Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.201961304
Vol. 6, No. 2, April 2019, hlm. 195-200 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 30/E/KPT/2018 e-ISSN: 2528-6579

PERANCANGAN SPESIFIKASI KEAMANAN KONTROL AKSES PADA APLIKASI LAYANAN INFORMASI DI LINGKUNGAN INSTANSI PEMERINTAH

Faizal Achmad[1], Esti Rahmawati Agustina[2]

[1,2] Badan Siber dan Sandi Negara
Email: [1]faizal.achmad@bssn.go.id, [2]esti.rahmawati@go.id

(Naskah masuk: 28 November 2018, diterima untuk diterbitkan: 07 Januari 2019)

Abstrak

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik mengamanatkan kepada setiap instansi pemerintah untuk meningkatkan pengelolaan dan pelayanan informasi di lingkungannya sehingga menghasilkan layanan informasi yang berkualitas. Setiap informasi publik bersifat terbuka dan dapat diakses oleh setiap pengguna informasi publik, kecuali informasi publik yang dikecualikan karena bersifat ketat, terbatas dan rahasia. Untuk membatasi agar suatu informasi hanya dapat diakses oleh pihak-pihak yang berwenang, maka perlu adanya suatu mekanisme kontrol akses yang melakukan proses otentikasi, otorisasi, audit dan pengamanan informasi dalam rangka mengamankan informasi melalui aplikasi layanan informasi.
Penelitian ini dilakukan dengan menggunakan metode *Design Science Research Methodology (DSRM)* yang terdiri dari tahap identifikasi masalah, solusi perancangan dan evaluasi untuk menghasilkan perancangan spesifikasi keamanan berdasarkan model kontrol akses yang menerapkan proses otentikasi, otorisasi, audit dan pengamanan informasi dengan kriptografi. Penyusunan spesifikasi keamanan sistem layanan informasi menggunakan *Common Criteria for Information Technology Security Evaluation* versi 3.1 (REV 5). Hasil perancangan diharapkan dapat menjadi acuan spesifikasi keamanan aplikasi layanan informasi di lingkungan instansi pemerintah, khususnya keamanan informasi yang terkait dengan kontrol akses.

Kata kunci: *informasi publik, keamanan informasi, kontrol akses, kriptografi, common criteria*

DESIGN OF ACCESS CONTROL SECURITY SPESIFICATION IN INFORMATION SERVICES APPLICATION FOR GOVERNMENT INSTITUTION

Abstract

Law Number 14 Year 2008 on Public Information Openness mandates to every government agency to improve management and information service in its environment so as to produce quality information service. Any public information is open and accessible to any user of public information, except for excluded public information because it is strict, limited and confidential. In order to limit information to access only by authorized parties, it is necessary to have an access control mechanism, which processes authentication, authorization, audit and information security in order to secure information through the application of information services.
In this research we implement Design Science Research Methodology (DSRM) to design the security specifications based on the access control model. The model implements the process of authentication, authorization, audit and information security that implements cryptography techniques. The design of the security specification using Common Criteria for Information Technology Security Evaluation version 3.1 (REV 5). The design result is expected to become the reference of information security application specification in government institution, especially related to access control.

Keywords: *public information, information security, access control, cryptography, common criteria*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi memungkinkan setiap individu atau kelompok untuk dapat mengakses suatu informasi tanpa kenal batas ruang dan waktu. Setiap instansi pemerintah wajib meningkatkan pengelolaan dan pelayanan informasi di lingkungannya untuk menghasilkan layanan informasi yang berkualitas, sesuai dengan amanat Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik. Setiap informasi publik bersifat terbuka dan dapat diakses oleh setiap pengguna informasi publik,

kecuali informasi publik yang dikecualikan karena bersifat ketat, terbatas dan rahasia.

