk melakukan identifikasi setiap lembaga. Selain itu, kode lembaga ini juga akan digunakan selama proses pembentukan surat berharga, proses pembentukan *digital signature* serta proses validasi dari suatu surat berharga.

Gambar 2
Tampilan Proses Pendaftaran Lembaga

2. Prosedur Penerbitan Surat Berharga

Setiap kali suatu lembaga yang telah mendaftarkan diri kedalam sistem ini ingin menerbitkan suatu surat berharga, terdapat sebuah prosedur yang harus dipatuhi oleh lembaga tersebut agar dapat diperoleh manfaat dari sistem ini.

Ketika suatu lembaga ingin menerbitkan sebuah surat berharga, tentu saja ada beberapa data yang pasti akan dicatat. Oleh karena itu, setiap kali dilakukan penerbitan surat berharga oleh suatu lembaga, terdapat beberapa data yang harus diberikan sebagai berikut:

a. Nomor Surat
   Merupakan nomor resmi dari surat berharga yang diterbitkan.
b. Jenis Surat
   Merupakan jenis dari surat berharga. Berupa pilihan berdasarkan data jenis surat berharga yang diberikan pada saat registrasi lembaga.
c. Nama Penerima Surat
   Merupakan nama lengkap dari penerima surat berharga.
d. Tanggal Penerbitan Surat
   Merupakan tangga dari penerbitan surat berharga.
e. Petugas Bertanggung Jawab
   Merupakan nama dari petugas yang bertanggung jawab ataupun menandatangani surat berharga tersebut.
f. Scan Surat
   Merupakan scan digital dari surat berharga yang diterbitkan.

Keseluruhan data tersebut diinputkan ke dalam sistem untuk selanjutnya dilakukan proses pembubuhan *digital signature*. *Digital signature* yang akan diberikan ke dalam surat berharga tersebut dihasilkan dengan menggunakan *plain teks* berupa nama penerima surat, jenis surat, tanggal penerbitan surat dan petugas yang bertanggung jawab serta kode lembaga penerbit surat tersebut.

Misalkan saja dapat diamati dalam contoh seperti berikut:

Nama Lembaga : Institut Teknologi Bandung
Kode Lembaga : U-001
Jenis Surat : Ijazah
Nomor Surat : ARS-PF-001-2013
Nama Penerima : Okharyadi Saputra
Tanggal Penerbitan : 14 Mei 2013
Petugas : Indra Wijoyo

Maka *plain text* yang akan digunakan untuk proses pembentukan *digital signature* adalah sebagai berikut:

"Institut Teknologi Bandung"-"U-001"-"Ijazah"-"ARS-PF-001-2013"-"Okharyadi Saputra"-"14 Mei 2013"-"Indra Wijoyo"

Proses pembentukan *digital signature* ini dilakukan secara otomatis dengan menggunakan kunci publik yang dimiliki oleh lembaga tersebut. Kunci publik dan kunci privat diperoleh lembaga ketika melakukan proses registrasi/pendaftaran lembaga ke dalam sistem.

Kunci privat dan kunci publik dari suatu lembaga dapat dilihat oleh siapapun yang menggunakan sistem. Hal ini dimaksudkan agar setiap pihak yang berkepentingan untuk melakukan validasi terhadap suatu surat berharga dapat langsung melakukannya dengan menggunakan kunci privat dan kunci publik dari lembaga penerbit surat berharga tersebut.

Gambar 3
Tampilan Proses Peneribitan Surat Berharga

Proses dekripsi haruslah dilakukan untuk melakukan proses validasi surat berharga. Setiap pihak yang ingin melakukan validasi suatu surat berharga haruslah menginputkan kunci publik dan kunci privat dari lembaga tersebut yang dapat diperoleh melalui halaman profil lembaga.

3. Prosedur Validasi Surat Berharga

Ketika suatu waktu terdapat pihak yang butuh untuk melakukan validasi terhadap surat berharga tertentu, proses validasi tersebut dapat dilakukan dengan menggunakan sistem ini. Prosedur yang perlu dilakukan untuk dapat melakukan validasi

adalah sebagai berikut:

1. Pihak yang berkepentingan untuk melakukan proses validasi terlebih dahulu dapat memeriksa kunci privat dan kunci publik yang dimiliki oleh lembaga tersebut melalui halaman profil lembaga yang dapat diakses melalui sistem.

