JIKO (Jurnal Informatika dan Komputer) Akreditasi KEMENRISTEKDIKTI, No.105/E/KPT/2022
Vol. 5, No. 2, Agustus 2022, hlm. 125-131 p-ISSN: 2614-8897
DOI: 10.33387/jiko e-ISSN: 2656-1948

IMPLEMENTASI *DIGITAL SIGNATURE* DAN *QUICK RESPONSE CODE* PADA APLIKASI KUITANSI DIGITAL

Fransiskus Ariyanto[1], Suprihadi[2]

[1,2]Teknik Informatika, Teknologi Informasi, Universitas Kristen Satya Wacana
Email: [1]672017040@student.uksw.edu, [2]suprihadi@uksw.edu

(Naskah masuk: 15 Juli 2022, diterima untuk diterbitkan: 24 Juli 2022)

Abstrak

Proses transaksi memegang peranan penting sebagai sarana untuk memenuhi kebutuhan manusia sebagai makhluk sosial. Transaksi terjadi antar dua pihak atau lebih. Proses transaksi terus berkembang, hingga kinin dilakukan proses pencatatan ke dalam dokumen, salah satunya berbentuk kuitansi sebagai validitas untuk membuktikan keaslian transaksi yang terjadi. Kuitansi cetak sebagai instrumen vital dalam proses transaksi tentu harus dijaga keaslian serta ketersediaannya untuk menghindari terjadinya tindak kecurangan yang dapat dilakukan oleh pihak yang tidak bertanggung jawab, maupun kejadian yang berpeluang menimbulkan kecurigaan antar pelaku transaksi dikemudian hari. Menjawab keresahan tersebut, peneliti membangun aplikasi kuitansi digital dengan tanda tangan digital (digital signature) yang telah terenkripsi menggunakan algoritma kriptografi Rivest Shamir Adleman (RSA) demi memenuhi empat syarat sahnya suatu dokumen yang ditinjau dari acara hukum perdata, yaitu dapat menjamin keaslian sebuah dokumen, keutuhan sebuah dokumen, anti penyangkalan, serta dapat menjaga kerahasiaan isi dokumen. Proses pembangunan aplikasi dimulai dengan melakukan identifikasi masalah, setelah itu dilakukan analisis kebutuhan, berikutnya dilakukan perancangan dan pembangunan aplikasi, setelah itu dilakukan pengujian terhadap aplikasi, pada tahap akhir dilakukan penyimpulan hasil yang menghasilkan kesimpulan bahwa algoritma kriptografi RSA masih layak digunakan digunakan dalam pembuatan digital signature, karna dapat menjamin empat syarat sahnya sebuah dokumen yang ditinjau dari acara hukum perdata.

Kata kunci: *QR code*, tanda tangan digital, RSA, kuitansi digital

IMPLEMENTATION OF QUICK RESPONSE CODE AND DIGITAL SIGNATURE ON DIGITAL RECEIPT APPLICATION

Abstract

The transaction process plays an important role as a means to meet human needs as social beings. Transactions occur between two or more parties. The transaction process continues to develop, until now the process of recording into documents, one of which is in the form of receipts as validity to prove the authenticity of the transactions that occur. Printed receipts as a vital instrument in the transaction process, of course, must be kept authentic and available to avoid fraud that can be carried out by irresponsible parties, as well as events that have the opportunity to raise suspicion between transaction actors in the future. Responding to this concern, the researcher built a digital receipt application with a digital signature that has been encrypted using the Rivest Shamir Adleman (RSA) cryptographic algorithm to fulfill four legal requirements for a document that is reviewed from a civil law procedure, which can guarantee the authenticity of a document, integrity of a document, anti-denial, and can maintain the confidentiality of the contents of the document. The application development process begins with identifying the problem, after that a needs analysis is carried out, then the application design and development is carried out, after that testing of the application is carried out, in the final stage the results are concluded which results in the conclusion that the RSA cryptographic algorithm is still suitable for use in making digital signatures, because it can guarantee the four legal requirements of a document that is reviewed from a civil law procedure.

