Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 4 No. 6 (2020) 1058 – 1069 ISSN Media Elektronik: 2580-0760

Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi

Trihastuti Yuniati[1], Muhammad Fajar Sidiq[2]
[1, 2] Program Studi S1 Teknik Informatika, Fakultas Informatika, Institut Teknologi Telkom Purwokerto
[1]trihastuti@ittelkom-pwt.ac.id, [2]fajar@ittelkom-pwt.ac.id

Abstract

With a pandemic that has hit all over the world, the government has issued policies for doing physical distancing and work from home (WFH), include in education field. That policies made a significant change in the way people work and interact. WFH require every student, lecturer and employee to work online from home. In fact, there are many activities that require document approval with a signature. Digital signature is one of technologies that can be applied to overcome this problem. There are various algorithms and schemes that have been applied in previous studies, such as hash function, RSA, AES, or ElGamal, with PKCS, Digital Signature Algorithm (DSA), Schnorr, or Security as a Service (SaaS)-based scheme. This paper describes a review of several literatures related to document legalization using digital signatures. The results can be concluded that the appropriate algorithm or scheme to be applied in the digital signature process for document legalization which the verification process will be carried out by external parties is DSA or SaaS-based scheme by embedding a QR Code and/or barcode in the document. Meanwhile, the appropriate scheme for document legalization which the verification process will be carried out by internal parties is using PKCS scheme.

Keywords: digital signature, document legalization, electronic document, literature review, pandemic.

Abstrak

Adanya pandemi yang melanda hampir di seluruh dunia menjadikan pemerintah mengeluarkan kebijakan untuk *physical distancing* dan *work from home* (WFH). Kebijakan tersebut menjadikan perubahan yang signifikan dalam cara orang-orang bekerja dan berinteraksi. Kebijakan WFH berlaku di sebagian besar bidang kerja, salah satunya di bidang pendidikan. Aturan WFH mengharuskan setiap mahasiswa, dosen dan pegawai untuk melaksanakan kuliah atau bekerja secara daring dari rumah. Padahal banyak kegiatan-kegiatan yang memerlukan pengesahan dokumen dengan tanda tangan, baik urusan akademik maupun non-akademik. Tanda tangan digital adalah salah satu teknologi yang dapat diterapkan untuk mengatasi permasalahan tersebut. Berbagai algoritma dan skema telah diterapkan pada penelitian-penelitian sebelumnya, seperti algoritma fungsi *hash* MD5, SHA-1, SHA-3, algoritma enkripsi RSA, AES, atau ElGamal dengan skema PKCS, *Digital Signature Algorithm* (DSA), Schnorr, maupun skema berbasis *Security as a Service* (SaaS) dengan menyematkan *Quick Response Code* (*QR Code*) dan/atau *barcode*. Pada *paper* ini dipaparkan hasil *review* terhadap beberapa literatur yang berkaitan dengan legalisasi dokumen elektronik menggunakan tanda tangan digital. Hasil dari *literature review* diperoleh kesimpulan bahwa algoritma atau skema yang cocok diterapkan pada proses pembuatan tanda tangan digital untuk legalisasi dokumen yang proses verifikasinya dilakukan oleh pihak luar kampus adalah skema DSA atau skema berbasis SaaS dengan menyematkan *QR Code* dan/atau *barcode* di dokumen. Sedangkan untuk legalisasi dokumen yang proses verifikasinya dilalukan oleh pihak internal kampus maka penggunaan skema PKCS dengan membangkitkan tanda tangan digital melalui aplikasi pembaca berkas berformat pdf seperti *Adobe Reader* atau *Foxit Reader* dapat digunakan, karena cara ini cukup sederhana, mudah diterapkan, dan tidak memerlukan infrastruktur tambahan lainnya.

Kata kunci: dokumen elektronik, *literature review*, pandemi, pengesahan dokumen, tanda tangan digital.

Diterima Redaksi : 25-09-2020 | Selesai Revisi : 16-12-2020 | Diterbitkan Online : 20-12-2020

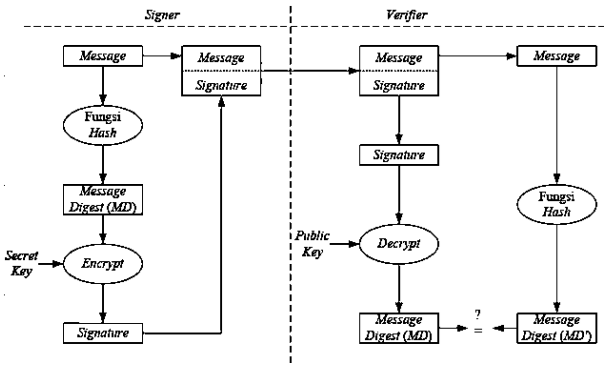
1. Pendahuluan

Semenjak pandemi COVID-19 mewabah di Indonesia, pemerintah segera menetapkan sejumlah kebijakan sebagai upaya untuk memutus mata rantai penyebaran COVID-19. Salah satu kebijakan di bidang pendidikan adalah pembelajaran daring untuk anak sekolah yang merujuk pada Surat Edaran Mendikbud No. 3 Tahun 2020 tentang Pencegahan COVID-19 pada Satuan Pendidikan, yang kemudian juga diterapkan dengan kuliah daring di jenjang perguruan tinggi [1]. Pemerintah juga mengeluarkan kebijakan untuk bekerja dari rumah atau *Work From Home* (WFH) yang merujuk pada Undang-Undang No.13 Tahun 2003 tentang Ketenagakerjaan Pasal 8 ayat 1 huruf a [2], [3]. Kedua kebijakan tersebut mengharuskan setiap mahasiswa, dosen, dan pegawai untuk bekerja secara daring dari rumah. Padahal banyak kegiatan-kegiatan yang memerlukan pengesahan dengan tanda tangan, baik untuk urusan akademik maupun non-akademik, misalnya legalisir ijazah/transkrip nilai oleh mahasiswa atau pengajuan cuti oleh dosen. Pengesahan untuk kegiatan-kegiatan tersebut pada awalnya masih dilakukan secara manual dengan membubuhkan tanda tangan dan cap basah. Adanya kebijakan WFH selama pandemi COVID-19, mengharuskan seluruh civitas akademika beralih dari sistem manual ke sistem digital. Seluruh dokumen pengajuan atau pelaporan yang pada mulanya dalam bentuk *print out* beralih menjadi bentuk dokumen digital. Proses pendistribusian dokumen juga dilakukan menggunakan media elektronik, baik melalui email maupun sistem terkomputerisasi.

Kehadiran Teknologi Informasi dan Komunikasi (TIK) dapat menjadi solusi bagi permasalahan di atas karena sifatnya yang tidak terbatas ruang dan waktu. Solusi TIK yang dapat diterapkan untuk mengatasi permasalah tersebut yaitu teknologi tanda tangan digital. Tanda tangan digital di Indonesia diatur dalam Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya, serta Peraturan Pemerintah No.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik [4]. Tanda tangan digital berfungsi sebagai alat untuk autentikasi dan verifikasi atas identitas penandatangan serta keutuhan dan keautentikan informasi elektronik [5]. Salah satu contoh pemanfaatan tanda tangan digital adalah untuk legalisasi dokumen elektronik.

Dalam sistem digital, tindakan pengesahan atau persetujuan dokumen yang sah dan diakui adalah berupa tanda tangan digital, bukan tanda tangan basah hasil pemindaian yang disematkan di dokumen atau dengan menandatangani langsung di dokumen menggunakan fitur *draw* di *Microsoft Word* atau PDF *Reader*. Namun masih kurangnya pengetahuan dan pemahaman civitas akademika mengenai teknologi tanda tangan digital mengakibatkan di banyak instansi pendidikan masih menggunakan cara semi-manual, yaitu dengan menyematkan hasil pemindaian tanda tangan. Cara semi-manual tidak dapat menjamin keabsahan dan keautentikan dokumen elektronik karena cara ini mudah untuk dilakukan pemalsuan serta sulit mengetahui adanya perubahan terhadap informasi elektronik dan waktu penandatanganan [6]. Salah satu cara untuk mengatasi permasalahan tersebut adalah dengan menerapkan teknologi tanda tangan digital.