Ancaman yang kerap terjadi terhadap suatu informasi berklasifikasi antara lain pengubahan, penyadapan, dan pemalsuan. Untuk membatasi agar suatu data informasi hanya dapat diakses oleh pihak-pihak yang berwenang, maka perlu adanya suatu mekanisme kontrol akses pada aplikasi yang bertujuan untuk melakukan proses otentikasi, otorisasi, audit dan pengamanan informasi dalam rangka mengamankan informasi pada aplikasi layanan informasi yang terhubung dengan jaringan internet.

Penelitian ini akan merumuskan perancangan persyaratan keamanan berdasarkan konsep otentikasi, otorisasi dan kontrol audit dari suatu model kontrol akses dengan menggunakan *common criteria*, untuk dapat diimplementasikan pada aplikasi layanan informasi di lingkungan instansi pemerintah. Sehingga penelitian ini diharapkan dapat menjadi acuan spesifikasi keamanan aplikasi layanan informasi di lingkungan instansi pemerintah, khususnya keamanan informasi yang terkait dengan kontrol akses.

2. LANDASAN TEORI

2.1 Keterbukaan Informasi Publik

Undang-Undang Nomor 14 Tahun 2008 (UU No.14, 2008) tentang Keterbukaan Informasi Publik (KIP) bertujuan mengatur Badan Publik, untuk meningkatkan pengelolaan dan pelayanan informasi di lingkungan Badan Publik agar menghasilkan layanan informasi yang berkualitas. Berdasarkan Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik (Kemenkominfo, 2011) yang diterbitkan oleh Kementerian Komunikasi dan Informatika, informasi diklasifikasikan menjadi 3 (tiga) bagian sebagai berikut:

a. Informasi rahasia, yaitu aset informasi yang sangat peka dan berisiko tinggi yang pembocoran atau penyalahgunaan akses terhadapnya bisa mengganggu kelancaran usaha instansi/lembaga secara temporer atau mengganggu citra dan reputasi perusahaan;
b. Informasi internal, yaitu informasi yang telah terdistribusi secara luas di lingkungan internal instansi/lembaga yang penyebarannya secara internal tidak lagi memerlukan izin dari pemilik informasi dan risiko penyebarannya secara tak berwenang tidak menimbulkan kerugian signifikan;
c. Informasi publik, yaitu informasi yang secara sengaja disediakan instansi/lembaga untuk dapat diketahui publik.

Pada Undang-Undang KIP tersebut juga diatur mengenai informasi yang dikecualikan, yaitu Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat membahayakan pertahanan dan keamanan Negara.

2.2 Keamanan Informasi dan Kriptografi

Aspek utama dari keamanan yang biasa ditangani oleh layanan web adalah identifikasi, otentikasi, otorisasi, integritas, dan kerahasiaan, serta nir-penyangkalan (Erl, 2005), yang diimplementasikan dengan menggunakan teknik kriptografi. Kriptografi adalah studi tentang teknik – teknik matematika yang berhubungan dengan aspek – aspek keamanan informasi seperti kerahasiaan, keutuhan data, otentikasi entitas, dan otentikasi keaslian data (Menezes dkk, 1997).

2.3 Kontrol Akses

Kontrol akses merupakan suatu mekanisme yang digunakan untuk mengamankan dan memastikan kerahasiaan data Setiap pengguna mencoba untuk mengakses suatu data objek. Mekanisme kontrol akses akan melakukan pengecekan hak dari pengguna, berdasarkan otorisasi yang telah ditetapkan. (Patil dan Meshram, 2012). Kontrol akses dapat diimplementasikan dengan tahapan sebagai beriku (Salunke, dkk, 2013):

