Implementasi *Digital Signature* pada Transaksi Digital

13517034 Muhammad Fariz Luthfan Wakan[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13517034@std.stei.itb.ac.id

***Abstrak*—Aktivitas daring bukan merupakan hal yang asing lagi, terutama di era pandemi COVID-19. Peningkatan aktivitas daring selama transisi era pandemi COVID-19, meningkatkan minat masyarakat akan transaksi digital. Hal tersebut dapat menjadi peluang, tetapi dapat menjadi ujung tombak bagi mereka yang mengesampingkan keamanan. Hal ini karena, pesatnya teknologi dalam bertransaksi sama dengan pesatnya teknologi dalam memanipulasi data. *Digital signature* dapat menyelesaikan permasalahan pada transaksi digital, terutama pada pemalsuan bukti transfer dan pemalsuan invoice. Pada makalah ini akan dibahas mengenai implementasi *digital signature* pada transaksi digital yang difokuskan pada topik pemalsuan bukti transfer, dengaan aloritma *digital signature* yang digunakan adalah *Elliptic Curve Digital Signature Algorithm* (ECDSA).**

***Kata kunci*—COVID-19, *digital signature*, ECDSA, manipulasi data, bukti transfer.**

I. Pendahuluan

Di zaman yang modern ini, aktivitas daring bukanlah merupakan hal yang asing, apalagi di era pandemi COVID-19, era *New Normal*, seperti kegiatan belajar mengajar yang dilaksanakan melalui *video conferencing*, *work from home* (WFH), dan lainnya. Hal ini disebababkan, di era ini, aktivitas daring dijadikan prioritas utama demi menjaga kesehatan dan mencegah terpaparnya virus yang tersebar di lingkungan luar, sehingga tidak keluar rumah selama sepekan sudah menjadi hal yang umum di kalangan masyarakat.

Dengan adanya peningkatan aktivitas daring, persentase transaksi digital pun meningkat hingga 38,3% selama pandemi COVID-19[1]. Shopee, yang merupakan salah satu *online marketplace* di Indonesia melaporkan terjadi peningkatan transaksi sebesar 130% selama Q2 2020[2].

Tingginya minat akan transaksi digital dapat menjadi peluang yang sangat besar, baik bagi pendatang baru maupun yang sudah mapan. Namun, hal ini dapat menjadi ujung tombak bagi mereka yang mengesampingkan keamanan dalam transaksi digital.

Keamanan pada transaksi digital perlu dipertahankan dan ditingkatkan, karena manipulasi data sudah bukan merupakan hal yang sulit di zaman ini, seperti pemalsuan bukti transfer, pemalsuan *invoice*, dan pemalsuan dokumen lainnya yang berkaitan dengan transaksi digital.

Digital Signature (tanda-tangan digital) yang merupakan salah satu cara dalam membuktikan keaslian pesan atau dokumen digital, dapat memiliki peranan yang penting dalam menyelesaikan permasalahan tersebut.

II. Dasar Teori

A. Transaksi Digital

Berdasarkan KBBI, transaksi merupakan persetujuan jual beli (dalam perdagangan) antara dua pihak[3], sehingga transaksi digital merupakan persetujuan jual beli antara dua pihak yang dilakukan secara digital (atau daring), seperti transaksi jual beli di *e-commerce*, *online marketplace*, dan lainnya.

B. Tanda-tangan Digital

Tanda-tangan digital (*digital signature*) merupakan skema matematis yang digunakan untuk membuktikan keaslian pesan atau dokumen digital. Skema ini menjadi jaminan bahwa data dan informasi benar-benar berasal dari sumber yang benar[4][5].

Pada dasarnya, tanda-tangan digital merupakan tanda-tangan untuk data digital. Tanda-tangan digital merupakan nilai kriptografis yang bergantung pada isi pesan dan kunci, sehingga tanda-tangan digital pada suatu dokumen akan berbeda dengan dokumen lainnya yang isinya berbeda[6]. Tanda-tangan digital yang *valid*, dengan syarat-syarat yang terpenuhi, memberikan penerima pesan alasan yang sangat kuat untuk percaya bahwa pesan tersebut dibuat oleh pengirim yang dikenal (otentikasi), dan bahwa pesan itu tidak diubah dalam transit (integritas)[4]. Selain itu tanda tangan digital juga dapat memastikan aspek *non-repudiation* sehingga penulis pesan tidak bisa menyangkal di kemudian hari bahwa pesan tersebut bukan ditulis oleh dirinya.