Pada dasarnya teknologi tanda tangan digital sudah ada sejak tahun 1976, diperkenalkan oleh Whitfield Diffie dan Martin Hellman [7], namun baru mulai dikenal luas di Indonesia pada tahun 2008. Tanda tangan digital dibuat menggunakan fungsi *hash* dan algoritma kriptografi kunci publik [8]. Skema tanda tangan digital dapat dilihat di Gambar 1.



Gambar 1. Alur tanda tangan digital dengan fungsi *hash* dan algoritma kriptografi kunci publik [8]

Dalam kurun waktu 2 tahun belakangan ini penggunaan tanda tangan digital di Indonesia semakin pesat, apalagi setelah adanya instansi penyedia layanan tanda tangan digital. Penyedia layanan tanda tangan digital di Indonesia beroperasi di bawah pengawasan Kementerian Komunikasi dan Informatika (Kominfo), yaitu melalui Permenkominfo No.11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik. Salah satu perusahaan penyedia layanan tanda tangan digital di Indonesia yang sudah diakui secara legal adalah Privy Identitas Digital (PrivyID), yang terdaftar sejak 7 Desember 2018 [9]. Pesatnya pertumbuhan penggunaan tanda tangan digital dapat terlihat dari banyaknya pengguna PrivyID. Pada akhir tahun 2019 pengguna PrivyID telah mencapai 4,5 juta orang dengan 205 perusahaan [10], atau tumbuh sekitar 2 juta pengguna dari pencapaian tahun 2018. Jumlah tersebut terus meningkat seiring dengan penerapan kebijakan *physical distancing* dan WFH selama pandemi COVID-19.

Penelitian ini merupakan sebuah *literature review* terhadap beberapa jurnal penelitian terdahulu mengenai legalisasi dokumen elektronik menggunakan tanda tangan digital, metode-metode yang digunakan, kelebihan dan kekurangan, serta diskusi atau pembahasan mengenai metode-metode tersebut.

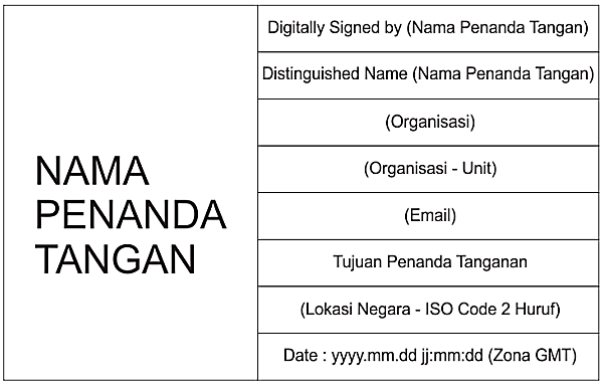
2. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah *literature review* pada *paper-paper* yang terkait dengan legalisasi dokumen elektronik menggunakan tanda tangan digital. Langkah-langkah dari *literature review* meliputi 4 tahapan, yaitu: (1) formulasi permasalahan, (2) pencarian literatur, (3) evaluasi data, serta (4) analisis dan interpretasi [11]. Formulasi permasalahan dilakukan dengan memilih topik. Pada penelitian ini topik yang dipilih adalah mengenai tanda tangan digital dan legalisasi dokumen elektronik. Langkah selanjutnya adalah pencarian literatur yang relevan dengan topik penelitian. Langkah ini dapat memberikan gambaran mengenai tanda tangan digital dan legalisasi dokumen elektronik. Proses pencarian dan pengumpulan artikel atau jurnal penelitian dilakukan menggunakan *Google Scholar, IEEE Xplore*, dan *Science Direct* dengan kata kunci "legalisasi dokumen elektronik", "tanda tangan digital" dan "*digital signature*". Dari hasil pencarian ditemukan sebanyak 392.813 artikel jurnal. Langkah ketiga adalah evaluasi data, yaitu dengan menyaring, memilih dan memilah artikel jurnal yang benar-benar relevan dan baru. Keterbaruan dibatasi dengan memilih artikel jurnal yang terbit dalam kurun waktu 5 tahun terakhir, yaitu antara tahun 2015 sampai dengan tahun 2020. Sedangkan relevansi dilihat dari kesesuaian judul *paper* dengan topik penelitian, yaitu mengenai legalisasi dokumen elektronik menggunakan tanda tangan digital. Berdasarkan hasil evaluasi data, kemudian dipilih sebanyak 20 jurnal untuk di-*review*. Setelah keempat tahapan tersebut dilakukan, proses selanjutnya adalah pelaksanaan *literature review*. Adapun cara melakukan *literature review* yaitu: mencari kesamaan (*compare*), mencari ketidaksamaan (*contrast*), memberikan pandangan (*criticize*), membandingkan (*synthesize*), dan meringkas (*summarize*) dari beberapa penelitian terkait [11].

3. Hasil dan Pembahasan

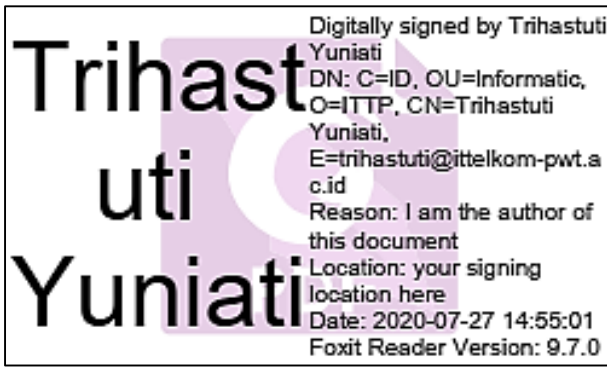
Hasil penelitian dengan metode *literature review* pada jurnal-jurnal penelitian terkait dengan tanda tangan digital dan legalisasi digital elektronik dijabarkan di bawah ini.

Paper [5] 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 menandatangai sebuah dokumen atau *file* digital, sementara kata sandi tetap dirahasiakan dan sudah disimpan di aplikasi pengolah dokumen. PKCS#12 yang menempel pada dokumen memiliki struktur standar seperti terlihat pada Gambar 2.



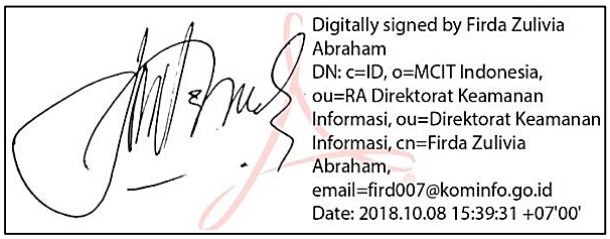
Gambar 2. Struktur PKCS#12 [5]

Masing-masing aplikasi pengolah dokumen dapat memiliki struktur tampilan tanda tangan digital yang berbeda. Misalnya pada aplikasi *Foxit Reader*, contoh tampilan tanda tangan digital terlihat seperti Gambar 3.



Gambar 3. Contoh tanda tangan digital yang dibuat di *Foxit Reader*

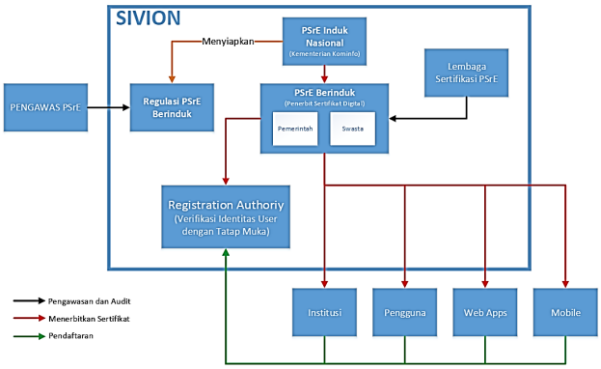
Teknologi tanda tangan digital juga sudah diakui secara resmi oleh pemerintah Indonesia. Sertifikat digital dikeluarkan oleh *Registration Authority* (RA) Direktorat Keamanan Informasi, Kementerian Komunikasi dan Informatika (Kominfo). Contoh tanda tangan digital yang dibuat pada aplikasi *Adobe Reader* menggunakan sertifikat dari RA Direktorat Keamanan Informasi, Kominfo dapat dilihat di Gambar 4.



