SISTEM PENGELOLAAN DOKUMEN ELEKTRONIK UNTUK DIGITALISASI PADA LAYANAN PUBLIK

Agung Nugraha
Badan Siber dan Sandi Negara
Jl. Harsono RM No 70 Ragunan, Jakarta Selatan 12550
Email: agha.nugraha@bssn.go.id

ABSTRAK

Digitalisasi terhadap data dan dokumen masyarakat di Indonesia belum dilakukan sepenuhnya sehingga pemanfaatan data digital untuk layanan publik belum dilaksanakan secara maksimal. Sebagai contoh, masyarakat masih harus melakukan input data secara manual dan menyerahkan fotokopi dokumen asli sehingga dapat menjadi permasalahan terkait lamanya waktu untuk pengisian data secara manual, pengelolaan dan keaslian dokumen fisik. Akan tetapi ketika digitalisasi dilakukan, terdapat permasalahan keamanan seperti integritas data (integrity), nir penyangkalan (non repudiation), otentikasi (authentication) dan kerahasiaan (confidentiality). Oleh karena itu, penulis membuat sebuah sistem yang dapat digunakan untuk pengelolaan data dan dokumen digital secara terpusat bagi masyarakat. Berdasarkan hasil penelitian, sistem yang diajukan dapat memberikan keamanan terhadap data dan dokumen digital dan dapat diintegrasikan dengan layanan publik elektronik.

Kata kunci: tanda tangan elektronik, dokumen, layanan publik, digitalisasi

ABSTRACT

Digitalization of citizens data and documents in Indonesia has not been fully implemented so that the use of digital data for public services has not been carried out to the fullest. For example, people still have to input data manually and submit copies of the original documents so that it can become an issue for the length of time for manually filling data, the management, and authenticity of physical documents. However, when digitizing is done, there are security issues such as data integrity, non-repudiation, authentication, and confidentiality. Therefore, we make a system that can be used for centrally managing digital data and documents for the citizen. The proposed system can provide security for digital data and documents and can be integrated with electronic public services.

Kata kunci: *digital signature, documents, public services, digitalization*

1. PENDAHULUAN

Saat ini penggunaan internet di Indonesia berkembang sangat pesat dimana pada tahun 2018 jumlah pengguna internet di Indonesia mencapai 171,17 juta pengguna[1]. Hal ini memicu munculnya bisnis – bisnis baru di layanan berbasis internet seperti Gojek, Lazada, Ruang Guru, Midtrans dan masih banyak lagi. Perkembangan layanan berbasis internet tersebut tidak hanya pada sektor bisnis saja, akan tetapi berdampak juga pada sektor pemerintahan seperti pembuatan SIM, Paspor, Perbankan dan layanan publik lainya. Layanan tersebut dinilai dapat memberikan pelayanan yang lebih baik kepada masyarakat dikarenakan dapat diakses secara cepat, mudah, dimanapun dan kapanpun. Dalam pelaksanaannya, layanan publik berbasis elektronik masih membutuhkan dokumen fisik seperti Kartu Keluarga, Akta Lahir, Ijazah dan dokumen pribadi lainnya yang digunakan sebagai syarat penggunaan layanan. Di sisi lain, saat ini penggunaan tanda tangan elektronik untuk dokumen digital sudah populer karena memiliki aspek keamanan sehingga dokumen tidak dapat dipalsukan. Tanda tangan elektronik sendiri sudah dijamin oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan PP Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dimana tanda tangan elektronik telah diakui dan memiliki kedudukan hukum yang sama dengan tanda tangan manual. Berdasarkan hal tersebut, maka penggunaan dokumen fisik pada layanan publik

ISSN 1410-7228 (Versi Cetak)
ISSN 2716-4233 (Versi Elektronik)

elektronik sudah dapat digantikan dengan dokumen digital yang telah ditandatangani secara elektronik. Akan tetapi, penggunaan dokumen digital pada sistem elektronik tentunya menimbulkan permasalahan baru terutama terkait pengelolaan dan keamanannya. Oleh karena itu, pada paper ini penulis mengajukan sebuah sistem yang dapat digunakan oleh masyarakat untuk pengelolaan dokumen digital secara terpusat dan aman

