TANDA TANGAN DIGITAL: OTORITAS PADA ARSIP ELEKTRONIK

Muhammad Usman Noor

Program Studi Manajemen Rekod dan Arsip, Program Pendidikan Vokasi, Universitas Indonesia
Email: usmannoor@ui.ac.id

Received : 06 October 2020
Revised : 08 May 2021
Accepted : 15 May 2021
DOI :

Abstract

The Covid19 pandemic has triggered more massive and extensive use of electronic records due to the Work from Home policy. One of the keys in using electronic records is a digital signature as an authorization stamp for the electronic record. The concept of authentic digital signature and integrity is still unfamiliar to policymakers, which can lead to legality problems in the future. Digital signatures have three levels of validity from basic, advanced, to high. Not all levels produce electronic records that have legal force, so it is necessary to handle with extra concern to their use of digital signature in institutions or organizations. This writing aims to provide an overview of the concept of a digital signature that is authentic, accountable, and integrity. This writing uses a qualitative method. The result of this writing is that the digital signature must go through encryption and verification so that the digital signature has legal force and what its implementation of digital signature in several countries, including Indonesia.

Keywords: Digital Signature, Electronic Records, Records Encryption

PENDAHULUAN

Pandemik dapat menimbulkan revolusi pada beberapa aspek kehidupan dan merubah tatatan kehidupan. Kondisi pandemik memaksa berbagai kalangan untuk berubah dan beradaptasi dengan kehidupan yang baru. Dunia kearsipan bisa jadi adalah satu dari beberapa sektor yang paling terdampak, hal ini disebabkan pandemik COVID-19 yang dideklarasikan oleh WHO pada tahun 2020 secara global memaksa para pelaku industri untuk menjalankan bisnisnya tidak lagi di kantor namun dilakukan dari rumah. Sehingga proses administrasi yang semula masih bisa dilakukan dengan menggunakan arsip konvensional, praktis menjadi tidak efisien apabila dilakukan dari rumah. Hal ini mendorong untuk pelaku bisnis menggunakan arsip digital secara lebih ekstensif dan masif. Namun masih menjadi pertanyaan bagi berbagai kalangan mengenai keautentikan dari arsip digital tersebut, penggunaan arsip digital yang tidak tepat justru akan menambah masalah legalitas di masa yang akan datang.

Autentisitas dan Integritas adalah hal prinsip dalam kearsipan. Arsip baru bisa kapabel bila memenuhi syarat autentisitas dan integritas. Semenjak meluasnya penggunaan

komputer dan kemunculan file digital, upaya memastikan keintegritasan dan autentisitas dari arsip digital menjadi tantangan tersendiri. Konsep daur hidup arsip sulit diterapkan pada arsip digital karena ketidakadaan material fisiknya lagi, sehingga konsep rekod kontinum dianggap lebih sesuai dan cocok dengan sifat dasar arsip digital(Almgren & Stengård, 2015). Pada rekod kontinuum dimana arsip terus berubah sesuai dengan penggunaannya. Perubahan konsep tersebut semakin menuntut kepastian dalam hal integritas dan autentisitas dari arsip tersebut.

Salah satu yang menjadi kunci dalam auntensitas arsip adalah authorship atau kewenangan dari arsip tersebut. Dalam konteks arsip konvensional, penandaan authorship digunakan melalui pembubuhan tanda tangan pada arsip tersebut. Tujuan tanda tangan adalah memberikan autentikasi bahwa arsip tersebut adalah benar dan memiliki tanggung jawab dan pelimpahan wewenang pada arsip tersebut. Luciana Duranti dan Corinne Roger(2012) menyimpulkan bahwa kepercayaan pada arsip berbasis pada empat jenis pengetahuan mengenai pencipta atau penanggungjawab berkaitan dengan jabatan, posisi, peran dari orang tersebutr antara lain: reputasi, berdasar pada rekam jejak dari wakil tersebut; performa, hubungan antara aksi yang dilakukan wakil sesuai dengan tanggungjawab yang diakui oleh pihak lainnya; kompetensi, terdiri dari kecakapan pengetahuan, keterampilan, dan sifat yang dibutuhkan untuk menyelesaikan tugas dia wakili; dan kepercayaan, adalah jaminan akan ekspektasi dari aksi oleh pihak yang memberi kepercayaan.