Terdapat 2 (dua) cara untuk menandatangani pesan, mengenkripsi pesan (menggunakan kriptografi simetri atau menggunakan kriptografi kunci-publik) atau menggunakan kombinasi kriptografi kunci-publik dan fungsi *hash*.

C. Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm (ECDSA) merupakan salah satu algoritma yang diterapkan dalam pembuatan tanda tangan digital yang menggunakan analogi kurva elips. Teknik ini memungkinkan siapapun untuk mengecek validitas *signature* yang dipasangkan kepada sebuah data. Terdapat 3 (tiga) proses yang dilakukan pada ECDSA:

pembangkitan kunci, pembuatan tanda-tangan, dan verifikasi tanda-tangan.

Pada protokol ECDSA, pihak yang akan melakukan tanda tangan digital menyimpan informasi parameter pembentuk kurva eliptik, yaitu a, b, p, n, dan G(x, y). Parameter tersebut yang akan digunakan sebagai informasi masukan di ketiga proses ECDSA.

1) Pembangkitan Kunci
    a. Memilih sebuah bilangan bulat random d_A (kunci privat), yang nilainya di antara [1, n – 1]
    b. Menghitung kunci publik, $Q_A = d_A \bullet G = (x_1, y_1)$.
2) Pembuatan Tanda-tangan
    a. Memilih sebuah bilangan bulat random k, yang nilainya diantara [1, n – 1].
    b. Menghitung $Q_A = k \bullet G = (x_1, y_1)$ dan $r = x_1 \bmod n$, jika r = 0, maka kembali ke langkah pertama.
    c. Menghitung $k^{-1} \bmod n$
    d. Menghitung e = *hash*(m)
    e. Menghitung $s = k^{-1} \{e + d_A \bullet r\} \bmod n$ tanda tangan untuk *message* m adalah (r, s)
3) Verifikasi Tanda-tangan
    a. Memastikan bahwa r dan s adalah bilangan bulat yang antara [1, n – 1]
    b. Menghitung e = *hash*(m)
    c. Menghitung $w = s^{-1} \bmod n$
    d. Menghitung $u_1 = ew \bmod n$ dan $u_2 = rw \bmod n$
    e. Menghitung $u_1 \bullet G + u_2 \bullet Q_A = (x_1, y_1)$
    f. Menghitung $v = x_1 \bmod n$
    g. Menerima tanda tangan jika dan hanya jika v = r

III. Aplikasi *Digital Signature* pada Transaksi Digital

A. Tanda-tangan Digital pada Invoice

Invoice merupakan sebuah alat yang memuat daftar barang kiriman yang dilengkapi dengan keterangan nama, jumlah, dan harga yang dapat digunakan sebagai tanda bukti adanya proses jual beli produk atau jasa.

Sebagai tanda bukti yang sah, *invoice* digunakan untuk banyak hal, seperti *reimbursement*, garansi, dan lainnya.

Sayangnya, tidak sedikit *invoice* yang diberikan tidak terdapat suatu skema yang membuktikan validitas isi dari *invoice* tersebut. Dengan kata lain, *invoice* tersebut dapat dengan mudah dimanipulasi, seperti dilakukannya penggantiaan tanggal pembelian untuk memperpanjang masa garansi, memperbesar harga barang agar nominal *reimbursement* yang diberikan melebihi nominal seharusnya, dan tujuan-tujuan lainnya. Hal ini memberikan dampak yang sangat besar bagi individu/kelompok yang terkait dengan pemalsuan *invoice* tersebut.

Dengan adanya tanda-tangan digital, hal tersebut dapat dicegah, dan terselesaikan dengan baik.

B. Tanda-tangan Digital pada Bukti Transfer

Bukti transfer atau bukti transaksi merupakan sebuah alat dalam transaksi antara dua pihak, yang dapat menjadi bukti bahwa suatu pihak telah memberikan sejumlah uang kepada pihak lainnya.

