e-ISSN: 2964-2531
DOI : 10.36499/psnst.v12i1.7010
p-ISSN: 2964-5131

MODEL PENGENDALIAN INTERNAL IMPLEMENTASI TANDA TANGAN ELEKTRONIK PADA SISTEM PEMERINTAHAN DAERAH

Muhammad Tajuddin[1*], Andi Sofyan Anas[2], Rifqi Hammad[2] dan Ahmad Zuli Amrullah[2]
[1] Jurusan Ilmu Komputer, Fakultas Teknik, Universitas Bumigora Mataram
[2] Jurusan Rekayasa Perangkat Lunak, Fakultas Teknik, Universitas Bumigora Mataram
Jl. Ismail Marzuki No 22 Karang Tapen Cakranegara, Mataram, NTB 83131
[*]Email: tajuddin@universitasbumigora.ac.id

Abstrak

Layanan tanda tangan elektronik telah menimbulkan berbagai masalah dalam lingkup pemerintahan daerah. Teknologi otentikasi keamanan perlu dimanfaatkan untuk menciptakan layanan yang sesuai dengan era Revolusi Industri. Untuk menjaga kerahasiaan dan keamanan penggunaan tanda tangan elektronik, perlu memperhatikan syarat dan ketentuan sehingga otentikasi dokumen-dokumen ini dijamin. Untuk itu, penggunaan tanda tangan elektronik harus dilakukan dengan menggunakan tanda tangan dalam sistem yang tersertifikasi. Penelitian ini memberikan gambaran tentang pentingnya menjaga kerahasiaan dan keamanan dalam penggunaan tanda tangan elektronik. Tanda tangan elektronik membantu menciptakan kepercayaan dan keyakinan dalam lingkungan tanpa kertas. Penelitian ini membahas implikasi hukum dan perbedaan antara berbagai jenis tanda tangan elektronik, teknologi pendukung, aplikasinya dalam proses bisnis, dan implikasinya terhadap sistem pengendalian internal. Kerangka Manajemen Risiko diusulkan untuk mengelola keamanan dan kontrol menggunakan tanda tangan elektronik. Tidak semua tanda tangan elektronik dibuat sama. Beberapa lebih aman daripada yang lain tetapi biaya lebih dan kompleks untuk diterapkan. Penelitian ini juga mengkaji biaya dalam penerapan tanda tangan elektronik dan risiko yang terlibat. Tidak dapat dihindari bahwa hal-hal akan tetap salah bahkan dengan tanda tangan elektronik yang paling aman, penting untuk memiliki sistem pengendalian internal yang efektif untuk melengkapi keamanan dan kontrol yang difasilitasi oleh tanda tangan elektronik.

***Kata kunci**: Tanda, tangan, elektronik, otentikasi.*

1. PENDAHULUAN

Indonesia yang berada di era globalisasi ditandai dengan era teknologi informasi yang memperkenalkan dunia maya (*cyberspace*) melalui internet (Zubov, 2020), komunikasi dengan media elektronik *paperless*. Melalui media elektronik ini, seseorang akan memasuki dunia maya yang abstrak, universal, tidak bergantung pada keadaan tempat dan waktu (Lertxundi and Landeta, 2022). Masyarakat Indonesia meyakini bahwa peran informasi dalam memberikan kontribusi bagi pembangunan ekonomi, sosial, dan budaya. Selain itu, kemajuan teknologi informasi juga mempengaruhi kondisi sosial di masa depan, seperti sistem pelayanan kesehatan, sistem pelayanan pendidikan, sistem pelayanan administrasi pemerintahan, dan berbagai aspek kehidupan lainnya sudah mulai menggunakan tanda tangan elektronik(Nugraha and Mahardika, 2016).

