PENERAPAN TANDA TANGAN ELEKTRONIK PADA SISTEM ELEKTRONIK PEMERINTAHAN GUNA MENDUKUNG *E-GOVERNMENT*

Agung Nugraha[1)], Agus Mahardika [2)]
Lembaga Sandi Negara
Jl. Harsono RM No 70 Ragunan, Jakarta Selatan 12550
Telp. (021) 7805814 Fax (021) 78844104
agha.nugraha@lemsaneg.go.id[1)], agus.mahardika@lemsaneg.go.id[2]

Abstrak

Instansi pemerintah di Indonesia telah menerapkan e-government dengan membangun sistem elektronik pemerintahan untuk membantu pelaksanaan tugas dan fungsi instansi. Akan tetapi, penggunaan dokumen pada sistem elektronik tidak diringi dengan penggunaan tanda tangan elektronik yang tersertifikasi. Hal ini dapat menjadi celah keamanan karena konten dokumen elektronik dapat dengan mudah dirubah dan penerima tidak dapat melakukan verifikasi terhadap keaslian dokumen. Oleh karena itu, paper ini membahas mengenai penggunaan tanda tangan elektronik pada dokumen atau persuratan dalam pemerintahan untuk mempermudah proses birokrasi.

Kata kunci: *tanda tangan elektronik, dokumen elektronik, e-government*

Abstract

Indonesian government have implemented e-government by build electronic system to assist the implementation of the tasks and functions of the agency. However, the use of documents in the electronic system does not lacks the use of digital signature. This can become a vulnerability because the content of document can be easily changed and the recipent cannot verify the integrity of document. Therefore, this paper discusses the use of digital signature on goverment documents to simplify the bureaucratic process.

Keywords: *electronic signature, electronic document, e-government*

1. PENDAHULUAN

Kemajuan teknologi dan informasi yang tumbuh dengan pesat serta potensi pemanfaatannya membuka peluang bagi pengaksesan, pengelolaan dan pendayagunaan informasi secara cepat dan akurat. Pemanfaatan teknologi dan informasi dalam proses pemerintahan (*e-government*) akan meningkatkan efisiensi, efektifitas, transparansi dan akuntabilitas penyelenggaraan pemerintahan. Pengembangan *e-government* merupakan upaya untuk mengembangkan penyelenggaraan kepemerintahan berbasis elektronik guna meningkatkan kualitas pelayanan publik secara efektif dan efisien. Pengembangan *e-government* dapat dilakukan pada penataan sistem manajemen dan proses kerja di lingkungan pemerintah dengan mengoptimasikan pemanfaatan teknologi informasi. Pemanfaatan teknologi informasi tersebut mencakup 2 (dua) aktivitas yang berkaitan yaitu :

1) pengolahan data, pengelolaan informasi, sistem manajemen dan proses kerja secara elektronis;
2) pemanfaatan kemajuan teknologi informasi agar pelayanan publik dapat diakses secara mudah dan murah oleh masyarakat di seluruh wilayah negara[6].

Dalam penyelenggaraan pemerintahan, birokrasi menjadi alur yang digunakan dalam mengkoordinasikan tugas dan diskusi untuk menghasilkan kebijakan dan keputusan. Akan tetapi, birokrasi selalu dijadikan sebagai alasan terlambatnya keputusan dalam sebuah kebijakan. Oleh karena itu, diperlukan metode dan cara yang lebih efektif dan efisien pada proses birokrasi namun tidak mengurangi faktor akuntabilitas terhadap perubahan dokumen yang terjadi, yaitu dengan menggunakan tanda tangan elektronik pada dokumen atau persuratan dalam pemerintahan.