2. Pasca mendapatkan kunci privat dan kunci publik yang dibutuhkan, pihak yang butuh untuk melakukan validasi surat berharga dapat melakukan validasi dengan menginputkan data sebagai berikut:
   a. Nama Lembaga
      Merupakan nama lembaga yang tercantum dalam surat berharga.
   b. Jenis Surat
      Merupakan jenis surat yang akan divalidasi, apakah ijazah, KTP dan sebagainya.
   c. Nomor Surat
      Merupakan nomor surat yang tercantum dalam surat berharga tersebut.
   d. Nama Penerima
      Merupakan nama lengkap dari penerima surat berharga.
   e. Tanggal Penerbitan
      Merupakan tanggal penerbitan dari surat berharga yang akan divalidasi.
   f. Petugas
      Merupakan nama lengkap dari petugas yang menerbitkan surat.

Gambar 4
Tampilan Proses Validasi Surat Berharga

4. Prosedur Mendaftarkan Surat Berharga Lama
   Jika suatu lembaga ingin mendaftarkan surat berharga yang sudah lama (sudah diterbitkan dari dulu sebelum terdapat sistem), maka lembaga tersebut dapat mendaftarkan surat berharga tersebut dengan melakukan prosedur yang sama seperti dengan prosedur nomor satu.

V. UJI COBA SISTEM

Pasca proses implementasi yang telah dilakukan, selanjutnya penulis melakukan proses uji coba dengan melakukan prosedur lengkap mulai dari pendaftaran lembaga, penerbitan surat berharga, hingga proses validasi surat berharga. Berikut uji coba yang penulis lakukan beserta hasilnya:

1. Uji Coba Pendaftaran Lembaga
   Sebagai tahap awal uji coba, penulis melakukan pendaftaran terhadap sebuah lembaga baru. Lembaga yang penulis daftarkan adalah sebagai berikut:

   Nama Lembaga : Institut Teknologi Bandung
   Lokasi Lembaga : Jalan Ganesha 10 Bandung
   Contact Person : Zaenudin
   Surat Berharga : Ijazah

   Pasca proses registrasi yang dilakukan, penulis selaku lembaga akan mendapatkan dua buah kunci, yaitu kunci publik dan kunci privat serta kode lembaga. Berikut adalah data yang penulis peroleh:

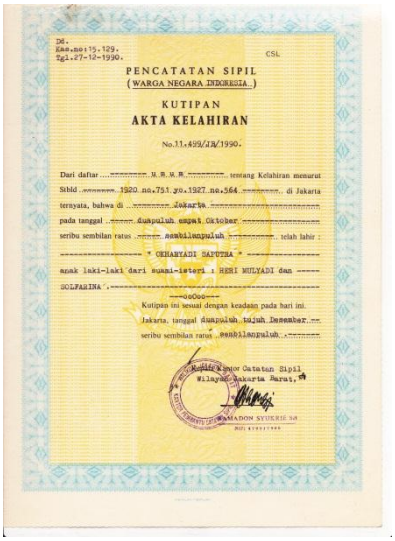
   Kode Lembaga : U-001
   Kunci Publik: 4270582D0000AAD320395923
   Kunci Privat : 4270582D00000F34

Gambar 5
Tampilan Hasil Pendaftaran Lembaga

2. Uji Coba Penerbitan Surat Berharga
   Tahap selanjutnya yang penulis lakukan adalah melakukan uji coba penerbitan sebuah surat berharga. Data yang penulis gunakan untuk uji coba kali ini adalah sebagai berikut:

   Nomor Surat : ARS-PF-001-2013
   Jenis Surat : Ijazah
   Nama Penerima : Okharyadi Saputra
   Tanggal Penerbitan : 14 Mei 2013
   Petugas : Indra Wijoyo

   Untuk scan data yang penulis masukan ke dalam sistem ini adalah file berikut:



PENCATATAN SIPIL
(WARGA NEGARA INDONESIA)

KUTIPAN
AKTA KELAHIRAN

No.11.499/DR/1990.