Konsep awal tanda tangan digital sudah dimulai ketika Ronald Rivest, Adi Shamir, dan Leonard Adleman mengembangkan sandi praktis untuk public-key yang dapat digunakan untuk keperluan kerahasiaan dan tanda tangan digital pada tahun 1977(Whitman & Mattord, 2016). Dokumen atau arsip digital dibutuhkan untuk mengautentikasi dokumen digital agar dapat dipertanggungjawabkan. Istilah Tanda Tangan digital mulai dikenal ketika penggunaan computer makin massif, namun dari penelusuran dokumen dikatakan bahwa penggunaan tanda tangan digital dimulai di tahun 1991(Bhatia & Wright de Hernandez, 2019). Dahulu tanda tangan digital seringkali disebut juga sebagai document timestamp(stempel waktu). Namun pada awal perkembangan tanda tangan digital masih sulit untuk membuktikan atau sebagai sarana auntentikasi karena belum dapat diverifikasi oleh pihak lain, karena keterbatasan teknologi dan jaringan. Kemudian konsep berkembang, menyebut bahwa tanda tangan digital adalah pesan yang terenkripsi yang dapat dibuktikan autentik secara matematis.

Kini penggunaan tanda tangan digital dibutuhkan agar system berbasis jaringan aman dari serangan siber, dan dapat menyediakan opsi pelimpahan wewenang dengan cara remote. Tanda Tangan digital dibutuhkan untuk penyediaan sertifikat untuk kebutuhan keamanan

dalam jaringan tersebut(Ustundag & Cevikcan, 2018). manajemen tanda tangan digital dapat digunakan pada hampir seluruh web browser. Namun yang menjadi perhatian adalah penggunaan tanda tangan harus diperhatikan secara jeli, karena tanda tangan digital memiliki beberapa tingkatan yang perlu diketahui. Hal ini sering luput bagi pemangku kebijakan yang memiliki kewenangan dalam implementasi tanda tangan digital di lingkup wewenangnya. Sehingga artikel ini mencoba menjelaskan konsep tanda tangan yang lazim berkembang di kalangan pemangku kepentingan, seperti apa konsep tanda tangan yang akuntabel, autentik dan integritas nya terjaga dan seperti apa implementasi tanda tangan digital di beberapa negara.

TINJAUAN LITERATUR

Tingkatan tanda tangan digital

Tanda tangan digital dapat dilihat dari beberapa tingkatan keabsahan. Secara umum dibagi menjadi beberapa tingkat tingkatan tanda tangan digital , yaitu simple atau dasar, advanced, dan qualified advanced. Jika dikupas lebih lanjut Badan electronic Identification, Authentication and trust Services regulation (eIDAS), membaginya menjadi Simple atau Basic electronic signature (SES), Advanced electronic or digital signature (AES), Qualified advanced electronic or digital signature (QES)(Connective, 2019).

Pada tanda tangan digital level basic atau dasar, Seluruh jenis tandatangan dalam bentuk digital dengan sertifikat jenis apapun. Tanda tangan digital yang simple adalah tanda tangan digital dalam bentuk paling sederhana karena tidak dilindungi dengan metode enkripsi apa pun(Privy, 2018). Contoh paling awam adalah tanda tangan basah yang dipindai oleh perangkat elektronik kemudian dimasukkan ke dalam dokumen. Termasuk juga diantaranya tandatangan yang secara manual ditulis dengan menggunakan mesin pembaca tertentu, hasil digitasi, dan persetujuan melalui klik tombol seperti “I ACCEPT” “Saya menyetujui” dan sejenisnya; Tanda tangan digital simple ini memiliki berbagai kelemahan. Tanda tangan ini tidak terenkripsi sehingga tidak mampu menunjukkan identitas penandatangan maupun perubahan yang terjadi pada dokumen setelah dokumen ditandatangani. Selain itu, tanda tangan digital kategori basic sangat mudah untuk digandakan atau dipalsukan.

