Implementasi *Digital Signature* Pada Resep Obat Dokter

Valentinus Devin Setiadi / 13518116
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
13518116@std.stei.itb.ac.id

***Abstraksi*— Aktivitas daring menjadi salah satu hal yang tidak asing lagi di era pandemi COVID-19. Pandemi COVID-19 membuat segala aktivitas dibuat agar dapat dilakukan secara daring, salah satunya adalah dalam melakukan konsultasi kesehatan dengan dokter sampai diberikan resep obat untuk dibeli. Sekarang banyak platform yang menyediakan layanan untuk menjual obat sesuai resep yang diunggah oleh pengguna. Hal tersebut menjadi peluang yang baik dalam kemajuan teknologi, namun dapat menjadi ujung tombak bagi mereka yang mengesampingkan keamanan karena adanya manipulasi data dari resep dokter tersebut. *Digital signature* dapat menyelesaikan permasalahan pemalsuan resep dokter yang diunggah oleh pengguna. Pada makalah ini akan dibahas mengenai implementasi *digital signature* pada resep obat dokter yang diberikan secara daring dengan menggunakan algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA).**

***Kata Kunci*— COVID-19, *digital signature,* ECDSA, resep obat Dokter, manipulasi data.**

I. Pendahuluan

Saat ini, teknologi menjadi salah satu aspek yang tidak dapat terpisahkan dalam kehidupan modern. Dengan adanya teknologi, manusia semakin dimudahkan karena dapat melakukan sebagian besar aktivitasnya secara daring. Salah satu aktivitas yang dapat dilakukan oleh manusia secara daring adalah berkomunikasi satu sama lain. Pada zaman dahulu, manusia hanya dapat melakukan komunikasi dengan sesamanya secara langsung tatap muka. Namun seiring berkembangnya teknologi, manusia dapat melakukan komunikasi dengan mudah secara daring baik melalui pesan, telepon, maupun panggilan video.

Pandemi COVID-19 membuat aktivitas daring bukan merupakan hal yang asing bagi sebagian besar masyarakat. Hampir semua aktivitas dibuat agar dapat dilakukan secara daring, contohnya seperti kegiatan belajar mengajar yang dilakukan melalui *video conferencing*, *work from home,* berbelanja, konsultasi kesehatan dengan dokter, membeli obat dengan resep obat digital, dan lainnya. Aktivitas - aktivitas daring ini menjadi prioritas utama demi menjaga kesehatan agar tidak terpapar virus yang terus muncul varian baru di lingkungan luar.

Banyak platform digital menawarkan jasa konsultasi kesehatan secara daring disaat pandemi ini. Orang - orang cenderung memilih untuk melakukan konsultasi kesehatan secara daring daripada datang langsung ke klinik atau dokter umum atau rumah sakit untuk menghindari terpapar virus yang mungkin dapat berdampak lebih buruk terhadap kesehatannya. Konsultasi kesehatan tersebut dilakukan untuk diagnosis awal terhadap gejala yang dialami oleh pasien. Hasil dari konsultasi tersebut dapat berupa hasil diagnosis, anjuran dari dokter, dan resep obat secara digital yang dapat dibeli di apotek. Resep obat dari dokter tersebut bisa saja dibeli secara daring melalui beberapa platform yang menyediakan layanan pembelian obat resep secara daring tanpa perlu mengantre atau datang langsung ke apotek.

Dengan adanya teknologi pembelian resep obat secara daring membuat keamanan dalam hal validasi keaslian dan keabsahan resep obat perlu diperhitungkan. Hal tersebut perlu diperhitungkan karena pada zaman ini manipulasi data bukanlah hal yang sulit dan sangat mungkin untuk terjadi. Dalam hal ini, resep obat dari dokter merupakan sesuatu yang sangat penting untuk divalidasi keaslian dan keabsahannya.

Digital signature (tanda tangan digital) merupakan salah satu cara dalam membuktikan keaslian pesan atau dokumen digital. Dalam kasus ini *digital signature* dapat menjadi salah satu alternatif untuk memvalidasi keaslian dan keabsahan dari resep obat secara digital.