Gambar 4. Contoh tanda tangan digital yang dibuat di *Adobe Reader* dengan sertifikat RA Direktorat Keamanan Informasi, Kominfo [5]

Tanda tangan digital pada dasarnya merupakan gabungan dari teknik *hash* dan enkripsi. Berkas dokumen digital asli dilakukan *hashing*, kemudian hasil *hash* tersebut dilakukan enkripsi. Teknik *hash* menjamin integritas dokumen, karena jika ada perubahan sedikit saja pada dokumen maka hasil *hash* juga akan berbeda, yang mengakibatkan tanda tangan digital menjadi tidak valid [8].

Pada tahun 2016, Direktorat Jenderal Aplikasi Informasi, Kementerian Kominfo telah merilis suatu sistem untuk permohonan sertifikat digital kepada para penggunanya, baik individu, organisasi, maupun *server* aplikasi milik pemerintah maupun swasta, yang disebut sebagai Sistem Verifikasi *Online* (SiVION). Validasi sertifikat digital langsung dilakukan pada tiap-tiap Penyelenggara Sertifikat Elektronik (PSrE) Berinduk penerbit sertifikat (*Root Certification Authoriry*/*Root* CA). Selain itu, Kominfo juga menyiapkan *Root* CA Nasional dengan melegalisasi CA Pemerintah dan CA Swasta dan juga memberikan edukasi bagi masyarakat karena ada penambahan bisnis proses pada transaksi daring[12]. Gambar 5 menunjukkan alur proses SiVION.



Gambar 5. Alur proses SiVION [12]

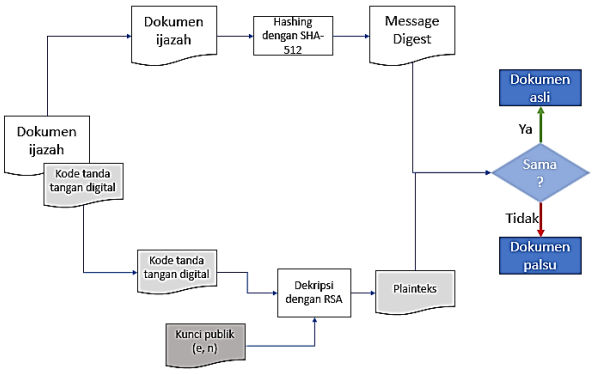
Menurut *paper* [5] tersebut, meskipun dari sisi infrastruktur tanda tangan digital sudah tersedia dengan cukup memadai dan juga sudah ada legalitas hukumnya melalui PP dan UU ITE, namun masih terdapat permasalahan yang terjadi, yaitu antara lain: (1) aspek legalitas mengenai Sistem Legal Digital dan Identitas Digital Pengguna, (2) keraguan dari para pejabat untuk menerapkan tanda tangan digital, (3) pola pikir yang sulit menerima penerapan tanda tangan digital, dan (4) perlunya penyesuaian budaya. Langkah yang dapat diambil untuk mengatasi permasalahan yang disebutkan di *paper* [5] antara lain melaksanakan sosialisasi kepada masyarakat secara menyeluruh mengenai teknologi tanda tangan digital dan menyusun aturan atau undang-undang untuk mendukung legalitas tanda tangan digital.

Paper [13] membahas mengenai pemanfaatan tanda tangan digital untuk legalisasi salinan dokumen ijazah dan transkrip nilai mahasiswa. Jika biasanya untuk proses legalisir salinan ijazah dan transkrip nilai menggunakan tanda tangan dan cap basah dari pejabat institusi yang berwenang, maka pada *paper* ini dikembangkan sebuah aplikasi berbasis *web* untuk legalisir salinan dokumen menggunakan algoritma *hashing* SHA-1 dan *Digital Signature Standard* (DSS). Penelitian ini dilatarbelakangi oleh masih banyaknya tindak pemalsuan dokumen ijazah dan transkrip nilai untuk keperluan tertentu. SHA-1 diterapkan pada pesan yang berisi informasi nama mahasiswa, nomor induk, tanggal lahir, dan tanggal legalisir. Keluaran dari proses *hashing* dengan SHA-1 berupa *message digest* dengan ukuran 160-*bit*. *Message digest* tersebut kemudian dienkripsi menggunakan kunci privat untuk membuat tanda tangan digital. Proses ini dilakukan oleh institusi, dalam kasus ini adalah pihak kampus, untuk keperluan validasi dan pengecekan validitas dokumen. Tanda tangan digital hasil enkripsi tersebut kemudian disimpan di basis data aplikasi dan juga disematkan di dokumen salinan ijazah dan transkrip nilai bersamaan dengan tanggal legalisir

dokumen. Pihak yang ingin memvalidasi dokumen dapat mengecek di *website* institusi yang relevan dengan memasukkan data tanda tangan digital yang tersemat di dokumen. Apabila dokumen valid, maka informasi mengenai nama mahasiswa, nomor induk, tanggal lahir, dan tanggal legalisir dokumen akan ditampilkan di *website*. Gambar 6 berikut menunjukkan contoh tanda tangan digital yang disematkan pada salinan ijazah.

Gambar 6. Contoh penerapan tanda tangan digital pada proses legalisir salinan ijazah [13]

Paper [14] juga membahas mengenai penerapan tanda tangan digital pada proses legalisasi ijazah. Mekanisme yang diterapkan pun hampir sama, bedanya di *paper* ini penulis menggunakan algoritma RSA dan SHA-512. Langkah pertama yang dilakukan adalah pembangkitan kunci publik dan kunci privat untuk proses *signing* menggunakan algoritma RSA. Setelah pasangan kunci dibangkitkan, langkah kedua adalah proses *hashing* menggunakan SHA-512 untuk menghasilkan *message digest*. Secara garis besar terdapat 4 tahapan pada proses *hashing*, yaitu input data ijazah ke sistem, *padding*, inisialisasi *digest* awal, dan fungsi kompresi yang terdiri atas 80 *round*. Hasil dari proses *hashing* ini adalah *message digest* berukuran 512-*bit* atau 64 *byte*. Langkah ketiga adalah proses *signing*. Pada proses *signing*, *message digest* yang dihasilkan dari tahap *hashing* dienkripsi menggunakan kunci privat yang telah dibangkitkan sebelumnya. Hasil enkripsi adalah kode tanda tangan digital. Kode ini kemudian dilampirkan di dokumen ijazah. Pada proses verifikasi dokumen, langkah yang dilakukan dapat dilihat di Gambar 7 berikut.



Gambar 7. Proses verifikasi dokumen ijazah [14]

Pihak yang ingin memverifikasi dokumen mengakses fitur legalisasi ijazah yang ada di *website* kampus yang bersesuaian dengan dokumen, kemudian memasukkan data-data yang ada di dokumen, bisa dilakukan dengan cara ditulis manual atau dengan mengunggah *file* dokumen. Keluaran dari proses verifikasi ini adalah status berupa dokumen valid atau dokumen tidak valid.