2. METODE PENELITIAN

2.1 Tanda Tangan Elektronik

Tanda tangan elektronik menurut PP Nomor 82 Tahun 2012 adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Tanda tangan elektronik terdiri dari tanda tangan elektronik yang tersertifikasi dan tanda tangan elektronik yang tidak tersertifikasi. Pada paper ini, digunakan tanda tangan elektronik yang tersertifikasi dimana dalam pembuatannya melibatkan sertifikat elektronik. Dalam ilmu kriptografi, tanda tangan elektronik tersertifikasi adalah tanda tangan digital (*digital signature*). *Digital signature* merupakan kombinasi dari fungsi hash dan enkripsi dengan metode asimetrik[11]. Untuk membangkitan sebuah *digital signature,* dokumen elektronik akan dijadikan sebagai input pada fungsi hash dan akan menghasilkan nilai hash yang unik. Nilai hash tersebut kemudian dienkripsi menggunakan *private key* dan menghasilkan nilai *signature*. Dari s*ignature* tersebut kemudian dilakukan verifikasi untuk mengetahui keaslian dari dokumen.

2.2 Infrastruktur Kunci Publik

Infrastruktur Kunci Publik (IKP) adalah sebuah *framework* yang terdiri dari *hardware, software,* kebijakan dan prosedur, untuk melakukan manajemen kunci dan sertifikat[7]. Kunci yang digunakan pada algoritma kunci publik terdiri dari kunci privat dan kunci publik yang berpasangan. Dalam penerapannya, terkendala dalam otentikasi kepemilikan kunci publik, sehingga dibutuhkan pihak ketiga terpercaya *(Trusted Third Party)* untuk membantu menjamin identitas dari para pihak pelaku transaksi elektronik melalui IKP dan menyediakan mekanisme untuk melakukan transaksi elektronik secara aman. IKP banyak digunakan oleh bank, pemerintah atau perusahaan swasta lainnya untuk pengamanan dalam proses bisnis yang *confidential*. Hal tersebut dikarenakan IKP dapat memberikan aspek keamanan *confidentiality*, *authentication* dan *non- repudiation* yang dikombinasikan dengan fungsi Hash untuk memberikan aspek *integrity* [10]. Menurut Choudhury, terdapat lima komponen untuk mendukung penyelenggaraan PKI yang terdiri dari *Certification Authority (CA), Registration Authority (RA), PKI Clients, Digital Certificates* dan *Certificate Distribution Systems or Repository* [3].

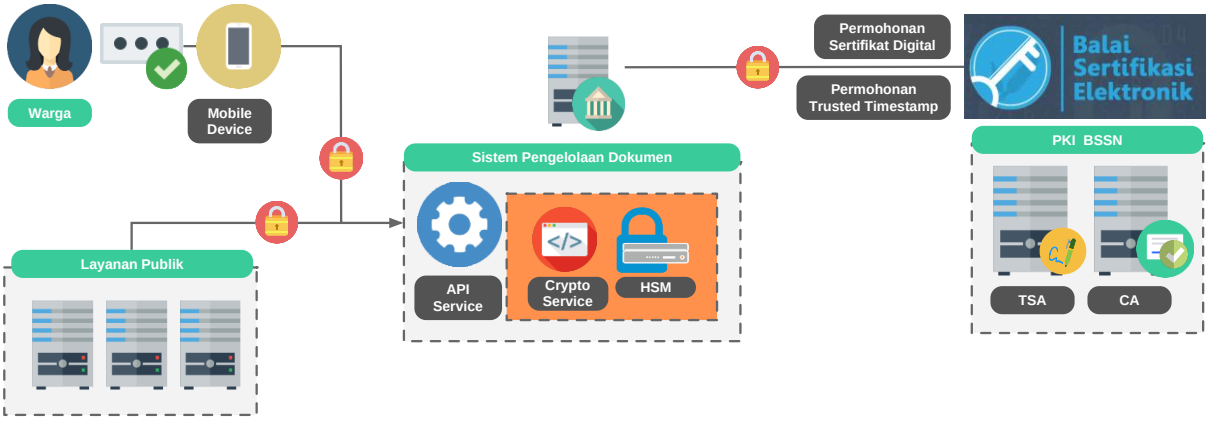
3. HASIL DAN PEMBAHASAN

Sistem yang diajukan oleh penulis merupakan sistem pengelolaan dokumen digital yang terpusat dan dapat dijadikan sebagai platform pengelolaan dokumen oleh masyarakat di Indonesia. Melalui sistem ini, masyarakat dapat menyimpan data dan dokumen pribadi secara digital dan layanan publik di Indonesia dapat menggunakan data tersebut untuk keperluan pelayanan bagi masyarakat.

