IJAI (Indonesian Journal of Applied Informatics)
Vol. 6 No. 2 Tahun 2022 pISSN: 2548-3846, eISSN: 2598-5981

# Rancang Bangun Validitas Dokumen Elektronik Menggunakan Metode Algoritma RSA dan AES

**Mokhammad Iqbal,** Fatkhul Amin
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Stikubank
Email: kangmas.iqbal@gmail.com, fatkhulamin@edu.unisbank.ac.id

**Info Artikel**

**Kata Kunci :**
Validitas dokumen elektronik, tanda tangan digital, QR-Code, RSA, AES

**Keywords :**
Validity of electronic documents, digital signatures, QR-Code, RSA, AES

**Tanggal Artikel**
Dikirim : 20 Januari 2022
Direvisi : 21 Januari 2022
Diterima : 30 Mei 2022

**Abstrak**

Tanda tangan digital adalah skema matematis untuk memverifikasi keaslian suatu pesan atau dokumen digital sehingga keberadaan tanda tangan digital pada suatu dokumen elektronik dapat menunjukkan keaslian suatu dokumen yang dijamin. Dokumen elektronik ini tetap merupakan dokumen resmi yang penting seperti dokumen cetak. Tanda tangan digital sangat bergantung pada isi dokumen yang ditandatangani, sehingga setiap dokumen akan menghasilkan tanda tangan digital yang berbeda dengan dokumen lainnya. Perkembangan teknologi memungkinkan untuk dilakukan pembuktian matematis, dimana informasi yang diperoleh satu pihak dari pihak lain dapat ditentukan untuk menjamin keaslian informasi atau dokumen elektronik yang diterima. Tanda tangan digital yang dirancang pada penelitian ini mengimplementasikan QR-Code, fungsi hashing MD5 dan algoritma yang akan ditambahkan adalah kombinasi enkripsi RSA dan AES dengan ukuran blok 256 bit.

**Abstarct**

*Digital signature is a mathematical scheme to verify the authenticity of a message or digital document so that the presence of a digital signature on an electronic document can indicate the authenticity of a guaranteed document. These electronic documents remain as important official documents as printed documents. Digital signatures are very dependent on the contents of the signed document, so each document will produce a digital signature that is different from other documents. Technological developments make it possible to do mathematical proofs, where information obtained by one party from another can be determined to ensure the authenticity of the information or electronic documents received. The digital signature designed in this study implements a QR-Code, MD5 hashing function and the algorithm that will be added is a combination of RSA and AES encryption with a block size of 256 bits.*

## 1. PENDAHULUAN

### 1.1 *Latar Belakang Masalah*

Pandemi Covid-19 menjadikan kesehatan sebagai prioritas utama. Namun, banyak orang takut untuk melakukan konsultasi ke tenaga medis di fasilitas kesehatan. Khawatir tertular virus Covid-19 jika pergi ke layanan kesehatan membuat banyak pasien dengan penyakit kronik tidak bisa mengontrol penyakitnya. Mereka juga menunda melakukan konsultasi ke tenaga medis jika ada keluhan sehingga kondisinya bisa terlanjur parah. Penggunaan dan peningkatan inovasi digital di bidang kesehatan dapat dijadikan sebagai solusi. Melalui program atau aplikasi kesehatan masyarakat, mereka dapat berkonsultasi dengan tenaga medis jika mereka memiliki keluhan sebelum mereka berobat ke fasilitas kesehatan atau rumah sakit. Beberapa fasilitas kesehatan saat ini sudah menerapkan klinik virtual dan rekam medik elektronik sehingga informasi mengenai kondisi pasien sudah berupa dokumen elektronik, baik dokumen pemeriksaan rawat jalan, rawat inap, resep obat, order pemeriksaan penunjang dan hasil dari pemeriksaan dimana seluruh dokumen elektronik yang diterbitkan sudah terdapat tanda tangan digital berupa QR-Code.

Tanda tangan digital adalah mekanisme otentikasi yang memungkinkan pembuat dokumen untuk menambahkan sebuah kode yang berfungsi untuk memastikan keaslian sebuah informasi atau dokumen elektronik. Perkembangan teknologi memungkinkan untuk

dilakukan pembuktian matematis, dimana informasi yang diperoleh satu pihak dari pihak lain dapat ditentukan untuk menjamin keaslian informasi atau dokumen elektronik yang diterima. Tujuan dari penelitian ini menerapkan QR-Code dan algoritma yang akan ditambahkan, yaitu RSA (*Rivest – Shamir – Adleman*) dan AES (*Advanced Encryption Standard*) sebagai tanda tangan digital, adalah untuk memfungsikannya sebagai otentikasi yang sah dari informasi dan dokumen elektronik yang diterbitkan oleh fasilitas kesehatan. Dokumen elektronik dapat digunakan oleh pemiliknya baik sebagai surat pengantar ke unit pemeriksaan penunjang, pengambilan resep obat, dan hasil dari pemeriksaan. Namun, karena bentuknya berupa file digital yang ditransmisikan melalui internet, dokumen elektronik rentan adanya pemalsuan, baik fabrikasi maupun modifikasi data, sehingga diperlukan sebuah aplikasi yang bisa digunakan untuk melakukan *crosscheck* terhadap dokumen elektronik yang diterbitkan oleh fasilitas kesehatan baik melalui scan QR-Code maupun *upload* dokumen PDF yang sudah diterbitkan.