Keywords: *QR code, digital signature, RSA, Digital Receipt*

1. PENDAHULUAN

Dalam peradaban manusia, proses transaksi memegang peranan penting sebagai sarana untuk memenuhi kebutuhan manusia sebagai makhluk sosial. Transaksi memungkinkan interaksi antara dua pihak atau lebih yang dimana memiliki dua entitas utama, yaitu produsen dan konsumen yang saling tukar menukar barang, jasa, dan lain sebagainya. Proses transaksi terus berkembang, hingga kini dilakukan proses pencatatan ke dalam dokumen, salah satunya berbentuk kuitansi sebagai validitas untuk membuktikan keaslian transaksi demi menghindari potensi tindak kecurangan yang dapat dilakukan oleh pihak yang tidak bertanggungjawab dikemudian hari.

Pasal 1867 Kitab Undang-undang Hukum (KUH) perdata menyatakan bahwa terdapat dua jenis alat bukti surat, yaitu akta otentik dan akta dibawah tangan. Kuitansi dalam hal ini dapat menjadi akta dibawah tangan dengan syarat kuitansi harus memiliki isi yang jelas [1].

Kuitansi merupakan intrumen vital dalam proses transaksi yang harus dijaga keaslian serta ketersediaannya. peneliti melakukan pengembangan terhadap instrumen transaksi tersebut, maka terciptalah aplikasi kuitansi gital yang didalamnya memuat tanda tangan digital (*digital signature*) berbentuk *QR code* sebagai salah satu syarat sahnya sebuah perjanjian seperti tercatat pada pasal 1320 KUH perdata [2].

Digital signature pertama kali diperkenalkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976 yang merupakan pakar kriptografi [3].

Penggunaan *digital signature* pada proses transaksi yang melibatkan alat tukar berupa uang telah diatur pada Undang-undang Informasi dan Transaksi Elektronik (UU ITE) yang terdapat pada peraturan Menteri Komunikasi dan Informatika nomor 11 tahun 2018 tentang penyelenggaraan surat elektronik, peraturan Bank Indonesia nomor 19/12/PBI/2017 tentang penyelenggaraan teknologi finansial, serta peraturan Anggota Dewan Gubernur nomor 19/15/PADG/2017 tentang tata cara pendaftaran, penyampaian informasi, dan pamantauan penyelenggara teknologi finansial [4].

Digital signature merupakan hasil proses enkripsi data yang menghasilkan intisari pesan (*message digest*) yang dapat menjamin keaslian sebuah dokumen (*authentication*), keutuhan sebuah dokumen (*integrity*), serta anti penyangkalan (*non-repudiation*) [5].

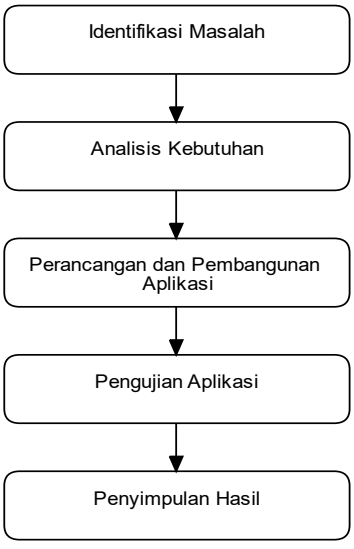
QR code adalah kode dua dimensi yang merupakan pengembangan dari kode batang (*barcode*). *QR code* diperkenalkan pertama kali pada tahun 1994 oleh perusahaan otomotif Jepang, Denso Wave. Pembuatan *QR code* awalnya bertujuan untuk menampun huruf kanji dan karakter kana yang tidak dapat ditampung oleh *barcode* [6][7]. Penggunaan *QR code* sebagai *digital signature* pada kuitansi yang merupakan instrument vital dalam proses transaksi dikatakan sah apabila dapat menjamin empat syarat sahnya suatu dokumen yang ditinjau dari hukum acara perdata, yaitu dapat menjamin keaslian sebuah dokumen, keutuhan sebuah dokumen, anti penyangkalan, serta dapat menjaga kerahasiaan isi dokumen [8]. Dalam upaya memenuhi keempat syarat tersebut, peneliti menerapkan algoritma kriptografi *Rivest Shamir Adleman* (*RSA*) dengan melakukan enkripsi terhadap teks datar (*plaintext*) yang terkandung dalam kuitansi sehingga menghasilkan *message digest* yang kemudian digunakan sebagi *digital signature* [9].