II. Dasar Teori

A. *Digital Signature* (Tanda tangan digital)

Tanda tangan digital adalah sebuah mekanisme autentikasi yang dapat digunakan oleh seseorang dalam proses pengiriman pesan atau dokumen digital melalui media digital dengan menambahkan kode unik di akhir pesan mereka untuk membuktikan keaslian pesan atau dokumen digital yang dikirimnya. Mekanisme ini menjadi jaminan bahwa data dan informasi yang dikirimkan adalah berasal dari sumber yang benar. Keberadaan dari kode unik tersebut menjadi penanda yang dapat divalidasi oleh penerima pesan apakah pesan tersebut memiliki integritas yang baik. Dalam kriptografi terdapat 3 prinsip atau karakteristik yang dimiliki tanda tangan digital, yaitu:

1. *Authentication* (otentikasi)

Otentikasi berguna sebagai cara untuk memastikan identitas pesan berasal dari pengirim yang tepat dan bukan dari pihak yang salah. Otentikasi sangat penting terutama dalam pengiriman pesan yang melalui media yang tidak dapat dipastikan keamanannya. Otentikasi ini juga berguna untuk mengetahui apakah identitas seseorang memiliki hak untuk mengakses atau menuliskan suatu pesan yang berisi sebuah informasi.

2. *Data Integrity* (keaslian pesan)

Integritas merupakan sebuah konsep yang berguna untuk menjaga keutuhan dan keaslian pesan atau data yang berisi suatu informasi. Aspek ini dibutuhkan untuk mendeteksi apakah sebuah pesan telah dimanipulasi atau diubah oleh pihak yang tidak berwenang. Hal ini melibatkan transmisi pesan yang harus tetap menjaga aspek integritas agar pesan yang dikirim asli dan sesuai dengan pesan yang diterima.

3. *non-Repudiation* (Anti-penyangkalan)

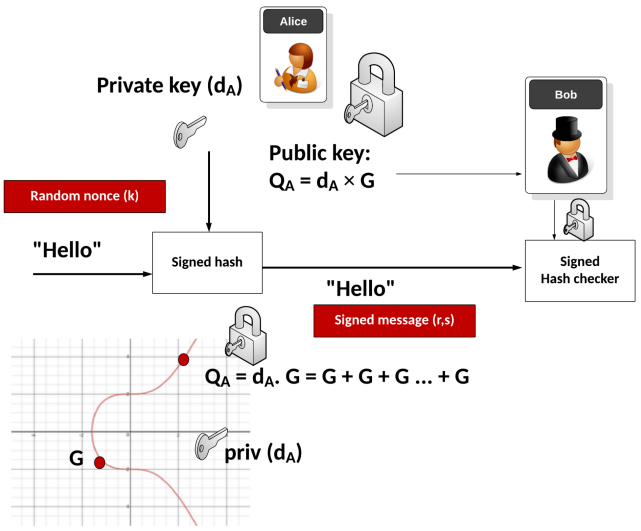
Aspek ini memberikan keamanan dari penyangkalan bahwa suatu pesan atau data berasal dari pihak tertentu atau menjaga kebenaran dari seseorang telah melakukan sebuah aksi terhadap pesan atau data yang berisi informasi. Hal ini berguna dalam proses pertanggungjawaban oleh pengirim terhadap konten dari pesan.

Berdasarkan aspek - aspek tersebut, dengan tanda tangan digital, pengirim pesan dapat mengirimkan pesan dengan memberikan penanda keaslian atau keabsahan dari pesan tersebut berupa identitas pengirim pesan dan penerima pesan dapat melakukan validasi dan verifikasi keaslian pesan tersebut. Hal itu menunjukkan bahwa tanda tangan digital memberikan layanan integritas data pada pesan yang dikirimkannya. Tanda tangan digital menjamin hanya penerima yang tepat dapat melakukan proses verifikasi tersebut sehingga aspek - aspek kriptografi tetap terpenuhi seperti otentikasi tetap terjaga dan pengirim tidak dapat menyangkal telah mengirimkan pesan karena identitasnya tercantum dalam pesan tersebut berupa tanda tangan digital.

