Implementasi Tanda Tangan Digital Pada Tagihan Kartu Kredit

Ahmad Rizal Alifio / 13517076
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13517076@std.stei.itb.ac.id

***Abstract*—Luasnya penggunaan sistem informasi digital dalam berbagai transaksi menuntut pengembang mengimplementasi sebuah sistem transaksi. Salah satu bentuk transaksi yang terkenal karena penipuannya adalah transaksi kartu kredit. Dalam praktiknya, penipuan dengan kartu kredit merupakan sebuah bentuk pencurian identitas dalam bentuk pembelian barang dengan mengatasnamakan orang lain. Sementara, untuk menggunakan kartu kredit sebagai alat pembayaran hanya membutuhkan nomor kartu dan kode CVV 3 digit, sebuah sekuens data yang sangat mudah ditebak. Dalam artikel ini akan dijelaskan penggunaan algoritma tanda tangan digital menggunakan ECDSA dalam pengiriman data tagihan kartu kredit sebagai sebuah *proof of concept* dalam penggunaan tanda tangan digital sebagai pengganti kode CVV.**

***Keywords*—kartu kredit, tagihan, tanda tangan digital, kriptografi.**

I. Pendahuluan

Dalam era informasi, penggunaan internet sebagai perantara berbagai aspek dalam kehidupan sangat mudah dijumpai. Mulai dari pencarian pengetahuan, perdagangan, perbankan, hingga pekerjaan dapat dilakukan melalui sebuah dunia virtual yang dapat diakses dengan mudah oleh siapapun dan dimanapun.

Namun rupanya kemudahan akses yang ditawarkan era informasi tidak hanya memberikan kemudahan namun juga potensi kerugian bagi penggunanya. Dilansir dari fool.com, pada tahun 2019 di Amerika Serikat terdapat 650.572 kasus pencurian identitas dan 270.000 kasus diantaranya merupakan kasus penipuan kartu kredit, dimana pelaku menggunakan identitas dan kartu kredit orang lain untuk melakukan transaksi. Jumlah yang melebihi 650 ribu kasus tersebut menimbulkan kerugian mencapai 9,47 miliar USD, dan dengan asumsi perbandingan yang sama dengan jumlah kasus, penipuan kartu kredit menyumbang kerugian lebih dari 3,9 miliar USD.

Padahal, sistem keamanan yang ada dalam rentetan proses transaksi menggunakan kartu kredit dapat terbilang sudah canggih. Sejak kemunculan pertamanya pada 1950, kartu kredit modern telah mengalami banyak iterasi dan peningkatan keamanan. Dalam sejarah kartu kredit pada experian.com peningkatan kualitas keamanan kartu kredit dapat dilihat mulai dari strip magnetik dan keping CMV pada kartu kredit, hingga yang paling terkenal tentu saja kode CVV 3 digit yang ditentukan secara acak kepada pemilik kartu kredit yang diperkenalkan pertama kali pada tahun 1990 an.

CVV sendiri merupakan sebuah langkah keamanan tambahan setelah pengecekan identitas dan tren transaksi yang dikenakan pada pemilik kartu kredit. Namun, penggunaan kode CVV tidak sepenuhnya aman. sebuah kode dengan 3 digit sangat mudah ditebak. Terlebih lagi, dengan semakin maraknya perdagangan daring yang mengharuskan pengguna memasukkan kode CVV maka semakin besar pula kemungkinan dilakukan *sniffing* pada paket jaringan yang mencantumkan kode CVV.

Maka dari itu, sebagai kasus pencurian identitas paling besar, maka keamanan dalam transaksi menggunakan kartu kredit perlu dikaji lebih jauh dan diimplementasi sebuah sistem yang lebih efektif. Dalam artikel ini akan dikaji sebuah konsep pengganti CVV yaitu tanda tangan digital.

Dengan penelitian ini, diharapkan tanda tangan digital dapat menjadi sebuah alternatif yang lebih aman terhadap CVV berkat aspek *authentication, integrity,* dan *non-repudiation* yang dimilikinya.