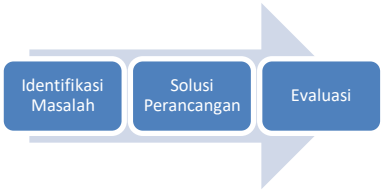
a. Otentikasi
   Pada tahap ini konfirmasi terhadap identitas pengguna dilakukan. Misalnya dengan melakukan pengecekan terhadap informasi *username* dan *password* dari pengguna aplikasi.
b. Otorisasi
   Pada tahap ini hal – hal yang dapat dilakukan oleh pengguna diatur. Misalnya pengguna A hanya dapat membaca informasi tertentu dan tidak dapat mengubah informasi tersebut.
c. Kontrol audit
   Pada tahap ini dilakukan pelacakan transaksi sensitif. Audit harus memungkinkan untuk meninjau ”siapa melakukan apa” dan ”kapan dan siapa yang memberikan izin untuk pengguna yang mana” dalam suatu aplikasi.

2.4 Common Criteria

Common Criteria (CC) (www.commoncriteriaportal.org) adalah standar internasional yang digunakan oleh negara – negara yang tergabung dalam *Common Criteria Recognitions Arrangements* (CCRA) sebagai panduan dalam hal evaluasi keamanan produk teknologi informasi (TI). CC memberikan panduan terkait dengan persyaratan keamanan yang ada dalam suatu produk TI serta bagaimana menjamin fungsi – fungsi keamanan tersebut.

3. METODOLOGI

Metodologi yang digunakan pada proses penelitian ini adalah *Design Science Research Methodology* (DSRM) (Offerman, 2009) yang dibagi menjadi 3 (tiga) tahapan yaitu identifikasi masalah, solusi perancangan dan evaluasi. Gambar 1 menunjukkan tahapan dari metode ini.



Gambar 1. Tahapan *Design Science Research Methodology*

Identifikasi masalah dilakukan dengan mengidentifikasi bagaimana merancang persyaratan keamanan berdasarkan *Common Criteria*. Selanjutnya melakukan solusi perancangan spesifikasi keamanan berupa metode dan mekanisme kontrol akses. Selanjutnya melakukan evaluasi dengan melakukan pengujian aplikasi layanan informasi. Namun pada penelitian ini, langkah yang dikerjakan adalah tahap identifikasi permasalahan dan solusi perancangan.

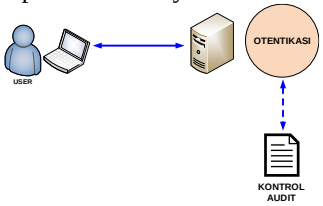
4. PEMBAHASAN DAN HASIL

Sistem yang dikembangkan diberi nama SISINFO. Perancangan persyaratan keamanan pada penelitian ini disusun dalam 6 (enam) bagian.

4.1 Bagian I : Pendahuluan

SISINFO merupakan produk atau aplikasi sistem layanan informasi yang akan dibuat, berdasarkan klaim yang memenuhi persyaratan keamanan CC dan merupakan subjek dari proses evaluasi yang dilakukan. SISINFO menyediakan suatu kontrol akses dalam rangka mengamankan sistem layanan informasi, terhadap ancaman akses dan operasi terhadap data informasi dari pihak yang tidak memiliki otoritas. SISINFO dirancang dengan menerapkan proses otentikasi, otorisasi dan kontrol audit sebagai komponen inti, untuk mencegah pihak yang tidak berwenang melakukan akses dan operasi terhadap suatu data informasi yang berklasifikasi. Berikut adalah penjelasan dari masing – masing komponen inti:

a. Otentikasi merupakan suatu komponen yang melakukan proses identifikasi dan otentikasi terhadap pengguna informasi, komponen ini memastikan bahwa pengguna informasi merupakan personil yang otentik dan telah terdaftar pada sistem layanan informasi.