B. Algoritma ECDSA

Algoritma Elliptic Curve Digital Signature Algorithm (ECDSA) merupakan algoritma variasi dari Digital Signature Algorithm (DSA) yang menggunakan elliptical curve. Algoritma tanda tangan digital ini berfungsi untuk mengecek apakah pesan yang dikirimkan dari pengirim ke penerima merupakan pesan yang memiliki keabsahan dan tidak diubah isinya.

ECDSA memiliki kesamaan dengan DSA yang menggunakan pasangan kunci public dan kunci privat dalam pembuatan sebuah tanda tangan digital. ECDSA merupakan perkembangan lebih lanjut dari DSA yang memiliki keamanan lebih ketat dalam kesulitan pemecahan persamaan kurva eliptik. ECDSA tidak memiliki algoritma yang bersifat *subexponential-time* sehingga memiliki kekuatan per bit kunci yang lebih besar dibandingkan algoritma tanda tangan digital yang tidak berbasis kurva eliptik.



Gambar 1. Algoritma ECDSA

Secara garis besar ada 3 tahapan yang harus dipenuhi di dalam algoritma ECDSA yaitu Key Generation, Sign, dan Verify.

1. Key Generation

Pada tahap ini dilakukan pembangkitan kunci baik kunci public maupun kunci privat. Kunci public akan digunakan penerima pesan untuk memastikan keaslian pesan dalam tahap *verify*. Kunci privat akan digunakan pada tahap *sign* untuk menghasilkan *sign* atau penandatanganan pesan.

2. Sign

Pada tahap ini dilakukan penandatanganan pesan atau data atau dokumen elektronik yang menggunakan kunci privat pengirim pesan. Namun, sebelum dilakukan penandatanganan, pesan tersebut dilakukan hashing terlebih dahulu dengan fungsi hash SHA-3.

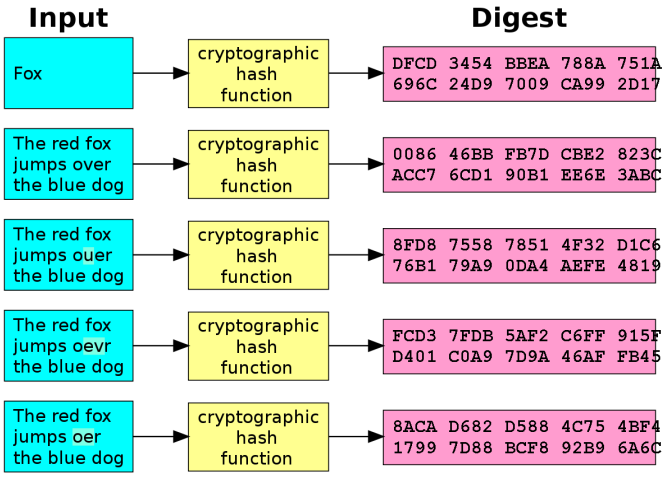
3. Verify

Pada tahap ini dilakukan oleh penerima pesan untuk memastikan keaslian dari pesan yang diterimanya. Penerima pesan melakukan pengecekan keabsahan pesan berikut tanda tangan digital yang ada dengan menggunakan kunci publik yang diberikan oleh pengirim pesan. Apabila validasi ini berhasil atau valid maka pesan ini dianggap asli, namun apabila sebaliknya maka bagian dari pesan tersebut ada yang berubah dengan pesan yang dikirimkan.

C. Fungsi Hash

Fungsi hash adalah sebuah fungsi yang digunakan untuk mengkompresi sebuah data berukuran sembarang menjadi sebuah string yang berukuran tetap. String yang berukuran tetap tersebut disebut dengan *hash value* atau *message digest. Message Digest* yang dihasilkan dapat digunakan untuk merepresentasikan data. Namun, *message digest* yang sudah dihasilkan tidak dapat diubah kembali menjadi data sebelumnya sehingga fungsi hash dapat disebut sebagai fungsi yang *irreversible.*

Fungsi hash dapat dijamin keamanannya karena apabila sebuah huruf atau bit diganti pada message, maka akan menghasilkan message digest yang berubah secara sepenuhnya. Hal tersebut dapat dilihat pada gambar sebagai berikut.