Tanda tangan elektronik bersifat *non-face (*tanpa tatap muka), *non-sign* (tidak menggunakan tanda tangan asli), dan tanpa batas wilayah (seseorang dapat menandatangani secara elektronik dengan pihak lain meskipun berada di negara yang berbeda) dengan menggunakan teknologi informasi(Zamrodah, 2016). Dalam perkembangannya, aspek keamanan informasi sudah mulai diperhatikan. Ketika informasi ini menjadi rusak atau akan ada resiko yang harus ditanggung oleh orang yang mengirim, membutuhkan, atau hanya melihatnya, karena penggunaan informasi elektronik ini, dengan menggunakan jaringan publik, di mana setiap orang dapat mengetahui informasi elektronik tersebut(Digital, 2022). Lembaga yang independen dan akuntabel yang dapat memverifikasi tanda tangan elektronik dan Indonesia memiliki aturan hukum untuk mengatur masalah ini dengan diterbitkannya Undang-Undang Nomor 11 Tahun 2008, tentang "Informasi dan Transaksi Elektronik" yang disahkan pada tanggal 21 April 2008.

Tanda tangan elektronik memudahkan dalam menentukan kehadiran pelanggan berdasarkan komunikasi perangkat seluler. Kehawatiran yang meningkat atas penipuan online dan undang-undang

serta peraturan pemerintah nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang mengizinkan penggunaan tanda tangan elektronik mengharuskan pemerintah daerah untuk memperkuat sistem kontrol internal mereka dan membangun proses otentikasi(Indonesia, 2016). Tujuan utama sistem pengendalian internal adalah untuk melindungi aset perusahaan, memastikan keandalan informasi, dan kepatuhan terhadap undang-undang dan peraturan yang ditetapkan.

Pemerintah daerah harus menyeimbangkan antara biaya penerapan sistem pengendalian internal dan manfaat yang dapat diperoleh. menunjukkan bahwa sementara *eSignature* lazim di seluruh dunia karena kenyamanannya (Mataram, 2015), persepsi orang tentang kesetaraan simbolis dari tulisan tangan dan *eSignature* bukanlah topik yang diteliti secara ekstensif. Studi ini menyoroti negativitas yang terkait dengan *eSignatures* karena rasa kehadiran dan keterlibatan sosial yang lebih lemah (Mataram, 2018), terlepas dari berbagai jenis tanda tangan dan kenyamanan dengan teknologi.

2. METODOLOGI

2.1. Lingkup Studi

Pemerintah daerah menggunakan tanda tangan elektronik seperti melakukan transaksi online, mengakses jaringan atau PC atau area keamanan, mengakses dan memverifikasi catatan atau informasi pribadi lainnya, identifikasi keamanan, aplikasi pemerintah dan militer, dan lain-lain (Sardjono *et al.*, 2021). Penelitian ini berfokus pada dampak tanda tangan elektronik terhadap pengendalian internal. Bukan maksud dari penelitian ini untuk fokus pada detail teknis dari berbagai teknologi yang digunakan untuk mengimplementasikan tanda tangan elektronik. Kajian ini pada dasarnya juga terbatas pada penerapan tanda tangan elektronik dalam lingkungan tanpa kertas menggunakan Internet (Scîrtocea, 2022).

2.2. Aplikasi Tanda Tangan Elektronik

Tanda tangan elektronik di Indonesia diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang berfungsi sebagai otentikasi dan verifikasi. Tanda tangan elektronik adalah tanda tangan biasa yang dibuat secara elektronik yang fungsinya sama dengan tanda tangan biasa pada suatu dokumen atau *file* (Sardjono *et al.*, 2021).

Tanda tangan elektronik atau *electronic signature* bukanlah konsep baru sama sekali. Ini telah digunakan oleh beberapa perusahaan selama bertahun-tahun untuk mengurangi biaya dengan meningkatkan proses alur kerja internal (Muhammad Tajuddin, 2020). Minat saat ini dalam topik ini adalah karena aplikasi potensialnya dalam pemerintah (Nugraha and Mahardika, 2016). Tanda tangan elektronik bisa sesederhana nama yang diketik yang dilampirkan individu ke email atau lebih canggih seperti gambar elektronik tanda tangan yang ditautkan ke algoritme matematika yang memverifikasi keaslian dokumen *online*, tanda tangan rusak dan tidak sah jika tanda tangan diubah setelah penandatanganan (Chong, Kim and Choi, 2021). Gambaran yang baik tentang potensi tanda tangan elektronik dalam transaksi online terutama yang menggabungkan dengan sertifikat elektronik dan teknologi kartu pintar, namun, kita harus ingat bahwa *hackers* tertarik pada tantangan baru (Digital, 2022). Teknologi saja tidak akan menyelesaikan masalah yang dihadapi tanda tangan elektronik, sistem kontrol internal yang kuat diperlukan karena sebagian besar penipuan atau kegagalan keamanan terutama disebabkan oleh faktor manusia.