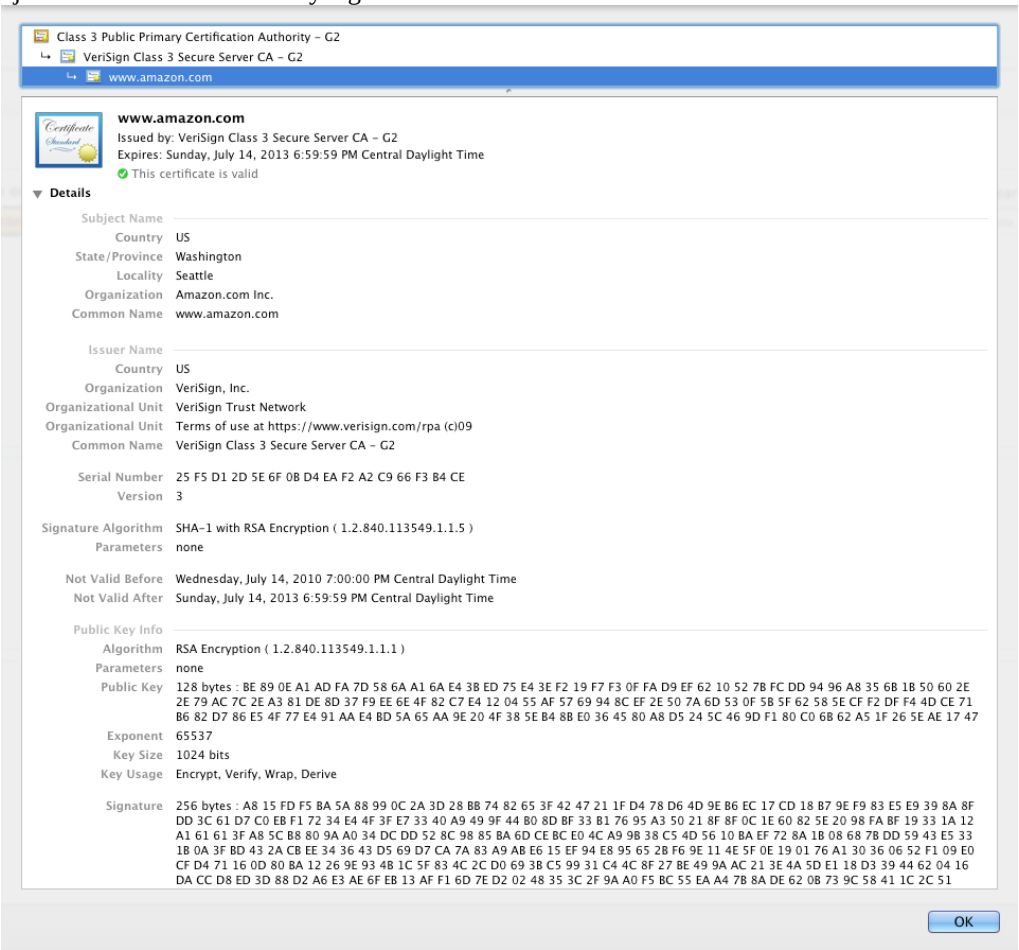
Proses kerja tanda tangan elektronik secara elektronis adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi[7]. Tanda tangan elektronis berbeda dengan tanda tangan yang dipindai kemudian ditempelkan ke dalam dokumen elektronik. Tanda tangan elektronik yang tersertifikasi atau tanda tangan digital berbentuk rangkaian data yang ditambahkan ke dalam dokumen elektronik menggunakan perhitungan matematika. Untuk memeriksa sebuah tanda tangan elektronik harus dilakukan secara elektronik pula. Dalam penerapannya, tanda tangan elektronik bersifat unik. Tanda tangan seseorang akan berbeda dengan tanda tangan orang lain. Sama seperti tanda tangan manual, tanda tangan ini harus dijaga oleh masing-masing personal agar tidak disalahgunakan oleh pihak yang tidak berwenang. Dengan menerapkan tanda tangan elektronik yang tersertifikasi, pemerintah telah melaksanakan dua dari enam tujuan strategis *e-government*, yakni poin b. menata sistem manajemen dan proses kerja pemerintah dan pemerintah daerah otonom secara holistik, serta poin c. memanfaatkan teknologi secara optimal[6].