Paper [15] membahas mengenai pentingnya penerapan tanda tangan digital pada skema *e-Governance*. *E-Governance* adalah sistem pemerintahan yang dibuat menjadi daring untuk memberikan layanan kepada masyarakat. Layanan tersebut dapat berupa *Government to Citizen* (G2C), *Government to Business* (G2B), *Government to Government* (G2G), serta *Government to Employee* (G2E). Tujuan dari penerapan tanda tangan digital pada skema *e-Governance* tersebut adalah untuk meningkatkan keamanan, reliabilitas, dan anti-penyangkalan terhadap data-data pengguna. Proses tanda tangan digital dibagi dalam 5 tahap, yaitu: *Key Generation*, *Digital Signing*, *Encryption*, *Decryption*, dan *Signature Verification*. Pada tahap *Key Generation* sistem membangkitkan sepasang kunci, yaitu kunci publik dan kunci privat. Kunci privat disimpan oleh *user* sedangkan kunci publik disimpan di *cloud*. Di tahap *Digital Signing*, sistem membangkitkan *message digest* MD1 dari pesan yang akan dikirimkan dengan menggunakan algoritma MD5. Tanda tangan digital S dibangkitkan dari hasil *message digest* MD1 menggunakan kunci privat pengirim dan kemudian dikirimkan kepada penerima. Dalam *paper* [15] ini tidak disebutkan dengan jelas algoritma apa yang digunakan untuk membuat tanda tangan digital. Tahap *Encryption* adalah tahap pengirim mengenkripsi pesan menggunakan kunci publik milik penerima pesan, kemudian mengirimkan pesan terenkripsi tersebut kepada penerima. Pada tahap *Decryption*, penerima mendekripsi pesan menggunakan kunci privatnya sendiri. Tahap terakhir, *Signature Verification*, penerima pesan memverifikasi tanda tangan digital dengan cara: membangkitkan integer V

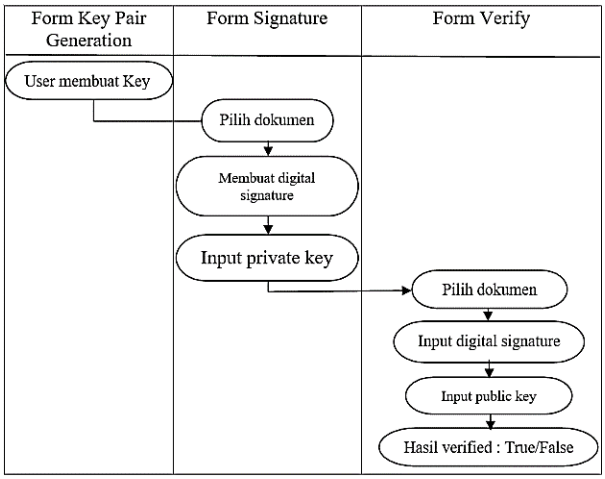
menggunakan kunci publik dan tanda tangan digital pengirim (S), mengekstraksi *message digest* MD1, menghitung *message digest* MD2 dari tanda tangan digital S, dan membandingkan MD1 dengan MD2. Jika MD1 = MD2 maka tanda tangan digital dinyatakan valid. Beberapa skema *e-Governance* yang perlu menerapkan mekanisme ini antara lain: *e-Payment*, yaitu pada proses penerimaan pembayaran layanan sebagai pengganti kuitansi, *e-Tourist card* yaitu pada proses pengajuan visa dan dokumen wisata lainnya bagi para calon pelancong untuk berkunjung ke negara lain, *e-Training* yaitu pada proses pemberian sertifikat pelatihan akademik atau profesional untuk karyawan, *e-Learning* yaitu pada proses penyediaan materi pembelajaran dalam berbagai format, misal video, audio, dan sebagainya sehingga tidak disalahgunakan, diklaim atau dibajak oleh orang lain.

Paper [16] membahas mengenai pemanfaatan *digital signature* untuk validasi disposisi surat. Pada suatu instansi, terutama instansi pemerintahan, apabila ada suatu surat masuk, sebelum surat tersebut diserahkan kepada pimpinan maka akan terlebih dahulu diterima oleh bagian administrasi dan diberi lembar disposisi. Disposisi surat adalah catatan, saran, atau instruksi yang ditandatangani oleh pimpinan setelah surat tersebut dibaca, untuk dilaksanakan atau ditindaklanjuti oleh para stafnya. Permasalahan yang terjadi adalah seringkali ada surat masuk di saat pimpinan sedang tidak berada di tempat, misalnya karena pimpinan sedang perjalanan dinas atau cuti, sehingga instruksi dalam surat tersebut tidak dapat ditindaklanjut oleh para stafnya. Sebagai solusi untuk mengatasi permasalahan tersebut maka dibuatlah suatu sistem berbasis *web* yang mengimplementasikan *digital signature* untuk memvalidasi disposisi surat.

Mekanisme *digital signature* pada *paper* [16] ini adalah dengan cara menempelkan tanda tangan asli yang telah dipindai dan disimpan di dalam basis data sistem. Hasil pindaian tanda tangan tersebut hanya akan muncul di disposisi surat jika *user* yang bersesuaian memasukkan *password* yang benar. Ketika ada surat masuk, langkah pertama adalah bagian administrasi mengisi *form* disposisi surat dan menyimpannya di dalam sistem. Kemudian sistem akan mengirimkan notifikasi kepada pimpinan yang memberitahukan bahwa ada disposisi surat yang perlu tindakan lebih lanjut. Selanjutnya, untuk menindaklanjuti surat tersebut pimpinan diharuskan memilih salah satu kepala bidang, memasukkan isi disposisi surat dan dilanjutkan mengisikan *password*-nya untuk membubuhkan tanda tangan. *Password* yang dimasukkan akan dilakukan *hashing* yang akan menghasilkan *string* dengan panjang 255 karakter. String hasil *hash* tersebut kemudian dibandingkan dengan *hash password* yang telah tersimpan di *database*. Jika hasil *hash password* yang dimasukkan bersesuaian, maka *password* dianggap benar dan pindaian tanda tangan akan tertempel pada tempat yang telah disediakan. Mekanisme tersebut diulangi lagi di tingkat kepala pelaksana sampai dengan pelaksana akhir sehingga status disposisi surat berubah menjadi selesai.

Pada dasarnya mekanisme yang diterapkan di *paper* [16] tidak dapat dikatakan sebagai mekanisme *digital signature*, melainkan pembubuhan tanda tangan hasil pemindaian. Penggunaan *password* pada saat pembubuhan tanda tangan tidak sepenuhnya dapat memvalidasi keabsahan disposisi surat, karena dimungkinan *password* tersebut diketahui oleh orang lain, misalnya *password* sengaja diberikan oleh pemilik asli kepada rekannya atau *password* tanpa sengaja diketahui oleh pihak lain dengan berbagai cara, dan kemudian *password* tersebut disalahgunakan. Pada mekanisme tersebut juga tidak ada proses *hashing* pada dokumen untuk menjaga integritasnya, sehingga memungkinkan isi dokumen diubah oleh orang yang tidak berhak karena tidak dapat diverifikasi dengan mengecek nilai *hash*-nya. Pengguna tidak dapat memastikan bahwa isi dokumen masih asli dan disposisi surat benar-benar ditandatangani oleh orang yang berhak.

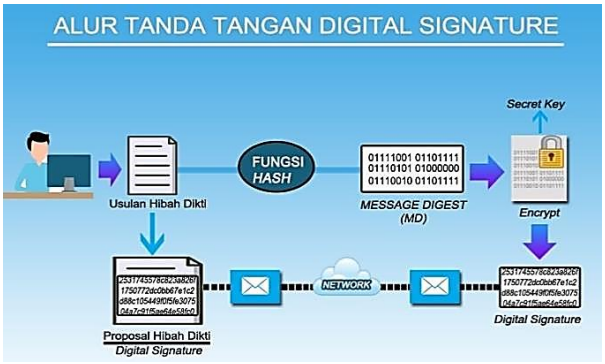
Paper [17] membahas mengenai pemanfaatan *Digital Signature Algorithm* (DSA) untuk memeriksa integritas dari sebuah dokumen elektronik. Permasalahan yang melatarbelakangi adalah perlunya tanda tangan dari suatu pihak untuk mengesahkan suatu dokumen tertentu, namun terkendala dengan kondisi dimana pihak tersebut tidak berada di tempat. Mekanisme *digital signature* yang diterapkan terbagi menjadi beberapa tahap. Tahap pertama adalah pembangkitan kunci (*key generation*) oleh pengirim dokumen yang berupa kunci publik dan kunci privat. Tahap kedua pengirim memilih dokumen yang akan ditandatangi dan membuat *digital signature* menggunakan *private key* yang telah dibangkitkan. Dokumen beserta dengan *signature* dan *public key* kemudian dikirimkan kepada penerima. Tahap terakhir adalah proses verifikasi oleh penerima dokumen untuk mengecek keabsahan dan integritas dokumen. Jika antara dokumen, *signature*, dan *public key* bersesuaian, maka keluaran bernilai *true*, artinya dokumen masih terjaga integritasnya, sebaliknya jika salah satu komponen tidak bersesuaian, maka keluaran bernilai *false*, artinya dokumen tersebut sudah tidak terjamin integritasnya. Alur lebih lebih jelasnya dapat dilihat di Gambar 8.