Sampai saat ini, masih banyak sekali modus penipuan dalam transaksi digital dengan memalsukan bukti transfer. Sama halnya dengan *invoice*, hal ini disebabkan oleh tidak adanya skema yang dapat membuktikan validitas isi dari bukti transfer yang dikirimkan oleh suatu pihak, sehingga bukti transfer dapat dengan mudah dimanipulasi. Hal ini mungkin tidak akan terjadi jika media dimana transaksi terjadi menyediakan bukti transfer dengan tanda-tangan digital dan menyediakan sistem untuk melakukan validasi terhadap bukti transfer tersebut.

Selain itu, dengan adanya sistem tersebut, validitas suatu transaksi dapat diotomasi, sehingga tidak diperlukan pengecekan secara manual.

IV. Implementasi Tanda-Tangan Digital Pada Bukti Transfer

A. Implementasi ECDSA

Elliptic Curve Digital Signature Algorithm (ECDSA) yang merupakan salah satu algoritma *digital signature*, digunakan pada implementasi tanda-tangan digital pada bukti transfer. Algoritma ECDSA terdiri atas 4 (empat) kelas, `Curve`, `Key`, `Signature`, dan `ECDSA`.

1) Kelas `Curve`
   Kelas `Curve` dirancang untuk menciptakan kurva eliptik berdasarkan parameter domain kurva elpitik `a`, `b`, `p`, `n`, dan `G(x, y)`.
2) Kelas `Key`
   Kelas `Key` dirancang untuk menciptakan kunci, baik kunci publik maupun kunci privat, berdasarkan kurva eliptik. Pada kelas ini terdapat 2 (dua) *method*, `Key.public()` yang akan membangkitkan kunci publik dan `Key.secret()` yang akan membangkitkan kunci privat.
3) Kelas `Signature`
   Kelas `Signature` dirancang untuk menciptakan tanda-tangan digital berdasarkan parameter `r` dan `s`.
4) Kelas `ECDSA`
   Kelas `ECDSA` terdiri dari 2 (dua) *static method*, `ECDSA.sign()` yang akan mengeksekusi algoritma *sign* pada ECDSA seperti yang dijelaskan pada subbab II.F. hingga menghasilkan kelas `Signature` dan `ECDSA.verify()` yang mengeksesekusi algoritma *verify* pada ECDSA hinggaa menghasilkan tipe data `boolean` yang menyatakan validitas tanda-tangan.

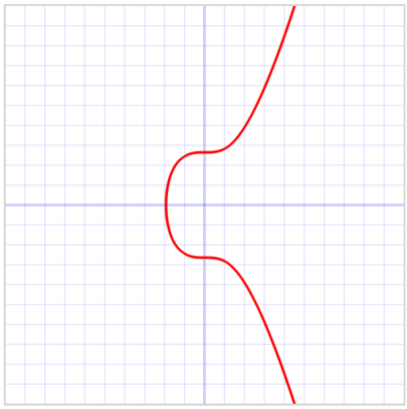
B. Implementasi ECDSA pada Bukti Transfer

Tipe antarmuka ECDSA pada bukti transfer menggunakan *Application Programming Interface* (API) dengan 3 (tiga) *endpoint*,

No	*Endpoint*	Method	Deskripsi
1	`/generate`	POST	Pembangkitan Kunci
2	`/sign`		Tanda-tangan Bukti Transfer

3	`/verify`		Verifikasi Tanda-tangan

Dengan kurva eliptik yang terdefinisi menggunakan standar kurva *secp256k1*[8],



Gambar IV.1 Kurva Eliptik *secp256k1*

Parameter		Nilai
a		0x0000000000000000000000000000000000000000000000000000000000000000
b		0x0000000000000000000000000000000000000000000000000000000000000007
p		0xfffffffffffffffffffffffffffffffffffffffffffffffffffffffefffffc2f
n		0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141
G	x	0x79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798
	y	0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8

1) Pembangkitan Kunci
Pada *endpoint* `/generate`, dilakukan pembangkitan kunci dengan menciptakan objek dari kelas `Key` berdasarkan kurva eliptik yang telah didefinisikan di awal. Sebelum penciptaan objek dilakukan, akan dilakukan pengecekan `id` dari *request payload* terlebih dahulu untuk mengetahui apakah kunci sudah pernah dibangkitkan. Selain itu, terdapat `reset` pada *request payload* yang bersifat optional (*default*: `false`) untuk membangkitkan kunci baru. Berikut ilustrasi *request payload* dan *response* pada pembangkitan kunci,

