Implementasi Tanda Tangan Digital pada Surat Perintah Kerja

Hizbulloh Ash-Shidiqy - 13518047
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
13518047@std.stei.itb.ac.id

***Abstrak*— Surat Perintah Kerja sering digunakan sebagai surat untuk melakukan perjanjian kontrak kerja antar instansi pemberi kerja dan instansi penerima kerja. Didalamnya terdapat poin-poin yang terkait pekerjaaan yang disepakati oleh kedua belah pihak. Namun, bisa jadi suatu pihak melakukan pengubahan isi dari Surat Perintah Kerja tersebut untuk menguntungkan pihaknya. Digital Signature dapat digunakan untuk menyelesaikan masalah ini dengan layanan keamanan yang ditawarkan seperti otentikasi, keaslian pesan, dan anti-penyangkalan. Pada makalah ini, akan dibahas mengenai implementasi kriptografi kunci publik DSA dan fungsi *hash* SHA-256 sebagai digital signature pada Surat Perintah Kerja.**

***Kata Kunci*— *Surat Perintah Kerja, digital signature*, algoritma SHA-256**

I. PENDAHULUAN

Dewasa ini teknologi sudah sangat melekat pada masyarakat. Dari tua maupun muda, kaya maupun kurang mampu, semua lapisan masyarakat terpapar oleh teknologi. Terlebih pada masa pandemi seperti saat ini, teknologi semakin dibutuhkan lagi oleh masyarakat karena pertemuan secara langsung tidak disarankan kecuali sangat genting dan penting. Banyak usaha-usaha online yang laku keras dengan adanya pandemi ini, seperti konsultasi online dan lainnya. Segala hal menjadi serba online dan digital. Sistem kerja perusahaan pun banyak yang berubah secara drastis dari WFO (*Work From Office*) menjadi WFH (*Work From Home*). Dengan diberlakukannya sistem kerja yang WFH ini, berarti hampir segala hal dilakukan secara daring seperti meeting dengan klien. Biasanya untuk menandatangani kerja sama kontrak dengan klien dilakukan dengan bertemu secara langsung. Namun, dengan adanya pandemi, banyak juga yang melakukannya secara online dan menghasilkan dokumen digital. Salah satu dokumen digital tersebut adalah Surat Perintah Kerja.

Surat Perintah Kerja atau yang sering disebut SPK adalah surat resmi yang digunakan untuk memberi perintah pada suatu pihak untuk melakukan suatu pekerjaan. Surat ini biasanya dibuat ketika terjalin kerja sama antar instansi. Dalam SPK terdapat komponen yang berupa isi perintah atau dengan kata lain adalah lingkup kerja dan lingkup kerja ini perlu disepakati oleh kedua belah pihak. Namun, dalam dokumen digital, bisa jadi isi perintah ini diubah secara sepihak sehingga merugikan pihak yang lainnya. Oleh karena itu, perlu dilakukan otentikasi apakah kedua belah pihak menyetujui adanya penambahan atau pengurangan dalam isi perintah tersebut atau perubahan terjadi secara sepihak. Hal ini dapat dilakukan dengan memberi tanda tangan digital dari kedua belah pihak terhadap dokumen digital yang telah disetujui. Terjadinya suatu penambahan atau pengurangan isi surat dalam SPK dapat diketahui dari verifikasi pada tanda tangan digital.

Oleh karena itu, pada makalah ini akan dibahas mengenai implementasi kriptografi kunci publik DSA dan fungsi *hash* SHA-256 sebagai salah satu metode untuk menjaga keaslian dan keotentikasian dari SPK yang telah disepakati bersama antara pemberi pekerjaan dan penerima pekerjaan.

II. DASAR TEORI

A. Surat Perintah Kerja (SPK)

Surat Perintah Kerja (SPK) adalah surat resmi yang dikeluarkan oleh suatu instansi yang berisikan pernyataan dan instruksi untuk memulai, melaksanakan, dan menyelesaikan suatu pekerjaan tertentu. SPK dikeluarkan jika akan dibangun kerjasama antar instansi antara pihak pemberi pekerjaan dan penerima pekerjaan. Surat ini mengikat antara pihak pemberi pekerjaan dan penerima pekerjaan sehingga perlu dibuat detail seperti kepastian waktu, kepastian pekerjaan yang harus dilaksanakan oleh penerima pekerjaan, dan nominal harga yang akan diterima oleh penerima pekerjaan.

