Implementasi Tanda Tangan Digital Pada Surat Vaksin Covid-19

Arya Beri Argya Rasidi - 131518131
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
13518131@std.stei.itb.ac.id

***Abstrak*— Saat ini pemerintah sedang gencarnya menyuruh masyrakat untuk melakukan vaksin covid-19, bahkan mereka membuatkan aturan untuk menunjukan surat vaksin covid–19 saat hendak memasuki suatu kawasan atau tempat. namun sebagian masyarakat masih tidak mau melakukan vaksin covid-19 dengan berbagai alasan. Hal ini menjadikan peluang untuk sebagian oknum untuk melakukan pemalsuan surat vaksin covid-19. tanda tangan digital menjadi salah satu solusi untuk mengatasi masalah tersebut. Pada makalah ini akan dibahas pengimplementasian tanda tangan digital pada surat vaksin covid-19 untuk mencegah terjadinya pemalsuan. Algoritma yang diterapkan adalah ECDSA**

Keywords—Covid-19, Surat Vaksin, Pemalsuan,* tanda tangan digital, *ECDSA

I. Pendahuluan

Dalam langkah menangani pandemi covid-19, pemerintah menggencarkan vaksinasi kepada masyarakat, mereka bahkan membuat aturan untuk menunjukan surat vaksin covid-19 apabila seseorang ingin memasuki sebuah tempat seperti pasar tradisional dan mall. masyarakat yang tidak bisa menunjukan surat vaksin mereka tidak diperbolehkan memasuki tempat tersebut.

Dilain sisi masih banyak dari masyarakat Indonesia yang belum melakukan vaksinasi dengan berbagai alasan, mulai dari yang kontra dengan vaksin itu sendiri maupun karena tidak kebagian stock dari vaksin. Hingga 5 Desember kemarin tercatat baru sekitar 99.009.581 orang yang telah menerima vaksin dosis kedua, atau sekitar 36% dari jumlah total penduduk Indonesia yang berjumlah sekitar 272 juta jiwa.

Hal ini menyebabkan sebagian masyarakat tidak bisa memasuki tempat-tempat yang telah menerapkan aturan untuk menunjukan surat vaksin covid-19. Dan menjadikan peluang untuk sebagian oknum membuatkan surat vaksin covid-19 palsu untuk masyarakat yang belum vaksin dan ingin memasuki tempat-tempat tersebut.

Hal tersebut tentunya merugikan pemerintah, selain karena mereka yang belum divaksin lebih rentan terkena virus covid-19 di tempat-tempat yang ramai. Adanya surat vaksin palsu juga dapat menjadi penghalang bagi pemerintah untuk melangsungkan vaksinasi kepada masyarakat. Karena masyarakat dapat memiliki surat vaksin covid-19 meskipun belum mendapatkan suntikan vaksin.

Karenanya dibutuhkan sebuah sistem yang dapat menentukan keaslian dari surat vaksin covid-19, salah satu caranya adalah dengan mengimplementasikan tanda tangan digital pada surat vaksin covid-19

I. Dasar Teori

A. Surat/Sertifikat Vaksin Covid-19

Surat/sertifikat vaksin covid-19 adalah sebuah surat/sertifikat yang menunjukan jika seseorang telah melakukan vaksinasi covid-19. Surat/Sertifikat ini dapat diunduh melalui laman pedulilindungi.id bagi masyarakat yang telah melakukan vaksinasi. Umumnya surat/sertifikat ini kemudian dicetak dalam ukuran KTP agar mudah untuk dibawa dan ditujukan kepada petugas apabila diminta menunjukan bukti telah melakukan vaksin saat akan memasuki suatu tempat.

B. Tanda Tangan Digital

Tanda tangan digital (*digital signature)* adalah sebuah skema matematis untuk membuktikan keaslian pesan atau dokumen digital. Tanda Tangan digital bukanlah sekedar tanda tangan yang di-digitisasi (*digitized signature)* dengan cara dipindai atau di foto Tanda tangan digital dibuat dengan membubuhkan *sign* berupa code-code yang diletakan pada akhir dokumen.