### 1.2 *Pustaka Yang Terkait Dengan Penelitian*

Pada penelitian terdahulu yang dilakukan oleh Abdul Gani Putra Suratma, Abdul Azis pada tahun 2017 dalam jurnal dengan judul "Tanda Tangan Digital Menggunakan QR-Code Dengan Metode *Advanced Encryption Standard*" dijelaskan bahwa metode penelitian yang digunakan adalah metode eksperimen. Eksperimen dalam penelitian ini bertujuan untuk menerapkan sistem tanda tangan secara digital yang akurat dan dapat memangkas waktu serta biaya. Dengan metode penelitian ini, informasi dalam QR-Code yaitu data dokumen dienkripsi dan didekripsi dengan menggunakan algoritma AES, sehingga dokumen tetap terjamin keasliannya dari penyalahgunaan informasi. Implementasi aplikasi menggunakan dua buah system, system pertama berbasis web digunakan oleh administrator dan pimpinan untuk pembuatan dokumen yang diterapkan tanda tangan digital, system kedua berbasis desktop digunakan oleh operator gudang untuk scan QR-Code dokumen dan verifikasi. Hasil pemindaian kemudian didekripsi oleh sistem. Jika hasil dekripsi menunjukkan bahwa dokumen disetujui, maka permintaan barang dapat ditindaklanjuti [1].

Penelitian lain yang dilakukan oleh Fitri Nuraeni, Yoga Handoko Agustin, Dede Kurniadi, Imas Dewi Ariyanti pada tahun 2020 dalam jurnal dengan judul "Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik" dijelaskan tanda tangan digital yang dirancang pada penelitian ini terdiri dari fungsi hashing SHA-3 dan super enkripsi kombinasi RSA dan AES dengan ukuran blok 128bit dan mode operasi CBC. Penggunaan super enkripsi ini terbukti dapat meningkatkan jaminan keamanan dengan kualitas enkripsi yang bagus yaitu 1) rata-rata waktu proses enkripsi dan dekripsi cepat di bawah 0,1 milisecond; 2) nilai entropi cukup bagus sebesar 4,96 yang lebih mendekati 8; serta nilai avalanche effect 40,61% yang bagus karena mendekati 50% perubahan pada perbedaan 1bit plainteksnya. Sistem tanda tangan digital ini menjadi lebih mudah digunakan karena disisipkan pada file sertifikat elektronik menggunakan skema QR-Code. Implementasi aplikasi menggunakan dua buah system, system pertama berbasis web digunakan untuk penerbitan tanda tangan digital, system kedua berbasis mobile untuk kemudahan proses verifikasi dengan tambahan fasilitas untuk membaca QR-Code [2].

Penelitian lain yang dilakukan oleh Firda Zulivia Abraham, Paulus Insap Santosa, dan Wing Wahyu Winarno pada tahun 2018 dalam jurnal dengan judul "Tandatangan Digital Sebagai Solusi Teknologi Informasi dan Komunikasi (TIK) Hijau: Sebuah Kajian Literatur". Penelitian ini membahas mengenai pemanfaatan tanda tangan digital untuk mendukung program Green Information and Communication Technology (*Green* ICT), dengan bertujuan salah satunya adalah untuk mengurangi penggunaan kertas di lingkungan perkantoran. Metode yang digunakan adalah PKCS#12, karena metode ini tidak memerlukan infrastruktur tersendiri sehingga dapat lebih menghemat biaya. Microsoft mengadopsi PKCS#12: *Personal Information Exchange Syntax Standard* yang disediakan oleh RSA. Pada metode ini semua informasi dapat diuraikan melalui pengiriman sintaks. Informasi yang tersimpan dalam PKCS#12 adalah informasi pribadi, termasuk kunci privat, sertifikat, serta data rahasia lainnya yang terkait dengan pengguna. Model tanda tangan digital dengan PKCS#12 hanya seperti menempelkan sebuah tanda air (segel) pada dokumen. Segel pada dokumen tersebut menurut UU ITE setara dengan tanda tangan dan stempel basah tradisional. Sertifikat PKCS#12 berbentuk *file* dan dapat disimpan pada semua media penyimpanan, termasuk pada penyimpanan *cloud*, sehingga metode ini dapat dikatakan fleksibel untuk digunakan. Keamanan dan fleksibilitas PKCS#12 bergantung pada kata sandi pengguna. Salah satu keunggulan penggunaan tanda tangan digital yaitu tidak dapat dipalsukan, tidak seperti tanda tangan basah dengan pena yang masih dapat ditiru atau dijiplak oleh orang lain. Sehingga tanda tangan digital ini memberikan jaminan anti penyangkalan, yang artinya seseorang tidak bisa menyangkal bahwa dia tidak menandatangani sebuah dokumen atau *file* digital, sementara kata sandi tetap dirahasiakan dan sudah disimpan di aplikasi pengolah dokumen [3].