II. Dasar Teori

A. Tanda Tangan Digital

Tanda tangan digital adalah sebuah mekanisme otorisasi yang dapat digunakan oleh seseorang dalam proses pengiriman pesan melalui media digital seperti internet, sedemikian rupa sehingga konten yang dikirim akan terkirim dengan aman.

Algoritma pertama yang mendukung kemunculan tanda tangan digital diciptakan oleh Rivest, Shamir, dan Adleman dalam algoritmanya yang bernama RSA. RSA adalah sebuah algoritma kunci-publik.

Konsep kunci-publik yang dimiliki algoritma ini sangat krusial dalam terciptanya mekanisme tanda tangan digital karena sebelumnya, kunci yang dibutuhkan dalam mengenkripsi dan mendekripsi sebuah pesan sama, sehingga tidak mendukung identifikasi pengirimnya.

Tanda tangan digital memiliki 3 karakteristik yang mendukung keamanan pengiriman pesan, karakteristik tersebut adalah:

a. Authentication

Otentikasi berguna sebagai cara untuk memastikan identitas pengirim pesan. Dengan konsep ini, asal muasal pesan dapat ditentukan sehingga pencurian identitas dapat dicegah. Otentikasi sangat berguna terutama dalam pengiriman pesan melalui media yang tidak dapat dipastikan keamanannya, seperti protokol pengiriman paket melalui jaringan internet

b. Integrity

Integritas merupakan sebuah konsep yang berguna dalam memastikan isi pesan yang diterima sama dengan pesan yang dikirim oleh pengirim pesan. Hal ini berguna untuk memastikan bahwa pesan tidak diubah dalam fase pengirimannya.

c. Non-repudiation

Anti-penyangkalan merupakan sebuah prinsip dimana pengirim tanda tangan digital tidak bisa menyangkal bahwa tanda tangan yang dikeluarkan adalah miliknya. Hal ini berguna dalam proses pertanggungjawaban terhadap konten dari pesan.

B. Algoritma ECDSA

Algoritma ECDSA merupakan algoritma variasi dari Digital Signature Algorithm (DSA) yang menggunakan elliptical curve. Basis keamanan sistem kriptografi elliptical curve berasal dari ketegasan komputasi dari persoalan logaritma diskrit kurva elips.

Algoritma ini memiliki keuntungan pada ukuran key nya, dimana dengan ukuran key lebih kecil dapat menghasilkan ukuran signature yang sama besarnya dengan metode Discrete Logarithm (DL) standar.

Algoritma ini tidak seperti logaritma diskrit biasa dan masalah faktorisasi integer, masalah logaritma diskrit kurva elips tidak mengenal algoritma perkalian sub-eksponensial. Karenanya, kekuatan per bit kunci algoritma yang menggunakan kurva elips lebih kuat secara substansial daripada algoritma biasa.

Dalam ECDSA, terdapat 3 tahap utama yang harus dipenuhi yaitu *key generation, sign,* dan *verify*.

a. Key Generation

Pada tahap ini, dilakukan pembangkitan kunci publik dan privat. Kunci privat akan digunakan dalam tahap *sign* untuk menghasilkan *sign,* sementara kunci publik akan digunakan penerima pesan untuk memastikan keaslian pesan dalam tahap *verify*.

b. Sign

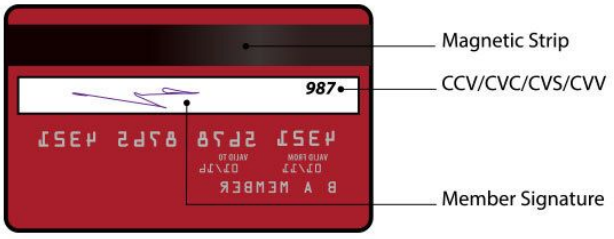
Tahap ini merupakan tahap penandatanganan dokumen elektronik menggunakan kunci privat pengirim pesan. Sebelum dilakukan penandatanganan, akan dilakukan *hashing* pesan dengan algoritma SHA3

c. Verify

Tahap ini dilakukan oleh penerima pesan untuk memastikan keaslian pesan. Penerima pesan akan melakukan pengecekan antara tanda tangan digital yang ada pada pesan dengan menggunakan kunci publik yang dipublikasi oleh pengirim pesan. Apabila valid maka pesan dianggap asli.

