Jurnal Infosecure Vol.2 No.2, Oktober 2021
p-ISSN: 2087-1023
MTI-UNLA

Metode Otentikasi Menggunakan Sertifikat Elektronik Pada Aplikasi Administrasi Pemerintahan

Studi Kasus : Aplikasi Dashboard Executive Pemerintah Kota Cimahi

Hadiyanto

Program Studi Magister Teknik Informatika, Universitas Langlangbuana

hadiyantokenaz@gmail.com

Abstrak— Aplikasi administrasi pemerintah banyak menggunakan *paltform* berbasis web yang diakses secara publik sehingga rentan terhadap serangan keamanan yang salah satunya serangan dari sisi otentikasi. Salah satu aplikasi yang digunakan di Pemerintah Kota Cimahi yang mengandung informasi sensitif dan penting adalah aplikasi Dashboard Executive yang diakses melalui jaringan publik dan digunakan oleh pimpinan instansi beserta jajarannya. Untuk mengamankan aplikasi tersebut dengan tidak menyulitkan pimpinan perlu penerapan metode otentikasi berbasis sertifikat elektronik yang diterbitkan oleh Balai Sertifikat Elektronik (BSrE) Badan Siber dan Sandi Negara (BSSN). Pemilihan sertifikat elektronik ini didasarkan pada pertimbangan pengguna aplikasi Dashboard Executive merupakan pejabat pemerintah yang sesuai kebijakan Pemerintah Kota Cimahi harus memiliki sertifikat elektronik yang diterbitkan oleh BSrE sehingga semua pejabat di Pemerintah Kota Cimahi termasuk pimpinan selaku pengguna aplikasi Dashboard Executive memiliki sertifikat elektronik. Untuk lebih meningkatkan keamanan terutama dari kehilangan perangkat yang terinstal sertifikat elektronik perlu kombinasi faktor otentikasi lain yang memudahkan seperti One Time Password (OTP).

Kata kunci— Otentikasi, sertifikat elektronik, Dashboard Executive, BSrE, Certification Authority

I. PENDAHULUAN

Dalam rangka transparansi manajemen badan publik khususnya Pemerintahan Daerah, Pemerintah Pusat telah mengeluarkan Undang-undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik yang memberikan kewajiban kepada Badan Publik untuk meningkatkan perencanaan dan pengelolaan serta pelayanan informasi, serta membuka akses atas Informasi Publik. Di samping itu, untuk meningkatkan pelayanan publik melalui pemanfaatan teknologi informasi dan komunikasi telah terbit Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). Peraturan Presiden ini salah satunya mengatur tentang aplikasi SPBE yang terdiri dari aplikasi administrasi pemerintahan dan aplikasi layanan publik untuk mendukung proses bisnis dalam meningkatkan kinerja administrasi pemerintahan dan layanan publik.

Pengembangan aplikasi SPBE tersebut banyak menggunakan *platform* berbasis web yang diakses secara publik sehingga rentan terhadap serangan keamanan yang salah satunya serangan dari sisi otentikasi. Sistem otentikasi pada aplikasi berbasis web tersebut masih banyak dijumpai dengan menerapkan metode satu faktor atau *Single Factor Authentication* (SFA) yang secara umum menggunakan kombinasi *user* dan *password*. Penggunaan SFA seperti kombinasi *user* dan *password* ini mudah terkena serangan keamanan seperti *brute force login*, *key logger* dan serangan otentikasi lainnya. Di samping itu, banyaknya aplikasi SPBE yang digunakan mengharuskan pengguna melakukan otentikasi berulang pada setiap aplikasi yang mengakibatkan semakin tinggi pula risiko terkena serangan keamanan.

Salah satu aplikasi yang digunakan di Pemerintah Kota Cimahi yang mengandung informasi sensitif dan penting adalah aplikasi Dashboard Executive. Aplikasi ini diakses melalui jaringan publik dan digunakan oleh pimpinan instansi beserta jajarannya seperti Wali Kota, Wakil Wali Kota, Sekretaris Daerah dan Kepala Perangkat Daerah untuk melihat seluruh informasi kepemerintahan secara terpusat melalui interoperabilitas data dari seluruh aplikasi yang ada. Kecenderungan pihak eksekutif, pada umumnya tidak dapat mengelola banyak akun dari berbagai aplikasi sehingga meminta orang lain untuk dapat membantu melakukan proses otentikasi ke aplikasi sehingga orang lain mengetahui akun pimpinan yang berdampak pada tidak terjaminnya kerahasiaan informasi yang ada di aplikasi tersebut. Hal ini juga diperparah dengan adanya kemungkinan serangan keamanan serta dampak yang dapat ditimbulkan berupa tersebarnya data-data sensitif apabila aplikasi Dashboard Executive ini terkena serangan keamanan salah satunya dari sisi otentikasi.