Penelitian lain yang dilakukan oleh Mohamad Ihwani pada tahun 2016 dalam jurnal dengan judul "Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma RSA" membahas mengenai penerapan algoritma RSA pada tanda tangan digital. Mekanisme yang diterapkan yaitu dokumen terlebih dahulu dilakukan fungsi hash MD5 sehingga menghasilkan *message digest*. *Message digest* yang dihasilkan kemudian dienkripsi menggunakan kunci publik dari algoritma RSA yang sebelumnya telah dibangkitkan terlebih dahulu bersama dengan pasangan kunci privatnya. Hasil enkripsi ini yang digunakan menjadi tanda tangan digital. Selanjutnya dokumen beserta tanda tangan digital dan kunci privat dikirimkan kepada penerima pesan. Pada proses verifikasi, penerima pesan mendekripsi tanda tangan digital menggunakan kunci privat yang diterimanya dan membandingkan dengan *message digest* dari dokumen. Apabila hasilnya bersesuaian, maka dokumen dinyatakan valid, sebaliknya jika hasil dekripsi dengan *message digest*

dokumen tidak bersesuaian maka dokumen tersebut dinyatakan tidak valid. Ketidaksesuaian tersebut dapat terjadi misalnya dikarenakan ada pihak yang tidak berhak yang telah mengubah-ubah isi dokumen, sehingga *message digest* dari dokumen juga akan berubah [4].

Penelitian lain yang dilakukan oleh Trihastuti Yuniati, Muhammad Fajar Sidiq pada tahun 2019 dalam jurnal dengan judul "*Literature Review*: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi" Pada penelitian ini topik yang dipilih adalah mengenai tanda tangan digital dan legalisasi dokumen elektronik. Langkah-langkah dari literature review meliputi 4 tahapan, yaitu: (1) formulasi permasalahan, (2) pencarian literatur, (3) evaluasi data, serta (4) analisis dan interpretasi. Adapun cara melakukan literature review yaitu: mencari kesamaan (*compare*), mencari ketidaksamaan (*contrast*), memberikan pandangan (*criticize*), membandingkan (*synthesize*), dan meringkas (*summarize*) dari beberapa penelitian terkait [5].

### 1.3 *Perbedaan Dengan Penelitian Sebelumnya*

Ringkasan perbedaan yang dilakukan dengan penelitian sebelumnya ditunjukkan pada tabel 1 berikut

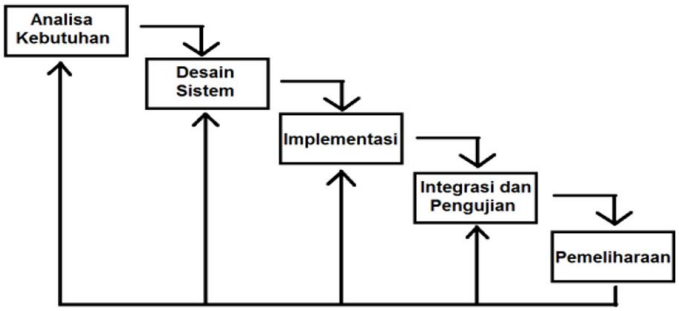
**Tabel 1. Perbedaan yang dilakukan dengan penelitian sebelumnya**

| Nama Peneliti | Judul Penelitian | Perangkat Lunak Pengembangan Sistem | Metode Pengembangan Sistem | Gambaran Sistem |
|---|---|---|---|---|
| 1. Abdul Gani Putra Suratma, Abdul Azis (2017) | 1. Tanda Tangan Digital Menggunakan QR-Code Dengan Metode Advanced Encryption Standard. | 1. ASP.Net, C#, SQL Server | 1. Metode yang digunakan untuk penelitian ini adalah Eksperimen. | 1. Membangun sistem Informasi permintaan barang di gudang perusahaan dengan implementasi tanda tangan digital untuk melakukan verifikasi permintaan barang dari pimpinan perusahaan. |
| 2. Fitri Nuraeni, Yoga Handoko Agustin, Dede Kurniadi, dan Imas Dewi Ariyanti (2020) | 2. Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik. | 2. HTML, PHP, Android Studio | 2. Metode yang digunakan untuk penelitian ini adalah Eksperimen. | 2. Membangun sistem informasi penggunaan sertifikat elektronik pada kegiatan webinar dan kursus online. |
| 3. Firda Zulivia Abraham, Paulus Insap Santosa, dan Wing Wahyu Winarno (2018) | 3. Tandatangan Digital Sebagai Solusi Teknologi Informasi dan Komunikasi (TIK) Hijau: Sebuah Kajian Literatur. | 3. – | 3. Metode yang digunakan untuk penelitian ini adalah Literature Review. | 3. Sebuah jurnal yang berisi kumpulan penelitian tentang tanda tangan digital dengan menggunakan metode literature review. |
| 4. Mohamad Ihwani (2016) | 4. Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma RSA. | 4. PHP | 4. Metode yang digunakan untuk penelitian ini adalah Eksperimen. | 4. Merancang sistem informasi untuk pengiriman pesan dan untuk membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital. |
| 5. Trihastuti Yuniati, Muhammad Fajar Sidiq (2019) | 5. *Literature Review*: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi | 5. – | 5. Metode yang digunakan untuk penelitian ini adalah Literature Review. | 5. Sebuah jurnal yang berisi kumpulan penelitian tentang tanda tangan digital dengan menggunakan metode literature review. |
| 6. Mokhammad Iqbal (2022) | 6. Rancang Bangun Validitas Dokumen Elektronik Menggunakan Metode Algoritma RSA dan AES. | 6. Android Studio, Codeigniter, ASP.Net dan SQLServer 2008 R2. | 6. Metode yang digunakan untuk penelitian ini adalah Waterfall. | |

6. Merancang sistem informasi validitas dokumen elektronik untuk *crosscheck* keabsahan atau validitas dari dokumen elektronik yang dikeluarkan oleh fasilitas kesehatan.