3.1 Arsitektur Sistem

Infrastruktur yang diajukan terdiri dari aplikasi client dan server dimana dimana aplikasi server berfungsi untuk menyimpan data dan dokumen digital masyarakat dan menyediakan *service* yang dapat digunakan oleh layanan publik di Indonesia. Sedangkan aplikasi client digunakan oleh warga yang selanjutnya disebut pengguna sebagai *interface* untuk melakukan penyimpanan data dan dokumen serta memberikan persetujuan penggunaan data kepada layanan publik. Pada infrastruktur server, digunakan beberapa perangkat keamanan untuk melakukan fungsi kriptografi dan sistem yang berada di *Public Key Infrastructure (PKI)* milik Badan Siber dan Sandi Negara (BSSN) untuk permohonan penerbitan

sertifikat digital dan permohonan *trusted timestamp*. Desain infrastuktur server ditunjukkan pada gambar 1.



Gambar 1. Infrastruktur Sistem

Berdasarkan gambar 1, perangkat keamanan dan sistem yang digunakan adalah sebagai berikut :

1) Sistem Pengelolaan Dokumen
   - *API Service*
     Merupakan web service yang digunakan untuk komunikasi antara aplikasi *mobile*, sistem pengelolaan dokumen dan Layanan Publik. Aplikasi *mobile* akan melakukan pendaftaran, penyimpanan data dan persetujuan pengiriman data melalui *web service* tersebut. Begitu juga dengan layanan publik akan menggunakan *web service* yang telah disediakan untuk melakukan permintaan data.
   - *Crypto Service*
     Merupakan komponen *software* yang digunakan sebagai interface untuk melakukan akses ke HSM dalam proses pembangkitan digital signature dan pembangkitan pasangan kunci pengguna.
   - *Hardware Security Module*
     Merupakan komponen hardware yang digunakan untuk proses kriptografi. Semua proses *signing* dilakukan di HSM secara aman sehingga dapat menghindari adanya keterbatasan dari sisi *software*.
2) PKI BSrE, BSSN
   PKI merupakan infrastruktur kunci publik yang digunakan untuk pengelolaan sertifikat digital. Saat ini BSSN telah memiliki BSrE yang berfungsi sebagai institusi negara yang berhak menerbitkan sertifikat digital bagi pengguna. Dalam layanannya, BSrE memiliki TSA untuk menerbitkan *trusted timestamp* dan CA untuk pengelolaan sertifikat digital.
   - *TimeStamp Authority* (TSA)
     Merupakan entitas yang membangkitkan *trusted timestamp*. *Trusted timestamp* digunakan sebagai salah satu komponen yang diletakkan pada *signature object* dan menjadi bagian dari parameter verifikasi.
   - *Certification Authority* (CA)
     Merupakan entitas yang mengelola sertifikat digital pengguna yang meliputi penerbitan, pencabutan dan pembaharuan. Sertifikat digital digunakan untuk proses penandatanganan data dan dokumen.
3) Entitas Pengguna
   Entitas pengguna terdiri dari *mobile device* dan layanan publik. Pengguna diberikan aplikasi berbasis *mobile* karena dinilai lebih memiliki mobilitas yang tinggi sehingga pengguna dapat melakukan proses penandatanganan, pengisian data dan *upload* dokumen dimanapun dan kapanpun. Sedangkan layanan publik merupakan entitas yang menggunakan data dan dokumen digital masyarakat