Algoritma kriptografi *RSA* merupakan salah satu ilmu kriptografi asimetris yang terdiri dari kunci public (*public key*) dan kunci rahasi (*private key*) yang ditemukan pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman. *RSA* sendiri merupakan gabungan dari ketiga nama penemu algoritma kriptografi tersebut [10].

Penggunaan kriptografi *RSA* sebagai pembuatan dan pengamanan *digital signature* didasari dari segi kelayakan penggunaan kriptografi *RSA* yang sampai saat ini masih dipercaya dalam melakukan enkripsi data. Kelayakan penggunaan kriptografi *RSA* didasari dari proses enkripsi dan dekripsi yang terjadi dengan menggunakan dua kunci yang berbeda, yaitu *public key* dan *private key* [11].

2. METODE PENELITIAN

Metode penelitian ini merupakan tahapan yang disusun secara sistematis, untuk memperoleh hasil yang baik.



Gambar 1 Tahapan Penelitian

Gambar 1 merupakan tahapan penelitian yang dilakukan peneliti, dengan penjelasan sebagai berikut:

2.1 Identifikasi Masalah

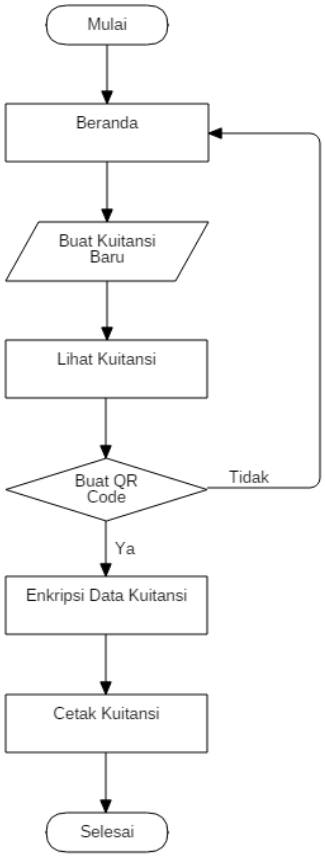
Metode penelitian pada penelitian ini dimulai dengan melakukan identifikasi masalah yang akan peneliti coba untuk selesaikan. Identifikasi masalah yang dilakukan peneliti juga berfungsi untuk memberi batasan-batasan penelitian agar peneliti dapat lebih fokus pada topik yang diteliti.

2.2 Analisis Kebutuhan

Tahap kedua pada penelitian ini adalah analisis kebutuhan. Proses analisis kebutuhan yang dilakukan menghasilkan simpulan kebutuhan akan sistem yang dapat mengamankan data kuitansi sebagai instrument vital dalam proses transaksi, sistem yang dapat memberikan luaran berupa *digital signature* yang telah memenuhi syarat sahnya sebuah dokumen perjanjian, serta sistem yang dapat melakukan validasi terhadap *digital signature* yang diterbitkan, dalam hal ini berupa *QR code* yang telah diamankan menggunakan algoritma kriptografi *RSA*.

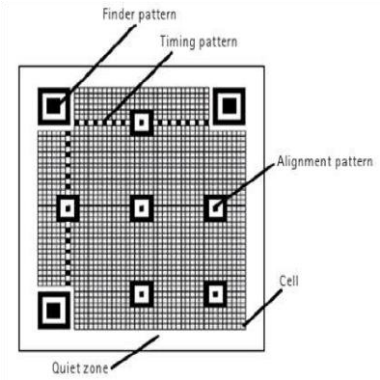
2.3 Perancangan dan Pembangunan Aplikasi

Perancangan dan pembangunan aplikasi dilakukan setelah analisis kebutuhan sistem menghasilkan simpulan yang pasti, agar proses perancangan dan pembangunan aplikasi dapat berjalan dengan baik.