Gambar 8. *Activity diagram* sistem berbasis DSA [17]

Sistem yang dikembangkan pada *paper* [17] tidak perlu adanya pihak ketiga, misalnya CA, karena proses pembangkitan kunci untuk *digital signature* dilakukan sendiri oleh pengirim dokumen. Namun kelemahannya, penerima dokumen tidak dapat mengetahui apabila ada peniru atau *impostor* yang berperan menjadi pengirim dokumen. Dikarenakan siapapun dapat membangkitkan kunci dan melakukan *signature* sendiri, sehingga tidak dapat dipastikan bahwa orang tersebut adalah benar-benar orang yang berhak atau orang lain.

Paper [18] membahas mengenai penerapan *digital signature* untuk pengesahan dokumen menggunakan algoritma SHA-1. Penelitian dilatarbelakangi oleh perlunya pengesahan proposal hibah DIKTI untuk riset dan pengabdian kepada masyarakat oleh jajaran pejabat institusi, yaitu antara lain ketua program studi, dekan fakultas, hingga kepala pusat penelitian dan pengabdian kepada masyarakat. Dengan adanya sistem tanda tangan digital diharapkan proses pengesahan dokumen tidak perlu lagi dilakukan secara manual yang memiliki banyak keterbatasan. Adapun mekanismenya dapat dilihat di Gambar 9.

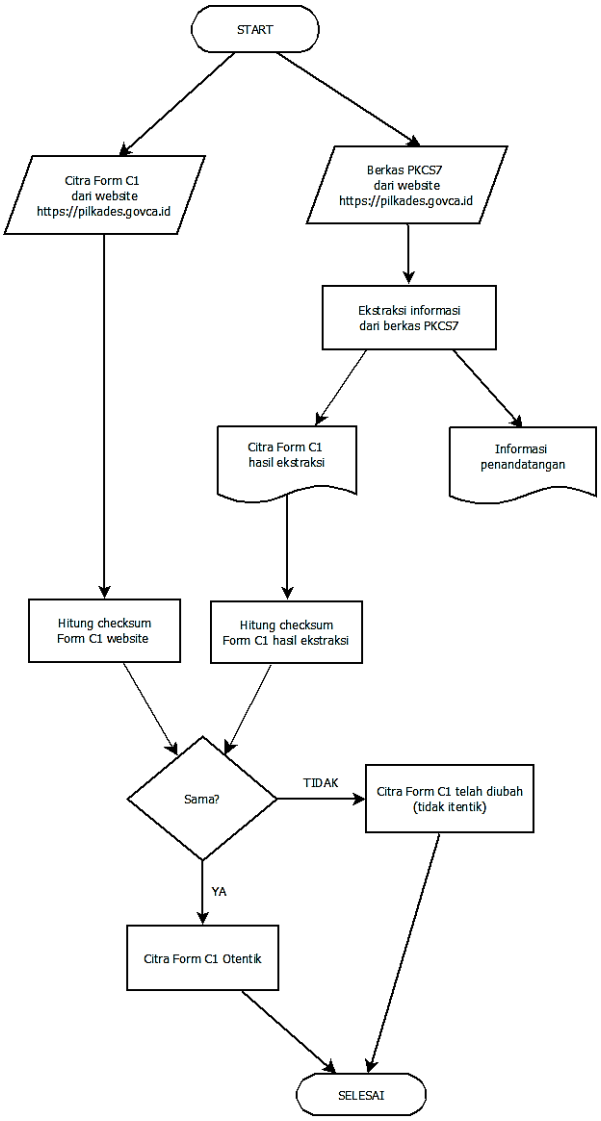


Gambar 9. Alur *digital signature* pada proposal hibah [18]

Dosen pengusul memasukkan data-data ajuan, data pejabat pengesah dokumen dan berkas proposal ke sistem. Selanjutnya para pejabat pengesah dokumen memasukkan data yang akan dilakukan *hashing* dengan SHA-1. *Paper* [18] tidak menyebutkan dengan jelas data apa yang dimasukkan. Hasil *hashing* tersebut merupakan *digital signature*. Selanjutnya proses verifikasi dokumen dilakukan oleh admin DIKTI. Di dalam *paper* tidak dijelaskan dengan rinci bagaimana proses verifikasi dilakukan. Secara garis besar, mekanisme *digital signature* di *paper* ini hanya dengan membandingkan hasil *hashing* SHA-1 terhadap suatu data yang dimasukkan oleh pengguna, baik itu dosen pengusul maupun pejabat pengesah dokumen. Apabila hasil *hashing* yang tersimpan di basis data bernilai sama dengan *hashing* yang tersemat di dokumen maka dokumen dianggap sah, sebaliknya jika hasil *hashing* yang tersimpan di basis data tidak sama dengan hasil *hashing* yang tersemat di dokumen maka dokumen tersebut dianggap tidak sah.

Paper [19] membahas mengenai penerapan tanda tangan digital pada gambar formulir C1.Plano-KWK. Formulir C1.Plano-KWK adalah formulir yang berisi berita acara hasil pemungutan dan penghitungan suara pada proses pemilihan umum di Tempat Pemungutan Suara (TPS). Hal ini dilatarbelakangi oleh kasus sengketa pemilihan presiden tahun 2014 lalu yang menggunakan gambar *form* C1, yang merupakan salinan rekapitulasi hasil di TPS yang diunggah di situs Komisi Pemilihan Umum (KPU), sebagai bukti di persidangan. Gambar *form* C1 tersebut ternyata tidak dapat dijadikan sebagai bukti hukum karena tidak dapat dibuktikan keabsahannya. Sebagai upaya untuk mengatasi permasalahan tersebut, di *paper* ini diterapkan tanda tangan digital di gambar *form* C1. Sistem yang dibangun adalah aplikasi berbasis *mobile* yang dapat dipasang di perangkat Android. Mekanismenya adalah *form* C1 diambil gambarnya oleh petugas yang bertanggungjawab di TPS menggunakan ponsel Android. Dengan aplikasi tanda tangan digital yang telah dipasang di ponsel, gambar *form* C1 tersebut kemudian dikirim ke situs KPU oleh petugas. Sebelum proses pengiriman, terlebih dahulu petugas meregistrasikan sertifikat digital untuk dirinya menggunakan NIK dan surel yang menyatakan bukti diri dan identitasnya. Dengan mekanisme ini, gambar *form* C1 yang dikirimkan ke situs KPU sudah dapat dijamin keabsahannya, sehingga suatu saat ketika diperlukan dapat dijadikan sebagai bukti di persidangan. Tanda tangan digital yang diterapkan di *paper* [19] ini menggunakan sertifikat yang diterbitkan oleh Badan Pengkajian dan Penerapan Teknologi (BPPT) yang bernama iOTENTIK. Sertifikat digital iOTENTIK yang digunakan menggunakan format X.509 versi 3. Sertifikat digital berformat X.509 memiliki beberapa field yaitu *Version, Serial Number, Signature, Issuer, Validity, Subject, Subject Public Key Info, Unique Identifiers*, dan *Extensions*. Sertifikat digital,

kunci privat, dan kunci-kunci simetrik yang terkait dengannya disimpan dalam suatu format berkas yang disebut *keystore*. iOTENTIK menggunakan format *keystore* PKCS#7. Konten-konten dalam *keystore* PKCS#7 dilindungi dengan *passphrase* (kata kunci). *Entry* dalam berkas PKCS#7 yang didistribusikan oleh iOTENTIK adalah bertipe *key entry*. Penerbitan sertifikat diberikan kepada setiap TPS atas nama salah satu petugas KPPS. Hasil gambar yang telah ditandatangani berupa gambar yang telah dibubuhi tanda air. Gambar tersebut sebelum ditampilkan di situs KPU terlebih dahulu dilakukan verifikasi sertifikat digitalnya oleh *server* KPU. Jika verifikasi berhasil maka gambar *form* C1 tersebut valid dan kemudian ditampilkan pada situs *web* beserta tanda tangan digitalnya yang berekstensi p7s. Tanda tangan digital ini berisi informasi penandatangan dan hirarki penerbitan sertifikat, sehingga dapat dipertanggungjawabkan keabsahan dan keasliannya. Gambar 10 menunjukkan alur verifikasi keabsahan gambar *form* C1.Plano-KWK bertanda-tangan digital.