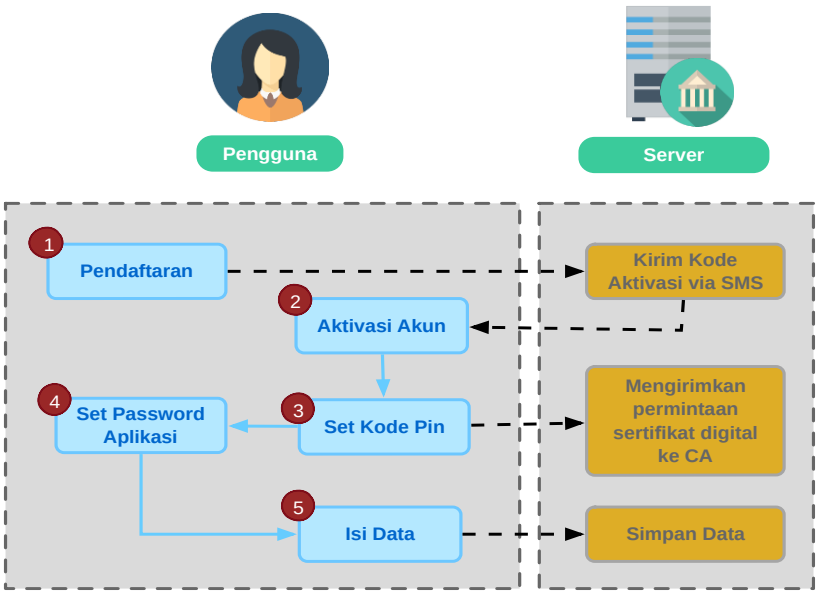
3.2 Proses Bisnis

ISSN 1410-7228 (Versi Cetak)
ISSN 2716-4233 (Versi Elektronik)

Proses bisnis yang terdapat pada sistem terdiri dari pendaftaran pengguna, pengisian data oleh pengguna dan permintaan data oleh layanan publik.

3.2.1 Pendaftaran dan Pengisian Data Pengguna

Untuk menggunakan sistem ini, pengguna harus melakukan pendaftaran terlebih dahulu melalui aplikasi *mobile*. Pendaftaran dilakukan dengan tujuan untuk melakukan verifikasi akun pengguna dan pendaftaran sertifikat digital. Tahapan pendaftaran ditunjukkan pada gambar 2

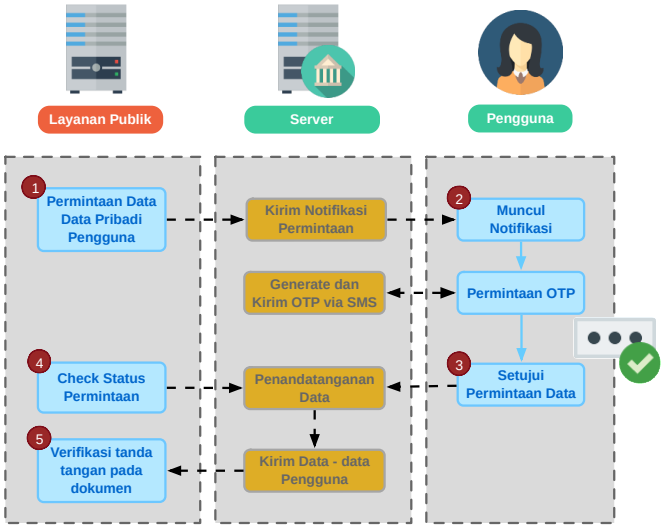


Gambar 2. Pendaftaran dan Pengisian Data Pengguna

Pada proses pendaftaran, pengguna akan diminta melakukan input Nomor Induk Kependudukan (NIK), alamat email dan nomor telepon. Setelah pendaftaran, server akan mengirimkan kode aktivasi melalui sms ke perangkat *mobile* pengguna. Jika aktivasi berhasil maka pengguna akan diminta melakukan input 6 digit kode pin yang nantinya digunakan sebagai *seed* untuk pembangkitan passphrase. Passphrase digunakan untuk proses penandatanganan data dan dokumen digital. Kemudian pengguna akan diminta melakukan input password untuk pengamanan aplikasi sehingga jika aplikasi dalam keadaan *sleep* maka pengguna akan diminta memasukkan password sebelum aplikasi dapat digunakan. Pada tahap ini proses pendaftaran selesai, selanjutnya pengguna sudah dapat menggunakan aplikasi dan melakukan input data – data pribadi. Input data pribadi dilakukan pengguna dengan terlebih dahulu memilih jenis data yang akan dimasukkan.

3.2.2 Penggunaan Data

Data yang sudah disimpan oleh pengguna dapat digunakan oleh beberapa layanan publik sesuai kebutuhan. Proses penggunaan data digital dimulai dari permintaan data oleh layanan publik sesuai kebutuhan untuk selanjutnya permintaan tersebut akan disetujui oleh pengguna. Gambar 3 menunjukkan tahapan penggunaan data.