Gambar 2 Proses Pembuatan Kuitansi dan QR Code

Proses perancangan aplikasi dilakukan dengan merancang alur pembuatan kuitansi, alur pembuatan *digital signature*, serta alur pembuatan *QR code* seperti pada Gambar 2. Proses pembuatan kuitansi digital dimulai dengan pengguna memasukan data yang akan dimuat didalam kuitansi. Setelah proses pembuatan kuitansi selesai dilakukan, maka akan dilakukan proses pembuatan *QR code* sebagai *digital signature* yang memuat data kuitansi yang telah terenkripsi menggunakan algoritma *RSA*.



Gambar 3 Struktur QR code

Gambar 3 merupakan struktur *QR code* yang terdiri dari pola *finder* (*finder pattern*) yang berfungsi untuk menentukan orientasi simbol yang benar. Pola waktu (*timing pattern*) digunakan untuk membantu

perangkat lunak dekoder (*decoder software*) dalam menentukan area pola. Pola penyelaras (*alignment pattern*) merupakan bagian yang digunakan *decoder software* dalam melakukan dekripsi terhadap pesan yang terkandung didalam *QR code*. Sel (*cell*) merupakan bagian yang menampung data terenkripsi, serta fungsi pengoreksi kesalahan (*error correcting*). Zona tenang (*quite zone*) merupakan jarak yang diberikan antar *QR code* dan data lainnya untuk memudahkan *decoder software* dalam melakukan pemindaian (*scanning*) terhadap *QR code* [12].

Proses enkripsi data menggunakan algoritma kriptografi *RSA* dimulai dengan menentukan dua buah bilangan prima secara acak, bilangan prima tersebut disimbolkan dengan p dan q. Kemudian dilakukan perkalian terhadap bilangan prima p dan q sehingga menghasilkan nilai n (1). Selanjutnya mencari nilai φ untuk menentukan banyak bilangan $1,2,3,\dots,n$ yang relatif prima terhadap nilai n (2). Setelah itu menentukan nilai e yang merupakan *public key* (3). Berikutnya menentukan nilai d yang merupakan *private key* (4).

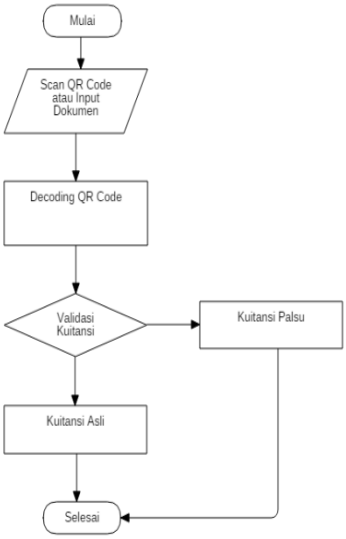
$$n = p * q \quad (1)$$
$$\varphi = (p-1)(q-1) \quad (2)$$
$$PBB(e * \varphi) = 1 \quad (3)$$
$$d = (e * d)\%\varphi = 1 \quad (4)$$

Setelah mendapatkan nilai d, e, dan nilai n, proses enkripsi data dilakukan berdasarkan rumus (5).

$$C = P^d \% n \quad (5)$$

Nilai C merupakan *ciphertext* yang akan digunakan sebagai *digital signature*, nilai P merupakan *plaintext* [13]. Setelah *digital signature* dan *QR code* berhasil dibuat, maka pengguna dapat memilih untuk menerbitkan kuitansi dalam bentuk cetak atau digital.

Proses perancangan selanjutnya dilakukan dengan merancang proses validasi kuitansi untuk membuktikan validitas dari sebuah kuitansi.



Gambar 4 Proses Uji Validitas Kuitansi

Proses uji validitas kuitansi dimulai dengan pengguna melakukan *scanning* terhadap *QR code* atau memasukkan (*input*) dokumen yang akan diuji validitasnya. Tahap uji validitas dilakukan dengan sistem melakukan *decoding* terhadap *QR code* yang akan diuji terlebih dahulu.