Gambar 2. Contoh hasil input dan message digest dari fungsi hash

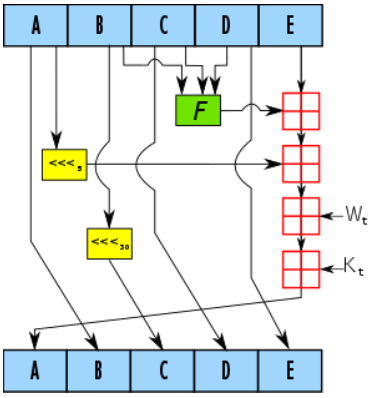
SHA merupakan sebuah grup fungsi hash yang dipublikasikan oleh *National Institute of Standards and Technology* (NIST). Terdapat beberapa fungsi *hash,* yaitu:

1. SHA-0

SHA-0 merupakan fungsi *hash* pertama dari grup SHA yang dikembangkan oleh NIST pada tahun 1993. SHA-0 menghasilkan message digest sepanjang 160-bit. Namun terdapat kelemahan yang cukup signifikan sehingga SHA-0 dikembangkan lebih lanjut dan menjadi SHA-1.

2. SHA-1

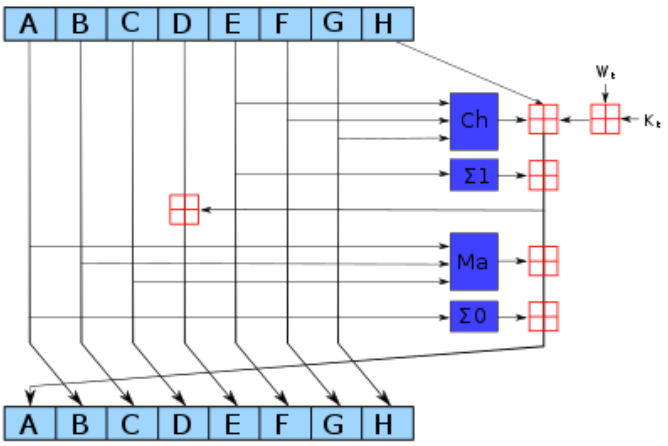
SHA-1 dikembangkan oleh NIST pada tahun 1995 untuk menggantikan SHA-0. SHA-1 menghasilkan *message digest* sepanjang 160-bit. Namun terdapat kelemahan pada SHA-1 yang rentan terhadap *collision attack* dan *chosen-prefix attack* sehingga tidak digunakan lagi khususnya untuk tanda tangan digital.



Gambar 3. SHA-1

3. SHA-2

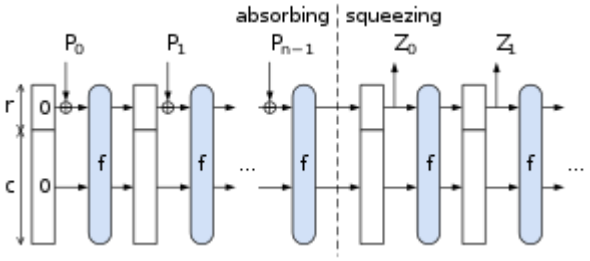
SHA-2 dikembangkan pada tahun 1995 untuk menggantikan SHA-1. SHA-2 menghasilkan keluaran sepanjang 224, 256, 384, dan 512 bits. SHA-2 menggunakan struktur yang sama dengan SHA-1, tetapi lebih kompleks dengan penambahan fungsi non linear ke fungsi kompresi. Namun hal tersebut malah membuat SHA-2 memiliki kinerja yang kurang cepat dibandingkan SHA-1, tetapi lebih aman daripada SHA-1.