Request payload
```
{
    "id":
"e369853df766fa44e1ed0ff613f563bd",
    "reset": true
}
```

Response
```
{
    "id":
"e369853df766fa44e1ed0ff613f563bd",
    "public":
"ODE4Njk5OTI4NzM0NDY2NDE0MTg5NTI1OTE4Nj
EwMDgwNzI0NDA3OTQyMjgwODMwOTk4OTk4NDEwO
Dk1Nzg1OTg0MzQ3Mzg3MjQ1MzMKMTEwMjgwMjg4
MjI4MTgyOTA3Mzg1MDQ0ODc3NjI4NDQyNzg1ODg
4NDA5ODAxNzYyOTQxNzczMzI5NDUzMzA1MTEyOD
MzMjA5NzMwMzE5",
    "private":
"MzYwOTg3ODY4ODcxMDY4MTMwNTU5ODIzMzQxMT
AyNjkzOTc3NjE3MDIyMTQ3NjcwMjcyNDY3MzMzM
DM5NTQ4NDI1NDA5MzM2MzM4OA=="
}
```

2) Tanda-tangan Bukti Transfer
Pada *endpoint* `/sign`, dilakukan pemanggilan *static method* `ECDSA.sign()` dengan masukan berupa bukti transfer dan kunci privat. Kunci privat ditemukan melalui `reciever_id` pada *request payload*.

Request payload
```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5",
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000
}
```

Response
```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"MTA2NDE2MzQzMzQ1MzMzODExMzkzMDU5OTI4OT
UxNjQ5MDA4MDAzNjQzOTMxNTkxMDQ2NTkwNDA2M
jEzMDI4MTMzMjc2MDkxNDE2NTAyCjQwMDc0NzY3
OTE2MzAzNjMxNDI4NzkxMTc3MDUyNDI2NzAwMzk
wNTIwNDg1MTc3NjAzNDA0MTAyNTczNzYxMDI1MD
c3MDI5MjM3NDc4"
}
```

3) Verifikasi Tanda-tangan
Pada *endpoint* `/verify`, dilakukan pemanggilan *static method* `ECDSA.verify()` dengan masukan berupa bukti transfer dengan *signature* dan kunci publik. Kunci publik ditemukan melalui `reciever_id` pada *request payload*.

Request payload
```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
```

```
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"MTA2NDE2MzQzMzQ1MzMzODExMzkzMDU5OTI4OT
UxNjQ5MDA4MDAzNjQzOTMxNTkxMDQ2NTkwNDA2M
jEzMDI4MTMzMjc2MDkxNDE2NTAyCjQwMDc0NzY3
OTE2MzAzNjMxNDI4NzkxMTc3MDUyNDI2NzAwMzk
wNTIwNDg1MTc3NjAzNDA0MTAyNTczNzYxMDI1MD
c3MDI5MjM3NDc4"
}
```


Response


```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"MTA2NDE2MzQzMzQ1MzMzODExMzkzMDU5OTI4OT
UxNjQ5MDA4MDAzNjQzOTMxNTkxMDQ2NTkwNDA2M
jEzMDI4MTMzMjc2MDkxNDE2NTAyCjQwMDc0NzY3
OTE2MzAzNjMxNDI4NzkxMTc3MDUyNDI2NzAwMzk
wNTIwNDg1MTc3NjAzNDA0MTAyNTczNzYxMDI1MD
c3MDI5MjM3NDc4",
    "is_valid": true
}
```


V. Eksperimen dan Hasil Analisis

A. Eksperimen

Tedapat 4 (empat) eksperimen yang dilakukan dalam *Elliptic Curve Digital Signature Algorithm* (ECDSA) pada bukti transfer, yaitu eksperimen dengan mengubah data pada bukti transfer, eksperimen dengan menggunakan kunci privat yang tidak sesuai, eksperimen dengan menggunakan kunci publik yang tidak sesuai, dan eksperimen dengan mengubah tanda-tangan digital.

1) Perubahan data pada bukti transfer
   Pengujian pada eksperimen ini dilakukan dengan mengubah nominal pada bukti transfer, yang pada mulanya 500000 (lima juta) menjadi 50000000 (lima puluh juta).