Tingkat lanjutan, Pada level lanjutan ini tanda tangan harus memenuhi beberapa kebutuhan minimum yang memberikan tambahan keamanan untuk tujuan verifikasi, keamanan, dan segel(sebagai tandan bahwa ketika sudah diberi tandatangan dokumen tidak bisa diubah); Meski sudah menggunakan metode asymmetric cryptography, penyedia layanan

tanda tangan digital basic tidak melakukan proses verifikasi identitas penggunanya secara optimal. Proses penandatanganan juga tidak melalui 2-factor authentication. Akibatnya, dokumen yang ditandatangani dengan tanda tangan digital kategori ini masih belum memiliki kekuatan dan akibat hukum yang sah(Privy, 2018).

Tingkat Atas atau tingkat tertinggi tanda tangan digital dianggap memenuhi syarat dan tidak tertolak sebagai tanda tangan elektronik yang memiliki status legal yang sama dengan tandatangan basah. Tanggung jawab pada dokumen tersebut ada pada yang menandatangani. Pada tingkatan ini tanda tangan digital didukung oleh sertifikat yang dikeluarkan oleh jasa penyedia layanan terpercaya(qualified trust services provider (QTSP)) yang terdaftar atau ditunjuk secara consensus yang kemudian penyedia jasa ini memastikan bahwa tanda tangan tersebut memiliki kekuatan hukum yang sah dan diakui(Connective, 2019). Yang membuat penyedia layanan tanda tangan digital level ini lebih spesial adalah proses verifikasi identitas pengguna yang mereka terapkan. Bahkan, penyedia layanan tanda tangan digital advanced dan qualified diwajibkan untuk memberlakukan 2-factor authentication sebelum dokumen dapat ditandatangani penggunanya. Metode otentikasi yang digunakan pun beragam: mulai dari pengiriman one time passwordmelalui SMS, hingga pemindaian biometrik di telepon genggam. Proses verifikasi dan autentikasi yang ekstensif ini lah yang membuat dokumen yang ditandatangani dengan tanda tangan digital kategori ini sudah memiliki sertifikat elektronik yang melekat secara unik ke identitas si penandatangan(Privy, 2018).

Enkripsi pada Tanda Tangan Digital

Tanda tangan digital adalah hash-code terenkripsi yang dapat ditarik dan melekat pada informasi/arsip elektronik untuk keperluan autentikasi(Dumortier & Eynde, 2002). Enkripsi dan tanda tangan digital menegaskan hak seseorang di negara Amerika Serikat untuk menggunakan dan menjual produk yang didalamnya terdapat enkripsi dan melonggarkan kontrol untuk produk sejenis itu hal ini tertuang pada Security and Freedom Through Encryption Act of 1999.

Proses enkripsi asimetris telah digunakan untuk menciptakan tanda tangan digital. Ketika proses enkripsi asimetris menggunakan private key pengirim untuk mengenkripsi pesan, maka public key penerima harus digunakan untuk mendekripsi pesan tersebut. Dan ketika proses dekripsi berhasil maka proses tersebut adalah verifikasi bahwa pesan telah diterima dan tidak bisa disanggah. Proses tersebut disebut sebagai Anti

Penyangkalan(NonRepudiation), dan prinsip kriptografi dengan metode autentikasi tersebut dikenal sebagai tanda tangan digital(Whitman & Mattord, 2016).