## 2. METODE PENELITIAN

Penelitian ini dilakukan dengan menggunakan metode *waterfall* dilanjutkan dengan proses pembangunan aplikasi untuk penerapan dari tanda tangan digital. Pada gambar 1 menunjukkan metode penelitian yang digunakan yaitu metode *waterfall*.




**Gambar 1. Metode *waterfall***

Rosa dan Shalahuddin (2013) mengungkapkan bahwa "Model SDLC air terjun atau yang sering disebut sekuensial linier atau alur hidup klasik, dimana di dalam model air terjun ini menyedikan pendekatan alur perangkat lunak secara sekuential atau berurutan dimulai dari tahap analisa, desain, pengkodingan, pengujian dan pemeliharaan sistem (*maintenance*)" [6].

### 2.2 *Objek Penelitian*

Objek penelitian pada penulisan skripsi ini adalah RSUP Dr. Kariadi Semarang.

### 2.2 *Metode Pengumpulan Data*

Teknik yang digunakan untuk menyusun penelitian ini adalah dengan melakukan wawancara pada orang-orang yang bersangkutan dalam proses pembuatan sistem, pengamatan langsung proses suatu pengelolaan pemeriksaan pasien dari pendaftaran, pemeriksaan hingga hasil pemeriksaan selesai, dan mempelajari buku-buku literatur serta hasil dari penelitian yang berkaitan sebelumnya.

### 2.3 *Analisis Masalah*

Permasalahan yang didapatkan adalah saat ini informasi mengenai kondisi pasien sudah berupa dokumen elektronik, baik dokumen pemeriksaan rawat jalan, rawat inap, resep obat, order pemeriksaan penunjang dan hasil dari pemeriksaan. Dokumen elektronik ini tetap menjadi dokumen resmi yang penting layaknya dokumen hasil cetak, namun karena bentuknya berupa file digital yang ditransmisikan melalui internet, dokumen elektronik rentan adanya pemalsuan, baik fabrikasi maupun modifikasi data. Dengan dibangunnya aplikasi validitas dokumen elektronik ini diharapkan dapat menjadi solusi praktis yang dapat digunakan oleh siapapun dan kapanpun untuk melakukan *crosscheck* atas dokumen elektronik yang diterbitkan, apakah dokumen elektronik ini merupakan dokumen elektronik asli atau tidak.

### 2.4 *Analisis Algoritma*

Analisis data dan algoritma merupakan tahapan untuk melakukan penganalisa terhadap data-data yang dibutuhkan algoritma untuk melakukan perhitungan dalam merancang sebuah sistem dibuat. Berikut metode algoritma penyelesaiannya :

#### 2.4.1 *Algoritma RSA*

Algoritma RSA dibuat oleh tiga orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun 1976, yaitu Ron Rivest, Adi Shamir dan Leonard Adleman. RSA adalah salah satu teknik kriptografi dimana kunci untuk melakukan enkripsi berbeda dengan kunci untuk melakukan dekripsi. Kunci untuk melakukan enkripsi disebut sebagai kunci publik, sedangkan kunci untuk melakukan dekripsi disebut sebagai kunci privat. Orang yang mempunyai kunci publik dapat melakukan enkripsi tetapi yang dalam melakukan dekripsi hanyalah orang yang memiliki kunci privat. Kunci publik dapat dimiliki oleh sembarang orang, tetapi kunci privat

hanya dimiliki oleh orang tertentu saja [7]. RSA dikatakan aman, karena sulitnya memfaktorkan bilangan n, dimana n = p x q, p dan q adalah bilangan prima yang sangat besar.

### 2.4.2 *Algoritma AES*

Algoritma *Advanced Encryption Standard* (AES) adalah suatu algoritma block chiper dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (National Institute of Standard and Technology) sebagai pengganti algoritma DES (*Data Encryption Standard*) yang sudah berakhir masa penggunaannya. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Perbedaan dari ketiga urutan tersebut adalah panjang kunci yang mempengaruhi jumlah *round* (perputaran) yang dapat digambarkan dalam tabel 2 berikut [8].