2. LANDASAN TEORI

Pada penelitian ini, ada berbagai literatur yang menjadi landasan teori penulis dalam melakukan penelitian, literatur tersebut terdiri dari berbagai buku ilmu pengetahuan dan makalah-makalah yang sesuai dengan penelitian. Berikut ini adalah beberapa literatur utama yang menjadi landasan teori penulis :

2.1 Sertifikat Elektronik

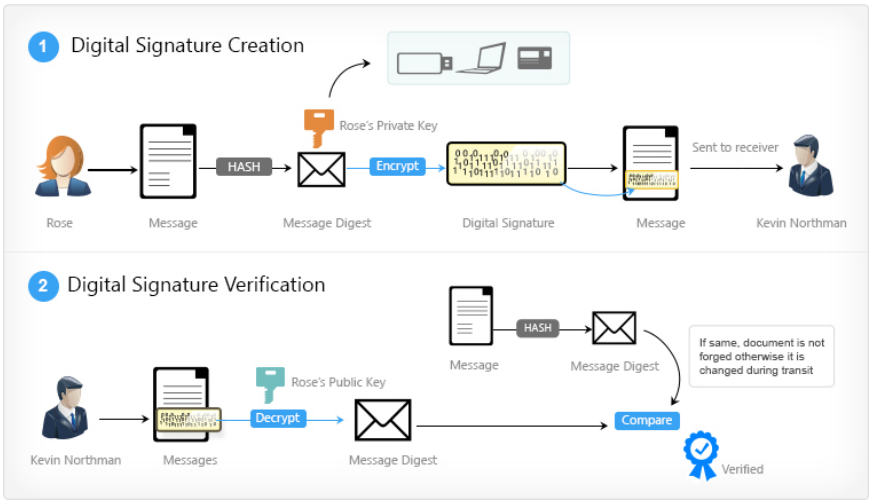
Sertifikat digital memiliki peranan penting dalam pembangkitan *digital signature*. Dalam sertifikat digital terdapat info publik key dan info pemilik publik key. Info-info tersebut dimasukkan ke dalam informasi *siganture* pada dokumen elektronik yang ditandatangani. Melalui info signature tersebut maka penerima dapat memastikan identitas dari pemberi tanda tangan elektronik. Setiap sertifikat elektronik dibangkitkan oleh *Certification Authority* (CA). CA adalah badan yang memiliki kewenangan dalam melakukan manajemen sertifikat elektronik seperti penerbitan, pencabutan dan pembaharuan[2]. Gambar 1 menunjukkan sertifikat elektronik yang telah diterbitkan oleh CA.



Gambar 1. Sertifikat elektronik

2.2 Tanda Tangan Elektronik

Tanda tangan elektronik atau *digital signature* merupakan kombinasi dari fungsi *hash* dan enkripsi dengan metode asimetrik[4]. Untuk membangkitan sebuah *digital signature*, dokumen elektronik akan dijadikan sebagai input pada fungsi *hash* dan akan menghasilkan nilai *hash* yang unik. Fungsi *hash* merupakan fungsi satu arah dan akan menghasilkan nilai unik untuk setiap data yang dimasukkan[3]. Oleh karena itu, jika ada perubahan satu bit saja pada konten dokumen maka nilai *hash* yang dihasilkan akan berbeda. Nilai *hash* kemudian di enkripsi menggunakan *private key* untuk selanjutnya nilai dari hasil enkripsi tersebut adalah nilai *signature* dari suatu dokumen. *Signature* kemudian ditambahkan dengan dokumen. Proses verifikasi dilakukan dengan melakukan dekripsi *signature* dokumen. Hasil dekripsi tersebut akan menghasilkan nilai *hash* untuk selanjutnya dibandingkan dengan nilai *hash* dari dokumen yang dibangkitkan oleh penerima dokumen. Jika nilai *hash* sama, maka dokumen yang diterima adalah asli. Sebaliknya jika nilai *hash* yang dibandingkan tidak sama, maka dapat dipastikan bahwa dokumen mengalami perubahan oleh pihak yang tidak berhak. Gambar 2 menunjukkan proses pembangkitan *digital signature* dan proses verifikasi.