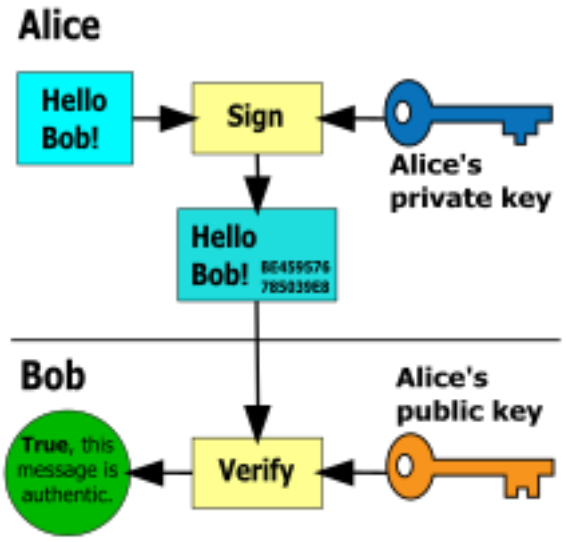
METODE

Penelitian ini menggunakan metode kualitatif dengan metode pengumpulan data melalui penelusuran bahan pustaka dalam pengumpulan data melalui metode partisipatori. Proses yang dilakukan dalam penelitian kali ini, pertama penulis melakukan studi literature mengenai tanda tangan digital yang digunakan secara luas di berbagai industri. Tahap berikutnya menghubungkan literature tersebut dengan pengalaman sebagai pengguna aplikasi persuratan yang sudah terintegrasi dengan sertifikat tanda tangan elektronik yang dikeluarkan BSSN sebagai acuan analisis dan implikasi pada praktik proses bisnis sehari-hari di lingkungan kerja. Tahap ketiga adalah menyusun data-data yang telah didapatkan. Dalam penelitian kali ini memiliki keterbatasan cakupan penelitian. Penulis hanya memiliki pengalaman menggunakan aplikasi persuratan yang telah terintegrasi dengan BSSN saja, sehingga terdapat kemungkinan ada informasi lebih yang didapat apabila menggunakan aplikasi yang terintegrasi dengan penyedia sertifikat tanda tangan elektronik pihak ketiga lainnya.

HASIL DAN PEMBAHASAN

Konsep Kerja Tanda Tangan Digital yang Terkualifikasi

Tanda tangan digital yang berkekuatan hukum setara dengan tanda tangan basah, apabila digunakan metode kriptografi hashing dan kriptografi asimetris private-to-public. Salah satu proses yang menguatkan tanda tangan digital adalah tanda tangan digital tersebut melalui proses hashing. Hashing berperan memastikan integritas suatu file, data, atau informasi berbasis digital. Sebagai contoh, pada sebuah file digital jika dijalankan fungsi hashnya maka akan diperoleh nilai tertentu yang menjadi wakil dari file tersebut. Apabila ada perubahan pada file digitalnya, sesedikit apapun, maka nilai hashnya akan berubah dari nilai hash aslinya. Sehingga dari nilai hash suatu file dapat dibuktikan integritasnya. Ini dapat digunakan pada Penciptaan tanda tangan, verifikasi data dengan menggunakan tanda tangan dan identifikasi penggelapan/penipuan dengan menggunakan tanda tangan(Drescher, 2017)



Gambar 1. Alur enkripsi

Sebagai contoh aplikasinya adalah seperti gambar diatas. Alice menandatangani pesan "Halo Bob" dengan melampirkan pada pesan aslinya sebuah versi terenkripsi dengan kunci privat. Bob menerima baik pesan dengan tanda tangannya. Dia menggunakan kunci public Alice untuk memverifikasi autentik pesan tersebut. Sebagai contoh, pesan tersebut terdeskripsi menggunakan kunci public, persis dengan pesan aslinya. Sehingga jika ada yang mencoba membuka pesan tanpa memiliki kunci yang tepat hanya akan mendapati data yang tidak beraturan/acak.