**Tabel 2. Jumlah putaran pengoperasian AES**

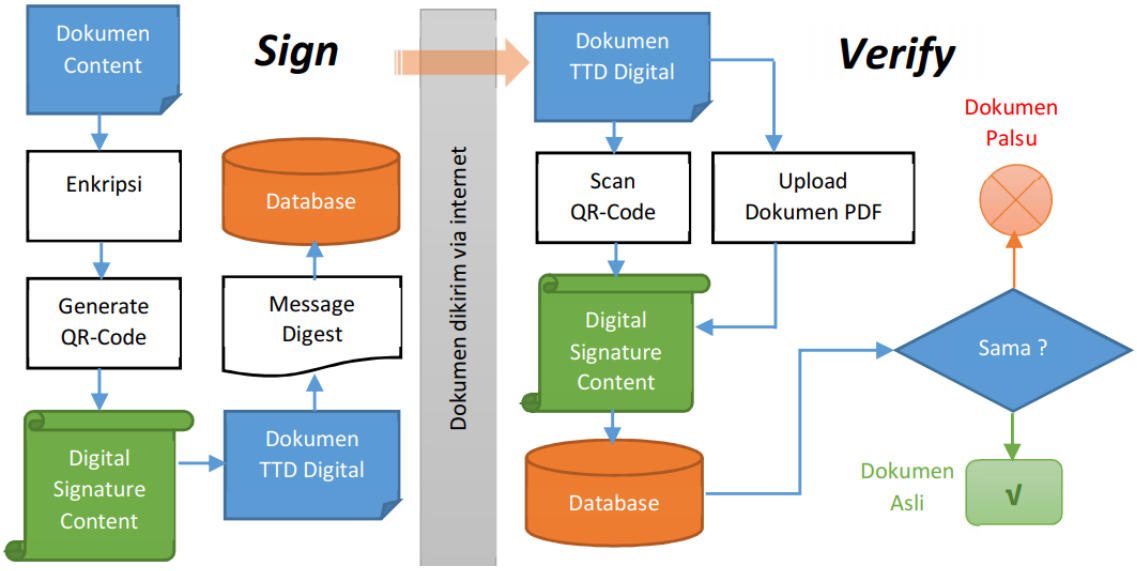
| *Tipe* | *Panjang Kunci* | *Panjang Blok Input* | *Jumlah Putaran* |
|---|---|---|---|
| AES-128 | 4 | 4 | 10 |
| AES-192 | 6 | 4 | 12 |
| AES-256 | 8 | 4 | 14 |

## 3. HASIL DAN PEMBAHASAN

Penelitian, analisis dan perancangan sistem informasi validitas dokumen elektronik menghasilkan sebuah aplikasi mobile berbasis Android. Aplikasi ini dapat digunakan oleh oleh siapa saja yang akan mengecek keaslian dokumen elektronik untuk berbagai keperluan lainnya. Penelitian ini mengimplementasikan dua buah sistem, sistem pertama berupa aplikasi mobile berbasis Android, digunakan untuk melakukan melakukan *crosscheck* atas dokumen elektronik yang diterbitkan, sistem kedua berbasis web, digunakan untuk menerbitkan dokumen elektronik yang sudah ditandatangani secara digital serta sebagai webapi dari aplikasi mobile.

### 3.1 *Desain Tanda Tangan Digital*

Tanda tangan digital memiliki dua proses utama yaitu *sign* dan *verifiy*. Pada gambar 2 menunjukkan proses *sign* dan *verify* dokumen elektronik. Proses penandatanganan (*sign*) diawali dengan user melakukan permintaan cetak atau *download* dokumen elektronik. Data permintaan cetak dokumen elektronik (*document content*) dikirim melalui jaringan internet dengan format JSON.




**Gambar 2. Skema proses *sign* dan *verify* dokumen elektronik.**

### 3.2 *Proses Tanda Tangan Digital*

Proses enkripsi akan menerbitkan kode autentifikasi, kode token dan QR-Code dari data yang dikirimkan. Setelah penerbitan kode autentifikasi dan token selesai maka proses selanjutnya adalah pembangkitan kode QR dengan proses enkripsi menggunakan kunci private yang dihasilkan dari algoritma RSA. Algoritma RSA ini merupakan sistem kriptografi asimestris yang dapat digunakan untuk memberikan layanan privacy dan keaslian data digital sehingga banyak digunakan untuk mengamankan lalu lintas dokumen elektronik melalui internet. Untuk meningkatkan keamanan pada penelitian ini dilakukan proses enkripsi sebanyak dua kali. Setelah proses dienkripsi mengunakan RSA lalu dienkripsi kembali menggunakan algoritma AES. Advance Encryption Standard (AES) cukup berbeda dengan RSA, karena merupakan kriptografi kunci simetris, yaitu sistem kriptografi menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya. AES merupakan algoritma yang memproses data dalam ukuran blok 128, 256 atau 512 bit. Algoritma ini juga memiliki tingkat keamanan dan performa yang bagus. Proses enkripsi AES inilah yang menghasilkan QR-Code. Gambar dari QR-Code kemudian dimasukan pada dokumen elektronik dan dikonversi ke dalam bentuk Byte.

Langkah selanjutnya adalah melakukan penandatanganan dokumen elektronik dari dokumen yang sudah disisipkan QR-Code dengan menggunakan teknologi PKCS#12. Dengan teknologi PKCS#12, semua informasi dapat diuraikan melalui pengiriman sintaks, informasi yang tersimpan dalam metode PKCS#12 adalah identitas dokumen elektronik, kode MD5, QR-Code, dan ekstensi-ekstensi lainnya yang berhubungan dengan keabsahan dokumen elektronik.