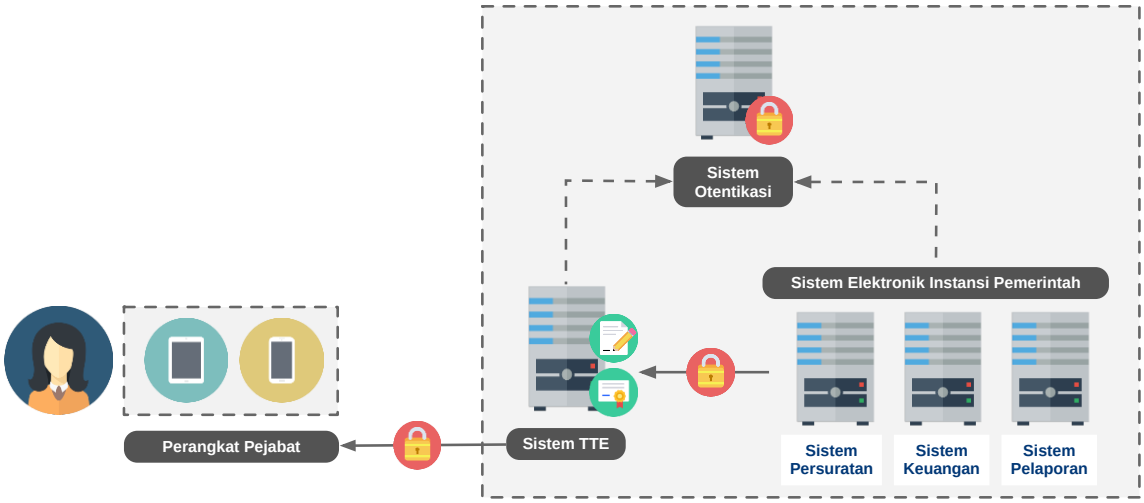
Gambar 2. Tanda Tangan Elektronik

3. TANDA TANGAN ELEKTRONIK PADA SISTEM PEMERINTAHAN

3.1 Arsitektur Sistem

Sistem yang dibangun terdiri dari *client* dan server dimana server berfungsi untuk memberikan layanan penerbitan dan permintaan tanda tangan elektronik, sedangkan *client* berfungsi sebagai perangkat yang melakukan proses tanda tangan elektronik. Setiap sistem elektronik instansi yang membutuhkan persetujuan atau tanda tangan elektronik dari pejabat yang terkait akan mengirimkan dokumen elektronik kepada sistem Tanda Tangan Elektronik (TTE). Sistem TTE kemudian akan mengirimkan notifikasi ke perangkat yang digunakan oleh pejabat yang bersangkutan dan pejabat tersebut dapat menandatangani secara elektronik dokumen yang telah diterima. Gambar 3 menunjukkan gambaran umum sistem yang dibangun.

Sistem TTE dibuat secara terpisah dengan sistem elektronik instansi pemerintah dengan tujuan memudahkan tahapan implementasi. Melalui desain sistem yang diajukan, layanan tanda tangan elektronik dapat digunakan secara bersama tanpa perlu melakukan pengembangan kembali sistem TTE baru untuk setiap sistem elektronik instansi pemerintah yang menerapkan tanda tangan elektronik. Sistem TTE menggunakan sistem otentikasi milik sistem elektronik instansi pemerintah sehingga pejabat tidak perlu melakukan registrasi kembali untuk menggunakan layanan sistem TTE.



Gambar 3. Gambaran Umum Sistem

3.2 Keamanan

Keamanan pada sistem di implementasikan dengan menggunakan protokol dan algoritma kriptografi. Melalui protokol kriptografi, setiap transaksi data antara *client* dan server akan dienkripsi terlebih dahulu sebelum dikirimkan dan hanya pengguna yang terdaftar saja yang dapat menggunakan sistem. Berikut ini merupakan protokol yang digunakan untuk pengamanan sistem.

3.2.1 OAuth

OAuth (*Open Authorization*) merupakan protokol otentikasi yang memungkinkan aplikasi pihak ketiga mendapatkan akses kepada layanan terbatas atau terproteksi yang disediakan dengan persetujuan pemilik layanan. Terdapat empat metode otorisasi pada OAuth yaitu *authorization code, implicit, resource owner password credential* dan *client credential* [5]. Pada sistem ini, metode otorisasi yang digunakan adalah *resource owner password credential* dan *client credential*.