Verifikasi Tanda Tangan Digital

Metode DSS(Digital Signature Standard) adalah metode verifikasi tanda tangan digital. Secara umum pembuatan dan penggunaan tanda tangan digital harus berdasarkan pada Standar tanda tangan digital (Digital Signature Standard(DSS)). Khususnya di Amerika Serikat, dimana tanda tangan yang diakui adalah tanda tangan yang telah tersertifikasi dan sesuai dengan standar DSS. DSS ini tidak hanya digunakan di Amerika Serikat saja namun telah diakui dan digunakan oleh banyak negara. Sehingga dapat menjadi salah satu acuan global untuk standar tanda tangan digital. Algoritma DSS dapat digunakan sebagai penghubung antara kunci public dan privat pengirim pesan, kunci public penerima pesan, dan standar pengaman hash (Secure Hash Standard) untuk menciptakan pesan yang terenkripsi dan anti penyangkalan dengan cepat(Whitman & Mattord, 2016).

Digital Forensik

Digital Forensik adalah proses mempresentasikan bukti digital pada persidangan. Memastikan autentisitas dari barang bukti digital yang dibuktikan dengan otoritas yang berkompeten dan ditunjuk. Pada digital forensic, beberapa hal yang dapat mempengaruhi kekuatan bukti digital antara lain melalui metadata mengenai (1)kapan tanggal dan waktu pasti dokumen dikirim dan diterima, (2) computer mana yang menjadi tempat penciptaan dokumen tersebut, dan (3) computer mana yang menerima dokumen tersebut(Duranti & Rogers, 2012). Digital forensik memberikan deklarasi oleh ahlinya berdasar pada keterpercayaan pada system rekod dan prosedur pengawasannya baik secara system maupun Teknik pada dokumen digital tersebut. Ahli digital forensic harus memastikan rekod tersebut berasal dari system yang berfungsi baik, bebas dari kemungkinan manipulasi tanpa sepengetahuan system baik yang disengaja maupun tidak disengaja.

Implementasi Tanda Tangan Digital di Berbagai Negara

Estonia menyatakan dirinya sebagai negara pertama yang menggunakan tanda tangan digital lebih dahulu ketimbang dengan negara di uni Eropa lainnya dalam hal implementasi tanda tangan digital. Estonia menyebut tanda tangan digital sebagai e-identity. Mereka mengklaim bahwa 98% dari warga negaranya sudah memiliki tanda tangan digital yang kemudian digunakan untuk berbagai layanan sipil seperti id Card, Kartu jaminan kesehatan nasional, paspor, transaksi perbankan, rekam medik, dan e-voting.

Pada beberapa negara, salah satunya negara Uni Eropa, menyatakan dapat menerima tanda tangan digital dengan tingkat terkualifikasi yang berbasis pada Public Key Infrastructure sebagai syarat tanda tangan tersebut dapat dijadikan bukti autentik. Tanda tangan digital dan *public key infrastructure(*PKI) adalah contoh teknologi yang dikembangkan dan diimplementasikan untuk keperluan autentikasi arsip elektronik yang terdistribusi. Perlu diperhatikan bahwa meskipun arsiparis, atau public menaruh kepercayaan pada system autentikasi tersebug namun teknologi PKI dan tanda tangan digital tidak ditujukan, dan sanggup untuk menjadi system auntetikasi yang dapat diandalkan dalam waktu yang lama ke depannya(Dumortier & Eynde, 2002). Hal tersebut sangat mungkin terjadi perubahan teknologi, keusangan teknologi dan ketidaksesuaian format.