Gambar 4. SHA-2

4. SHA-3

SHA-3 atau disebut juga dengan Keccak merupakan komplementer dari fungsi hash SHA-1 dan SHA-2. SHA-3 menggunakan *sponge construction* yang didasarkan pada perhitungan fungsi bilangan acak dan fungsi permutasi acak. Setiap pesan akan terbagi menjadi beberapa bagian yang disebut 'spons' berisi data dan dimampatkan menjadi subset yang lebih padat dan digunakan sebagai message digest. SHA-3 menghasilkan message digest sepanjang 224, 256, 384, dan 512 bits



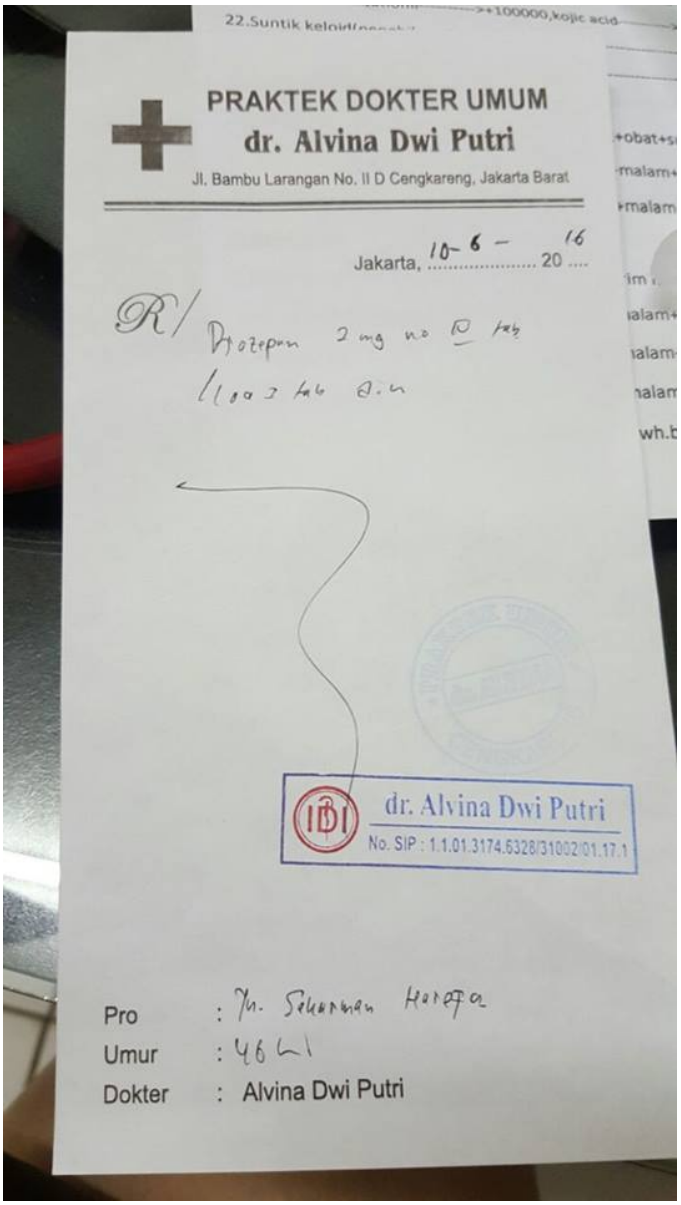
Gambar 5. SHA-3

D. Resep obat

Resep adalah suatu permintaan tertulis dari dokter, dokter gigi atau dokter hewan kepada apoteker untuk membuatkan obat dalam bentuk sediaan tertentu dan menyerahkannya kepada pasien. Resep merupakan perwujudan akhir dari kompetensi, pengetahuan dan keahlian dokter dalam

menerapkan pengetahuannya dalam bidang farmakologi dan terapi.

Penulisan resep harus ditulis dengan jelas sehingga dapat dibaca oleh petugas di apotek. Resep yang ditulis dengan tidak jelas akan menimbulkan terjadinya kesalahan saat peracikan / penyiapan obat dan penggunaan obat yang diresepkan. Berikut gambar dibawah ini merupakan contoh resep obat yang diberikan dokter kepada pasiennya.