2.3. Pengendalian Internal

COSO (*Committee of Sponsoring Organizations*) mencantumkan lima komponen pengendalian internal yang saling terkait(Velentzas *et al.*, 2022):

1. Lingkungan pengendalian-dasar dari semua komponen pengendalian internal lainnya, menyediakan disiplin dan struktur untuk integritas, nilai-nilai etika dan kompetensi orang-orang dalma pemerintahan.
2. Penilaian risiko-identifikasi dan analisis risiko yang relevan untuk pencapaian tujuan organisasi dengan membentuk dasar dalam mengelola risiko.
3. Aktivitas pengendalian-kebijakan dan prosedur untuk memastikan arahan manajemen dilaksanakan di semua tingkatan dan di semua fungsi organisasi untuk mengatasi risiko.

e-ISSN: 2964-2531
DOI : 10.36499/psnst.v12i1.7010
p-ISSN: 2964-5131

4. Informasi, komunikasi, dan informasi internal dan eksternal harus diidentifikasi, ditangkap dan dikomunikasikan tepat waktu untuk menjalankan dan mengendalikan pemerintahan.
5. Pemantauan-proses penilaian kualitas kinerja sistem dari waktu ke waktu dengan melaporkan kekurangan ke tingkat manajemen yang relevan.

Meskipun COSO menyatakan dengan jelas cara dan peran dan tanggung jawab semua pemangku kepentingan dalam pengendalian internal, itu benar-benar kerangka kerja dan efektivitasnya akan sangat bergantung pada kemampuan organisasi untuk melaksanakan rekomendasi (Zhong *et al.*, 2022).

2.4. Teknologi Tanda Tangan Elektronik

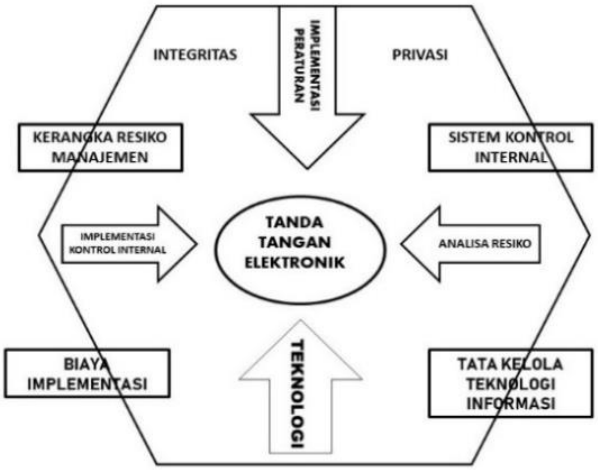
Gambaran luas tentang teknologi biometrik, penggunaannya, dan pengukuran kinerja, bagaimana sistem dibangun dan masalah implementasi praktik (Fitriani and Muhammad, 2016). Nomor identifikasi pribadi atau PIN adalah salah satu teknik paling awal yang digunakan untuk menawarkan pengenalan otomatis. Namun, tidak dapat mengenali orang yang mempresentasikannya (Ida Bagus Gede Sarasvananda, I Putu Eka Giri Gunawan, I Komang Arya Ganda Wiguna , Made Suci Ariantini, 2022). Hal yang sama berlaku untuk kartu dan token lainnya. Biometrik tidak dapat dengan mudah ditransfer antar individu dan mewakili pengidentifikasi unik (Zamrodah, 2016). Hal ini dinilai lebih akurat dan aman karena perangkat biometrik tidak mudah tertipu. Teknologi ini diharapkan dapat digunakan secara luas di area komersial seperti penggunaan mesin ATM, *workstation* dan akses jaringan, perjalanan dan pariwisata, transaksi internet *online*, transaksi telepon, dan kartu identitas publik. teknologi biometrik. Teknologi otentikasi biometrik memberikan keamanan yang jauh lebih besar daripada kata sandi tradisional, PIN, dan mekanisme keamanan. Ini juga menggerakkan fokus keamanan untuk mencegah intrusi dari dalam organisasi yang merupakan sumber utama akses tidak sah ke informasi(Ribeiro, De Almeida and Canedo, 2021).