Oleh karena itu perlu penerapan metode otentikasi yang aman namun tidak menyulitkan bagi pimpinan dalam mengakses aplikasi SPBE, salah satunya aplikasi Dashboard Executive. Hal tersebut yang melatarbelakangi peneliti untuk menentukan metode otentikasi yang tepat yang dapat digunakan oleh pimpinan untuk mengakses aplikasi SPBE.

II. METODE

Metode penelitian yang digunakan dalam penelitian ini adalah menggunakan metode penelitian terapan dan kualitatif yang dilakukan terlebih dahulu mempelajari

teori-teori dan penelitian terdahulu. Sedangkan metode pengumpulan data yang digunakan menggunakan studi literatur, wawancara dan observasi langsung untuk mengumpulkan data-data terkait penggunaan sertifikat elektronik dan metode otentikasi yang selama ini digunakan di Pemerintah Kota Cimahi. Studi literatur dilakukan dengan menggunakan literatur paper jurnal bereputasi nasional maupun internasional, regulasi terkait sertifikat elektronik untuk dijadikan sebagai data primer.

III. HASIL DAN PEMBAHASAN

A. Kondisi Saat Ini

Berdasarkan hasil observasi dan wawancara terhadap kondisi eksisting pada Pemerintah Kota Cimahi, aspek keamanan aplikasi terutama terkait otentikasi belum memenuhi standar keamanan. Sebanyak 143 aplikasi yang dikembangkan, digunakan dan dikelola semunya menggunakan metode otentikasi satu faktor (*Single Factor Authentication*) dengan menggunakan *user* dan *password*. Salah satu dari aplikasi tersebut adalah aplikasi Dashboard Executive yang berisi informasi-informasi penting yang dibutuhkan oleh pimpinan instansi maupun pimpinan perangkat daerah.

TABEL I
REKAPITULASI APLIKASI

Platform Aplikasi	Jumlah Akses Jaringan Publik	Jumlah Akses Jaringan Intranet	Jumlah
Berbasis Web	118	25	143
Berbasis Mobile	7	0	7
Berbasis Desktop	0	6	6

Sebagian besar aplikasi yang digunakan merupakan aplikasi berbasis web yang diakses secara publik. Aplikasi-aplikasi ini rentan terhadap serangan *cyber* sehingga perlu dilakukan tindakan pencegahan dengan meminimalisir celah keamanan (*vulnerability*) dan menerapkan standar keamanan aplikasi.

TABEL II
DAFTAR INSIDEN KEAMANAN TAHUN 2023

Insiden Keamanan	Jenis Serangan	Jumlah
Percobaan Login	Brute force	2
Perubahan halaman web	Web deface	3
Akun aplikasi tidak dapat digunakan	Pengambilalihan Akun	1

Dari tabel daftar insiden keamanan selama tahun 2023 terdapat enam serangan keamanan dengan tiga di antaranya terkait dengan otentikasi aplikasi. Serangan otentikasi ini dapat mengakibatkan terancamnya kerahasiaan data dan informasi yang terdapat pada aplikasi. Hal ini perlu dilakukan tindakan pencegahan salah satunya dengan penerapan metode otentikasi yang lebih aman sehingga dapat terhindar dari serangan otentikasi.