Request payload


```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"ODIzMzc2MzAwNjAyOTcwNzI3NzA4ODk5MjIyND
Q4NTY0NDc3NTQwMTA2MTczMDM1NjQ4MzY2MDY3O
TkzMTczMTYyOTA3MTEwNTA2MzUKODI4MzMxNTkz
Njg1NDAzMzAzNDY4ODgzMTgwNTA5ODk3NzMxODE
5MzgyMDc3MDI4ODMzOTk0NzM3MDg5NTEyMTQ5MD
IwMDUzODI2ODY="
}
```


Response


```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"ODIzMzc2MzAwNjAyOTcwNzI3NzA4ODk5MjIyND
Q4NTY0NDc3NTQwMTA2MTczMDM1NjQ4MzY2MDY3O
TkzMTczMTYyOTA3MTEwNTA2MzUKODI4MzMxNTkz
Njg1NDAzMzAzNDY4ODgzMTgwNTA5ODk3NzMxODE
5MzgyMDc3MDI4ODMzOTk0NzM3MDg5NTEyMTQ5MD
IwMDUzODI2ODY=",
    "is_valid": false
}
```


2) Penggunaan kunci privat yang tidak sesuai
   Untuk mengetahui kunci publik dan privat, *endpoint* `/generate` digunakan.

Request payload


```
{
    "id":
"e369853df766fa44e1ed0ff613f563bd",
    "reset": false
}
```


Response


```
{
    "id":
"e369853df766fa44e1ed0ff613f563bd",
    "public":
"ODE4Njk5OTI4NzM0NDY2NDE0MTg5NTI1OTE4Nj
EwMDgwNzI0NDA3OTQyMjgwODMwOTk4OTk4NDEwO
Dk1Nzg1OTg0MzQ3Mzg3MjQ1MzMKMTEwMjgwMjg4
MjI4MTgyOTA3Mzg1MDQ0ODc3NjI4NDQyNzg1ODg
4NDA5ODAxNzYyOTQxNzczMzI5NDUzMzA1MTEyOD
MzMjA5NzMwMzE5",
    "private":
"MzYwOTg3ODY4ODcxMDY4MTMwNTU5ODIzMzQxMT
AyNjkzOTc3NjE3MDIyMTQ3NjcwMjcyNDY3MzMzM
DM5NTQ4NDI1NDA5MzM2MzM4OA=="
}
```


Pengujuan pada eksperimen ini akan dilakukan perubahan karakter ke-3 dari terakhir, `A`, menjadi `Q`, sebagai berikut.


```
MzYwOTg3ODY4ODcxMDY4MTMwNTU5ODIzMzQxMTAy
NjkzOTc3NjE3MDIyMTQ3NjcwMjcyNDY3MzMzMDM5
NTQ4NDI1NDA5MzM2MzM4OQ==
```


Setelah mengetahui kunci privat, dilakukan *signing* dengan memanggil *endpoint* `/sign`.

Request payload


```
{
```

```
    "id":
"e4da3b7fbbce2345d7772b0674a318d5",
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000
}
```


Response


```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"Mzg3ODY0MjYyOTk4ODYyMDQ4ODE0OTEzMzEzNj
EwNTI3NjA3ODIzODgwMTMwODMyODc5OTEzMDIwO
DY4MzQyMzY2ODQ2MjU1MzgxOTQKODA3MzcwODk0
ODc0MDgwNTA1OTYwMjExMTM0NTY1NzQ3OTMyNDc
2MTEwODI1ODMxNzM1MDc3NjUzMTU0NTc2MjYyOT
M3NjEwNDc4NDI="
}
```


Setelah *signature* telah dibentuk berdasarkan kunci privat yang tidak sesuai tersebut, dilakukan *verifying* dengan memanggil *endpoint* `/verify`.