2.5. Manajemen Risiko

Salah satu risiko untuk pemerintah daerah adalah pencurian data elektronik oleh karyawan internal dan peretas serta administrasi kata sandi yang buruk menimbulkan risiko terbesar. Penulis menganjurkan bahwa prosedur kontrol akses fisik (Lertxundi and Landeta, 2022), prosedur kontrol kata sandi, enkripsi data menggunakan infrastruktur kunci publik dan prosedur kontrol keamanan berbasis perangkat lunak seperti *firewall* dan sistem deteksi intrusi harus dimasukkan untuk mengendalikan risiko infrastruktur TI. Risiko *spoofing email, spoofing IP,* situs web palsu dapat dikendalikan dengan mengadopsi tanda tangan elektronik dan sertifikat yang menetapkan identitas pihak dalam transaksi (Nawar, 2011). Identifikasi biometrik yang menggunakan karakteristik fisik yang khas (seperti pola suara, sidik jari, struktur wajah, atau dinamika tanda tangan) juga dapat digunakan untuk mengurangi risiko pemalsuan identitas dalam pemerintahan. Karena setiap organisasi adalah unik (apakah melakukan e-bisnis atau tidak)(Tajuddin *et al.*, 2013), tidak ada paket standar prosedur pengendalian yang paling cocok untuk semua. Paket kontrol yang optimal harus menyeimbangkan biaya dan manfaat dari aplikasi spesifiknya. Analisis biaya-manfaat harus dilakukan pada setiap prosedur pengendalian perspektif.

2.6. Metodologi Penelitian

Desain penelitian ini didasarkan pada sumber-sumber pemerintah daerah berdasarkan informasi yang dikumpulkan dari berbagai sumber. Kerangka kerja penelitian untuk diskusi, analisis dan temuan ditunjukkan pada diagram berikut (Anwar, 2019):



Gambar 1. Model kerangka penelitian

3. HASIL DAN PEMBAHASAN

Tanda tangan elektronik dan tanda tangan digital adalah dua hal yang sering membingungkan makna dan fungsinya, terutama saat menandatangani dokumen. Meski tidak terlihat jauh berbeda, pada kenyataannya tanda tangan digital tidak sama dengan tanda tangan elektronik. Tanda tangan elektronik mencakup berbagai aplikasi, sedangkan tanda tangan digital diklasifikasikan sebagai salah satu jenis tanda tangan elektronik(Eka Putra and Riswadi, 2022).

Tabel 1. Perbandingan perbedaan tanda tangan elektronik dan tanda tangan digital

Tanda Tangan Digital	Tanda Tangan Elektronik
1. Digunakan untuk memverifikasi dokumen	1. Digunakan untuk mengamankan dokumen
2. Bisa dalam bentuk gambar, tulisan, bahkan daftar periksa	2. Bentuk tanda tangan tidak menentukan keabsahan
3. Tidak memiliki sistem keamanan dokumen	3. Memiliki sistem keamanan dokumen
4. Tidak dapat divalidasi	4. Dapat divalidasi oleh semua individu yang bersangkutan engan dokumen
5. Tidak dapat menjamin integritas dokumen Tidak memiliki kekuatan hukum	5. Integritas dokumen dapat dijamin
6. Tidak memiliki peraturan yang jelas	6. Memiliki kekuatan hukum
	7. Terdaftar dan diatur di bawah otoritas