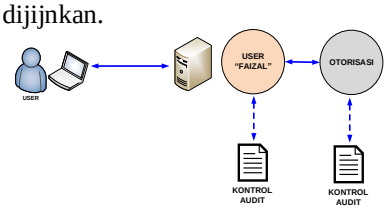


Gambar 2. Proses Otentikasi

Proses otentikasi yang paling sederhana adalah dengan menggunakan dua faktor input yaitu *username* dan *password*. Semakin banyak faktor input (*multifactor authentication*) akan membuat otentikasi makin kompleks dari sisi serangan. Pada Gambar 2, seorang *user* atau pengguna informasi memasukkan *username* dan *password*, untuk menyatakan kepada sistem SISINFO bahwa dirinya merupakan pengguna informasi yang otentik.

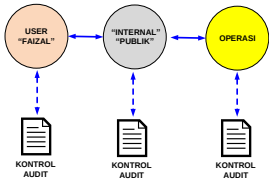
b. Otorisasi merupakan suatu komponen yang melakukan proses otorisasi terhadap pengguna informasi berdasarkan hasil proses otentikasi. Komponen otorisasi memberikan wewenang kepada pengguna informasi berupa otoritas dalam melakukan akses dan operasi terhadap data informasi berdasarkan klasifikasi informasi yaitu internal, publik, dan rahasia.

Pada Gambar 3 dibawah ini terlihat bahwa pengguna sebelumnya telah melewati proses otentikasi dan telah dinyatakan otentik sebagai "FAIZAL" oleh sistem SISINFO. Selanjutnya sistem SISINFO melakukan proses otorisasi untuk memberikan *user privileges* kepada "FAIZAL" berupa otoritas klasifikasi informasi yang dijijnkan.



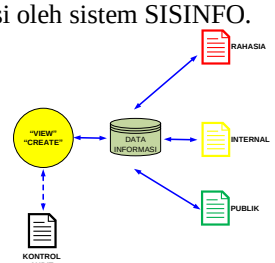
Gambar 3. Proses Otorisasi

Pada Gambar 4 dibawah ini terlihat bahwa user telah teronterikasi dan mendapatkan otoritas terhadap informasi yang berklasifikasi internal dan publik. Selanjutnya system SISINFO memberikan kewenangan operasi terhadap klasifikasi informasi yang diijinkan.



Gambar 4. Pemberian Wewenang Operasi

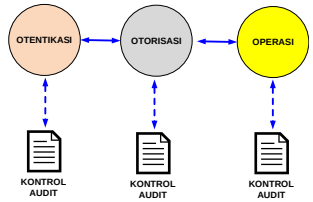
Pada Gambar 5 dibawah ini, terlihat bahwa pengguna informasi sebelumnya telah melewati proses otentikasi, dan telah dinyatakan otentik sebagai "FAIZAL", telah mendapatkan otoritas terhadap data informasi berklasifikasi "INTERNAL" dan "PUBLIK", serta kewenangan melakukan operasi "VIEW" (membaca) dan "CREATE" (membuat) informasi oleh sistem SISINFO.



Gambar 5. Operasi Data Informasi

Teknik kriptografi diimplementasikan untuk mengamankan data informasi yang bersifat rahasia. Salah satunya dengan mengimplementasikan algoritma enkripsi yaitu *Advanced Encryption Standard (AES).*

c. Audit merupakan komponen yang melakukan proses perekaman secara rinci mengenai setiap proses yang terjadi pada aplikasi layanan informasi seperti proses otentikasi dan otorisasi *pengguna informasi*, akses dan operasi terhadap data informasi, serta proses administrasi akun pengguna informasi dan data informasi.



Gambar 6. Kontrol Audit pada Proses Otentikasi, Otorisasi, dan Operasi

Pada Gambar 6 diatas, terlihat bahwa setiap proses melakukan perekaman terhadap semua kejadian yang terjadi. Perekaman ini digunakan dalam proses kontrol audit secara rutin atau terjadi peristiwa yang membutuhkan proses audit

4.2 Bagian II : Klaim Kesesuaian

Persyaratan keamanan dari SISINFO disusun berdasarkan *Common Criteria for Information Technology Security Evaluation* versi 3.1 (REV 5), serta mengacu sebagian pada model kontrol akses yang dibuat oleh Jim Reynolds dan Ramaswamy Chandramouli pada tahun 1998 (Reynolds dan Chandramouli, 1998).