C. Kode CVV pada Kartu Kredit

Kode CVV adalah sebuah kode 3 digit yang umumnya tertera pada bagian belakang kartu kredit. Kode ini adalah sebuah fitur keamanan tambahan yang digunakan pada transaksi kartu kredit. Karena pada umumnya laman yang menyediakan transaksi dengan kartu kredit dapat menyimpan nomor kartu kredit, namun tidak menyimpan kode CVV yang digunakan. Sehingga dalam sebuah transaksi pengguna yang ingin melakukan transaksi harus melihat kode yang tertera pada kartu kreditnya. Berikut adalah gambar contoh bagian belakang sebuah kartu kredit.



Gambar 1. Kode CVV pada Kartu Kredit. Sumber: https://www.idfcfirstbank.com/cvv.html

III. Rancangan Dan Implementasi

A. Algoritma ECDSA

Berikut adalah implementasi struktur ECDSA dalam bahasa C++.

```
struct gfp {
    uint512_t val;

    gfp();
    gfp(const uint256_t& val);
    gfp(const uint512_t& val);

    bool operator==(const gfp& g) const;
    bool operator!=(const gfp& g) const;
    gfp operator+(const gfp& g) const;
    gfp operator-() const;
    gfp operator-(const gfp& g) const;
    gfp operator*(const gfp& g) const;
    gfp operator/(const gfp& g) const;
    gfp pow(const uint256_t& p) const;
    gfp inv() const;
    gfp sqrt() const;

    operator uint256_t() const;
};

typedef std::pair<gfp, gfp> point;

const gfp d = uint256_t(

"37095705934669439343138083508754565189542113879843219016388785533085940283"
    "555");
const point B{

uint256_t("151122213495354007725011514095885315114540126930418572060461132
8"
              "3949847762202"),
```

```
uint256_t("463168356949264781694283940034
751631413079938662562256157830360"
              "3165251855960")};
const uint256_t L =
    (uint256_t(1) << 252) +
uint256_t("277423177773723535358519377908
83648493");

ucharVec encodePoint(const point& p);
point decodePoint(const ucharVec& p);

typedef std::tuple<gfp, gfp, gfp, gfp>
xPoint;

xPoint extend(const point& p);
point retract(const xPoint& xp);

xPoint add(const xPoint& pa, const
xPoint& pb);
xPoint dbl(const xPoint& p);
xPoint mul(const xPoint& xp, const
uint256_t& p);

point add(const point& pa, const point&
pb);
point mul(const point& po, const
uint256_t& p);

ucharVec generateKey();
ucharVec sign(const ucharVec& data, const
ucharVec& privateKey);
bool verify(const ucharVec& data,
            const ucharVec& signature,
            const ucharVec& publicKey);

}
```

Algoritma 1. Implementasi kelas ECDSA

Secara umum, terdapat beberapa unsur utama yang kemudian diimplementasi dalam algoritma ECDSA. Unsur-unsur tersebut adalah kelas point, kurva ED25519, fungsi pembangkitan kunci, fungsi sign, dan fungsi verify.

B. Implementasi Tanda Tangan Digital pada Tagihan

Dalam praktiknya, tidak terdapat sebuah struktur khusus dalam sebuah form tagihan daring, maka dari itu dalam penelitian ini akan dibuat contoh tagihan dalam bentuk JSON. Berikut adalah sebuah contoh tagihan dalam format JSON dari CentralPay.


```
{
    "creditId":
"bd0004d3-10e2-4997-ad7d-22be54a6039a",
    "creationDate":
"2020-08-11T16:26:52.038969+02:00",
    "merchantCreditId": "MCID-01",
    "status": "UNCLEARED",
    "description": null,
    "currency": "EUR",
    "amount": 100,
    "country": null,
    "contractId":
"71602dd0-2790-4743-877b-e72530d7576d",
    "customerId": null,
    "card": {
      "cardId":
"bf605fc5-23d1-4c05-b515-1488669b5fcf",
      "creationDate":
"2020-08-11T16:26:52.309150+02:00",
      "customerId": null,
      "cardTokenId": null,
      "merchantCardId": null,
      "commercialBrand": "VISA",
      "first6": "400000",
      "last4": "0002",
      "expirationMonth": 10,
      "expirationYear": 2025,
      "country": null,
      "cardholderName": null,
      "cardholderEmail": null,
      "description": null,
      "fingerprint":
"e67c16dbf2dfd0d7c712755f6ac52d2a6653c6f7",
      "cardType": null,
      "region": null,
      "productType": null,
      "europeanEconomicArea": null,
      "additionalData": {}
    },
    "receiptEmail": null,
    "payoutCurrency": "EUR",
    "payoutAmount": 100,
    "commission": 0,
    "fee": 0,
    "transferGroup": null,
    "order": {
      "addressLine"
}
```