B. Rekomendasi Metode Otentikasi

Berdasarkan kondisi eksisting terhadap serangan insiden keamanan yang berkaitan dengan otentikasi, maka peneliti memberikan rekomendasi tindakan pencegahan dengan menerapkan metode otentikasi pada aplikasi menggunakan sertifikat elektronik. Pemilihan metode otentikasi menggunakan sertifikat elektronik dipilih dengan mempertimbangkan kemudahan penggunaan dalam proses otentikasi pada aplikasi Dashboard Executive dari kalangan pimpinan yang mempunyai kecenderungan tidak dapat mengelola akun aplikasi. Sertifikat elektronik yang direkomendasikan berhubungan dengan studi kasus pada aplikasi Dashboard Executive adalah sertifikat elektronik yang dimiliki oleh pegawai pemerintahan yang dikeluarkan oleh Balai Sertifikat Elektronik (BSrE) Badan Siber dan Sandi Negara (BSSN) selaku Penyelenggara Sertifikasi Elektronik (PSrE) atau *Certification Authority* (CA). Pemilihan sertifikat elektronik ini didasarkan pada pertimbangan pengguna aplikasi Dashboard Executive merupakan pejabat pemerintah yang sesuai kebijakan Pemerintah Kota Cimahi harus memiliki sertifikat elektronik yang diterbitkan oleh BSrE sehingga semua pejabat di Pemerintah Kota Cimahi termasuk pimpinan selaku pengguna aplikasi Dashboard Executive memiliki sertifikat elektronik.

1. Infrastruktur Kunci Publik

   Infrastruktur Kunci Publik (IKP) adalah sebuah cara untuk otentikasi, pengamanan data dan perangkat anti sangkal. IKP merupakan implementasi dari berbagai teknik kriptografi yang bertujuan untuk mengamankan data, memastikan keaslian data dan pengirimnya serta mencegah penyangkalan. Teknik-teknik kriptografi yang digunakan antara lain fungsi hash, algoritma kriptografi simetrik, dan algoritma kriptograsi asimetrik. Fungsi hash digunakan bersama dengan algoritma kriptografi asimetrik dalam bentuk tanda tangan digital untuk memastikan integritas atau keaslian data berikut pengirimnya. Algoritma kriptograsi simetrik digunakan untuk mengamankan data saat berkomunikasi. IKP diwujudkan dalam bentuk kolaborasi antar komponen-komponennya menjadi suatu ekosistem. Salah satu implementasi IKP adalah dalam penggunaan sertifikat elektronik untuk otentikasi klien.

   Komponen yang membentuk struktur IKP, terdiri dari:

   a. *Certification Authority* (CA)

      Merupakan lembaga yang mengeluarkan sertifikat elektronik yang di Indonesia disebut sebagai Penyelenggara Sertifikasi Elektronik (PSrE). PSrE berinduk untuk instansi adalah Balai

Sertifkasi Elektronik (BSrE) yang disebut sebagai BSrE-CA.

b. *End Entity* (EE)

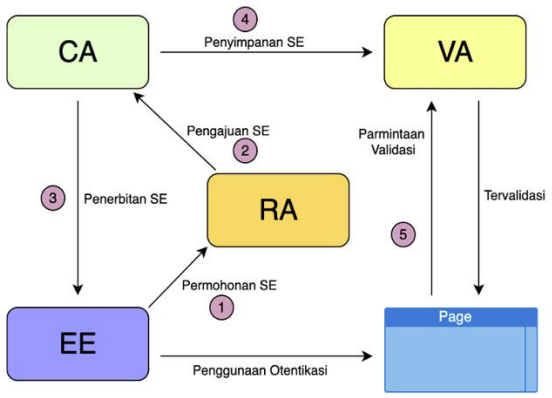
Merupakan individu atau lembaga yang bertindak sebagai pemilik sertifikat elektronik.

c. Registration Authority (RA)

Merupakan lembaga perantara antara CA dan EE. Lembaga ini berfungsi mengumpulkan data personal dari EE yang selanjutnya meminta pengeluaran sertifikat elektronik ke CA untuk EE. RA untuk instansi adalah unit kerja yang ditunjuk yang ada di Instansi Pemerintah Pusat dan Instansi Pemerintah Daerah.

d. Validation Authority (VA)

Merupakan lembaga independen pihak ketiga yang berperan mengatur proses verifikasi dan validasi sertifikat elektronik secara online. VA menyimpan daftar sertifikat elektronik yang dikeluarkan CA dan berfungsi sebagai repository database sertifikat elektronik. Peran VA secara umum masih dipegang oleh CA.