a) *Resource owner password credential*

Metode ini digunakan pada komunikasi antara perangkat pengguna dengan sistem TTE dimana setiap pengguna atau pejabat harus memasukkan pasangan username dan password yang telah terdaftar pada sistem. Selain parameter username dan password, terdapat juga parameter *client_id* dan *client_secret*. Kedua parameter tersebut diberikan kepada aplikasi *client* sehingga hanya aplikasi yang terdaftar saja yang dapat menggunakan API dari sistem TTE. Jika pengguna berhasil di otentikasi, maka sistem TTE akan mengirimkan *session token* kepada aplikasi pengguna untuk digunakan pada setiap *service* yang akan diakses.

b) C*lient credential*

Metode ini digunakan pada komunikasi antara sistem instansi dengan sistem TTE dimana sistem instansi. Sistem elektronik instansi pemerintah harus didaftarkan pada sistem TTE untuk dapat diotentikasi oleh sistem TTE. *Output* dari sesi otentikasi tersebut adalah *session token* yang dapat digunakan oleh sistem instansi dalam menyampaikan permintaan persetujuan dokumen kepada pejabat yang terkait.

3.2.2 *Secure Socket Layer* (SSL)

Setiap transaksi data pada sistem diamankan dengan menggunakan protokol SSL dimana data akan dienkripsi terlebih dahulu sebelum dikirimkan. Protokol SSL diimplementasikan menggunakan SSL versi 3 untuk menghindari adanya celah keamanan pada SSL versi sebelumnya[1].

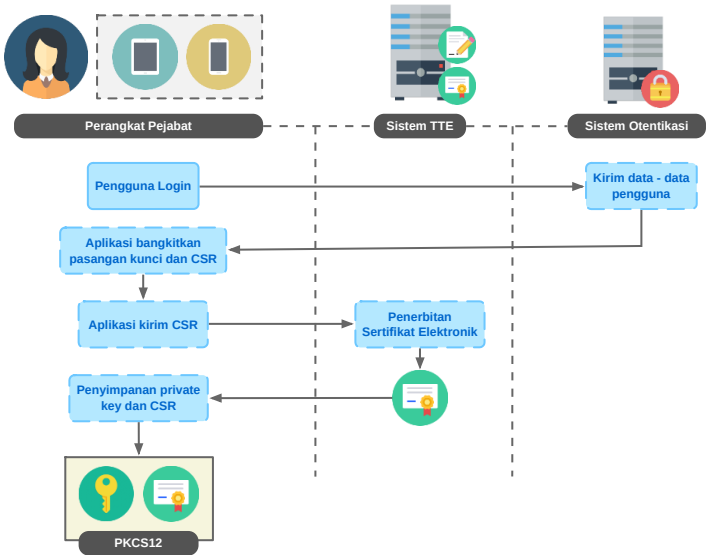
3.3 Penerapan

Penerapan tanda tangan elektronik pada sistem elektronik instansi pemerintah terdiri dari dua tahapan yaitu permohonan sertifikat elektronik dan persetujuan dokumen elektronik.

3.3.1 Permohonan Sertifikat Elektronik

Tanda tangan elektronik pada dokumen elektronik dapat dilakukan jika pengguna dalam hal ini pejabat memiliki *private key* dan sertifikat elektronik. Oleh karena itu, pengguna harus melakukan permohonan permintaan sertifikat elektronik terlebih dahulu kepada sistem TTE. Sistem TTE menggunakan database otentikasi pada sistem elektronik instansi pemerintah sehingga setiap pengguna yang sudah terdaftar dapat

melakukan permohonan sertifikat elektronik. Gambar 4 menunjukkan alur permintaan sertifikat elektronik