4.3 Bagian III : Permasalahan Keamanan

Permasalahan keamanan yang akan diatasi oleh SISINFO meliputi:

a. Ancaman.
   Identifikasi ancaman yang mungkin terjadi adalah sebagai berikut:
   1) Akses, jika pengguna yang tidak memiliki hak akses mencoba untuk mendapatkan hak akses;
   2) Operasional, jika terjadi kesalahan administrasi dan operasional SISINFO yang tidak tepat;
   3) Kewenangan, jika pemberian kewenangan dilakukan dengan merusak aspek keamanan;
   4) Transmisi, jika pengguna yang tidak terotorisasi mendapatkan informasi rahasia yang seharusnya sistem menjaga kerahasiaannya dan integritas datanya.
   5) Pengungkapan, jika pengguna yang tidak terotorisasi mengungkap data yang tersimpan pada server penyimpanan.
   6) Modifikasi, jika pengguna yang tidak terotorisasi melakukan modifikasi terhadap data sehingga membahayakan kerahasiaan dan integritas data.

b. Kebijakan. SISINFO memiliki kemampuan untuk menegakkan kebijakan organisasi yang meliputi pembagian tugas pengguna secara spesifik, pembagian hak akses pengguna berdasarkan tanggung jawabnya, penegakan peraturan untuk mencegah terjadinya konflik kepentingan dan kebijakan kriptografi yang diterapkan pada suatu organisasi.

c. Asumsi
   SISINFO menyediakan pengukuran tingkat keamanan yang efektif hanya jika di-*install*, diatur dan digunakan secara benar. Lingkungan operasional harus diatur sesuai dokumentasi SISINFO untuk pendistribusian, operasional dan panduan pengguna informasi. Kondisi di bawah ini diasumsikan telah berjalan pada lingkungan organisasi SISINFO berada. Lingkungan operasional ini terdiri dari asset, lokasi, perlindungan, akses, pengelolaan, pemilik, dan koneksi.

4.4 Bagian IV : Sasaran Keamanan

Sasaran keamanan adalah suatu pernyataan singkat yang dimasukkan untuk merespon masalah keamanan yang telah didefinisikan pada Bagian III. Selain itu sasaran keamanan juga memberikan arahan khusus mengenai keamanan yang diharapkan pada lingkungan dimana SISINFO beroperasi.

a. Sasaran Keamanan Aplikasi SISINFO
   Terdiri dari akun, admin, audit, tugas, *entry*, identifikasi, kewenangan, kriptografi dan modifikasi.

b. Sasaran Keamanan Lingkungan SISINFO
   SISINFO diasumsikan lengkap dan mandiri. Namun lingkungan operasional harus dipenuhi untuk mendukung kemampuan keamanan dari SISINFO. Sasaran keamanan yang dimaksud adalah otentikasi, koneksi, dan fisik.

4.5 Bagian V: Kebutuhan Keamanan Fungsional

Bagian ini menjelaskan kebutuhan keamanan secara fungsional yang jelas, tidak ambigu dan mendeskripsikan secara baik perilaku keamanan yang diharapkan dari SISINFO. Persyaratan fungsional dari SISINFO adalah sebagai berikut:

a. Persyaratan Audit Keamanan (*Class FAU : Security Audit*).
   Perekaman audit untuk setiap kegiatan pada SISINFO dilakukan untuk membantu proses audit keamanan dalam memberikan informasi mengenai suatu kejadian dan penyebab terjadinya kejadian tersebut.
   1) Rekaman audit dapat dibangkitan dari kejadian-kejadian dari seorang pengguna informasi. (FAU_GEN.1.1).