Langkah terakhir yaitu mengambil intisari dari dokumen (*message digest*) menggunakan fungsi hash MD5. Fungsi hash digunakan untuk mendapatkan nilai hash dari data yang ada pada dokumen, dan biasanya hanya proses satu arah, dimana hasil hashing tidak dapat diproses kembali untuk mendapatkan data aslinya seperti proses dekripsi pada sistem kriptografi. Setelah itu seluruh konten akan disimpan kedalam database. Dari seluruh rangkaian proses tersebut, maka hasil proses enkripsi dapat dilihat pada tabel 2 berikut:

**Tabel 2. Hasil enkripsi dan pembangkitan QR-Code.**

| | |
|---|---|
| **Data Pemeriksaan** | Nama Pasien : ARIFIN SIANTURI<br>No RM : C8xxxxx<br>Tgl Lahir/Umur : xx-xx-1970 50 Thn,3 Bln,22 Hari Th<br>Jenis Kelamin : L<br>No Register : 10901464<br>Tanggal Masuk : 07-07-2020<br>Ruang Rawat : ELANG I (JANTUNG LAMA)<br>Kelas Rawat : III<br>Nama DPJP : Aruman Yudanto Aribowo Binarso Mochtar,dr.,SpJP, FIHA<br>Nama PPJA : DINA WIJAYANTI |
| **Data Permintaan Cetak Dokumen** | json_encode(array(<br>'data'=>array(<br>'noRM' => $mrno,<br>'data_PPA' =>array(<br>array(<br>'userID' => $idPPA,<br>'tglCetak' => date('Y-m-d H:i:s')<br>),<br>'noRegister' => $noreg,<br>'noRM' => $mrno,<br>'tglCreated' => date('Y-m-d H:i:s'),<br>'documentContent' => $file_base64<br>)<br>)<br>)); |
| **QR-Code (enkripsi RSA dan AES)** | cc4965c28c6025d29d2277d58e4c1125710e3302215411e9e14556f328ae9a11 |

| **Gambar QR-Code** | |
|---|---|

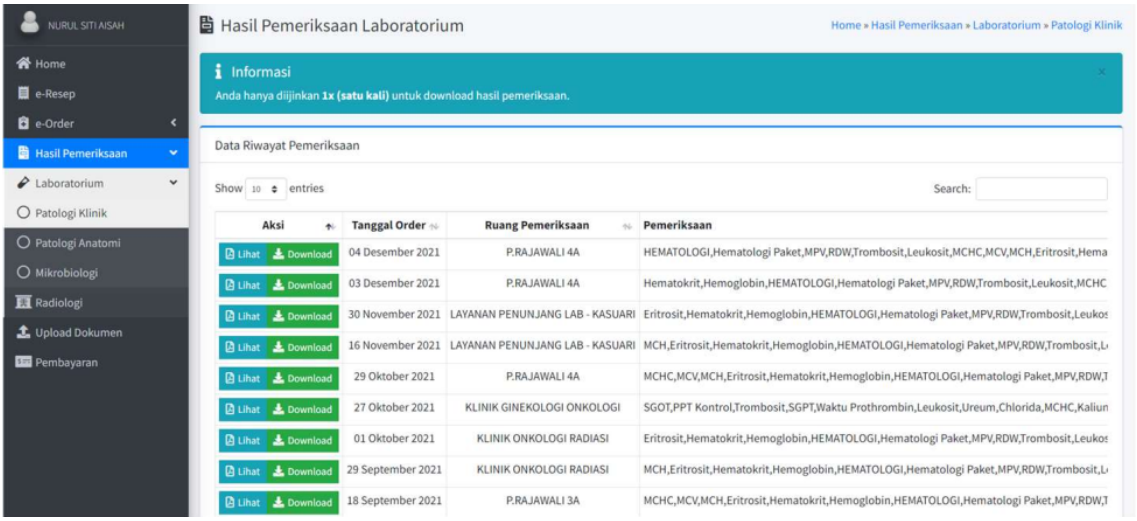
Untuk kebutuhan pengecekan otentifikasi dokumen elektronik tersebut, maka proses *verify* pada tanda tangan digital dilakukan. Proses ini dilakukan dengan dua cara, yaitu :

1. Membaca scan QR-Code. Proses scan QR-Code dilakukan untuk mendapatkan kode tanda tangan digital. Setelah kode didapatkan, maka langkah selanjutnya adalah mengirimkan kode tersebut ke server untuk mendapatkan Digital Signature Content. Apabila data ditemukan maka data terkait dokumen akan ditampilkan dalam bentuk tampilan validitas dokumen elektronik. Melalui aplikasi ini, pengguna juga dapat melihat dokumen melalui aplikasi yang telah di-scan QR-Code dengan format PDF.
2. Melakukan *upload* dokumen elektronik. Proses *upload* dokumen elektronik digunakan untuk verifikasi apakah dokumen tersebut merupakan dokumen elektronik yang di terbitkan atau tidak. Dokumen yang di *upload* harus berupa file PDF. Setelah pengguna memilih dokumen yang akan di *upload*, langkah selanjutnya aplikasi akan melakukan konversi file PDF tersebut kedalam bentuk byte yang selanjutnya dikonversi kembali menjadi format Base64 kemudian data tersebut dikirim ke server dalam bentuk JSON. Hasil dari proses ini akan ditampilkan dalam bentuk tampilan validitas dokumen elektronik.

### 3.3 *Hasil Penelitian, Implementasi dan Pengujian*

Setelah desain validitas dokumen elektronik telah dibuat, kemudian dibangun aplikasi yang merupakan hasil dari rancangan tersebut dengan menggunakan PHP untuk versi web klinik virtual dan sebagai webapi dari aplikasi mobile. Sedangkan untuk kemudahan proses cek dokumen dan verifikasi dibangun aplikasi berbasis mobile Android dengan tambahan fasilitas untuk membaca QR-Code dan *upload* dokumen PDF.

a. Halaman cetak atau *download* dokumen elektronik web klinik virtual
   Halaman cetak atau *download* dokumen elektronik ada dalam aplikasi Klinik Virtual. Sistem memiliki prosedur login bagi user yang akan menggunakannya. User disini adalah pasien. Gambar 3 menunjukkan halaman cetak atau *download* dokumen elektronik.