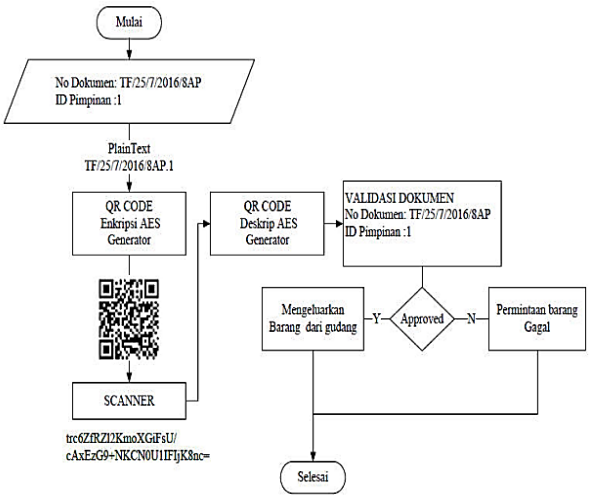


Gambar 10. Alur verifikasi keabsahan gambar form C1.Plano-KWK yang diunggah ke situs KPU [19]

Paper [20], [21], [22], [23], dan [24] membahas mengenai penerapan algoritma RSA pada tanda tangan digital. Mekanisme yang diterapkan yaitu dokumen terlebih dahulu dilakukan fungsi *hash* sehingga menghasilkan *message digest*. Pada *paper* [20] tidak disebutkan algoritma apa yang digunakan untuk *hashing*, di *paper* [21], [23], dan [24] menggunakan algoritma SHA-3 untuk *hashing*, sedangkan di *paper* [22] menggunakan MD5 untuk *hashing*. *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. Pada *paper* [20] dan [24] tanda tangan digital diterapkan pada *plainteks* yang diketikkan langsung di aplikasi. Pada *paper* [21] diterapkan pada berkas bertipe txt, docx, dan pdf. Pada *paper* [22] tanda tangan digital dapat diterapkan baik pada *plainteks* yang diketikkan langsung di aplikasi maupun pada berkas yang diunggah oleh pengguna. Sedangkan pada *paper* [23] diterapkan pada dokumen Surat Tanda Tashih untuk Al-Qur'an digital. Penggunaan fungsi *hash* dan RSA pada proses penandatanganan digital sudah banyak diterapkan karena RSA merupakan algoritma standar untuk tanda tangan digital.

Paper [25] membahas mengenai penerapan tanda tangan digital menggunakan *Quick Response Code* (QR Code) dengan algoritma *Advanced Encryption Standard* (AES) pada dokumen permintaan barang. Metode penelitian yang digunakan adalah metode eksperimen. Tanda tangan digital diterapkan di dokumen permintaan barang. Pada *paper* [25] ini, admin membuat dokumen permintaan di sistem dengan mengisikan nomor dokumen dan nomor id pimpinan yang perlu menyetujui dokumen tersebut. Berkas dokumen dikirimkan kepada pemimpin yang bersesuaian untuk diperiksa dan disetujui. Setelah disetujui oleh pimpinan, data nomor dokumen dan id pimpinan dienkripsi dengan algoritma AES. Kemudian sistem membangkitkan QR *Code* dari hasil enkripsi dan menyematkan QR *Code* di dokumen permintaan untuk kemudian dicetak. Proses verifikasi dilakukan oleh admin gudang dengan cara memindai QR *Code* yang tercetak di dokumen. Hasil pemindaian kemudian didekripsi oleh sistem. Jika hasil dekripsi menunjukkan bahwa dokumen disetujui, maka permintaan barang dapat ditindaklanjuti. Alur penerapan tanda tangan digital di dokumen permintaan barang dapat dilihat di Gambar 11.



Gambar 11. Teknik penerapan tanda tangan digital di dokumen permintaan barang dengan QR Code dan AES [25]

Penggunaan QR *Code* untuk tanda tangan digital sebagaimana yang diterapkan di *paper* [25] pada dasarnya kurang tepat. Hal ini merujuk pada pernyataan dari BSRE BSSN di artikel [26] dimana pada artikel tersebut dinyatakan bahwa QR *Code* berbeda dengan sertifikat elektronik. QR *Code* merupakan jenis tanda tangan elektronik yang tidak tersertifikasi, sehingga tidak direkomendasikan karena QR *Code* mudah untuk dipalsukan, misalnya dengan melakukan *crop* pada gambar QR *Code* dan menaruhnya di dokumen yang dipalsukan.

Paper [27] membahas mengenai penerapan tanda tangan elektronik pada dokumen atau persuratan dalam sistem *e-government*. Tujuannya adalah untuk mempermudah proses birokrasi. Sistem yang dibangun adalah sistem Tanda Tangan Elektronik (TTE) yang berbasis *client-server*. *Server* berfungsi untuk memberikan layanan permintaan dan penerbitan tanda tangan digital, sedangkan *client* berfungsi untuk memproses tanda tangan digital. Setiap dokumen yang membutuhkan persetujuan atau tanda tangan elektronik dari pejabat terkait harus diunggah ke sistem tersebut. Kemudian sistem akan mengirimkan pemberitahuan kepada pejabat terkait untuk menandatangani dokumen. Pengguna dapat menandatangi dokumen elektronik apabila ia sudah memiliki *private key* dan sertifikat elektronik, oleh karena itu pengguna terlebih dahulu harus mengajukan permohonan sertifikat elektronik di sistem TTE. Sertifikat elektronik yang diterbitkan dan *private key* disimpan dalam format PKCS#12 di aplikasi *client*. Tanda tangan digital yang dihasilkan dari sistem TTE merupakan kombinasi dari fungsi *hash* dan enkripsi dengan algoritma kriptografi asimetrik. Proses pembangkitan tanda tangan digital dilakukan dengan cara menghitung nilai *hash* dari dokumen elektronik. Nilai *hash* yang dihasilkan kemudian dilakukan enkripsi menggunakan *private key* dari pengguna, dalam hal ini pejabat yang

terkait. Hasil enkripsi tersebut yang kemudian menjadi tanda tangan digital yang disematkan di dokumen elektronik. Kendala yang dihadapi dalam penerapan tanda tangan digital adalah permasalahan humanis, yaitu masih adanya keraguan dan *mindset* bahwa penerapan tanda tangan digital ini sulit, serta sulitnya mengubah budaya lama yang berbasis kertas menjadi *paperless*. Selain kendala yang disebutkan di dalam *paper* [27], permasalahan lain yang mungkin muncul adalah masih kurangnya pemahaman pengguna mengenai tanda tangan digital. Hal tersebut dikarenakan masih kurangnya sosialisasi mengenai teknologi tanda tangan digital kepada masyarakat luas. Selain itu juga masih minimnya kebijakan mengenai penerapan tanda tangan digital. Langkah yang dapat diambil untuk mengatasi permasalahan-permasalahan tersebut antara lain dengan melakukan sosialisasi secara menyeluruh kepada masyarakat, serta melakukan pelatihan mengenai legalisasi dokumen elektronik menggunakan teknologi tanda tangan digital.

Paper [28] membahas mengenai penerapan tanda tangan digital menggunakan algoritma *Message Digest* 5 (MD5). Latar belakang yang mendasari adalah perlunya verifikasi atas keaslian dan integritas dokumen digital yang dikirimkan melalui media komunikasi elektronik. Terdapat dua proses dalam aplikasi tanda tangan digital yang dikembangkan, yaitu proses penandatanganan dan proses verifikasi. Berkas yang digunakan adalah berkas berekstensi .doc atau .docx. Proses penandatanganan dilakukan dengan cara: (1) membaca isi berkas berekstensi .doc atau .docx, (2) menyalin dan menyimpan isi berkas .doc atau .docx ke dalam format .txt, (3) menambahkan kata kunci pembuat tanda tangan, (4) menghitung nilai *hash* berkas berekstensi .txt, (5) menyematkan nilai *hash* hasil perhitungan ke berkas berekstensi .doc atau .docx. Sedangkan pada proses verifikasi dilakukan secara sebaliknya.