Setelah proses *decoding* berhasil dilakukan, sistem akan melakukan perbandingan data yang terkandung didalam *QR code* dengan data yang terdapat didalam basis data (*database*). Jika data yang terkandung didalam *QR code* dan *database* sama, maka kuitansi dinyatakan asli, namun jika data berbeda, maka kuintansi dinyatakan palsu, atau telah terdapat perubahan yang tidak dilakukan didalam aplikasi kuitansi digital yang sedang dibangun.

Setelah proses perancangan aplikasi selesai, peneliti mulai masuk pada tahap pembangunan aplikasi dengan menggunakan kerangka kerja (*framework*) *Laravel* dengan memanfaatkan perpustakaan (*library*) *bacon QR code* dalam membuat *QR code*, dan *library zxing* dalam membuat fungsi *scanning* dan *decoding* untuk *QR code*.

2.4 Pengujian Aplikasi

Proses pengujian aplikasi dilakukan peneliti dengan menggunakan metode pengujian *black box*. Metode pengujian *black box* adalah metode yang menguji fungsionalitas perangkat lunak tanpa mengacu pada struktur dalam aplikasi [14].

2.5 Penyimpulan Hasil

Proses penyimpulan hasil dilakukan dengan menarik kesimpulan berdasarkan dari hasil pengujian yang dilakukan peneliti.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Sistem

Proses implementasi *digital signature* dan *quick response code* pada aplikasi kuitansi digital dibangun menggunakan teknologi *Laravel* yang merupakan

kerangka kerja (*framework*) bahasa pemrograman *PHP*. Penggunaan teknologi *Laravel* didasari beberapa alasan, yaitu terdapatnya fungsi *Command Line Interface* (*CLI*) *Artisan*, kemudahan dalam menulis kode program, penerapan *Model View Controller* (*MVC*), dan masih banyak lagi keunggulan yang dimiliki *Laravel*, serta sangat membantu bagi peneliti dalam membangun aplikasi [15].

Penggunaan *digital signature* pada sebuah dokumen perjanjian yang ditinjau menurut acara hukum perdata harus dapat memenuhi empat syarat agar dinyatakan sah sebagai bukti transaksi dimata hukum. Menjawab hal tersebut, peneliti menerapkan algoritma kriptografi *RSA* dengan melakukan enkripsi terhadap nomor kuitansi, pelaku transaksi 1, serta pelaku transaksi 2 yang diambil dari kuitansi yang akan dibuatkan *digital signature*. Perubahan data sebelum dan sesudah proses enkripsi dilakukan dapat dilihat pada tabel 1 dan 2.

Tabel 1 Data Sebelum Dienkripsi

672017040 Fransiskus Ariyanto Suprihadi

Tabel 2 Data Setelah Dienkripsi

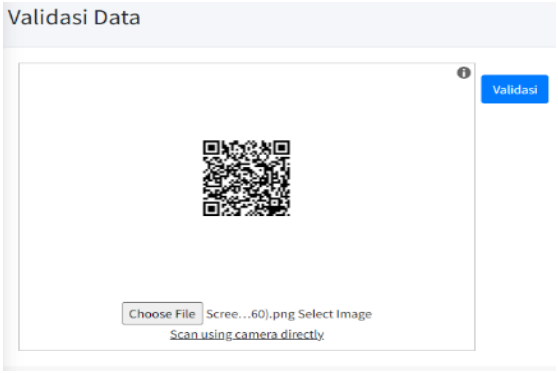
3199245212444853324726846132595212444726 8418092472684674541038148603591043537255 4415372122859861105372327681368521038145 5441118285860359104345393127674473144424 2283878944433333328323022724611928083332 832

Digital signature telah berhasil dibuat, kemudian diolah menjadi *QR code* seperti pada Gambar 5.