2) Tersedianya informasi audit mengenai tanggal dan waktu kejadian, pengguna informasi yang bertanggung jawab, operasi yang dilakukan terhadap objek, hasil dari kejadian tersebut dan pengenal sesi dari pengguna informasi pada saat kejadian.(FAU_SAR.1.1).
3) Hanya pengguna informasi yang memiliki otoritas saja yang mendapatkan ijin untuk akses-baca terhadap rekaman audit (FAU_SAR.2.1).
4) Rekaman audit terlindungi dari penghapusan pihak yang tidak memiliki otorisasi (FAU_STG.1.1).
5) Rekaman audit tidak dapat dimodifikasi (FAU_STG.1.2).

b. Persyaratan Operasi Kriptografi (*Class FCS : Cryptographic Support*)
Operasi kriptografi yang dilakukan oleh SISINFO meliputi proses pembangkitan dan pemusnahan kunci kriptografi serta pengoperasian kriptografi untuk hashing dan enkripsi/dekripsi data.
1) Proses pembangkitan kunci kriptografi dilakukan untuk membangkitan kunci kriptografi RSA dan AES (FCS_CKM.1a.1 dan FCS_CKM.1b.1).
2) Proses pemusnahan kunci dilakukan untuk setiap kunci sesi yang sudah tidak digunakan dengan melakukan proses overwrite dengan kunci sesi yang baru (FCS_CKM.4).
3) Proses enkripsi/dekripsi data dilakukan menggunakan algoritma kriptografi RSA dan AES (FCS_COP.1a.1 dan FCS_COP.1b.1).
4) Proses hashing dilakukan menggunakan *Secure Hash Algorithm* (SHA) (FCS_COP.1c.1).

Semua operasi kriptografi ini diterapkan berdasarkan standar PKCS#1, FIPS 197 dan FIPS 180-4.

c. Persyaratan Perlindungan Data Pengguna Informasi (*Class FDP : User Data Proection*)
Persyaratan yang terkait dengan perlindungan data pengguna informasi adalah sebagai berikut:
1) Kebijakan SISINFO yaitu Kebijakan Fungsi Keamanan harus ditegakkan pada pengguna informasi, data informasi dan operasi terhadap data informasi (FDP_ACC.1.1).
2) Pelaksanaan Kebijakan Fungsi Keamanan kepada data informasi berdasarkan pada atribut pengguna informasi dan data informasi (FDP_ACF.1.1).
3) Pengguna informasi dapat melakukan operasi pada suatu data informasi jika diberikan role (peran) yang memiliki hak akses operasi terhadap data informasi tersebut (FDP_ACF.1.2)
4) Akses operasi dari pengguna informasi kepada data informasi dapat dilakukan hanya jika pengguna informasi memiliki peran yang mengijinkan akses operasi kepada data informasi (FDP_ACF.1.3).
5) Akses operasi dari pengguna informasi kepada data informasi tidak dapat dilakukan jika pengguna informasi tidak memiliki peran yang mengijinkan permintaan akses operasi kepada data informasi (FDP_ACF.1.4).

d. Persyaratan Identifikasi dan Otentikasi (*Class FIA : Identification and Authentication*)
Pengguna sistem SISINFO harus memberikan parameter input pada proses identifikasi dan otentikasi. Misalnya *username* dan *password*. Setelah proses identifikasi dan otentikasi, sistem akan memberikan akses terhadap pengguna sesuai dengan perannya. Persyaratan keamanan pada proses identifikasi dan otentikasi adalah sebagai berikut:
1) Dapat melakukan pengelolaan terhadap atribut keamanan yang dimiliki oleh seorang pengguna informasi (FIA_ATD.1.1).
2) Seorang pengguna informasi harus terotentikasi terlebih dahulu, sebelum melakukan kegiatan atas nama identitas dari pengguna informasi tersebut (FIA_UAU.2.1).
3) Seorang pengguna informasi harus memperkenalkan identitas dirinya setiap akan melakukan kegiatan yang mengatasnamakan pengguna informasi tersebut (FIA_UID.2.1).