Algoritma 2. Contoh JSON Tagihan

Sementara, kedua kunci yang dibangkitkan adalah sebagai berikut:

Kunci Privat	F95E9D05B9EF72EE8A793BF85B6F7093626747A35DC061D9556E4458BBF940AA
Kunci Publik	1CB1153AF30CF550953865BDDC3A98F6B91EEB29CA9A024AC43053BDF3C9D22F

Tabel 1. Kunci privat dan kunci publik

Kemudian, berikut merupakan contoh tagihan tersebut setelah disisipi tanda tangan digital.

```
{
      "creditId":
"bd0004d3-10e2-4997-ad7d-22be54a6039a",
      "creationDate":
"2020-08-11T16:26:52.038969+02:00",
      "merchantCreditId": "MCID-01",
      "status": "UNCLEARED",
      "description": null,
      "currency": "EUR",
      "amount": 100,
      "country": null,
      "contractId":
"71602dd0-2790-4743-877b-e72530d7576d",
      "customerId": null,
      "card": {
         "cardId":
"bf605fc5-23d1-4c05-b515-1488669b5fcf",
         "creationDate":
"2020-08-11T16:26:52.309150+02:00",
         "customerId": null,
         "cardTokenId": null,
         "merchantCardId": null,
         "commercialBrand": "VISA",
         "first6": "400000",
         "last4": "0002",
         "expirationMonth": 10,
         "expirationYear": 2025,
         "country": null,
         "cardholderName": null,
         "cardholderEmail": null,
         "description": null,
         "fingerprint":
"e67c16dbf2dfd0d7c712755f6ac52d2a6653c6f7",
         "cardType": null,
         "region": null,
         "productType": null,
         "europeanEconomicArea": null,
         "additionalData": {}
      },
      "receiptEmail": null,
      "payoutCurrency": "EUR",
      "payoutAmount": 100,
      "commission": 0,
      "fee": 0,
      "transferGroup": null,
      "order": {
         "addressLine"
}

D9FB6C4EDDBA45BFA102B461426DBEF0854BE36434
7059DCD4D538F82E63553C3F6693697A1806959B45E01
EE7EBF631FDD76526D479425CA3AAFE2D8F7D1A0E
```


Algoritma 3. JSON Tagihan dengan tanda tangan digital.

IV. Eksperimen

Eksperimen akan dilakukan dengan melakukan beberapa perubahan, yaitu perubahan pada konten, tanda tangan digital, dan kunci privat.

A. Konten

Perubahan konten pada algoritma 2 diubah beberapa atributnya yaitu *creationDate* dan *amount* menjadi seperti berikut:


```
{
      "creditId":
"bd0004d3-10e2-4997-ad7d-22be54a6039a",
      "creationDate":
"2019-12-11T16:26:52.038969+02:00",
      "merchantCreditId": "MCID-01",
      "status": "UNCLEARED",
      "description": null,
      "currency": "EUR",
      "amount": 1000,
      "country": null,
      "contractId":
"71602dd0-2790-4743-877b-e72530d7576d",
      "customerId": null,
      "card": {
         "cardId":
"bf605fc5-23d1-4c05-b515-1488669b5fcf",
         "creationDate":
"2020-08-11T16:26:52.309150+02:00",
         "customerId": null,
         "cardTokenId": null,
         "merchantCardId": null,
         "commercialBrand": "VISA",
         "first6": "400000",
         "last4": "0002",
         "expirationMonth": 10,
         "expirationYear": 2025,
         "country": null,
         "cardholderName": null,
         "cardholderEmail": null,
         "description": null,
         "fingerprint":
"e67c16dbf2dfd0d7c712755f6ac52d2a6653c6f7",
         "cardType": null,
         "region": null,
         "productType": null,
         "europeanEconomicArea": null,
         "additionalData": {}
      },
      "receiptEmail": null,
      "payoutCurrency": "EUR",
      "payoutAmount": 100,
      "commission": 0,
      "fee": 0,
      "transferGroup": null,
      "order": {
         "addressLine"
}
```