Gambar 6
Tampilan Surat Berharga yang Digunakan

*Keterangan : Gambar yang penulis gunakan hanyalah gambar *"dummy"* sebagai bahan uji coba.

Seluruh data tersebut oleh sistem akan dimasukkan ke dalam database dan dicatat sebagai sebuah identitas unik. Selain itu, dalam proses penyimpanan ini sistem secara otomatis akan membentuk *digital signature* untuk surat ini dengan metode yang telah penulis bahas sebelumnya.

Gambar 7
Tampilan Proses Penerbitan Surat Berharga

3. Uji Coba Validasi Surat Berharga
   Uji coba selanjutnya yang penulis lakukan adalah melakukan validasi terhadap surat berharga yang ada. Misalkan dalam uji coba kali ini penulis mencoba melakukan uji coba dengan data sebagai berikut:

   Nama Lembaga : Institut Teknologi Bandung
   Jenis Surat : Ijazah
   Nomor Surat : ARS-PF-001-2013
   Nama Penerima : Okharyadi Saputra
   Tanggal Penerbitan : 14 Mei 2013
   Petugas : Indra Wijoyo

   Kunci Publik: 4270582D0000AAD320395923
   Kunci Privat : 4270582D00000F34

   Dengan menggunakan data seperti diatas, penulis memperoleh hasil bahwa surat berharga berupa ijazah dengan data diatas merupakan sebuah surat yang valid dan benar.

   Dapat dilihat pada gambar dibawah ini, surat berharga yang valid akan menampilkan hasil seperti berikut. Pada gambar dibawah dapat dilihat sistem menampilkan *scan* asli dari surat berharga sehingga pihak yang melakukan validasi surat tersebut dapat langsung membandingkan surat yang berada ditanggannya dengan *scan* resmi dari lembaga penerbit surat.

Gambar 8
Tampilan Hasil Validasi Surat Berharga

Uji coba selanjutnya penulis mencoba melakukan perubahan terhadap data yang ada. Data yang penulis masukan adalah sebagai berikut:

Nama Lembaga : Institut Teknologi Bandung
Jenis Surat : Ijazah
Nomor Surat : ARS-PF-001-2013
Nama Penerima : Ahmad Dani
Tanggal Penerbitan : 14 Mei 2013
Petugas : Indra Wijoyo

Kunci Publik: 4270582D0000AAD320395923
Kunci Privat : 4270582D00000F34

Data diatas telah mengalami perubahan pada bagian nama. Nomor surat dan data lain yang digunakan adalah sama dengan data yang sebenarnya. Kunci publik dan kunci privat yang

digunakanpun sama.

Dengan menggunakan data tersebut, penulis memperoleh hasil bahwa surat berharga tersebut tidaklah valid dan dianggap sebagai sebuah surat berharga palsu. Ketidakvalidan surat berharga diketahui dari nilai digital signature surat tersebut yang berbeda dengan nilai digital signature dari nomor surat yang dimaksud. Ketidakvalidan juga dapat diketahui jika tidak ada satupun digital signature dalam database yang sama dengan digital signature yang dihasilkan dari inputan user dalam sistem.

Gambar 9
Hasil Validasi Surat Berharga

VI. SIMPULAN DAN SARAN

Berdasarkan hasil implementasi dan uji coba terhadap desain sistem yang telah penulis lakukan, dapat disimpulkan bahwa sistem ini berhasil diimplementasikan dengan baik. Sistem ini terbukti mampu melakukan validasi terhadap surat berharga yang telah didaftarkan ke dalam sistem. Perubahan terhadap isi surat berharga terbukti dapat dideteksi.

Dibutuhkan pengembangan lebih lanjut terhadap sistem ini, terutama untuk desain sistem yang lebih baik dan efisien untuk melakukan proses validasi.

REFERENSI

[1] Sadikin, Rifki. 2012. Kriptografi Untuk Keamanan Jaringan. Yogyakarta : Penerbit Andi

[2] Welling, Luke. 2003. *PHP and MySQL Web Development*. New York : Sams Publishing

PERNYATAAN

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

Bandung, 14 Mei 2013

Okharyadi Saputra
13510072