Berdasarkan *paper* [28], tanda tangan digital yang berupa nilai *hash* dari dokumen asli ditambah dengan kata kunci pengguna tersemat di dalam *properties* berkas yang berekstensi .doc atau .docx. Apabila terjadi perubahan pada isi berkas, maka nilai *hash* yang dihasilkan akan berbeda. Cara ini cukup sederhana dan cukup mampu untuk menjaga keaslian isi dokumen. Namun, penerima dokumen tidak dapat memverifikasi apakah orang yang menyematkan kata kunci di dokumen yang diterimanya adalah benar-benar orang yang berhak atau bukan.

Paper [29] membahas mengenai penerapan skema tanda tangan Schnorr untuk pembuatan tanda tangan digital. Skema tanda tangan Schnorr merupakan variasi dari skema tanda tangan ElGamal. Urutan proses pada skema tanda tangan Schnorr yaitu: (1) pembentukan kunci oleh pengirim pesan, (2) pembuatan tanda tangan digital dengan menambahkan nilai *hash*, dan (3) verifikasi tanda tangan digital oleh penerima pesan. Pada tahap pembentukan kunci dibutuhkan dua buah bilangan prima *p* dan *q* untuk membangkitkan sepasang kunci publik dan kunci privat. Langkah selanjutnya adalah menghitung nilai $\alpha^k \bmod p$, dengan α dan p kunci publik serta k bilangan rahasia $1 \leq k \leq q\text{-}1$. Nilai $\alpha^k \bmod p$ kemudian digabungkan dengan pesan dan dihitung nilai *hash*-nya. Tahap kedua adalah proses pembuatan tanda tangan digital dengan menghitung nilai *hash* dari pesan asli *D*, yaitu $h(D \parallel \alpha^k \bmod p)$ menghasilkan tanda tangan pertama γ, dilanjutkan dengan menghitung nilai $\delta = k + \alpha \times \gamma \bmod q$ yang akan menjadi tanda tangan kedua. Hasil akhir dari tahap 2 adalah tanda tangan untuk pesan yaitu (γ, δ). Proses verifikasi dilakukan dengan menghitung nilai $\alpha^{\delta}\beta^{-\gamma} \bmod p$, dengan $\beta = \alpha^a \pmod p$ dimana a adalah sembarang bilangan bulat $0 \leq a \leq q\text{-}1$. Jika hasil $\alpha^{\delta}\beta^{-\gamma} \bmod p = \alpha^k \bmod p$ maka tanda tangan asli dan pesan belum diubah, sebaliknya jika $\alpha^{\delta}\beta^{-\gamma} \bmod p \neq \alpha^k \bmod p$ maka tanda tangan palsu dan pesan telah diubah.

Skema tanda tangan digital yang diterapkan pada *paper* [29] tersebut berbeda dengan skema tanda tangan digital di sebagian besar *paper* lainnya yang menggunakan *Digital Signature Algorithm* (DSA) maupun RSA. Skema Schnorr lebih mengacu pada algoritma ElGamal dengan berdasarkan pada masalah logaritma diskrit. Ukuran tanda tangan yang dihasilkan oleh skema Schnorr lebih kecil jika dibandingkan dengan skema tanda tangan lainnya, namun skema Schnorr memiliki kemampuan yang hampir sama dengan DSA. Permasalahan yang dihadapi adalah sulitnya menentukan nilai bilangan prima *p* dan *q* yang memenuhi $p\text{-}1 \equiv 0 \pmod p$ atau $p = nq+1$ karena tidak semua *n* yang diambil bisa mendapatkan nilai *p* prima.

Paper [30] membahas mengenai penerapan tanda tangan digital pada dokumen elektronik menggunakan fungsi *hash* SHA-1. Aplikasi yang dikembangkan berbasis *Software as a Service* (SaaS) dan diberi nama *Digital Signature System* atau DSign. Proses penandatanganan dilakukan dengan cara: (1) menghitung nilai *hash* dari informasi terkait dengan dokumen yang dimasukkan oleh pengguna di sistem, yaitu *header, subject, addressee,* dan *comment,* (2) sistem mengecek ke basis data DSign apakah ada dokumen yang sama (duplikasi) atau tidak, (3) apabila tidak ada duplikasi, sistem kemudian menambahkan data dokumen dan nilai hasil *hashing* ke basis data DSign, (4) sistem membangkitkan QR *Code* dan/atau *barcode* yang berisi *link* alamat *web* dari *record* tanda tangan digital di basis data DSign, dan (5) QR *Code* dan/atau *barcode* yang dibangkitkan disematkan ke dokumen sebagai pengganti tanda tangan atau

stempel untuk menyatakan keabsahan dokumen. Sistem DSign ini bersifat *online*, sehingga untuk proses verifikasi dokumen, pengguna cukup memindai QR *Code* dan/atau *barcode* yang tersemat di dokumen. Setelah dipindai, pengguna diarahkan ke sistem DSign yang akan mengecek ke basis datanya sekaligus memverifikasi keabsahan dokumen tersebut berdasarkan informasi *record* hasil pemindaian QR *Code* dan/atau *barcode*.

Berdasarkan *paper* [30] tersebut, QR *Code* dan/atau *barcode* yang disematkan di dokumen pada dasarnya bukanlah tanda tangan digital dari dokumen, melainkan keduanya hanya media untuk menyimpan *link* yang akan mengarahkan ke alamat sistem untuk mengecek tanda tangan digital yang disimpan di dalam basis data sistem. Tanda tangan digital yang sebenarnya diterapkan adalah hasil perhitungan dengan fungsi *hash*. Arsitektur sistem yang dikembangkan cukup sederhana, karena tidak diperlukan proses pengajuan sertifikat digital. Proses verifikasi dokumen oleh penerima pesan pun mudah, yaitu cukup dengan memindai QR *Code* dan/atau *barcode* yang tersemat di dokumen.

Berdasarkan hasil *literature review* terhadap beberapa *paper* di atas, dapat dibuat ringkasan algoritma atau skema yang digunakan untuk tanda tangan digital serta penerapannya sebagaimana ditunjukkan pada Tabel 1.

Tabel 1.Ringkasan hasil *literature review*

Paper	Algoritma/Skema	Penerapan
[5]	RSA, PKCS#12	*Green-ICT*
[11]	SHA-1, DSS	Legalisir ijazah dan transkrip nilai
[12]	SHA-512, RSA	Legalisir ijazah
[13]	MD5, DSA	*e-Government*
[14]	Hasil pindai tanda tangan asli, fungsi *hash*	Disposisi surat
[15]	DSA	Pemeriksaan integritas dokumen, *private key* dikirimkan bersamaan dengan dokumen dan *signature*
[16]	SHA-1	Pengesahan proposal hibah DIKTI. Tanda tangan digital berupa hasil *hash* dari *secret message* yang dimasukkan oleh *user*
[17]	*Checksum*, PKCS#17	Gambar C1.Plano-KWK. Ada CA dan *root* CA
[18]	Fungsi *hash*, RSA	Pengecekan keabsahan pesan (plainteks) yang dimasukkan oleh pengirim
[19]	SHA-3, RSA	Pengecekan keabsahan dokumen berformat txt, docx, atau pdf
[20], [21], [22], [23], [24]	RSA, fungsi *hash*	*Paper* [20] fungsi *hash* yang digunakan tidak disebutkan, diterapkan pada *plainteks* yang diketikkan langsung di aplikasi. *Paper* [21], [23], dan [24] menggunakan SHA-3, [21] diterapkan pada berkas bertipe txt, docx, dan pdf, [23] diterapkan pada dokumen Surat Tanda Tashih Al-Qur'an digital, sedangkan [24] diterapkan pada *plainteks* yang diketikkan langsung di aplikasi. *Paper* [22] fungsi *hash* menggunakan MD5, diterapkan pada plainteks yang diketikkan langsung di aplikasi atau pada berkas yang diunggah.
[25]	AES, QR *Code*	Dokumen permintaan barang
[27]	Fungsi *hash*, kriptografi asimetrik, PKCS12	Dokumen atau persuratan di sistem *e-government*
[28]	MD5	Dokumen berekstensi .doc atau .docx
[29]	Schnorr	Pengecekan keaslian dokumen yang dikirimkan oleh pengirim
[30]	SHA-1	Diterapkan pada aplikasi berbasis SaaS, dengan menyematkan QR *Code* dan/atau *barcode* di dokumen yang berisi *link* untuk verifikasi keabsahan dokumen.