Algoritma 4. JSON Tagihan yang sudah diubah.

Dengan perubahan tersebut, hasil tanda tangan digital berubah menjadi seperti berikut:

Tanda Tangan Digital Awal	D9FB6C4EDDBA45BFA102B461426DB EF0854BE364347059DCD4D538F82E63 553C3F6693697A1806959B45E01EE7E BF631FDD76526D479425CA3AAFE2D 8F7D1A0E
Tanda Tangan Digital dengan Perubahan	B4625869DD53D884A02C400A8AAF82 959FBD95E9A2A8C1B4C95D7F2AAD8 7D5E08B92C0D737E33E069938EADE7 0EBB032445FEC1B8994C3939AA70B0 E4354450B

Tabel 2. Perubahan Tanda Tangan Digital

Dapat dilihat bahwa kedua tanda tangan yang ada berbeda, sehingga dapat diketahui bahwa sudah ada perubahan konten.

B. Tanda Tangan Digital

Dalam pengujian ini, akan dilakukan percobaan verifikasi pada tanda tangan digital yang telah dilakukan perubahan dengan kunci publik yang ada pada tabel 1.

Kunci Publik	1CB1153AF30CF550953865BDDC3A9 8F6B91EEB29CA9A024AC43053BDF 3C9D22F
Tanda Tangan Digital Awal	D9FB6C4EDDBA45BFA102B461426 DBEF0854BE364347059DCD4D538F8 2E63553C3F6693697A1806959B45E01 EE7EBF631FDD76526D479425CA3A AFE2D8F7D1A0E
Tanda Tangan Digital dengan Perubahan	**E**9FB6C4EDDBA45BFA102B461426D BEF0854BE364347059DCD4D538F82 E63553C3F6693697A1806959B45E01 EE7EBF631FDD76526D479425CA3A AFE2D8F7D1A0E
Hasil Verifikasi	Invalid

Tabel 3. Percobaan Perubahan Tanda Tangan Digital

Dapat dilihat bahwa hasil verifikasi tidak valid. Sehingga bisa disimpulkan bahwa telah terjadi perubahan.

C. Kunci Privat

Dalam pengujian ini, akan dilakukan percobaan verifikasi pada tanda tangan digital dengan kunci privat yang tidak sesuai. Hal ini dapat menandakan bahwa pengirim bukanlah orang yang seharusnya.

Kunci Privat	F95E9D05B9EF72EE8A793BF85B6F7 093626747A35DC061D9556E4458BBF 940AA
Kunci Privat dengan Perubahan	F95E9D05B9EF72EE8A793BF85B6F7 093626747A35DC061D9556E4458BBF 940A**B**
Tanda Tangan Digital	D9FB6C4EDDBA45BFA102B461426 DBEF0854BE364347059DCD4D538F8 2E63553C3F6693697A1806959B45E01 EE7EBF631FDD76526D479425CA3A AFE2D8F7D1A0E
Hasil Verifikasi	Invalid

Tabel 4. Perubahan Kunci Privat

Dapat dilihat bahwa hasil verifikasi tidak valid. Sehingga kembali bisa disimpulkan bahwa telah terjadi kesalahan. Dalam hal ini, dapat berarti bahwa penandatangan bukanlah orang yang seharusnya.