3.1. Pengembangan Kerangka Manajemen Risiko untuk Tanda Tangan Elektronik

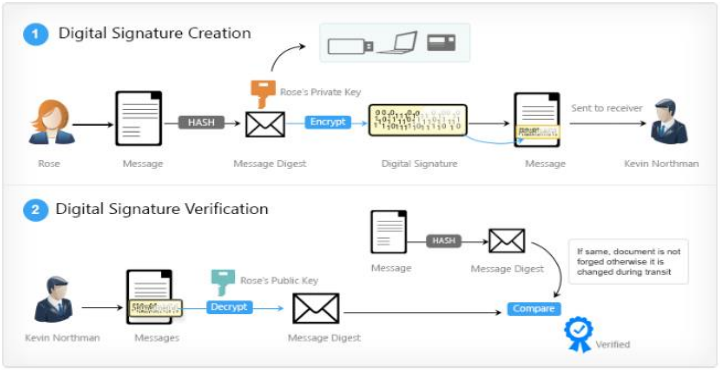
Penggunaan tanda tangan elektronik membantu memperkuat kepercayaan dan keyakinan dalam lingkungan tanpa kertas di mana informasi dan dokumen, transaksi keuangan atau informasi pribadi dikirimkan dengan cara yang aman. Namun, itu juga mengandung risiko potensial, beberapa di antaranya diketahui dan dipahami, yang lain diketahui tetapi kurang dipahami, dan yang lainnya tidak diketahui. *E-Government* menerapkan konsep *eID* dan *eSignature* untuk transaksi yang aman dan dapat digunakan dalam skala besar. Namun, karena variasi besar dalam aspek teknologi dan organisasi, ekosistem yang heterogen menghasilkan wawasan yang tidak memadai. Studi ini mengusulkan kerangka kerja untuk adopsi *eID* seluler dan solusi tanda tangan elektronik yang efektif dan efisien. Oleh karena itu, penting bagi bisnis dan manajemen untuk mengidentifikasi, mengukur, dan mengelola risiko yang terkait dengan tanda tangan elektronik.

3.2. Proses Tanda Tangan Elektronik

Komunikasi Penandatanganan secara elektronik, pengirim terlebih dahulu akan menghasilkan intisari pesan dari pesan asli menggunakan jenis huruf yang dapat dilepas dengan menggunakan perangkat lunak. Setiap intisari pesan asli adalah unik, seperti "sidik jari", oleh karena itu perubahan terkecil dalam intisari pesan akan menghasilkan perubahan pada "sidik jari". Keuntungannya adalah Pengirim dan Penerima dapat memverifikasi integritas pesan. Kunci pribadi pengirim akan digunakan

DOI : 10.36499/psnst.v12i1.7010
e-ISSN: 2964-2531
p-ISSN: 2964-5131

untuk menandatangani intisari pesan, yang berarti bahwa tanda tangan elektronik adalah intisari pesan yang dienkripsi dengan kunci pribadi pengirim. Komentar asli dan tanda tangan elektronik kemudian diteruskan ke penerima yang dituju. Penerima dapat memecahkan kode tanda tangan elektronik, berkat kunci publik Pengirim, yang ditransmisikan terlebih dahulu ke penerima pesan. Penerima kemudian akan membuat intisari pesan pada pesan asli yang diterima. Tahap terakhir adalah membandingkan dan membedakan keduanya. Jika keduanya memiliki "sidik jari" yang sama, Anda tahu itu pesan asli yang belum diubah.