Gambar 3. Alur Persetujuan Dokumen Elektronik

Penjelasan tahapan penggunaan data oleh layanan publik adalah sebagai berikut :

1) Layanan publik melakukan permohonan data – data pribadi sesuai dengan format yang telah ditentukan
2) Pengguna mendapatkan notifikasi bahwa terdapat layanan publik yang ingin melakukan permintaan data – data pribadi.
3) Selanjutnya pengguna memberikan persetujuan dengan melakukan input 6 digit kode pin milik pengguna dan *one time password* (otp) yang dikirim melalui sms. Di sisi server, data – data pribadi yang akan dikirimkan kepada layanan publik di tandatangani menggunakan *private key* pengguna.
4) Layanan publik melakukan pemeriksaan status permintaan data – data pribadi. Jika permintaan sudah disetujui oleh pengguna, maka data pribadi yang telah di *sign* dikirimkan kepada layanan publik untuk digunakan sebagaimana mestinya.
5) Sebelum data digunakan, layanan publik akan melakukan verifikasi terlebih dahulu melalui tanda tangan yang terdapat pada dokumen.

3.3 Keamanan

Keamanan pada sistem di implementasikan dengan menggunakan protokol dan algoritma kriptografi. Berikut ini merupakan teknik pengamanan yang digunakan.

3.3.1 Web Service

Web Service digunakan sebagai sarana komunikasi antara Layanan Publik, Sistem Pengelolaan Dokumen dan aplikasi pengguna. Web service perlu diamankan sehingga dapat dipastikan bahwa hanya entitas yang berhak saja yang dapat melakukan akses. Adapun pengamanannya adalah sebagai berikut.

a) Otentikasi

Otentikasi web service yang digunakan adalah protokol 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[14]. Sesi otentikasi dibangun ketika entitas pengguna baik itu aplikasi pengguna maupun layanan publik meminta *access token* dengan mengirimkan terlebih dahulu *client_id*, *client_secret*, *username* dan *password*. Jika kredensial yang dikirimkan sesuai, maka *access token* akan diberikan kepada entitas. Access token ini kemudian digunakan sebagai kode otorisasi oleh entitas pengguna untuk melakukan akses terhadap *web service* yang telah disediakan.

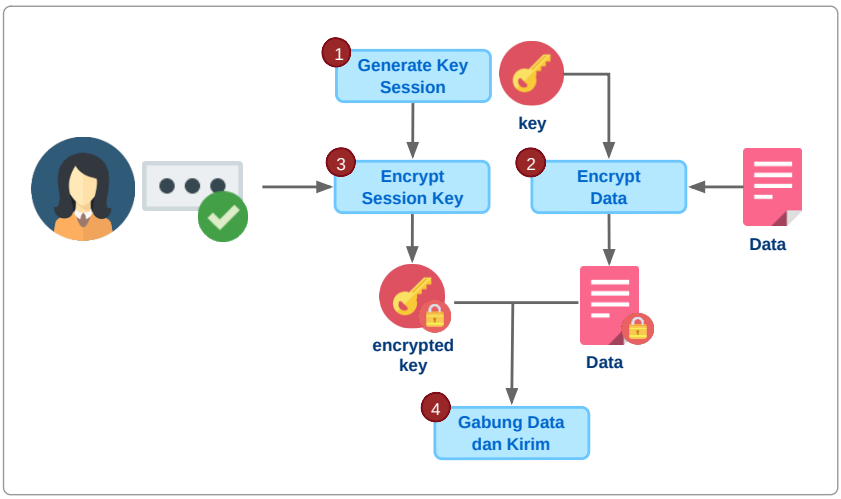
ISSN 1410-7228 (Versi Cetak)
ISSN 2716-4233 (Versi Elektronik)

b) 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[2].