Gambar. 1 Skema Infrastruktur Kunci Publik

2. Sertifikat Elektronik dari BSrE

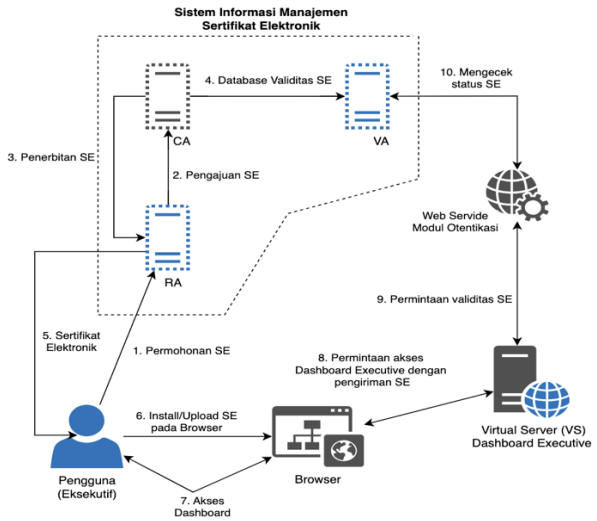
Sertifikat elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik. Sertifikat elektronik yang dikeluarkan oleh BSrE mengacu kepada sertifikat elektronik X.509 versi 3 sesuai dengan RFC 5280. BSrE selaku CA melakukan tinjauan terhadap profil sertifikat secara berkala minimal setahun sekali.

TABEL III
PROFIL SERTIFIKAT ELEKTRONIK
PEGAWAI PEMERINTAH

Nama	Deskripsi
Nomor Versi	BSrE CA menerbitkan sertifikat X.509 v3
Ekstensi Sertifikat	BSrE CA memakai ekstensi sertifikat standar yang mematuhi RFC 5280
Identifier Objek Algoritma	Pengidentifikasi objek algoritma kriptografi diisi sesuai dengan standar dan rekomendasi RFC 5280. *Object Identifier* (OID) standar X.509v3. Algoritma enkripsi RSA untuk kunci subjek dan SHA384 dengan enkripsi RSA untuk tanda tangan sertifikat.
Format Nama	Sesuai dengan konvensi penamaan dan batasan yang memenuhi standar ITU X.500
Batasan Nama	Sesuai dengan konvensi penamaan dan batasan yang memenuhi standar ITU X.500
Identifier Objek Kebijakan Sertifikat	OID CP yang tercantum dalam sertifikat adalah sesuai dengan daftar OID dengan penggunaan BSrE CA, CPS, Sertifikat Orang Perseorangan/Individu, Sertifikat Badan Usaha/Organisasi
Usage of Policy Constraints Extension	Tidak ditentukan
Policy Qualifiers Syntax and Semantics	Tidak ditentukan
Processing Semantics for the Critical Certificate Policies Extension	Tidak ditentukan

3. Desain Penerapan Sertifikat Elektronik pada Aplikasi Dashboard Executive

Penerapan sertifikat elektronik untuk otentikasi pada aplikasi Dashboard Executive secara umum dapat digambarkan sebagai berikut :



Gambar. 2 Desain penerapan otentikasi menggunakan sertifikat elektronik

Penjelasan langkah-langkah proses otentikasi menggunakan sertifikat elektronik secara umum yang ditawarkan dapat diuraikan sebagai berikut :

1) Pengguna mengajukan permohonan Sertifikat Elektronik kepada RA.
2) RA melakukan validasi persyaratan dan mengajukan penerbitan sertifikat elektronik kepada CA.
3) CA menerbitkan sertifikat elektronik dan menyerahkan kepada RA.
4) CA menyimpan database validitas sertifikat elektronik kepada VA sebagai repositori sertifikat elektronik untuk OCSP (*Online Certificate Status Protocol*) dan CRL (*Certificate Revoked List*) yang digunakan untuk verifikasi dan validasi sertifikat elektronik.
5) RA menyerahkan sertifikat elektronik kepada pengguna dan siap untuk digunakan.
6) Pengguna memasang atau mengunggah sertifikat elektronik pada Browser atau aplikasi Dashboard Executive.
7) Mengakses aplikasi Dashboard Executive melalui Browser yang sudah terpasang sertifikat elektronik.
8) Browser mengakses aplikasi Dashboard Executive dengan mengirimkan data sertifikat elektronik yang terpasang di Browser.
9) Aplikasi Dashboard Executive menerima sertifikat elektronik dari Browser dan meminta validasi sertifikat elektronik pada VA melalui web service modul otentikasi.
10) Web service modul otentikasi memverifikasi dan memvalidasi sertifikat eletkronik melalui VA.
11) Jika hasil pengecekan pada VA valid maka pengguna dapat mengakses aplikasi Dashboard Executive namun jika tidak valid misal masa berlaku kadaluarsa atau status dicabut maka pengguna tidak dapat mengakses aplikasi.