Tanda tangan digital merupakan nilai kriptografis yang bergantung pada isi dari pesan dan juga kunci nya. Karena nya nilai dari tanda tangan digital untuk setiap dokumen akan berbeda. Dengan adanya tanda tangan digital dapat meyakinkan penerima pesan jika pesan yang ia terima benar dan asli dibuat oleh pengirim yang dikenal dan tidak ada modifikasi pada dokumen dari pihak yang tidak dikenal.

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. Algoritma ECDSA

Algoritma ECDSA merupakan algoritma variasi dari *Digital Signature Algorithm* (DSA) dengan menggunakan kurva elips. Kekuatan per bit kunci algoritma yang menggunakan kurva elips lebih kuat secara substansial dibandingkan algoritma biasa lainnya, karena logaritma diskrit kurva elips tidak tidak mengenal algoritma perkalian sub eksponensial.

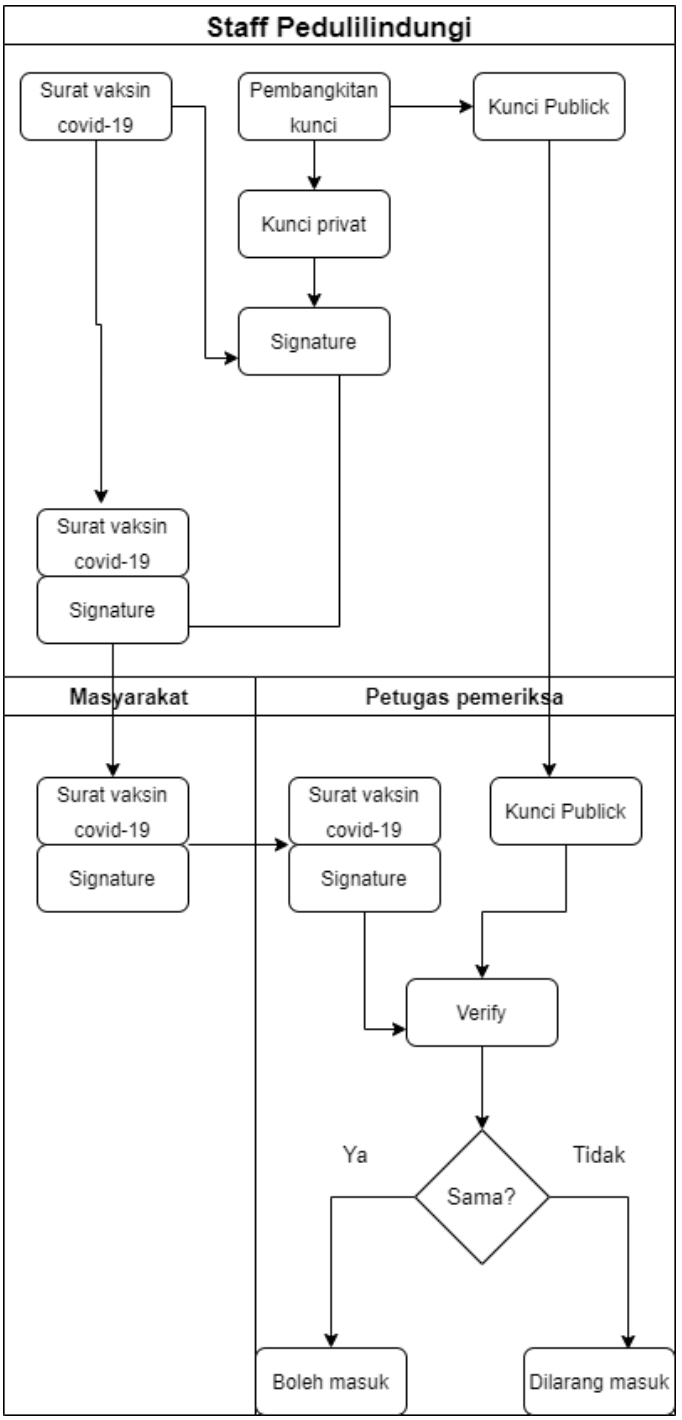
Algoritma ini juga memiliki keunggulan dalam ukuran key nya, dimana dengan ukuran key yang lebih kecil algoritma ini mampu menciptakan ukuran signature yang sama besarnya dengan metode Discrete Logarithm (DL) standar

Tahapan umum dalam menggunakan algoritma ECDSA yang pertama adalah melakukan pembangkitan kunci publik dan juga kunci privat. Kunci privat akan digunakan untuk membuat sign, sedangkan kunci publik akan digunakan untuk melakukan verify.