3.3.2 Data

Pengamanan data dilakukan dengan menerapkan konsep *cryptography as a service* untuk proses Tanda Tangan Elektronik dan *end to end encryption* untuk enkripsi data. Melalui konsep tersebut, proses Tanda Tangan Elektronik dilakukan secara aman pada *Hardware Security Module* menggunakan kunci pengguna. Kunci didapatkan melalui kode pin yang dimasukkan oleh pengguna pada tahap pengisian data pribadi dan persetujuan. Sedangkan proses enkripsi dokumen dilakukan secara langsung oleh pengguna pada perangkat *mobile.*

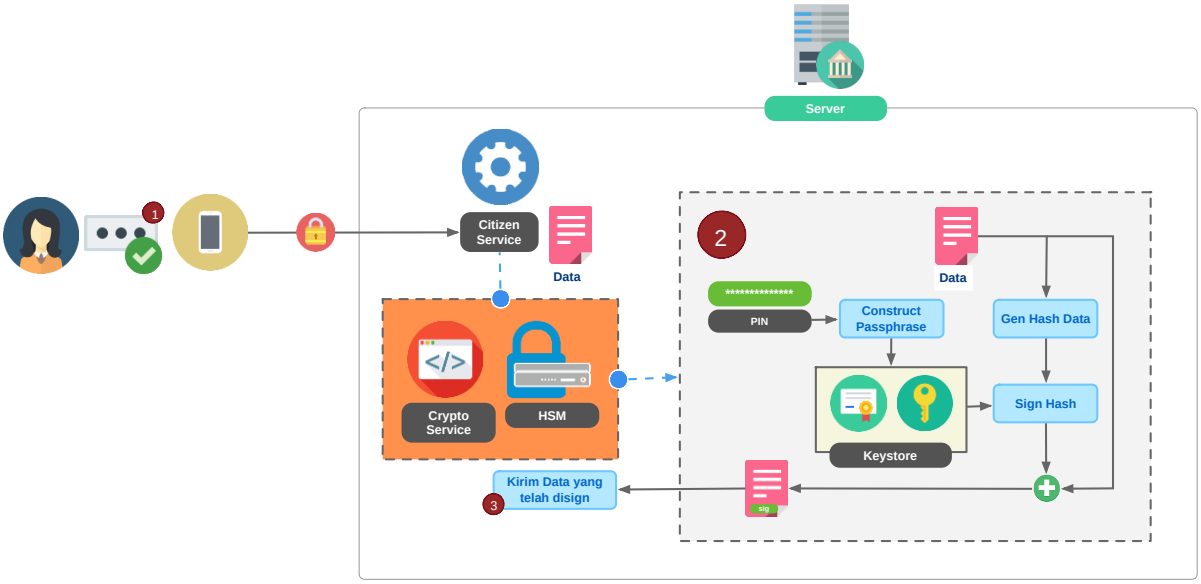
a) Enkripsi Data
Pada proses bisnis, terdapat tahapan pengisian data pengguna dimana pengguna melakukan upload data pribadi beserta dokumen pendukung. Pada tahapan tersebut, terdapat proses enkripsi data dengan menggunakan kunci sesi yang dibangkitkan oleh pengguna. Proses enkripsi dilakukan sebelum tahapan upload data seperti ditunjukkan pada gambar 4



Gambar 4. Proses enkripsi data dan dokumen

Adapun penjelasan proses enkripsi data dan dokumen yang diterapkan adalah sebagai berikut :
1) Pembangkitan kunci sesi. Kunci sesi dibangkitkan setiap kali akan melakukan enkripsi pada data / dokumen sehingga setiap file dienkripsi menggunakan kunci sesi yang berbeda.
2) Kunci sesi yang telah dibangkitkan kemudian dijadikan sebagai inputan pada proses enkripsi data dan dokumen. Algoritma yang digunakan adalah AES 256 mode CTR.
3) Kunci sesi kemudian dienkripsi menggunakan kode pin dan hasilnya ditambahkan dengan file yang terenkprisi
4) *Encrypted file* beserta *encrypted key* dikirimkan ke Server.

b) Tanda Tangan Elektronik
Tanda Tangan Elektronik dilakukan pada semua data dan dokumen yang akan dikirimkan kepada layanan publik. Proses Tanda Tangan Elektronik ditunjukkan pada gambar 5.