Walaupun tidak ada format pasti yang jelas karena SPK cenderung berbeda-beda bagi tiap perusahaan, beberapa contoh komponen-komponen yang umumnya ada di dalam surat perintah kerja antara lain kop surat, nomor surat, identitas pemberi perintah kerja, identitas penerima kerja, isi perintah, detail kewajiban, dan nama terang.

B. Tanda Tangan Digital

Tanda tangan digital (digital signature) adalah bentuk alternatif modern untuk menandatangani dokumen. Tanda tangan digital memanfaatkan skema matematika untuk memeriksa keaslian dan integritas dokumen digital. Tanda tangan digunakan untuk memberikan layanan keamanan

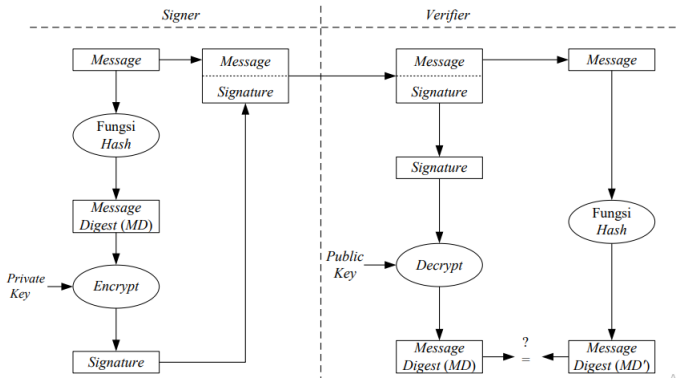
seperti otentikasi (*authentication*), keaslian pesan (*data integrity*), dan anti-penyangkalan (*nonrepudiation*).

Baik tanda tangan digital maupun tanda tangan biasa mempunyai karakteristik sebagai berikut:

1. Tanda tangan adalah bukti yang otentik
2. Tanda tangan tidak dapat dilupakan
3. Tanda tangan tidak dapat dipindah untuk digunakan ulang
4. Dokumen yang telah ditandatangani tidak dapat diubah
5. Tanda tangan tidak dapat disangkal

Tanda tangan digital bukanlah tulisan tanda-tangan yang di-digitisasi dengan cara dipindai atau difoto. Tanda tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci. Jika tanda tangan biasa akan selalu sama bentuknya jika dilakukan oleh orang yang sama, pada tanda tangan digital akan selalu berbeda walaupun ditandatangani oleh orang yang sama hal ini karena jika nilainya sama, maka akan sangat mudah untuk ditiru.

Dalam menandatangani pesan dapa dilakukan dengan dua cara yaitu dengan cara mengenkripsi pesan atau menggunakan kombinasi fungsi *hash* dan kriptografi kunci-publik. Alur kerja penandatanganan dengan kombinasi fungsi *hash* dan kriptografi kunci-publik dapat dilihat pada gambar II.1



Gambar II.1 Metode Tanda Tangan digital mengunakan Kriptografi kunci-publik dan Fungsi *Hash*
(sumber: http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/20 20-2021/Tanda-tangan-digital-2020.pdf)

Pada makalah ini, metode tanda tangan digital yang digunakan adalah kombinasi fungsi *hash* dan kriptografi kunci publik karena pada permasalahan yang disebutkan tidak diperlukan kerahasiaan pesan namun yang diperlukan adalah otentikasi, keaslian pesan, dan anti-penyangkalan.

C. DSS (Digital Signature Standard)

DSS adalah standar untuk tanda-tangan digital yang diresmikan pada bulan Agustus 1991 oleh NIST (The National Institute of Standard and Technology). DSS terdiri dari dua komponen yaitu

1. Algoritma tanda tangan digital: Digital Signature Algorithm (DSA)
2. Fungsi *hash* standard: Secure Hash Algorithm (SHA)

DSA termasuk ke dalam algoritma kriptografi kunci-publik dan memiliki dua fungsi utama yaitu pembangkitan tanda-tangan (signature generation) dan pemeriksaan keabsahan tanda-tangan (signature verification). Pembangkitan tanda-tangan dilakukan dengan menggunakan kunci privat, sedangkan pemeriksaan keabsahan tanda-tangan menggunakan kunci publik. Berikut parameter-parameter pada DSA:

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

Berikut langkah-langkah membangkitkan kunci pada DSA:

1. Pilih bilangan prima p dan q, sedemikian sehingga $(p-1) \bmod q = 0$
2. Hitung $g = h^{(p-1)/q}$ dengan $1 < h < p - 1$ dan $h^{(p-1)/q} \bmod p > 1$
3. Tentukan kunci privat x dengan $x < q$
4. Hitung kunci publik $y = g^x \bmod p$

Pembangkitan kunci menghasilkan parameter publik (p, q, g, y) dan parameter privat x.