II. Rancangan Solusi dan Implementasi

A. Rancangan Solusi

Pihak yang akan memberikan tanda tangan digital dalam contoh kasus ini adalah staff pedulilindungi.id akan membangkitkan kunci publik dan juga kunci privat. kunci public kemudian akan dibagikan kepada petugas pemeriksa surat vaksin covid-19 nantinya . Sedangkan kunci privat nya akan digunakan untuk membuat tanda tangan digital. Kemudian surat vaksin covid-19 yang sudah diberikan tanda tangan digital dapat diunduh oleh orang yang bersangkutan dalam kasus ini adalah masyarakat yang telah melakukan vaksin. Setelah itu petugas akan memverifikasikan surat vaksin covid-19 tersebut menggunakan kunci publik yang telah diberikan sebelumnya apabila masyarakat akan memasuki kawasan wajib vaksin. Flow dari rancangan dapat dilihat pada gambar III.1



Gambar III.1 flow rancangan solusi

B. Implementasi

Pada penelitian ini surat vaksin covid-19 direpresentasikan sebagai sebuah struktur dari file JSON, berikut contoh JSON surat vaksin covid-19

```
{
  "id": "605050f1dea6b4c394ab822b",
  "nik": "3209227004730020",
  "nama": "Corona Wati",
  "tanggalLahir": "01-April-1999",
  "tanggalVaksin": "25-Juni-2021",
  "dosis": "2",
  "vaksin": "Sinovac",
  "batchId": "202109149"
}
```


Kemudian contoh Key yang dibangkitkan adalah sebagai berikut:

Private Key	MHQCAQEEIBpv+BhAkl7Tj14kdI03mv9sAkbaYXHMrpi/exvpjRDMoAcGBSuBBAAK oUQDQgAEjGSa2e5GG7AJVxhfSrGWSoYbuBmhKYTxpYx48LHsfxNpP12byfUfhvOQ xK8UwmVHjW4MT54jpUulqqMUDabRiw==
Public Key	MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEjGSa2e5GG7AJVxhfSrGWSoYbuBmhKYTx pYx48LHsfxNpP12byfUfhvOQxK8UwmVHjW4MT54jpUulqqMUDabRiw==

Berikut contoh surat vaksin yang telah diberikan tanda tangan digital:


```
{
  "id": "605050f1dea6b4c394ab822b",
  "nik": "3209227004730020",
  "nama": "Corona Wati",
  "tanggalLahir": "01-April-1999",
  "tanggalVaksin": "25-Juni-2021",
  "dosis": "2",
  "vaksin": "Sinovac",
  "batchId": "202109149"
}
```

MEQCIAFwkB+G4PRPOD2JfB9K7ypUaUEELh1QLp7PtANVRst3AiBAnF+D2nY5CKwwBgQYDjYs0FDRQHIhLPne9Ttk2s+Xwg==

IV. Pengujian

Terdapat lima contoh kasus pengujian yaitu, pengujian dengan konten dan tangan tangan digital yang valid, pengujian dengan tanda tangan digital tidak valid, pengujian dengan private key yang tidak valid, pengujian dengan public key yang tidak valid dan pengujian dengan konten tidak valid..