Gambar 5. Proses Tanda Tangan Elektronik

Adapun penjelasan proses Tanda Tangan Elektronik yang akan diterapkan adalah sebagai berikut :

1) Pengguna memasukkan 6 digit kode pin melalui aplikasi *mobile* sebagai akses bagi *Crypto Service* untuk membuka *private key* yang berada pada HSM
2) *Crypto Service* melakukan proses signing data dan dokumen pada HSM. Proses signing dilakukan dengan membangkitkan nilai hash, membangkitkan nilai *signature* dari nilai hash kemudian melakukan *packing* nilai *signature* dengan data asli.
3) Server mengirimkan data dan dokumen yang telah disign kepada layanan publik

3.4 Pengujian

Pengujian yang dilakukan pada system adalah *fungtional test*, Static Application Security Testing (SAST) dan Dynamic Application Security Testing (DAST). Dari hasil pengujian fungsi menunjukkan bahwa system berjalan sesuai dengan yang diharapkan. Selain itu, hasil pengujian SAST dan DAST menghasilkan nilai 80% yang menunjukkan bahwa system aman untuk digunakan.

4. KESIMPULAN

Kebutuhan akan data digital masyarakat yang terpusat, aman dan valid dapat dijawab melalui desain sistem yang diajukan oleh penulis. Masyarakat dapat menyimpan data dan dokumen digital melalui aplikasi *mobile* dan layanan publik juga dapat memanfaatkan data tersebut sesuai dengan otorisasi yang diberikan oleh pemilik data. Sistem yang diajukan juga telah memenuhi aspek keamanan yang terdiri dari jaminan keaslian (*integrity*), anti sangkal (*non - repudiation*), otentikasi (*authentication*) dan keamanan data (*confidentiality*). Adapun saran untuk penelitian selanjutnya adalah sebagai berikut :

1. *Stress Testing.* Test ini dilakukan untuk mengetahui sejauh mana aplikasi atau system dapat menampung banyaknya *request* dalam satuan detik. Hal ini juga untuk menjamin bahwa sistem selalu dapat tersedia sehingga dapat meminimalisir ancaman serangan *Denial of Service (DOS)* yang dilakukan dengan tujuan untuk membuat sistem menjadi tidak dapat diakses.
2. Penggunaan teknologi *container*. Penerapan teknologi *container* untuk membangun system yang telah didesain pada paper ini. Teknologi *container* dapat memudahkan pemeliharaan dan meningkatkan ketersediaan system karena memiliki kelebihan *auto healing* dan *auto scaling*.

DAFTAR PUSTAKA

[1] APJII. 2018. *Penetrasi dan Perilaku Pengguna Internet Indonesia*. Jakarta
[2] Aviram, Nimrod, et.al, 2016. *DROWN : Breaking TLS using SSLv2*. Proceedings of the 25th USENIX Security Symposium.
[3] Choudhury, Suranjan; Bhatnagar, Kartik;& Haque, Wasim. 2002. Public Key Infrastructure Implementation and Design. New York : M&T Books.
[4] *Digital Signature in a PDF*. Adobe Acrobat. Sumber : https://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf. Akses Terakhir pada 8 Agustus 2019.
[5] Hook, David. 2005. *Beginnning Cryptography with Java.* Canada : Wiley Publishing.
[6] *Internet X.509 Public Key Infrastructure – Certificate and CRL Profile. IETF Request for Comments* (RFC) 2459. Sumber : http://www.ietf.org/rfc/rfc2459.txt .Akses Terakhir pada 8 Agustus 2019.
[7] Inoerawan, F. Abraham; Ali, Narang Tia. 2011. Desain Protokol Kriptografi Untuk Pengamanan Dokumen Pada Lelang Elektronik. Paper dipresentasikan pada Konferensi Nasional Sistem dan Informatika 2011. Jakarta : Lembaga Sandi Negara.
[8] Lembaga Sandi Negara. 2007.Jelajah Kriptologi. Jakarta : Lembaga Sandi Negara.
[9] Kuhn D.Richard, C.Hu Vincent, Polk W.Timothy, Chang Shu-Jen, Introduction to Public Key Technology and the Federal PKI Infrastructure , NIST, 2001
[10] Menezes, J. Alfred, Van Ooschot, C. Paul, Vanstone dan A.Scott A,. 1996. *Handbook of Applied Cryptography*, Boca Raton: CRC press LLC.
[11] Research Data Management Team. 2013. *Checksum Exercise*, UK Data Archive : University of Essex.
[12] *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 8 Juni 2017.
[13] Presiden Republik Indonesia, Dr. H. Susilo Bambang Yudhoyono. 21 April 2008. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008.