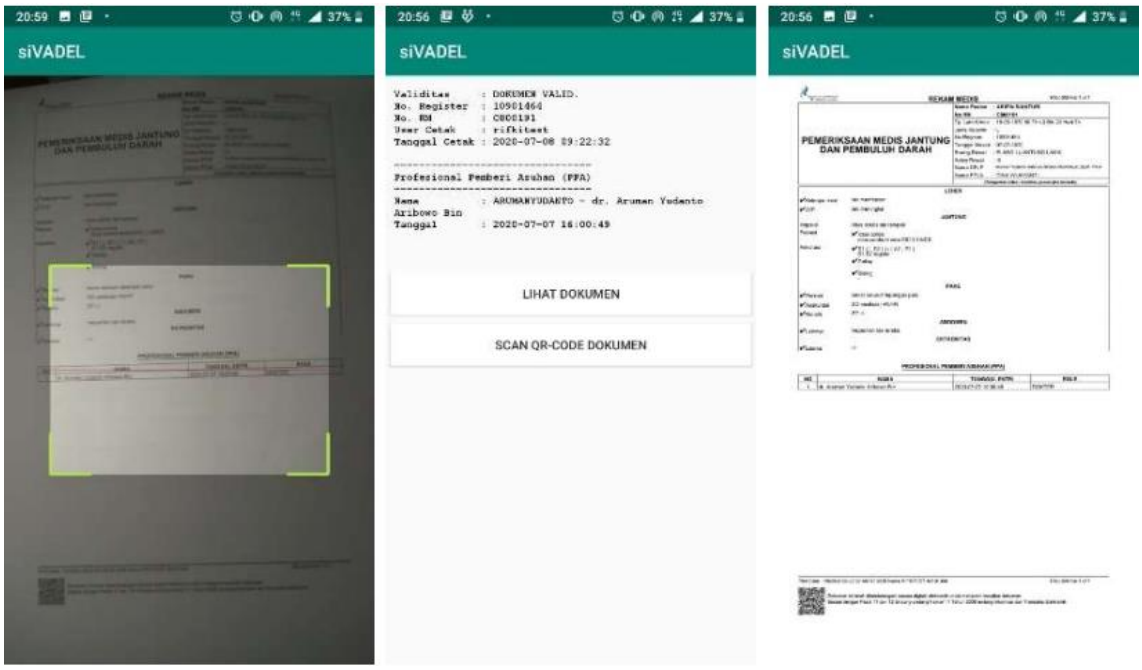



**Gambar 3. Halaman cetak atau *download* dokumen elektronik**

b. Halaman utama aplikasi Android
   Halaman utama adalah halaman yang akan tampil pada awal aplikasi dibuka. Pada gambar 4 halaman utama menampilkan menu scan QR-Code dokumen, *upload* dokumen PDF, dan tutup aplikasi. Setiap menu terdapat fungsinya masing-masing yaitu menu scan QR-Code dokumen untuk mengaktifkan kamera dan melakukan pengambilan gambar dari sebuah dokumen cetak yang terdapat QR-Code, menu *upload* dokumen PDF digunakan untuk memilih dokumen PDF yang terdapat QR-Code selanjutanya melakukan proses *upload* dokumen, menu tutup aplikasi untuk keluar dari aplikasi.