4. Modul Otentikasi

Penggunaan sertifikat elektronik untuk otentikasi membutuhkan verifikasi dan validasi untuk mengetahui validitas sertifikat elektronik yang digunakan. Proses ini perlu program aplikasi yang dapat menjalankan fungsi tersebut. Modul otentikasi dikembangkan dengan menggunakan bahasa Python yang memuat fungsi-fungsi dalam rangka verifikasi dan validasi sertifikat elektronik dalam bentuk layanan berbasis API (*Application Programming Interface*) yang terkoneksi dengan OCSP maupun CRL.

Fungsi yang terdapat dalam modul otentikasi mencakup tahapan verifikasi dan validasi yang meliputi:

a. Membaca isi sertifikat elektronik yang dikirim pengguna melalui Browser melalui proses encoding.
b. Mengekstrak isi sertifikat elektronik dalam format yang dapat digunakan untuk pengolahan data.
c. Melakukan verifikasi tanda tangan digital pada sertifikat elektronik menggunakan kunci publik CA.
d. Melakukan verifikasi masa berlaku sertifikat elektronik.
e. Memvalidasi status sertifikat elektronik untuk apakah masih aktif atau sudah dilakukan pencabutan melalui OCSP.

IV. SIMPULAN

Kesimpulan yang dapat diambil dalam penerapan sertifikat elektronik untuk otentikasi aplikasi adalah sebagai berikut :

1. Penggunaan sertifikat elektronik untuk otentikasi dapat meningkatkan keamanan otentikasi melalui proses verifikasi dan validasi sertifikat elektronik yang menggunakan teknologi kriptografi kunci publik yang jauh lebih aman dibandingkan menggunakan user dan password
2. Penggunaan sertifikat elektronik untuk otentikasi dapat memberikan kemudahan bagi pengguna terutama untuk kalangan pimpinan instansi karena tidak memerlukan *user* dan *password* yang harus diingat.
3. Untuk lebih meningkatkan keamanan terutama dari kehilangan perangkat yang terinstal sertifikat elektronik, perlu kombinasi faktor otentikasi lain yang memudahkan seperti *One Time Password* (OTP) meskipun sudah ada fungsi untuk pencabutan sertifikat elektronik melalui Sistem Informasi Manajemen Serifikat Elektronik.

REFERENSI

[1] Kim, Jae Jung., Hong, Seng Phil. (2011). A Method of Risk Assessment for Multi-Factor Authentication. *Journal of Information Processing Systems*, 7(1), 187-198.
[2] Andres, Steven. (2015). Zero Factor Authentication: A Four-Year Study of Simple Password-less Website Security via One-Time Emailed Tokens.
[3] Yusuf, Ryandi., Anggriawan, Egi. (2015). Penerapan Metode Smart Authentication dalam Layanan e-banking Menggunakan Two Channel Authentication dan QR-Code pada Perangkat Mobile Android.
[4] Is Mardianto, Kuswandi. (2016). Implementasi Keamanan pada Transaksi Data Menggunakan Sertifikat Digital X.509. Ultimatics, 8(1).
[5] Munadil, Rizal., Musliyana, Zuhar., Arif, Teuku Yuliar., Afdhal., Syahrial. (2016). Kombinasi Waktu Sinkronisasi dan Nilai Salt untuk Peningkatan Keamanan pada Single Sign-On. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, 5(3), 201-206.
[6] Musliyana, Zuhar., Arif, Teuku Yuliar., Munadi, Rizal. (2016). Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia Zuhar Musliyana. *Jurnal Rekayasa Elektrika*, 12(1), 21-29.
[7] Darmawana, Irfan., Rahmatullohb, Alam., Riantob., Orizab, Ilman Hilmi. (2020). Authentication System and Method for Improving Security Login without Typing Password. *Advanced Science Engineering Information Technology*, 10(2), 605-610.
[8] Ali, Guma., Dida, Mussa Ally., Sam, Anael Elikana. (2021). A Secure and Efficient Multi-Factor Authentication Algorithmfor Mobile Money Applications. *Future Internet*, 13(12), 299.
[9] Enabled Internet of Vehicles. *Sensors*, 21(18), 6018.
[10] Saqib, Rashad Mahmood., Khan, Adnan Shahid., Javed, Yasir., Ahmad, Shakil., Nisar Kashif. (2022). Analysis and Intellectual Structure of the Multi-Factor Authentication inInformation Security. *Intelligent Automation & Soft Computing*, 32(3), 1632-1647