Gambar 6. Contoh resep obat

III. Rancangan Solusi dan Implementasi

Dalam menyelesaikan permasalahan, terdapat langkah - langkah penyelesaian yaitu Deskripsi Umum, Rancangan, dan Implementasi Solusi.

A. Deskripsi Umum Solusi

Dalam menyelesaikan permasalahan otentikasi resep obat dokter digital, digunakan pendekatan tanda tangan digital (*digital signature)* dengan metode kombinasi fungsi *hash* dan kriptografi kunci publik. Dengan menggunakan tanda tangan digital, *request* tebus resep obat ke apotek secara digital dapat dipastikan aspek - aspek *authentication, data integrity,* dan *non-repudiation.*

Fungsi hash yang digunakan adalah SHA-3 dengan ukuran 256-bit (SHA3-256) dengan pertimbangan bahwa SHA3 merupakan fungsi hash yang menjadi standar dan masih belum ditemukan kolisi. Panjang message digest yang dipilih adalah 256-bit dengan pertimbangan keamanan dan kecepatan pemrosesan.

Terakhir, pada tanda tangan digital digunakan algoritma ECDSA yang berbasis pada konsep matematika *elliptic curve*. Pemakaian algoritma ini dengan pertimbangan bahwa salah satu keunggulan dari algoritma ECDSA dibandingkan dengan algoritma lain yaitu contohnya adalah RSA yaitu untuk menghasilkan tingkat keamanan yang sama, kebutuhan komputasi yang diperlukan oleh algoritma ECDSA lebih kecil dibandingkan dengan algoritma RSA.

B. Rancangan Solusi

Solusi yang dirancang terdiri dari 2 tahapan yaitu pada saat Dokter memberikan resep obat dengan mencantumkan tanda tangan digitalnya kepada pasien, lalu tahap selanjutnya saat apotek memverifikasi resep obat yang dikirimkan oleh pasien apakah memiliki keaslian dan keabsahan pada pesan tersebut. Namun pada program terdapat 3 tahapan, dimana di awal perlu dilakukan pembangkitan kunci privat dan kunci publik.

C. Implementasi Solusi

1. Pertama - tama dilakukan pembangkitan kunci privat dan kunci publik.

   Private key

   ```
   -----BEGIN EC PRIVATE KEY-----
   MHQCAQEEIEqpGEmMHClW1d9nlEYflGoX7
   UsW4OkST4G1GtAaFGlVoAcGBSuBBAAK
   oUQDQgAE2PjBL6EcJL+U292hmRnxMwscMo
   QN1TJhD7MmAIlRxsmGqKGiEHQ43KlU
   duAJRDuBUsHx0m2mSA0VhLcsuyIRAg==
   -----END EC PRIVATE KEY-----
   ```

   Public key

   ```
   -----BEGIN PUBLIC KEY-----
   MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAE2
   PjBL6EcJL+U292hmRnxMwscMoQN1TJh
   D7MmAIlRxsmGqKGiEHQ43KlUduAJRDuBUs
   ```

```
Hx0m2mSA0VhLcsuyIRAg==
-----END PUBLIC KEY-----
```

2. Setelah kunci telah dibangkitkan, pesan berupa resep obat diinput dan dilakukan fungsi hash

   Resep obat

```
R/ Ceftik 10 mg
 Epexol 5 mg
 Salbutamol 0,425 mg
 Longatin 4,5 mg
 Rhinofed 1/12 tab
 Dexametason 1/5 tab
 Mfla pulv dtd no XV
 S 3 dd pulv. I
 ----------z
 Pro : anak 8 bulan
```

   Hasil Hash

```
badd935c20a3d025c24b8d04503fd1e334ca25b8e0
99a0e8493286972d364d1f
```

   Lalu setelah itu digital signature dibuat

```
MEYCIQCu1dIYOtJtVhrQ9KFUM2i7yQ1FEuRw
YIka5se5WNTUSgIhAPlUu5cYbeoN7Zl3SFWXk
uX6tWTwh4aLnb8kmSzbx7Rx
```