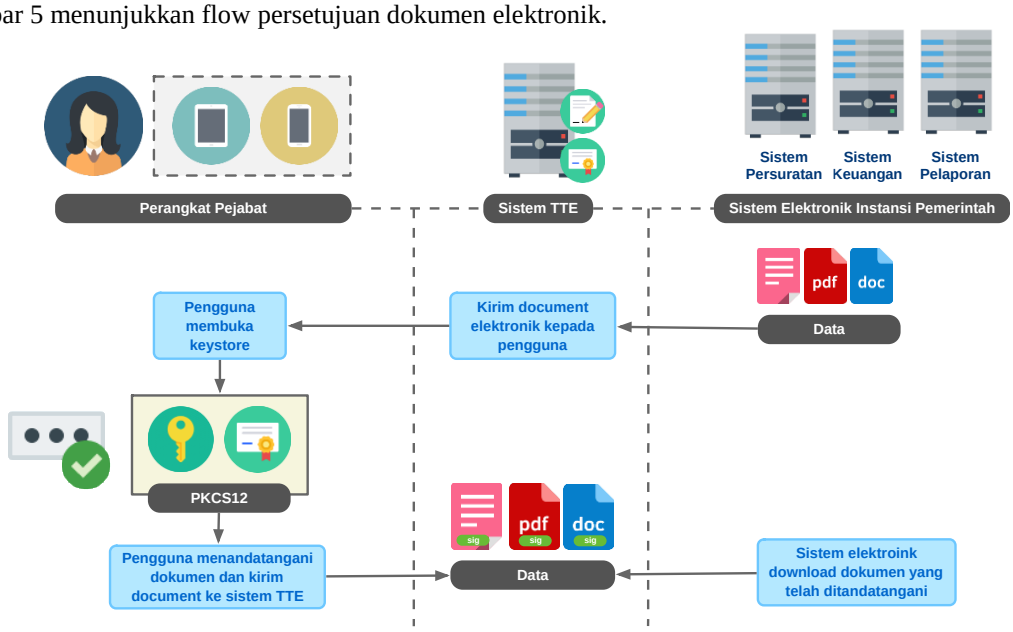


Gambar 4. Alur Permintaan Sertifikat Elektronik

Pada tahap permohonan permintaan sertifikat elektronik, pengguna akan melakukan login pada aplikasi *client* untuk mendapatkan data-data terkait pengguna. Data-data tersebut akan digunakan oleh aplikasi *client* dalam pembangkitan pasangan kunci privat dan publik serta *Certificate Signing Request* (CSR). CSR dikirimkan kepada sistem TTE untuk selanjutnya menjadi parameter *Certification Authority* (CA) dalam penerbitan sertifikat elektronik. Sertifikat elektronik yang telah diterbitkan kemudian akan disimpan bersama *private key* dalam format PKCS12 pada aplikasi *client*.

3.3.2 Persetujuan Dokumen Elektronik

Tahap persetujuan dokumen elektronik dilakukan dengan memberikan tanda tangan elektronik pada dokumen oleh pejabat tertinggi yang berwenang. Sebelum pejabat melakukan persetujuan terhadap dokumen elektronik, *staff* akan membuat konsep dokumen terlebih dahulu melalui sistem elektronik instansi pemerintah dan mengirimkan konsep tersebut sesuai alur birokrasi yang terdapat pada instansi. Setelah semua pejabat seperti kepala bidang atau kepala sub bagian yang berkaitan melakukan paraf pada konsep dokumen, maka sistem elektronik akan mengirimkan konsep dokumen kepada pejabat tertinggi untuk di tanda tangani secara elektronik. Tanda tangan elektronik dilakukan pada aplikasi *mobile* pejabat dengan menggunakan *private key* dan sertifikat elektronik yang telah didapatkan pada tahap sebelumnya. Gambar 5 menunjukkan flow persetujuan dokumen elektronik.



Gambar 5. Alur Persetujuan Dokumen Elektronik

Setiap dokumen elektronik yang memerlukan persetujuan dari pejabat akan dikirimkan kepada sistem TTE oleh sistem elektronik instansi pemerintah. Parameter yang dikirimkan adalah dokumen elektronik dan daftar pejabat yang berhak melakukan persetujuan pada dokumen elektronik. Sistem TTE selanjutnya akan mengirimkan notifikasi kepada pejabat bahwa terdapat dokumen yang perlu dilakukan persetujuan. Selanjutnya pengguna melakukan download dan persetujuan dokumen dengan menandatangani dokumen secara elektronik. Jika semua pihak telah menandatangani dokumen elektronik, maka dokumen dikirimkan kembali kepada sistem elektronik instansi pemerintah melalui sistem TTE.