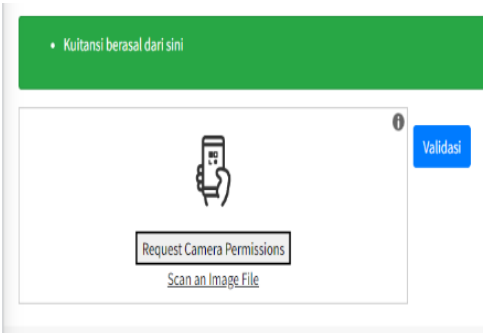
Gambar 5 *QR code Digital Signature*

3.2 Pengujian Sistem

Proses pengujian aplikasi dilakukan peneliti dengan menerapkan salah satu teknik pengujian *black box*, *fuzzing*. Penerapan teknik *fuzzing* dilakukan dengan memberikan *input digital signature* hasil aplikasi yang dibangun peneliti berupa *QR code* yang dapat dilihat pada Gambar 6, dengan hasil pengujian seperti yang terlihat pada Gambar 7 yang menunjukan hasil pengujian berwarna hijau, berarti data yang diuji dinyatakan data yang orisinal atau *digital signature* hasil dari aplikasi yang dibangun peneliti.



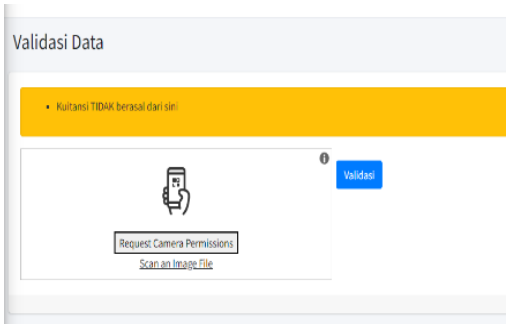
Gambar 6 *QR Code* Hasil Aplikasi Peneliti



Gambar 7 Hasil Validasi *QR Code* dari Aplikasi Peneliti

Pengujian berikutnya dilakukan dengan memberikan *input* berupa *QR code* hasil aplikasi luar dengan terdapat perubahan 1 karakter data yang ditampung didalamnya. Pengujian tersebut dapat dilihat pada Gambar 6 dengan hasil pungujian yang dapat dilihat pada Gambar 7 yang menunjukan hasil berwarna kuning, yang menunjukan bahwa telah terjadi perubahan data pada *digital signature* yang diuji atau *digital signature* tersebut tidak dibuat pada aplikasi yang dibangun peneliti.

Gambar 8 *QR Code* Hasil Aplikasi Luar



Gambar 9 Hasil Validasi *QR Code* dari Aplikasi Luar

Pengujian selanjutnya dilakukan dengan memberikan *input digital signature* berupa *QR code* cetak yang telah dirusak permukaannya oleh peneliti, dengan isi data didalamnya merupakan data orisinal dari aplikasi yang dibangun peneliti. Pengujian *QR code* cetak rusak dapat dilihat pada Gambar 10.

Gambar 10 Pengujian *QR Code* Cetak yang Rusak

Hasil pengujian pada *QR code* cetak yang rusak menunjukkan bahwa aplikasi yang dibangun oleh peneliti tidak menunjukan reaksi atau respon, yang dimana dapat disimpulkan bahwa aplikasi yang dibangun oleh peneliti tidak mampu membaca *QR code* yang rusak.

4. KESIMPULAN

Berdasarkan hasil pungujian yang peneliti lakukan, penggunaan algoritma kriptografi *RSA* masih layak digunakan dalam pembangkitan *digital signature*. Algoritma kriptografi *RSA* dapat memenuhi syarat kelayakan *digital signature*, yaitu dapat menjamin *authentication*, *integrity*, *non-repudiation*, serta *confidentiality*. Dari hasil pengujian yang peneliti lakukan, aplikasi yang dibangun peneliti masih dapat dikembangkan dari fungsi validasi serta fungsi pembuatan *QR code*, karna pada saat dilakukan pengujian menggunakan *QR code* cetak yang rusak, fungsi validasi pada aplikasi yang peneliti bangun tidak dapat berkerja dengan semestinya.

5. DAFTAR PUSTAKA

[1] F. S. Purworini, W. Wiryomartani, and W. Suryandono, "Kuitansi Sebagai Alat Bukti Perjanjian Utang Piutang (Studi Kasus Putusan Pengadilan Tinggi Samarinda Nomor 18/Pdt/2016/Pt. Smr Juncto Putusan Mahkamah Agung Nomor 2070 K/Pdt/2016)," *Indonesian Notary*, vol. 1, no. 3, pp. 1–21, 2019.