A. Pengujian dengan konten dan tanda tangan yang valid

Pada pengujian ini baik isi dari surat vaksin dan juga digital signature tidak mengalami perubahan apapun

Konten	{ "id": "605050f1dea6b4c394ab822b", "nik": "3209227004730020", "nama": "Corona Wati", "tanggalLahir": "01-April-1999", "tanggalVaksin": "25-Juni-2021", "dosis": "2", "vaksin": "Sinovac", "batchId": "202109149" }
Tanda tangan digital	MEQCIAFwkB+G4PRPOD2JfB9K7ypUaUEELh1QLp7PtANVRst3AiBAnF+D2nY5CKwwBgQYDjYs0FDRQHIhLPne9Ttk2s+Xwg==
Kunci public	MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEjGSa2e5GG7AJVxhfSrGWSoYbuBmhKYTx pYx48LHsfxNpP12byfUfhvOQxK8UwmVHjW4MT54jpUulqqMUDabRiw==
Hasil verifikasi	True

B. Pengujian dengan tanda tangan yang tidak valid

Pada pengujian kali ini tanda tangan digital telah mengalami perubahan sehingga menyebabkan tanda digital tersebut kini menjadi tidak valid

Konten	{
	"id": "605050f1dea6b4c394ab822b",
	"nik": "3209227004730020",
	"nama": "Corona Wati",
	"tanggalLahir": "01-April-1999",
	"tanggalVaksin": "25-Juni-2021",
	"dosis": "2",
	"vaksin": "Sinovac",
	"batchId": "202109149"
	}

Tanda tangan digital yang telah diubah	MEQCIAFwkB+G4PRPOD2JfB9K7ypUaUEELh1QLp7Pt**BCAR**st3AiBAnF+D2nY5CKwwBgQYDjYs0FDR**hQyu**LPne9Ttk2s+Xwg==
Kunci public	MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEjGSa2e5GG7AJVxhfSrGWSoYbuBmhKYTxpYx48LHsfxNpP12byfUfhvOQxK8UwmVHjW4MT54jpUulqqMUDabRiw==
Hasil verifikasi	False

C. Pengujian dengan private key yang tidak valid

Pada pengujian kali ini dilakukan perubahan pada kunci privat yang juga akan menyebabkan perubahan pada signature yang terbentuk nantinya

Konten	{
	"id": "605050f1dea6b4c394ab822b",
	"nik": "3209227004730020",
	"nama": "Corona Wati",
	"tanggalLahir": "01-April-1999",
	"tanggalVaksin": "25-Juni-2021",
	"dosis": "2",
	"vaksin": "Sinovac",
	"batchId": "202109149"
	}

Kunci privat asli	MHQCAQEEIBpv+BhAkl7Tj14kdI03mv9sAkbaYXHMrpi/exvpjRDMoAcGBSuBBAAKoUQDQgAEjGSa2e5GG7AJVxhfSrGWSoYbuBmhKYTxpYx48LHsfxNpP12byfUfhvOQxK8UwmVHjW4MT54jpUulqqMUDabRiw==
Kunci privat yang mengalami perubahan	MHQCAQEEIODvZuS34wFbt0X53+P5EnSj6tMjfVK01dD1dgDH02RzoAcGBSuBBAAKoUQDQgAE/nvHu/SQQaos9TUljQsUuKI15Zr5SabPrbwtbfT/408rkVVzq8vAisbBRmpeRREXj5aog/Mq8RrdYy75W9q/Ig==
Tanda tangan digital asli	MEQCIAFwkB+G4PRPOD2JfB9K7ypUaUEELh1QLp7PtANVRst3AiBAnF+D2nY5CKwwBgQYDjYs0FDRQHIhLPne9Ttk2s+Xwg==
Tanda tangan digital yang berubah akibat privat key berubah	MEUCIQDYJJ+vsqW0lWnQP/yYWZXfBXR1A2bSiCO5iAP9h6iSrgIgOE8UhmXRmIruh109TtBcnAbBRYHNN6tWfmVa7g6cZUE=
Kunci public	MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEjGSa2e5GG7AJVxhfSrGWSoYbuBmhKYTxpYx48LHsfxNpP12byfUfhvOQxK8UwmVHjW4MT54jpUulqqMUDabRiw==

Hasil verifikasi	False

D. Pengujian dengan public key yang tidak valid

Pengujian kali ini dilakukan dengan merubah kunci public

Konten	<pre>{
	  "id": "605050f1dea6b4c394ab822b",
	  "nik": "3209227004730020",
	  "nama": "Corona Wati",
	  "tanggalLahir": "01-April-1999",
	  "tanggalVaksin": "25-Juni-2021",
	  "dosis": "2",
	  "vaksin": "Sinovac",
	  "batchId": "202109149"
	}</pre>