Pembangkitan tanda-tangan dengan DSA dilakukan dengan langkah-langkah sebagai berikut:

1. Hitung *message digest* pesan m dengan fungsi hash, H(m)
2. Tentukan bilangan acak $k < q$
3. Tanda tangan dari pesan m adalah bilangan r dan s dengan perhitungan
   $r = (g^k \bmod p) \bmod q$
   $s = (k^{-1} (H(m) + x \, . \, r)) \bmod q$

Berikut langkah-langkah untuk melakukan verifikasi keabsahan tanda-tangan:

1. Hitung message digest pesan m dengan fungsi *hash* H(m)
2. Verifikasi tanda tangan r dan s dilakukan dengan perhitungan
   $w = s^{-1} \bmod q$
   $u_1 = (H(m) \, . \, w) \bmod q$
   $u_2 = (r \, . \, w) \bmod q$
   $v = ((g^{u1} \, . \, y^{u2}) \bmod p) \bmod q$
3. Jika $v = r$, maka tanda tangan digital sah atau terverifikasi dan jika $v \neq r$ maka tanda tangan tidak sah

D. Fungsi Hash SHA-256

Hash function atau fungsi hash adalah suatu fungsi yang dapat memetakan data dengan panjang sembarang menjadi suatu string dengan ukuran tertentu yang pasti. Hasil dari fungsi hash dinamakan message digest. Hash bukanlah

enkripsi karena tidak dapat mengembalikan nilai hash menjadi nilai aslinya (irreversible). Salah satu fungsi hash adalah SHA-256 (Secure Hash Algorithm 256) yang memetakan data teks dengan panjang sembarang ke string 256-bit atau 32-byte. Hash.

Proses dalam SHA-256 terbagi dari 3 tahap, yaitu:

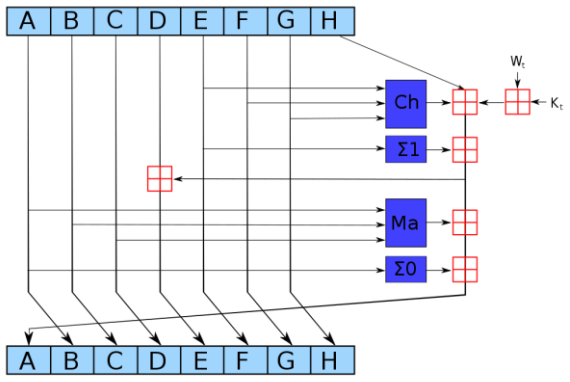
1. Praproses pesan
   Pada tahap ini pesan diproses dalam bentuk bit. Pertama-tama pesan akan ditambahkan padding bits sehingga bit pada pesan kongruen dengan 448 mod 512. Lalu, akan ditambahkan 64 bit yang merepresentasikan panjang pesan. Terakhir, bit akan dibagi-bagi menjadi blok-blok dengan panjang 512 bit yang terbagi menjadi 16 bagian 32 bit words.
2. Inisialisasi buffer
   Setelah pesan di praproses, dilakukan inisialisasi delapan buah buffer dengan nilai sebagai berikut

Buffer	Nilai	Buffer	Nilai
A_0	0x6A09E667	E_0	0x9B05688C
B_0	0xBB67AE85	F_0	0x510E527F
C_0	0x3C6EF372	G_0	0x1F83D9AB
D_0	0xA54FF53A	H_0	0x5BE0CD19

3. Proses Pengulanagan Algoritma SHA
   Fungsi yang digunakan dalam algoritma ini adalah:

$$\mathrm{Ch}(E,F,G) = (E \wedge F) \oplus (\neg E \wedge G)$$
$$\mathrm{Ma}(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$
$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$
$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

   Dari 8 buffer yang ada, dilakukan operasi sebagai berikut:



   Operasi dilakukan dengan t = 63.

   Untuk 16 putaran pertama nilai Wt akan sama dengan blok pesan. Untuk sisa putaran akan dijalankan suatu fungsi sehingga panjang Wt adalah 32 bit dengan nilai Kt yang sudah ditentukan.

   Setelah 64 putaran selesai dijalankan, nilai A-H akan ditambah nilainya dengan A0-H0, dan akan menghasilkan output A-H. Jika belum mencapai akhir blok pesan, A-H ini akan masuk ke dalam blok pesan selanjutnya. Jika sudah mencapai akhir blok pesan, maka A-H merupakan output dari SHA-256.