Pada kondisi hukum Eropa terkini, menunjukkan bahwa hanya tanda tangan digital yang berbasis PKI yang dianggap sebagai tanda tangan digital yang memenuhi kualifikasi. Teknik tanda tangan digital memungkinkan autentikasi informasi elektronik dengan informasi aslinya, dengan demikian integritas isi arsip tersebut dapat diverifikasi. Tanda

tangan digital adalah kode hash yang terenkripsi hasil turunan dan menempel pada informasi elektronik yang dapat diautentikasi(Dumortier & Eynde, 2002).

Praktik pemanfaatan tanda tangan digital di Indonesia

Penerapan di Indonesia, pihak ketiga yang memiliki otoritas untuk mengeluarkan tanda tangan digital adalah BSE(Balai Sertifikasi Elektronik) yang berada di bawah Badan Siber dan Sandi Negara(BSSN). Hal ini diinstruksikan presiden melalui Perpres Nomor 53 Tahun 2017. BSSN mempunyai tugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber. Salah satu lingkup tugasnya adalah menerbitkan dan mengelola tanda tangan elektronik bersertifikat.

Pemanfaatan tanda tangan digital di Indonesia belum menjangkau sector bisnis dan pelayanan public di seluruh Indonesia. Umumnya masih terpusat pada industry yang menjadi pelopor dalam implementasi digital seperti dunia perbankan. Di dunia birokrasi penggunaan tanda tangan digital mulai banyak digunakan secara ekstensif di tahun 2020 ketika terjadi pandemi, fenomena tersebut mendorong implementasi penggunaan tanda tangan digital lebih luas dan segera. Namun, penulis melihat implementasi tanda tangan digital di Indonesia tidak melulu bicara soal kesiapan teknologinya, namun lebih pada pemahaman stakeholder terkait seperti apa tanda tangan digital yang legal dan sah. Masih terdapat pemangku kepentingan atau pelaku bisnis yang menganggap tanda tangan digital hanya sebatas pembubuhan gambar tanda tangan ke dalam dokumen digital dengan kata lain tanda tangan digital pada tingkat basic. Stakeholder yang memahami akan pentingnya penggunaan tanda tangan digital pada tingkat lanjutan atau yang membutuhkan enkripsi, umumnya akan menggandeng Lembaga atau badan verifikator tanda tangan digital, dalam hal ini di Indonesia adalah BSSN. Pemahaman akan tanda tangan digital yang awam akan berujung pada masalah legal.

Manfaat Praktis Tanda Tangan Digital pada Proses Administrasi

Kemudahan proses kerjasama antara dua belah pihak. Sebagai contoh pada masa pandemik meniadakan kemungkinan untuk melakukan proses bisnis yang lazimnnya dilakukan, seperti salah satunya pengurangan tatap muka, berkumpul dalam jumlah besar, dan pembatasan pergerakan. Hal ini kemudian menimbulkan kantor harus menjalankan bisnisnya dari rumah atau secara remote. Penggunaan tanda tangan digital akan sangat

membantu proses legal ketika dibutuhkan kerjasama antara dua belah pihak, komunikasi kerjasama cukup terjadi melalui surat elektronik dan tetap berkekuatan hukum yang sah. Selama tanda tangan digital yang digunakan sudah memenuhi standar dan diatur dalam regulasi yang berlaku.

Penggunaan tanda tangan elektronik sudah mulai diterapkan di Universitas Indonesia, tempat penulis bekerja, dengan menggunakan bantuan sistem informasi kearsipan persuratan bernama ANDIENI tidak hanya untuk mendistribusi surat atau disposisi namun sudah bisa menghasilkan arsip elektronik yang bertanda tangan digital. Tanda tangan digital yang digunakan sudah terverifikasi oleh BSRE(Balai Sertifikasi Elektronik) sehingga sudah memiliki kekuatan hukum yang sah. Namun penggunaan tanda tangan digital ini baru dapat digunakan di nota dinas atau surat dinas, belum dapat digunakan ke semua jenis arsip. Ke depan penggunaan tanda tangan digital dapat membantu beberapa hal seperti, Penyingkatan waktu kerja bagi pemangku jabatan untuk pekerjaan penandatangan hal yang repetitive. Misal, penandatanganan ijazah mahasiswa oleh rector, rector mengalokasikan waktu khusus untuk menandatangani ribuan lembar ijazah lulusannya. Dengan penggunaan tanda tangan digital, maka proses tanda tangan bisa dikerjakan secara simultan dan tidak memerlukan waktu yang banyak. Sehingga waktu kerja dapat dialokasikan pada kegiatan strategis lainnya.