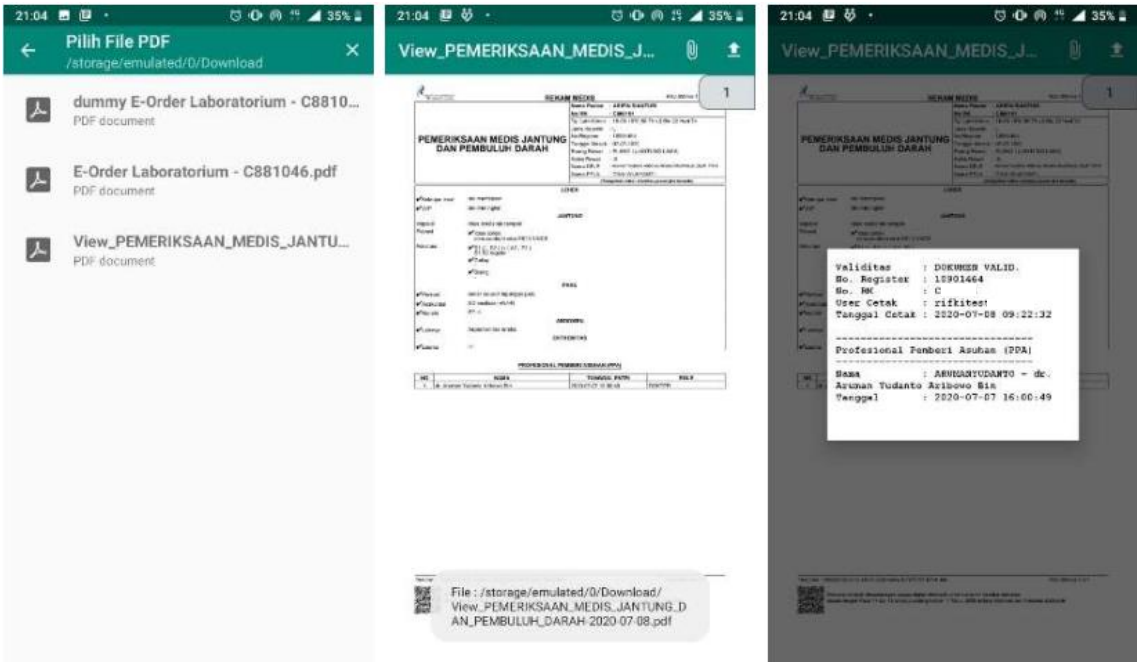

**Gambar 4. Halaman utama aplikasi Android**

c. Halaman scan QR-Code dokumen aplikasi Android
Halaman scan QR-Code dokumen adalah halaman untuk mengaktifkan kamera dan melakukan pengambilan gambar dari sebuah dokumen cetak yang terdapat QR-Code. Apabila pengambilan gambar berhasil, maka aplikasi secara otomatis akan menampilkan hasil validitas dokumen tersebut apakah valid atau tidak, beserta informasi lain terkait dokumen tersebut. Pada halaman ini terdapat menu lihat dokumen dan scan QR-Code dokumen. Menu lihat dokumen berfungsi untuk melakukan validitas secara fisik dengan cara mencocokkan antara dokumen fisik dengan dokumen elektronik yang di tampilkan pada halaman ini. Menu scan QR-Code dokumen untuk mengaktifkan kamera dan melakukan pengambilan gambar dari sebuah dokumen cetak yang terdapat QR-Code. Gambar 5 menunjukkan halaman scan QR-Code dokumen.




**Gambar 5. Halaman scan QR-Code dokumen**

d. Halaman *Upload* Dokumen PDF aplikasi Android
Halaman *upload* dokumen PDF adalah halaman untuk memilih dokumen PDF yang terdapat QR-Code selanjutanya melakukan proses *upload* dokumen. Gambar 6 menunjukkan halaman *upload* dokumen PDF.




**Gambar 6. Halaman *upload* dokumen PDF**

## 4. KESIMPULAN

Berdasarkan hasil implementasi yang telah dilakukan dalam penelitian ini, dapat ditarik kesimpulan dari penelitian ini, yaitu :

1. Penggunaan QR-Code pada dokumen elektronik dapat bermanfaat untuk mempermudah membubuhan tanda tangan digital yang memungkinkan memiliki kode yang cukup panjang, proses verifikasi dokumen menjadi lebih simple karena cukup menggunakan QR-Code reader untuk mendapatkan kode tanda tangan digital dan *upload* file PDF dari dokumen elektronik yang diterbitkan.
2. Aplikasi dapat menampilkan validitas dokumen elektronik yang dikeluarkan oleh layanan kesehatan.
3. Aplikasi memiliki kemampuan dalam menentukan validitas dokumen elektronik dengan tingkat keakuratan 100% dengan menggunakan metode RSA dan AES.

## DAFTAR PUSTAKA

[1] Abdul Gani Putra Suratma, Abdul Azis. (2017, Apr). Tanda Tangan Digital Menggunakan QR-Code dengan Metode Advanced Encryption Standard [online]. Available : http://jurnalnasional.ump.ac.id/index.php/Techno/article/view/1482/1360.

[2] Fitri Nuraeni, Yoga Handoko Agustin, Dede Kurniadi, Imas Dewi Ariyanti. (2020, Des.1). Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik [online]. Available : http://ejournal.uin-suska.ac.id/index.php/SNTIKI/article/view/11130/5811.

[3] Firda Zulivia Abraham, Paulus Insap Santosa, dan Wing Wahyu Winarno. (2018, Des.22). Tandatangan Digital Sebagai Solusi Teknologi Informasi dan Komunikasi (TIK) Hijau: Sebuah Kajian Literatur [online]. Available : https://mti.kominfo.go.id/index.php/mti/article/download/120/pdf.

[4] Mohamad Ihwan. (2016, Jan). Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma RSA [online]. Available : https://jurnal.unimed.ac.id/2012/index.php/cess/article/view/4037.

[5] Trihastuti Yuniati, Muhammad Fajar Sidiq. (2020, Des.24). Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi [online]. Available : https://jurnal.iaii.or.id/index.php/RESTI/article/view/2502.

[6] A. S., Rosa dan Shalahuddin, M., Rekayasa Perangkat Lunak Terstruktur Dan Berorientasi Objek. 2013. Bandung: Informatika.

[7] Tri Rahajoeningroem, Muhammad Aria. (2011, Mei.5). Studi Dan Implementasi Algoritma RSA Untuk Pengamanan Data Transkrip Akademik Mahasiswa [online]. Available : https://jurnal.unikom.ac.id/_s/data/jurnal/v08-n01/volume-81-artikel-9.pdf/pdf/volume-81-artikel-9.pdf.

[8] Asri Prameshwari, Nyoman Putra Sastra. (2018, Sep.28). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen [online]. Available : https://eksplora.stikom-bali.ac.id/index.php/eksplora/article/view/139.