III. Rancangan Solusi dan Implementasi

A. Rancangan Solusi

Dalam menyelesaikan permasalahan yaitu kecurangan oleh salah satu pihak dengan cara mengubah isi SPK tanpa persetujuan pihak lainnya dapat menggunakan pendekatan tanda tangan digital (*digital signature*) dengan metode yang akan digunakan adalah kombinasi fungsi *hash* SHA-256 dan algoritma Digital Signature Standard. Dengan menggunakan tanda tangan digital, dapat dicapai aspek-aspek keamanan seperti otentik, asli, dan anti-penyangkalan.

Perancangan solusi terdiri atas tiga tahap yaitu tahap pembangkitan kunci, tahap sign, dan tahap verify.

1. Tahap pembangkitan kunci
   Pada tahap pembangkitan kunci, pihak pemberi pekerjaan maupun pihak penerima pekerjaan akan membangkitkan kunci privat dan kunci publiknya masing-masing dengan menggunakan nilai p, q, dan x yang berbeda. Kemudian, masing-masing pihak akan saling memberikan kunci publiknya kepada pihak lainnya.
2. Tahap sign
   Kemudian, setelah pihak ketiga mendapatkan kunci publik dari kedua pihak, akan dilakukan tahap sign. Pada tahap ini, isi surat perlu disepakati terlebih dahulu. Jika masing-masing pihak telah sepakat, maka selanjutnya pesan akan dilakukan sign atau pemberian tanda tangal. Hasil dari tahap ini adalah tanda tangan digital dari masing-masing pihak yang saling diberikan kepada satu pihak ke pihak lainnya.
3. Tahap verify
   Kemudian, untuk mengecek apakah terjadi perubahan isi SPK secara sepihak atau tidak, dilakukan pada tahap verify. Misalnya terjadi perdebatan antara kedua pihak akan isi dari SPK di kemudian hari, maka akan diperiksa isi dari dokumen tersebut dengan melakukan verifikasi terhadap masing-masing digital signature. Pihak pemberi pekerjaan akan mengecek keabsahan dari digital signature dari pihak penerima pekerjaan dengan kunci publik pihak penerima pekerjaan. Begitu juga sebaliknya, pihak penerima pekerjaan akan mengecek keabsahan dari digital signature dari pihak pemberi pekerjaan dengan kunci publik pihak pemberi pekerjaan. Jika ada salah satu yang tidak valid, maka terjadi perubahan pada dokumen secara sepihak.

B. *Implementasi*

Setelah tercapai kesepakatan dalam poin-poin yang terdapat pada SPK, masing-masing pihak akan memnangmenandatangani dokumen sehingga dokumen akan memiliki 2 buah tanda tangan digital: tanda tangan digital milik pihak pemberi pekerjaan dan pihak penerima pekerjaan.

Implementasi dilakukan dengan membuat suatu program yang dapat membangkitkan kunci privat dan kunci publik, dapat membangkitkan tanda tangan, dan dapat melakukan verifikasi terhadap tanda tangan. Berikut fungsi-fungsi yang digunakan

```
def generate_key(p: int, q: int, x: int) ->
(key, key):
    g = 0
    while g <= 1:
        h = randint(2, p - 2)
        g = pow(h, (p - 1) // q, p)

    y = pow(g, x, p)

    p = str(p)
    q = str(q)
    y = str(y)
    g = str(g)
    x = str(x)

    pub_key: key = {'p': p, 'q': q, 'g': g,
'y': y}
    pri_key: key = {'x': x}

    return pub_key, pri_key

def sign(digest: int, p: int, q: int, g:
int, x: int) -> dsign:
    k = randint(1, q - 1)
    r = pow(g, k, p) % q
    s = (pow(k, -1, q) * ((digest + (x *
r)) % q)) % q

    return r, s

def verify(digest: int, sign: dsign, p:
int, q: int, g: int, y: int) -> bool:
    r, s = sign
    w = pow(s, -1, q)
    u1 = (digest * w) % q
    u2 = (r * w) % q
    v = ((pow(g, u1, p) * pow(y, u2, p)) %
p) % q

    return v == r
```

IV. PENGUJIAN DAN PEMBAHASAN

A. *Pengujian*

Pengujian dilakukan dengan 3 skema yaitu pengujian dengan signature dari pemberi pekerjaan dan penerima pekerjaan yang valid, pengujian dengan dokumen diubah oleh pihak pemberi pekerjaan, dan pengujian dengan dokumen diubah oleh pihak penerima pekerjaan.