4. SIMPULAN DAN SARAN

Penerapan tanda tangan elektronik perlu diimplementasikan pada dokumen elektronik pemerintahan karena dapat menyediakan proses verifikasi terhadap keaslian dokumen yang diterima. Akan tetapi, penerapan tanda tangan elektronik menjadi masalah baru karena saat ini instansi pemerintah telah memiliki sistem untuk tata naskah dinas elektronik sehingga membutuhkan strategi implementasi yang tepat. Desain sistem pada makalah ini telah memperhatikan aspek kompleksitas implementasi, keamanan dan kesesuaian proses bisnis tata naskah dinas sehingga diharapkan dapat menjadi solusi bagi intansi pemerintah dalam melakukan penerapan tanda tangan elektronik. Terdapat beberapa manfaat yang didapatkan oleh instansi pemerintah dalam implementasi tanda tangan elektronik sebagai berikut :

a) Keaslian dokumen elektronik dapat diverifikasi
   Dokumen elektronik dapat dengan mudah dimodifikasi dan dipalsukan. Dengan adanya tanda tangan elektronik, setiap terdapat perubahan maka nilai *hash* yang dihasilkan juga akan berbeda sehingga jika terdapat perubahan oleh pihak yang tidak berhak maka penerima dokumen dapat mengetahui perubahan tersebut.
b) Mengurangi waktu permohonan persetujuan
   Setiap pejabat dapat melakukan persetujuan dimanapun dan kapanpun karena dokumen elektronik dikirimkan langsung oleh sistem ke perangkat pejabat. Oleh karena itu, jika pejabat yang berwenang tidak berada di kantor atau sedang melakukan perjalanan dinas di luar kantor maka proses persetujuan masih tetap dapat dilakukan. Persetujuan yang dilakukan secara *real time* tersebut dapat mengurangi waktu yang dibutuhkan untuk persetujuan dibandingkang dengan waktu yang dibutuhkan pada persetujuan secara manual.
c) Mengurangi penggunaan kertas.
   Proses koordinasi penyusunan dokumen dilaksanakan secata elektronis,sehingga tidak perlu mencetak dokumen ketika ada perubahan. Pencetakan dokumen cukup dilaksanakan satu kali ketika dokumen telah selesai disahkan.

Penerapan tanda tangan elektronik pada instansi pemerintah tidak selalu dapat berjalan dengan baik. Hal in dikarenakan terdapat kendala – kendala sebagai berikut :

a) Adanya keraguan dari para pejabat untuk menjalankan penerapan dokumen secara elektronik.
b) Adanya *mindset* penerapan tanda tangan elektronik yang sulit bagi para pimpinan.
c) Perlunya penyesuaian budaya nota dinas berbasis kertas menjadi nota dinas elektronik (*paperless*).

Oleh karena itu, penulis mengharapkan pada penelitian selanjutnya dapat dikembangkan mengenai identifikasi dan strategi yang tepat dari sisi kebijakan dan sosialisasi secara menyeluruh kepada masyarakat terkait tanda tangan elektronik.

5. DAFTAR PUSTAKA

[1] Aviram, Nimrod, et.al, 2016. *DROWN : Breaking TLS using SSLv2*. Proceedings of the 25th USENIX Security Symposium.

[2] Hook, David. 2005. *Beginnning Cryptography with Java.* Canada : Wiley Publishing.

[3] Menezes, J. Alfred, Van Ooschot, C. Paul, Vanstone dan A.Scott A,. 1996. *Handbook of Applied Cryptography*, Boca Raton: CRC press LLC.

[4] Schneier, Bruce. 1996. *Applied Cryptography, Second Edition : Protocols, Algorithm, and Source Code in C*. Oak Park : John Wiley & Sons, Inc.

[5] *The OAuth 2.0 Authorization Protocol draft-ietf-oauth-v2-18.* 2011. Sumber : http://www.potaroo.net/ ietf/old-ids/ draft-ietf-oauth-v2-18.pdf. Akses terakhir pada tanggal 31 Juli 2016.

[6] Presiden Republik Indonesia, Megawati Soekarnoputri. 9 Juni 2003. Instruksi Presiden Republik Indonesia Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-Government*.

[7] Presiden Republik Indonesia, Dr. H. Susilo Bambang Yudhoyono. 21 April 2008. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008.