Gambar 2. Proses tanda tangan elektronik (Nugraha and Mahardika, 2016)

3.3. Perlunya Pengembangan Sistem Pengendalian Internal untuk Tanda Tangan Elektronik

Pemerintah daerah memerlukan beberapa bentuk pengendalian untuk mengatur kegiatan pemerintahan dan audit profesional tumbuh dari kebutuhan untuk melaksanakan *Good Governace* untuk mengatur perilaku yang membantu mereka menjalankan (Tajuddin, 2018). Dalam mengembangkan sistem pengendalian internal yang efektif untuk melengkapi pengendalian internal dengan tanda tangan elektronik, prinsip-prinsip dan tujuan pengendalian yang ditetapkan dalam Pengendalian Internal Kerangka Terintegrasi oleh COSO dapat diadopsi. COSO mendefinisikan pengendalian internal sebagai proses yang dipengaruhi oleh Dewan Direksi dan manajemen senior perusahaan. Pengendalian juga harus hemat biaya, oleh karena itu analisis biaya/manfaat harus dilakukan saat merancang dan mengevaluasi proses pengendalian meskipun tidak selalu mudah untuk mengukur manfaat dan mencocokkan pengendalian terbaik dengan risiko kerugian.

3.4. Model Masa Depan Tanda Tangan Elektronik

Masa depan tanda tangan elektronik atau tanda tangan elektronik disajikan secara singkat di bawah ini:

a. Kerahasiaan tanda tangan elektronik grup dijamin dengan menggunakan algoritma enkripsi kunci publik yang diusulkan.
b. Selama transaksi elektronik antara pemberi persetujuan dan penerima persetujuan, metode dan sistem *pool proof* akan ada dengan menampilkan kode unik di layar video elektronik untuk memverifikasi bahwa pemberi persetujuan masih hidup.
c. Skema tanda tangan elektronik baru akan diperkenalkan berdasarkan pemfaktoran dan logaritma diskrit untuk membuktikan keamanan tanda tangan elektronik.
d. Mempercepat operasi yang melibatkan tanda tangan elektronik, tanda tangan elektronik yang disempurnakan menggunakan representasi eksponen digit RNS akan dipasang sejalan dengan prosesor modern.
e. Kriptografi hibrida diadopsi untuk mengurangi overhead jaringan yang dibuat yang disebabkan oleh tanda tangan elektronik.
f. Penelitian berkelanjutan yang signifikan dilakukan di bidang tanda tangan elektronik kuantum (*Quantum digital signiture* (QDS) yang meminjam pendiriannya dari hukum-hukum penting fisika

kuantum. Kemajuan di bidang QDS menjanjikan untuk menghilangkan anggapan saluran kuantum yang diautentikasi meskipun tetap aman dari serangan kolektif.

4. KESIMPULAN

Penggunaan tanda tangan digital akan sangat efisien dalam proses pelaksanaan pemerintahan didaerah sebab tanda tangan elektronik dapat memverifikasi keaslian dokumen yang diterima. Selain itu penggunaan tanda tangan elektronik dapat mengurangi penggunaan kertas.

Penerapan tanda tangan elektronik harus dilengkapi dengan sistem pengendalian internal yang efektif. Pemerintah Daerah harus menyadari bahwa tanda tangan elektronik hanya membantu menjawab sebagian dari pengendalian internal yang diperlukan dalam lingkungan pemerintahan. Selain itu, tanda tangan elektronik tidak selalu berfungsi sebagaimana mestinya. Jika hal ini tidak dimitigasi dengan sistem pengendalian internal yang efektif, hal itu berpotensi mengakibatkan kerugian yang besar atau tindakan hukum terhadap pemerintah daerah.

DAFTAR PUSTAKA

Anwar, M. T. (2019) 'Model Blue Print Smart City Pemerintah Daerah Berbasis Four Stage Method (FSM) yang Sustainable', Jurnal Sistem Informasi Bisnis, 9(1), p. 63. doi: 10.21456/vol9iss1pp63-70.

Chong, K. W., Kim, Y. S. and Choi, J. (2021) 'A study of factors affecting intention to adopt a cloud-based digital signature service', Information (Switzerland), 12(2), pp. 1–15. doi: 10.3390/info12020060.

Digital, K. (2022) 'Keabsahan Digital Signature/Tanda tangan Elektronik Dinjau Dalam Perspektif Hukum Perdata dan UU ITE', Journal of Lex Generalis (JLS, 3(5), pp. 1082–1098.