Lingkungan pengujian yang digunakan ditunjukkan pada tabel berikut

Dokumen	
Surat Perintah Kerja	PT JAYA JAYA JAYA Jalan Jaya No.1 Jakarta Selatan SURAT PERINTAH KERJA Nomor: 001/SPK/2021 Kegiatan: Pengadaaan Barang A Memerintahkan: Nama : ZZZ Jabatan : Manager Sales and Marketing PT Kijang Rusa Untuk segera memulai pelaksanaan kerja dengan ketentuan 1. Macam pekerjaan: A dengan harga B 2. Tanggal mulai: 13 Desember 2021 3. Tanggal selesai: 15 Desember 2021
Pemberi Pekerjaan	
P	1291450057
Q	70157
X	70000
Kunci publik	(1291450057, 70157, 1259973810, 546492181)
Kunci privat	(1291450057, 70157, 1259973810, 70000)
Valid signature	536A 5179
Penerima Pekerjaan	
P	2134961839
Q	43353
X	40000
Kunci publik	(2134961839, 43353, 841823652, 1110048320)
Kunci privat	(2134961839, 43353, 841823652, 40000)
Valid signature	63BB 1642

Berikut 3 skema yang dilakukan untuk pengujian:

1. Pengujian tanpa pengubahan dokumen dan dengan valid signature dari masing-masing pihak
   Pada pengujian ini, dokumen yang divalidasi tidak diubah sama sekali, dan signature pemberi pekerjaan

dan signature penerima pekerjaan adalah signature yang valid.

Dokumen	
Surat Perintah Kerja	PT JAYA JAYA JAYA Jalan Jaya No.1 Jakarta Selatan SURAT PERINTAH KERJA Nomor: 001/SPK/2021 Kegiatan: Pengadaaan Barang A Memerintahkan: Nama : ZZZ Jabatan : Manager Sales and Marketing PT Kijang Rusa Untuk segera memulai pelaksanaan kerja dengan ketentuan 1. Macam pekerjaan: A dengan harga B 2. Tanggal mulai: 13 Desember 2021 3. Tanggal selesai: 15 Desember 2021
Pemberi Pekerjaan	
Kunci publik	(1291450057, 70157, 1259973810, 546492181)
signature	536A 5179
Penerima Pekerjaan	
Kunci publik	(2134961839, 43353, 841823652, 1110048320)
signature	63BB 1642

2. Pengujian dengan pengubahan dokumen dari pihak pemberi pekerjaan
   Pada pengujian ini, dokumen diubah oleh pihak pemberi pekerjaan dengan mengurangi harga yang perlu dibayarkan kepada penerima pekerjaan dengan maksud menguntungkan pihak pemberi pekerjaan. Oleh karena itu, signature dari pihak pemberi pekerjaan juga berubah sehingga akan valid jika diverifikasi dengan dokumen yang telah diubah

Dokumen	
Surat Perintah Kerja	PT JAYA JAYA JAYA Jalan Jaya No.1 Jakarta Selatan SURAT PERINTAH KERJA Nomor: 001/SPK/2021 Kegiatan: Pengadaaan Barang A Memerintahkan: Nama : ZZZ Jabatan : Manager Sales and Marketing PT Kijang Rusa Untuk segera memulai pelaksanaan kerja dengan ketentuan 1. Macam pekerjaan: A dengan harga B-100 2. Tanggal mulai: 13 Desember 2021 3. Tanggal selesai: 15 Desember 2021
Pemberi Pekerjaan	
Kunci publik	(1291450057, 70157, 1259973810, 546492181)
signature	ACF7 BB45
Penerima Pekerjaan	
Kunci publik	(2134961839, 43353, 841823652, 1110048320)
signature	63BB 1642

3. Pengujian dengan pengubahan dokumen dari pihak penerima pekerjaan
   Pada pengujian ini, pihak penerima pekerjaan mengubah dokumen dengan memperpanjang waktu selesai kerja dengan maksud menguntungkan pihak penerima pekerjaan. Oleh karena itu, signature dari pihak penerima pekerjaan berubah sehingga akan valid jika diverifikasi dengan dokumen yang diubah.