4. Kesimpulan

Berdasarkan hasil *review* dan perbandingan algoritma atau skema yang diterapkan pada beberapa *paper* di atas dan juga dengan mempertimbangkan kesiapan infrastruktur, aspek legalitas, serta kondisi saat ini dimana pandemi COVID-19 sedang melanda yang mengharuskan sebagian besar masyarakat untuk bekerja dari rumah atau *work from home*, maka sudah saatnya penerapan tanda tangan digital ini dapat dioptimalkan untuk mengatasi keterbatasan dan kendala pengesahan dokumen menggunakan cara tradisional, yaitu tanda tangan manual. Salah satu hal yang dapat dilakukan adalah dengan penerapan tanda tangan digital untuk pengesahan dokumen akademik maupun non-akademik di lingkungan perguruan tinggi. Skema yang dapat diterapkan di kasus tersebut yaitu: (1) untuk legalisasi dokumen ijazah dan transkrip nilai yang proses verifikasinya dilakukan oleh pihak luar kampus, maka skema *Digital Signature Algorithm* dengan menggunakan sertifikat digital cocok digunakan, selain itu juga dapat menggunakan skema berbasis SaaS dengan menyematkan QR *Code* dan/atau *barcode* di dokumen sebagaimana *paper* [30], (2) untuk legalisasi dokumen yang proses verifikasinya dilalukan oleh pihak internal kampus maka penggunaan skema PKCS dengan membangkitkan tanda tangan digital melalui aplikasi pembaca berkas berformat pdf seperti *Adobe Reader* atau *Foxit Reader* dapat digunakan, karena cara ini cukup sederhana, mudah diterapkan, dan tidak memerlukan infrastruktur tambahan lainnya.

Daftar Rujukan

[1] "Kuliah Daring Hingga UN, Ini 5 Kebijakan Pendidikan Masa Darurat Corona," 2020.
[2] B. A. Oktavira, "Ketentuan Pelaksanaan Work From Home di Tengah Wabah COVID-19," 2020.
[3] *Undang-Undang Republik Indonesia Nomor 13 Tahun 2003 tentang Ketenagakerjaan*. 2003.
[4] S. A. Poerana, "Cara Kerja Tanda Tangan Elektronik," 2020.
[5] F. Z. Abraham, P. I. Santosa, and W. W. Winarno, "Tandatangan Digital Sebagai Solusi Teknologi Informasi Dan Komunikasi (TIK) Hijau: Sebuah Kajian Literatur," *J. Masy. Telemat. dan Inf.*, vol. 9, no. 2, pp. 111–124, 2018, doi: 10.17933/mti.v9i2.120.
[6] "Jenis Tanda Tangan Elektronik," 2020.
[7] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, pp. 644–654, 1976, doi: 10.1007/3-540-44709-1_14.
[8] R. Munir, *Kriptografi 2nd Edition*. Penerbit Informatika, 2019.
[9] J. Aprilyani and Y. Winarto, "Kominfo Awasi Ketat Startup Penyedia Tanda Tangan Digital," 2018.
[10] F. A. Burhan, "Permintaan Tanda Tangan Digital PrivyID Naik 350% Selama Pandemi," 2020.
[11] Z. A. Hasibuan, *Metodologi Penelitian pada Bidang Komputer dan Teknologi Informasi: Konsep, teknik, dan aplikasi*. Fasilkom Universitas Indonesia, 2007.
[12] Aptika, "SiVION - Solusi Identitas Digital Terpercaya," 2016. .
[13] B. Triandi, S. Effendi, R. Puspasari, I. F. Rahmad, and E. Ekadiansyah, "Digital Document Security on Legalize Higher Education Diplomas with Digital Signature and SHA-1 Algorithm," in *The 7th International Conference on Cyber and IT Service Management (CITSM)*, 2019, pp. 5–9, doi: 10.1109/CITSM47753.2019.8965421.
[14] F. Nuraeni, Y. H. Agustin, and I. M. Muharam, "Implementasi Tanda Tangan Digital Menggunakan RSA dan SHA-512 Pada Proses Legalisasi Ijazah," in *Konferensi Nasional Sistem Informasi (KNSI)*, 2018, pp. 864–869.
[15] V. R. Pancholi, "A Study on Importance of Digital Signature for E-Governance Schemes," vol. 4, no. 10, pp. 7–10, 2018.
[16] E. A. Kriswanto and Fitriyadi, "Implementasi Digital Signature Untuk Validasi Disposisi Surat," *J. Ilm. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 1, pp. 11–22, 2020.
[17] D. Arisandi, Sukri, and M. B. Yusuf, "Pemeriksaan Integritas Dokumen dengan Digital Signature Algorithm," *J. Inf. Syst. Informatics Eng.*, vol. 4, no. 1, pp. 1–6, 2020.
[18] E. K. Suni and H. I. Maulana, "Penerapan Digital Signature Untuk Mengesahan Proposal Hibah Dikti Menggunakan Secure Hash Algorithm," *J. Inf. Technol. Comput. Sci.*, vol. 5, no. 2, pp. 105–112, 2020, doi: 10.31328/jointecs.v5i2.1318.
[19] R. A. Perdana, D. R. Anbiya, and A. Grahitandaru, "Penerapan Tanda Tangan Digital pada Gambar Formulir C1.PLANO-KWK di Pilkada Sulawesi Selatan," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 5, pp. 475–484, 2019, doi: 10.25126/jtiik.201961471.
[20] D. Puspitasari and Y. Permanasari, "Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," in *Prosiding Matematika*, 2020, vol. 6, no. 1, pp. 14–20, doi: 10.33633/tc.v18i2.2166.
[21] Y. Anshori, A. Y. E. Dodu, and D. M. P. Wedananta, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," *Techno.Com*, vol. 18, no. 2, pp. 110–121, 2019, doi: 10.33633/tc.v18i2.2166.
[22] M. Ihwani, "Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma Rsa," *CESSJournal Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 15–20, 2016.
[23] Liyanti and A. R. Hakim, "Perancangan Penerapan Tanda Tangan Digital sebagai Pengembangan Sistem Pelayanan Pentashihan Al Quran Digital," *SISTEMASI*, vol. 8, no. 1, pp. 41–54, 2019, doi: 10.32520/stmsi.v8i1.415.
[24] R. A. Azdy, "Tanda Tangan Digital Menggunakan Algoritme Keccak dan RSA," *JNTETI*, vol. 5, no. 3, pp. 184–191, 2016.
[25] A. G. P. Suratma and A. Azis, "Tanda Tangan Digital Menggunakan QR Code dengan Metode Advanced Encryption Standard," *Techno*, vol. 18, no. 1, pp. 59–68, 2017.
[26] Z. Suhardono, "Apakah Tanda Tangan Elektronik itu QRCODE?," 2020.
[27] A. Nugraha and A. Mahardika, "Penerapan Tanda Tangan Elektronik Pada Sistem Elektronik Pemerintahan Guna Mendukung E-Government," in *Seminar Nasional Sistem Informasi Indonesia*, 2016, pp. 359–364.
[28] D. P. Precilia and A. Izzuddin, "Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5)," *Energy*, vol. 5, no. 1, pp. 14–19, 2016.
[29] H. F. Isnaini and K. Karyati, "Penerapan Skema Tanda Tangan Schnorr pada Pembuatan Tanda Tangan Digital," *PYTHAGORAS J. Pendidik. Mat.*, vol. 12, no. 1, pp. 57–64, 2017, doi: 10.21831/pg.v12i1.11631.
[30] G. Saha, "DSign Digital Signature System for Paperless Operation," pp. 324–328, 2017