Percepatan perizinan di masyarakat, tidak bergantung keberadaan fisik pemangku jabatannya. Beberapa daerah di Indonesia sudah mulai mengeluarkan dokumen pencatatan sipil seperti Kartu Keluarga dengan tanda tangan digital, salah satunya adalah Provinsi Jawa Barat. Masyarakat dapat dengan sendiri melakukan pencetakan kartu keluarga di rumah dengan standar pencetakan tertentu, kartu keluarga yang diberikan sudah dibubuhi tanda tangan elektronik bersertifikat dan dapat diproses dengan menggunakan teknologi informasi.

PENUTUP

Implementasi tanda tangan digital yang tepat dapat membawa banyak benefit bagi organisasi, namun hal tersebut baru akan sesuai dan akuntabel apabila tanda tangan digital yang digunakan memang sudah terverifikasi dan sesuai dengan konsep auntentisitas arsip. Di sisi lain pemangku kepentingan yang belum memahami konsep tanda tangan digital yang akuntabel akan membawa dampak legal yang dapat merugikan dan membahayakan jalannya organisasi, karena sangat rentan penyalahgunaan tanda tangan. Keputusan pemanfaatan pengunaan tanda tangan digital tidak dapat dengan enteng diambil, namun perlu kesiapan

dan jaminan kepastian hukum. Sehingga pemahaman akan konsep dasar tanda tangan elektronik seperti penggunaan enkripsi, hashing, dan sertifikasi tanda tangan digital akan menghindarkan masalah legal yang dapat ditimbulkan karena penggunaan tanda tangan digital yang tidak sesuai dengan konsep auntentisitas dan integritas.

DAFTAR PUSTAKA

Almgren, H., & Stengård, M. (2015). How to maintain Authenticity and Integrity of Electronic Information without Utilizing Electronic Certificates. *INFUTURE*, 441–442. https://doi.org/10.17234/infuture.2015.45

Bhatia, S., & Wright de Hernandez, A. D. (2019). Blockchain Is Already Here. What Does That Mean for Records Management and Archives? *Journal of Archival Organization*, *16*(1), 75–84. https://doi.org/10.1080/15332748.2019.1655614

Connective. (2019). Three types of Electronic Signatures and how to choose the right type for your transactions. Retrieved February 1, 2020, from https://connective.eu/three-types-of-electronic-signatures/

Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Apress.

Dumortier, J., & Eynde, S. Van Den. (2002). Electronic Signatures and Trusted Archival Services. *DLMForum 2002*, (July), 520–524. https://doi.org/10.1.1.122.1484

Duranti, L., & Rogers, C. (2012). Trust in digital records: An increasingly cloudy legal area. *Computer Law and Security Review*, *28*(5), 522–531. https://doi.org/10.1016/j.clsr.2012.07.009

Privy. (2018). Kenali 3 Jenis Tanda Tangan Digital. Retrieved February 10, 2020, from https://blog.privy.id/3-jenis-tanda-tangan-digital/

Ustundag, A., & Cevikcan, E. (2018). *Industry 4.0: Managing The Digital Transformation*. (D. T. Pham, Ed.). Cham: Springer. https://doi.org/10.1007/978-3-319-57870-5

Whitman, M. E., & Mattord, H. J. (2016). *Principles of Information Security* (5th ed.). Cengage Learning. https://doi.org/10.1016/b978-0-12-381972-7.00002-6