Dokumen	
Surat Perintah Kerja	PT JAYA JAYA JAYA Jalan Jaya No.1 Jakarta Selatan SURAT PERINTAH KERJA Nomor: 001/SPK/2021 Kegiatan: Pengadaaan Barang A Memerintahkan: Nama : ZZZ Jabatan : Manager Sales and Marketing PT Kijang Rusa Untuk segera memulai pelaksanaan kerja dengan ketentuan 1. Macam pekerjaan: A dengan harga B 2. Tanggal mulai: 13 Desember 2021 3. Tanggal selesai: 20 Desember 2021
Pemberi Pekerjaan	
Kunci publik	(1291450057, 70157, 1259973810, 546492181)
signature	536A 5179
Penerima Pekerjaan	
Kunci publik	(2134961839, 43353, 841823652, 1110048320)
signature	1EB6 4374

B. Pembahasan

Berdasarkan pengujian yang telah dilakukan, didapatkan hasil sebagai berikut:

1. Pengujian tanpa pengubahan dokumen dan dengan valid signature dari masing-masing pihak
   Pengujian dengan dokumen yang telah disepakati kedua belah pihak dan ditandatangani menghasilkan nilai valid baik bagi verifikasi pihak pemberi pekerjaan maupun pihak penerima pekerjaan. Hal ini menandakan tidak terjadi perubahan dari salah satu pihak tanpa kesepakatan pihak lainnya.
2. Pengujian dengan pengubahan dokumen dari pihak pemberi pekerjaan
   Pengujian dengan dokumen yang telah diubah oleh pihak pemberi pekerjaan menghasilkan nilai valid bagi verifikasi signature pihak pemberi pekerjaan namun memberi nilai tidak valid bagi verifikasi signature pihak penerima pekerjaan. Hal ini menunjukkan terdapat kecurangan yaitu pengubahan dokumen secara sepihak oleh pihak pemberi pekerjaan.
3. Pengujian dengan pengubahan dokumen dari pihak penerima pekerjaan
   Pengujian dengan dokumen yang diubah oleh pihak penerima pekerjaan menghasilkan nilai tidak valid bagi verifikasi signature pihak pemberi pekerjaan namun memberi nilai valid bagi verifikasi signature pihak penerima pekerjaan. Hal ini menunjukkan terjadi pengubahan dokumen oleh pihak penerima pekerjaan secara sepihak tanpa persetujuan dari pihak pemberi pekerjaan.

V. KESIMPULAN DAN SARAN PENGEMBANGAN

Solusi yang diimplementasikan berhasil menjamin bahwa suatu dokumen ditandatangani atas dasar kesepakatan dari 2 belah pihak sehingga meningkatkan keamanan SPK dari perubahan secara sepihak oleh pihak mana pun tanpa persetujuan pihak lainnya. Solusi ini memenuhi aspek otentikasi, keaslian pesan, dan anti penyangkalan yang merupakan aspek keamanan yang disediakan oleh tanda tangan digital.

Kedepannya, solusi dapat dikembangkan dengan beberapa aspek pengembangan seperti ukuran pasangan kunci publik dan privat DSA yang lebih baik, penggunaan jenis algoritma kunci publik yang lainnya seperti Elgamal dan RSA, penggunaan algoritma fungsi hash yang lebih baik seperti Keccak dan MD5.

UCAPAN TERIMA KASIH

Ucapan terima kasih penulis sampaikan kepada Tuhan Yang Maha Esa karena dengan rahmat dan karunia-Nya lah penulis bisa menyelesaikan makalah ini dalam waktu yang telah ditetapkan.

Penulis juga mengucapkan terimakasih kepada Dr. Rinaldi Munir selaku dosen mata kuliah IF4020 Kriptografi Semester I Tahun 2021/2022 atas ilmu yang telah disampaikan kepada penulis sehingga makalah ini dapat ditulis.

REFERENSI

[1] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Fungsi Hash

[2] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Tanda Tangan Digital

[3] Munir, Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Digital Signature Standard (DSS)

[4] Contoh Surat Perintah Kerja Serta Format dan Komponennya! Diakses pada 12 Desember 2021 dari https://www.akseleran.co.id/blog/contoh-surat-perintah-kerja/

[5] Contoh Surat Perintah Kerja (SPK) Serta Cara Membuatnya. Diakses pada 12 Desember 2021 dari https://tambahpinter.com/surat-perintah-kerja/

[6] Apa Itu Digital Signature? Cara Kerja dan Keunggulan. Diakses pada 12 Desember 2021 dari https://zipmex.com/id/learn/apa-itu-digital-signature-cara-kerja-dan-keunggulan/

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, 20 Desember 2021

13518047 Hizbulloh Ash-Shidiqy