[2] R. Y. Bramantyo, H. Murti, N. Wahyuni, and Suwarno, "PENGGUNAAN KUITANSI SEBAGAI ALAT BUKTI TRANSAKSI JUAL BELI (Ditinjau Dari Perspektif Kitab Undang-Undang Hukum Perdata)," *Jurnal Ilmu Sosial dan Ilmu Administrasi Negara*, vol. 4, no. 1, pp. 92–103, 2020.

[3] E. v Waruwu, F. Sonata, and I. Zulkarnain, "PENERAPAN DIGITAL SIGNATURE MENGGUNAKAN METODE RSA UNTUK MENVALIDASI KEASLIAN IJAZAH SMA SWASTA BINA ARTHA," *J-SISKO TECH*, vol. 45, no. 2, pp. 45–55, 2020.

[4] T. N. Cahyadi, "ASPEK HUKUM PEMANFAATAN DIGITAL SIGNATURE DALAM MENINGKATKAN EFISIENSI, AKSES DAN KUALITAS FINTECH SYARIAH," *RECHTSVINDING*, vol. 9, no. 2, pp. 219–236, 2020.

[5] Y. Anshori, A. Y. E. Dodu, and D. M. P. Wedanata, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital Implementation of Rivest Shamir Adleman (RSA) Cryptography Algorithm On Digital Signatures," *Techno.COM*, vol. 18, no. 2, pp. 110–121, 2019.

[6] Norhikmah, A. R. Safitri, and L. A. Sholikhan, "Penggunaan QR Code dalam Presensi Berbasis Android," *Seminar Nasional Teknologi Informasi dan Multimedia 2016*, vol. 4, no. 7, pp. 97–102, 2016.

[7] N. L. N. Arianti, G. S. Darma, and L. P. Mahyuni, "Menakar Keraguan Penggunaan QR Code Dalam Transaksi Bisnis," *Manajemen dan Bisnis*, vol. 16, no. 2, pp. 67–78, 2019, [Online]. Available: http://journal.undiknas.ac.id/index.php/magister-manajemen/

[8] Sulaiman, N. Arifudin, and L. Triyana, "Kekuatan Hukum Digital Signature Sebagai Alat Bukti Yang Sah Di Tinjau Dari Hukum Acara Perdata," *Risalah Hukum*, vol. 16, no. 2, pp. 95–105, 2020.

[9] A. Lorien and T. Wellem, "Implementasi Sistem Otentikasi Dokumen Berbasis Quick Response (QR) Code dan Digital Signature," *Resti*, vol. 5, no. 4, pp. 663–671, 2021, doi: 10.29207/resti.v5i1.3316.

[10] R. Siringoringo, "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File 31," *KAKIFIKOM*, vol. 02, no. 01, pp. 31–42, 2020.

[11] M. A. Fahreza and H. Arif, "Aplikasi Keamanan Data Gambar Menggunakan Algoritma RSA

(Rivest Shamir Adleman) Berbasis Desktop," *Jurnal Ilmiah Teknologi-Informasi dan Sains (TeknoIS)*, vol. 9, no. 1, pp. 1–9, 2019.

[12] S. Singh, "QR Code Analysis," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 5, pp. 89–92, 2016, [Online]. Available: www.ijarcsse.com

[13] Sulistiyorini and A. Prihanto, "Perbandingan Efisiensi Algoritma RSA dan RSA-CRT Dengan Data Teks Berukuran Besar," *JINACS*, vol. 1, no. 2, pp. 84–90, 2019.

[14] E. V. Waruwu, F. Sonata, and I. Zulkarnain, "J-SISKO TECH Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD PENERAPAN DIGITAL SIGNATURE MENGGUNAKAN METODE RSA UNTUK MENVALIDASI KEASLIAN IJAZAH SMA SWASTA BINA ARTHA," v, vol. 45, no. 2, pp. 45–55, 2020.

[15] T. B. Tahir, M. Rais, and M. A. Hs, "Aplikasi Point OF Sales Menggunakan Framework Laravel," *Jurnal Informatika dan Komputer) p-ISSN*, vol. 2, no. 2, pp. 2355–7699, 2019, doi: 10.33387/jiko.