C. Faktor Keamanan

Dibandingkan dengan CVV, sebuah tanda tangan digital jauh lebih aman. Hal ini dikarenakan panjangnya kode yang digunakan, yaitu 128 karakter alfanumerik dibandingkan 3 karakter angka. Selain itu, tanda tangan digital dibangkitkan menggunakan algoritma tertentu dibandingkan CVV yang hanya diberikan secara acak. Sehingga, ada ketergantungan tambahan terhadap konten dan kunci yang digunakan oleh pengirim pesan. Kedua hal ini dapat meningkatkan taraf keamanan transaksi secara signifikan.

V. Pembahasan

Penelitian ini merupakan sebuah *proof of concept* terhadap usulan perubahan sistem keamanan transaksi kartu kredit dari CVV menjadi sebuah tanda tangan digital. Sehingga pada kenyataannya algoritma yang digunakan dapat lebih bervariasi.

Tentu hal ini tidak mudah dilakukan mengingat sudah menyebarluasnya penggunaan CVV sebagai fitur keamanan yang ada pada kartu kredit. Namun hal ini tidak melepas fakta bahwa berdasarkan analisis yang dilakukan, dalam segi keamanan penggunaan tanda tangan digital lebih superior terhadap CVV.

Di sisi lain, dalam implementasi dalam kondisi nyata pihak penyedia layanan kartu kredit tidak serta merta dapat menentukan kunci yang digunakan oleh setiap orang. Perlu dipertimbangkan kemampuan manusia dalam mengingat kunci.

Dalam penelitian ini digunakan kunci sepanjang 64 bit, sementara tidak semua orang dapat mengingat sebuah sekuens karakter acak sebanyak itu. Sehingga usulan penggunaan tanda tangan digital tidak cocok apabila ditentukan pada setiap nasabah.

Maka dari itu, sebuah implementasi yang mungkin dapat dilakukan adalah dengan membangkitkan kunci pada perangkat pribadi pemilik rekening kartu kredit. Setiap perangkat tersebut akan memiliki pasangan kunci publik dan privatnya masing-masing. Dengan cara ini maka kebutuhan mengingat kunci dapat digantikan.

Terdapat juga keperluan menjaga kunci privat agar tidak berubah selain oleh pihak berwajib. Hal ini perlu diatasi karena ada kemungkinan serangan atau perubahan yang menarget

perangkat pengguna. Salah satu cara pencegahannya adalah dengan melakukan sebuah pesan inisialisasi pada pertama kali pembangkitan kode. Sehingga untuk memeriksa apabila kunci berubah, bank dapat membandingkan tanda tangan digital yang ada pada pesan inisialisasi dengan tanda tangan yang ada pada saat ini.

Persoalan terakhir ada pada kerahasiaan kunci privat, mengingat terdapat ancaman kebocoran rahasia keberadaan kunci privat pada perangkat pengguna. Sehingga diperlukan pembangkitan ulang pasangan kunci secara berkala.

VI. Kesimpulan

Penggunaan tanda tangan digital pada transaksi kartu kredit untuk menggantikan kode CVV memiliki keuntungan dalam aspek keamanannya, namun bersama itu terdapat pula tantangan dalam implementasi dan unsur pendukung untuk memastikan bahwa sistem tanda tangan digital bekerja sebagaimana mestinya.

Referensi

[1] Slide kuliah IF4020 Kriptografi. Rinaldi Munir.

[2] Payment Card Fraud Losses Reach $27.85 Billion. Diakses pada 18 Desember 2020 dari https://www.prnewswire.com/news-releases/payment-card-fraud-losses-reach-27-85-billion-300963232.html#:~:text=CARPINTERIA%2C%20Calif.%2C%20Nov.,and%20mobile%20payments%20trade%20publication

[3] History of Credit Card. Diakses pada 19 Desember 2020 dari https://www.experian.com/blogs/ask-experian/the-history-of-credit-cards/#:~:text=The%20modern%20payment%20card%20was,month's%20statement%20balance%20in%20full.

[4] Identity Theft and Credit Card Fraud in 2020. Diakses pada 19 Desember 2020 dari https://www.fool.com/the-ascent/research/identity-theft-credit-card-fraud-statistics/#:~:text=With%20over%20270%2C000%20reports%2C%20credit,through%20data%20breaches%20in%202019. .

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 2020

Ahmad Rizal Alifio
13517076