Tanda tangan digital	MEQCIAFwkB+G4PRPOD2JfB9K7ypUaUEELh1QLp7PtANVRst3AiBAnF+D2nY5CKwwBgQYDjYs0FDRQHIhLPne9Ttk2s+Xwg==
Kunci public asli	MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEjGSa2e5GG7AJVxhfSrGWSoYbuBmhKYTx pYx48LHsfxNpP12byfUfhvOQxK8UwmVHjW4MT54jpUulqqMUDabRiw==
kunci public yang telah mengalami perubahan	MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAE/nvHu/SQQaos9TUljQsUuKI15Zr5SabP rbwtbfT/408rkVVzq8vAisbBRmpeRREXj5aog/Mq8RrdYy75W9q/Ig==
Hasil verifikasi	False

E. Pengujian dengan konten yang tidak valid

Pada pengujian kali ini telah terjadi perubahan pada isi konten sehingga menyebabkan konten menjadi tidak valid

Konten yang telah mengalami peruabahn	<pre>{
	  "id": "605050f1dea6b4c394ab822b",
	  "nik": "3209227004730020",
	  "nama": "**Luna** Wati",
	  "tanggalLahir": "01-**Januari**-1999",
	  "tanggalVaksin": "25-Juni-2021",
	  "dosis": "2",
	  "vaksin": "Sinovac",
	  "batchId": "202109149"
	}</pre>

Tanda tangan digital	MEQCIAFwkB+G4PRPOD2JfB9K7ypUaUEELh1QLp7PtANVRst3AiBAnF+D2nY5CKwwBgQYDjYs0FDRQHIhLPne9Ttk2s+Xwg==
Kunci public	MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEjGSa2e5GG7AJVxhfSrGWSoYbuBmhKYTx pYx48LHsfxNpP12byfUfhvOQxK8UwmVHjW4MT54jpUulqqMUDabRiw==
Hasil verifikasi	False

V. PEMBAHASAN

Berdasarkan pengujian yang telah dilakukan didapatkan hasil sebagai berikut:

1. Pengujian pertama menunjukan apabila tanda tangan digital dan juga konten masih asli tidak mengalami perubahan dari pihak luar, maka akan lulus ketika diverifikasi
2. Pengujian kedua menunjukan jika tanda tangan digital diubah secara paksa oleh pihak luar, maka ketika diverifikasi akan mengalami kegagalan

3. Pengujian ketiga menunjukan apabila ada pihak luar yang ingin menciptakan tanda digital dengan kunci privat yang berbeda, maka saat diverifikasi juga akan mengalami ke gagalan
4. Pengujian keempat menunjukan apabila kunci public yang digunakan untuk melakukan verifikasi berbeda dengan yang seharus nya, hasil nya juga gagal
5. Pengujian kelima menunjukan apabila isi dari konten yakni surat vaksin mengalami perubahan dari pihak luar maka akan mengalami ke gagalan saat tahap verifikasi

VI. KESIMPULAN

Penerapan tanda tangan digital pada surat vaksin covid-19 dapat memastikan keaslian dari isi surat vaksin dan juga memastikan jika surat vaksin dibuat oleh pihak yang berwenang. Sehingga dapat meningkatkan keamanan dari surat vaksin covid-19 dari kasus pembuatan surat palsu.

REFERENCES

[1] https://www.pikiran-rakyat.com/nasional/pr-013165058/capaian-vaksinasi-covid-19-indonesia-jumlah-orang-yang-sudah-divaksin-dua-kali-tembus-99-juta-jiwa, diakses pada 09/12/202

[2] https://id.wikipedia.org/wiki/Tanda_tangan_digital, diakses pada 09/12/2021

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

[4] Roy.Benny, dkk, "Elliptic Curve Digital Signature Algorithm (ECDSA)", Teknik Informatika STEI - ITB, Bandung

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

Arya Beri Argya Rasidi
13518131