Eka Putra, T. and Riswadi, R. (2022) 'Digital Signatures In the Minutes of Investigation By Investigators', MIC 2021 October 30, Jakarta, Indonesia, 1–9. doi: 10.4108/eai.30-10-2021.2315778.

Fitriani, R. and Muhammad, T. (2016) 'Desain Sistem Informasi Sekolah Berbasis Android', Matrik, 16(1), pp. 12–21.

Ida Bagus Gede Sarasvananda, I Putu Eka Giri Gunawan, I Komang Arya Ganda Wiguna , Made Suci Ariantini, and I. G. I. S. (2022) 'Pieces Analysis In The Influence Of The Designing', Jurnal Mantik Journal, 6(36), pp. 984–991.

Indonesia, P. R. (2016) Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik.

Lertxundi, A. and Landeta, J. (2022) 'The Impact of Digitalization On the Fundamental Rights of Public Employees in Spain', in Management Informational Conference (MIC) 2020, pp. 234–252.

Mataram, P. K. (2015) Perwal Nomor 20 Tahun 2015 Tentang Tata Naskah Dinas Di Lingkungan Pemerintah Kota Mataram. Mataram: Pemerintah Kota Mataram.

Mataram, P. K. (2018) 'Peraturan Walikota Mataram Nomor 30 Tahun 2018 Tentang Tata Kelola Penggunaan Sertifikat Elektronik Dilingkungan Pemerintah Kota Mataram'. Pemerintah Kota Mataram, pp. 1–15.

Muhammad Tajuddin, D. (2020) Peta Jalan Sistem Pemerintahan Berbasis Elektronik (SPBE) Kota Mataram 2021-2025.

Nawar, A.-H. (2011) 'E-Signature and the Digital Economy in Egypt', SSRN Electronic Journal, (November 2005). doi: 10.2139/ssrn.926584.

Nugraha, A. and Mahardika, A. (2016) 'Penerapan Tanda Tangan Elektronik Pada Sistem Elektronik Pemerintahan Guna Mendukung E-Government', Seminar Nasional Sistem Informasi Indonesia, pp. 359–364.

Ribeiro, R. C., De Almeida, M. G. and Canedo, E. D. (2021) 'A digital signature model using XAdES standard as a rest service', Information (Switzerland), 12(8). doi: 10.3390/info12080289.

Sardjono, W. et al. (2021) 'The use of digital signatures in the business world in the industrial revolution 4.0 era', ICIC Express Letters, Part B: Applications, 12(11), pp. 987–993. doi:

e-ISSN: 2964-2531
p-ISSN: 2964-5131

10.24507/icicelb.12.11.987.

Scîrtocea, L. (2022) 'Electronic Signature, Tool for Optimizing the Management of Information in Electronic Format', in STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment, pp. 101–107. doi: 10.53477/2668-6511-22-11.

Tajuddin, M. et al. (2013) 'Wireless-Based Integrated Information System between Private Higher Education Institutions and Local Government', International Journal of Science and Engineering Investigations (IJSEI), 2(15), pp. 58–63.

Tajuddin, M. (2018) 'Local Government Dimension Model in Building Information Technology Master Plan', International Journal of Science and Engineering Investigations, Vo, 7(77), pp. 44–54.

Velentzas, J. et al. (2022) 'Digital and advanced electronic signature: the security function, especially in electronic commerce', SHS Web of Conferences, 139, p. 03011. doi: 10.1051/shsconf/202213903011.

Zamrodah, Y. (2016) 'A Study of Electronic Signature and Its Legal Validity in Nigeria', Lawrit Student Journal of Law, 15(2), pp. 1–23.

Zhong, M. et al. (2022) 'China Pakistan Economic Corridor Digital Transformation', Frontiers in Psychology, 13(May), pp. 1–14. doi: 10.3389/fpsyg.2022.887848.

Zubov, V. V. (2020) 'An Electronic Signature Within The Digital Economy', in II International Scientific Conference GCPMED 2019. European Proceedings of Social and Behavioural Sciences EpSBS, pp. 621–625. doi: 10.15405/epsbs.2020.03.89.