   Pesan yang dikirimkan

```
R/ Ceftik 10 mg
 Epexol 5 mg
 Salbutamol 0,425 mg
 Longatin 4,5 mg
 Rhinofed 1/12 tab
 Dexametason 1/5 tab
 Mfla pulv dtd no XV
 S 3 dd pulv. I
 ----------z
 Pro : anak 8 bulan

MEYCIQCu1dIYOtJtVhrQ9KFUM2i7yQ1FEuRw
YIka5se5WNTUSgIhAPlUu5cYbeoN7Zl3SFWXk
uX6tWTwh4aLnb8kmSzbx7Rx
```

3. Melakukan validasi keabsahan dari pesan yang diterima

   Pesan tersebut dilakukan pengecekan berdasarkan digital signature yang ada.

   Dengan menggunakan tanda tangan digital yang sesuai, akan menghasilkan output valid

Kunci publik	-----BEGIN PUBLIC KEY----- MFYwEAYHKoZIzj0C AQYFK4EEAAoDQgA E2PjBL6EcJL+U292hm RnxMwscMoQN1TJh D7MmAIlRxsmGqKGiE HQ43KlUduAJRDuBUs Hx0m2mSA0VhLcsuyI RAg== -----END PUBLIC KEY-----
Tanda tangan digital awal	MEYCIQCu1dIYOtJtVh rQ9KFUM2i7yQ1FEuR wYIka5se5WNTUSgIhA PlUu5cYbeoN7Zl3SFW XkuX6tWTwh4aLnb8k mSzbx7Rx
Tanda tangan digital akhir	MEYCIQCu1dIYOtJtVh rQ9KFUM2i7yQ1FEuR wYIka5se5WNTUSgIhA PlUu5cYbeoN7Zl3SFW XkuX6tWTwh4aLnb8k mSzbx7Rx
Hasil verifikasi	Valid

   Namun, apabila terdapat perbedaan tanda tangan digital didalamnya akan menghasilkan hasil verifikasi invalid. Contohnya pada tanda tangan digital diubah pada 2 karakter terakhir sebagai berikut:

Kunci publik	-----BEGIN PUBLIC KEY----- MFYwEAYHKoZIzj0C AQYFK4EEAAoDQgA E2PjBL6EcJL+U292hm RnxMwscMoQN1TJh D7MmAIlRxsmGqKGiE HQ43KlUduAJRDuBUs Hx0m2mSA0VhLcsuyI RAg== -----END PUBLIC

	KEY-----
Tanda tangan digital awal	MEYCIQCu1dIYOtJtVhrQ9KFUM2i7yQ1FEuRwYIka5se5WNTUSgIhAPlUu5cYbeoN7Zl3SFWXkuX6tWTwh4aLnb8kmSzbx7Rx
Tanda tangan digital akhir	MEYCIQCu1dIYOtJtVhrQ9KFUM2i7yQ1FEuRwYIka5se5WNTUSgIhAPlUu5cYbeoN7Zl3SFWXkuX6tWTwh4aLnb8kmSzbx7**ZZ**
Hasil verifikasi	Invalid

IV. KESIMPULAN

Penggunaan tanda tangan digital pada resep obat yang diberikan dokter dapat sangat bermanfaat di masa pandemi Covid-19. Masyarakat diberi kemudahan tanpa perlu keluar rumah untuk melakukan pengobatan terhadap penyakit yang diidapnya dengan melakukan konsultasi dan memesan obat sesuai resep yang diberikan dokter secara daring. Tanda tangan digital ini menjadi suatu validasi dalam melakukan pertukaran informasi seperti resep obat ini.

REFERENSI

[1] R. Kaur and A. Kaur, "Digital Signature," 2012 International Conference on Computing Sciences, Phagwara, 2012, pp. 295-301, doi: 10.1109/ICCS.2012.25.

[2] Slide kuliah IF4020 Kriptografi. Rinaldi Munir

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

Valentinus Devin Setiadi -13518116