Request payload


```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"Mzg3ODY0MjYyOTk4ODYyMDQ4ODE0OTEzMzEzNj
EwNTI3NjA3ODIzODgwMTMwODMyODc5OTEzMDIwO
DY4MzQyMzY2ODQ2MjU1MzgxOTQKODA3MzcwODk0
ODc0MDgwNTA1OTYwMjExMTM0NTY1NzQ3OTMyNDc
2MTEwODI1ODMxNzM1MDc3NjUzMTU0NTc2MjYyOT
M3NjEwNDc4NDI="
}
```


Response


```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"Mzg3ODY0MjYyOTk4ODYyMDQ4ODE0OTEzMzEzNj
EwNTI3NjA3ODIzODgwMTMwODMyODc5OTEzMDIwO
DY4MzQyMzY2ODQ2MjU1MzgxOTQKODA3MzcwODk0
ODc0MDgwNTA1OTYwMjExMTM0NTY1NzQ3OTMyNDc
```



```
2MTEwODI1ODMxNzM1MDc3NjUzMTU0NTc2MjYyOT
M3NjEwNDc4NDI=",
    "is_valid": false
}
```


3) Penggunaan kunci publik yang tidak sesuai
Pengujuan pada eksperimen ini akan dilakukan perubahan 2 (dua) karakter terakhir, `E5`, menjadi `A=`, sebagai berikut.


```
ODE4Njk5OTI4NzM0NDY2NDE0MTg5NTI1OTE4NjEw
MDgwNzI0NDA3OTQyMjgwODMwOTk4OTk4NDEwODk1
Nzg1OTg0MzQ3Mzg3MjQ1MzMKMTEwMjgwMjg4MjI4
MTgyOTA3Mzg1MDQ0ODc3NjI4NDQyNzg1ODg4NDA5
ODAxNzYyOTQxNzczMzI5NDUzMzA1MTEyODMzMjA5
NzMwMzA=
```


Dengan menggunakan hasil bukti transfer dan *signature* pada IV.B., diberikan *response* oleh API sebagai berikut.

Request payload


```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"MTA2NDE2MzQzMzQ1MzMzODExMzkzMDU5OTI4OT
UxNjQ5MDA4MDAzNjQzOTMxNTkxMDQ2NTkwNDA2M
jEzMDI4MTMzMjc2MDkxNDE2NTAyCjQwMDc0NzY3
OTE2MzAzNjMxNDI4NzkxMTc3MDUyNDI2NzAwMzk
wNTIwNDg1MTc3NjAzNDA0MTAyNTczNzYxMDI1MD
c3MDI5MjM3NDc4"
}
```


Response


```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"MTA2NDE2MzQzMzQ1MzMzODExMzkzMDU5OTI4OT
UxNjQ5MDA4MDAzNjQzOTMxNTkxMDQ2NTkwNDA2M
jEzMDI4MTMzMjc2MDkxNDE2NTAyCjQwMDc0NzY3
OTE2MzAzNjMxNDI4NzkxMTc3MDUyNDI2NzAwMzk
wNTIwNDg1MTc3NjAzNDA0MTAyNTczNzYxMDI1MD
c3MDI5MjM3NDc4",
    "is_valid": false
}
```


4) Perubahan tanda-tangan digital
Untuk mendapatkan *signature*, dilakukan *signing* dengan memanggil *endpoint* `/sign`.

Request payload

```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5",
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000
}
```


Response


```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"OTkzODMwMDgzNzMyNzg2ODQwMDkyMDM4NzM1NT
g3MDU4MjA3MDQ1NTcyNDMwNzQ2MTYxNzYxNjk5N
TE1MzY5MDA3MDUzNzgwNzU5MjUKNTIwMzc3NDY0
MDY2MjI1MzYxNTI5Mjc0NjIwMDE2NjA5NDI4NTI
xOTgwNjEwNjUxMTc2OTg5OTE2NTM1MTQzNTgxMD
c1MDk3OTI5NTI="
}
```


Setelah signature diterima, dilakukan maanipulasi signature dengan menambahkan karakter M pada karakter ke-2 dari terakhir, sebagai berikut.


```
OTkzODMwMDgzNzMyNzg2ODQwMDkyMDM4NzM1NTg3
MDU4MjA3MDQ1NTcyNDMwNzQ2MTYxNzYxNjk5NTE1
MzY5MDA3MDUzNzgwNzU5MjUKNTIwMzc3NDY0MDY2
MjI1MzYxNTI5Mjc0NjIwMDE2NjA5NDI4NTIxOTgw
NjEwNjUxMTc2OTg5OTE2NTM1MTQzNTgxMDc1MDk3
OTI5NTM=
```


Kemudian dilakukan *verifying* dengan memanggil *endpoint* `/verify`.

Request payload


```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"OTkzODMwMDgzNzMyNzg2ODQwMDkyMDM4NzM1NT
g3MDU4MjA3MDQ1NTcyNDMwNzQ2MTYxNzYxNjk5N
TE1MzY5MDA3MDUzNzgwNzU5MjUKNTIwMzc3NDY0
MDY2MjI1MzYxNTI5Mjc0NjIwMDE2NjA5NDI4NTI
xOTgwNjEwNjUxMTc2OTg5OTE2NTM1MTQzNTgxMD
c1MDk3OTI5NTM="
}
```


Response


```
{
    "id":
"e4da3b7fbbce2345d7772b0674a318d5"
    "receiver_id":
"e369853df766fa44e1ed0ff613f563bd",
    "sender_id":
"33e75ff09dd601bbe69f351039152189",
    "created_at": 1608477764,
    "nominal": 5000000,
    "signature":
"OTkzODMwMDgzNzMyNzg2ODQwMDkyMDM4NzM1NT
g3MDU4MjA3MDQ1NTcyNDMwNzQ2MTYxNzYxNjk5N
TE1MzY5MDA3MDUzNzgwNzU5MjUKNTIwMzc3NDY0
MDY2MjI1MzYxNTI5Mjc0NjIwMDE2NjA5NDI4NTI
xOTgwNjEwNjUxMTc2OTg5OTE2NTM1MTQzNTgxMD
c1MDk3OTI5NTM=",
    "is_valid": false
}
```


B. Hasil Analisis

Berdasarkan eksperimen yang dilakukan, *Elliptic Curve Digital Signature Algorithm* (ECDSA) pada bukti transfer terimplementasi dengan baik. Hal ini dibuktikan dengan 4 (empat) *negative test cases* yang dgunakan pada eksperimen menghasilkan nilai `false` pada `is_valid` yang muncul di *response*. *Positive test case* pada subbab IV.B. pun menghasilkan nilai `true` pada `is_valid`.

V. KESIMPULAN DAN SARAN

Digital signature (tanda-tangan digital) mampu mengatasi permasalahan yang dialami pada transaksi digital, seperti bukti transfer. Dengan tanda-tangan digital, pemalsuan bukti transfer tidak dapat dilakukan dengan cara hanya dengan memanipulasi data seperti mengubah nominal, dan cara lainnya. Selain itu, implementasi tanda-tangan digital pada bukti transfer memberikan cara baru dalam melakukan verifikasi pembayaran. Dengan adanya tanda-tangan digital, transaksi dengan cara transfer daapat dengan mudah diverifikasi dan diotomasi, tanpa perlu pengecekan secara manual.

Penggunaan *digital signature* dalam rangka mempertahankan dan meingkatkan keamanan transaksi digital merupakan langkah yang tepat, baik pendatang baru maupun yang sudah mapan.

REFERENSI

[1] https://tirto.id/jumlah-pelanggan-e-commerce-tercatat-meningkat-383-selama-pandemi-f1eP, diakses pada tanggal 19-12-2020.

[2] https://inet.detik.com/cyberlife/d-5155740/masa-pandemi-transaksi-shopee-di-q2-2020-naik-hingga-130, diakses pada tanggal 19-12-2020.

[3] https://kbbi.kemdikbud.go.id/entri/transaksi, diakses pada tanggal 20-12-2020.

[4] HR, EMPTrust. "What is Digital Signature- How it works, Benefits, Objectives, Concept" (dalam bahasa Inggris).

[5] Hermawan, Tofan; Wardhani, Rini Wisnu (2016-10). "Implementation AES with digital signature for secure web-based electronic archive". 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE). Yogyakarta, Indonesia: IEEE: 1–6. doi:10.1109/ICITEED.2016.7863268. ISBN 978-1-5090-4139-8.

[6] R. Munir, "Tanda Tangan Digital," Teknik Informatika STEI - ITB, Bandung.

[7] https://en.bitcoin.it/wiki/Secp256k1, diakses pada tanggal 20-12-2020.

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, 3 Desember 2020

13517034 Muhammad Fariz Luthfan Wakan