e. Persyaratan Manajemen Keamanan (*Class FMT : Security Management*)
Persyaratan keamanan yang terkait dengan manajemen keamanan adalah sebagai berikut:
1) Kemampuan [*modify, delete, create*] terhadap atribut keamanan seorang pengguna informasi pada SISINFO secara administratif hanya dibatasi pada pengguna informasi yang memiliki otoritas (FMT_MSA.1a.1).
2) Parameter pada suatu atribut keamanan hanya menerima nilai yang dianggap aman (FMT_MSA.2.1).
3) Parameter pada suatu Data TSF hanya menerima nilai yang dianggap aman (FMT_MTD.3.1).
4) Kemampuan untuk mencabut atribut keamanan yang berkaitan dengan data informasi dibatasi hanya kepada Pemilik data informasi dan sekelompok peran pada SISINFO yang memiliki otoritas (FMT_REV.1.1).
5) Kemampuan untuk mencabut atribut keamanan yang berkaitan dengan pengguna informasi di dalam TSC dibatasi hanya

kepada sekelompok peran pada SISINFO yang memiliki otoritas (FMT_REV.1.2).

6) Pengaturan sekelompok peran pada SISINFO yang bersifat administratif dan peran sebagai Pemilik data informasi (FMT_SMR.2.1).
7) Pengguna informasi harus memiliki peran sesuai dengan yang tersedia (FMT_SMR.2.2).
8) Pemilik Objek dapat melakukan perubahan atribut keamanan hanya terhadap objek yang mereka miliki, sedangkan sekelompok peran administratif pada SISINFO dapat melakukan perubahan atribut keamanan terhadap semua objek berdasarkan kendali kontrol dari aplikasi layanan informasi.

4.6 Bagian VI : Ringkasan Spesifikasi

Bagian ini menyediakan rangkuman spesifikasi SISINFO, yang merupakan deskripsi teknis secara umum mengenai bagaimana mekanisme mengimplementasikan SISINFO sesuai klaim pada Kebutuhan Keamanan Fungsional.

1) Audit Keamanan
   SISINFO menyediakan fungsi untuk melakukan perekaman setiap aktifitas keamanan untuk keperluan audit, rekaman audit hanya dapat dibangkitkan dan di akses oleh pengguna informasi yang memiliki otoritas dan tersimpan secara aman pada secure storage.
2) Operasi Kriptografi
   SISINFO menyediakan operasi kriptografi seperti pembangkitan dan pemusnahan kunci kriptografi serta pengoperasian kriptografi untuk fungsi hash dan enkripsi/dekripsi data.
3) Perlindungan Data Pengguna Informasi
   SISINFO menegakkan kebijakan berdasarkan kebijakan organisasi yang telah ditetapkan terhadap pengguna informasi berdasarkan jabatan dan otoritasnya dalam melakukan akses dan operasi pada suatu data informasi.
4) Identifikasi dan Otentikasi
   SISINFO mewajibkan setiap pengguna informasi teridentifikasi dan terotentikasi dengan sukses sebelum dijinkan berinteraksi dengan data informasi yang dilindungi.
5) Manajemen Keamanan
   SISINFO menyediakan fungsi yang mengijinkan administrator yang memiliki otoritas untuk melakukan manajemen terhadap SISINFO dan fungsi keamanannya.

5. KESIMPULAN

Telah dilakukan perancangan spesifikasi keamanan kontrol akses aplikasi layanan informasi (SISINFO) dengan mengacu pada *Common Criteria for Information Technology Security Evaluation* versi 3.1 (REV 5). Spesifikasi ini terdiri audit keamanan, operasi kriptografi, perlindungan data pengguna informasi, identifikasi dna otentikasi, dan manajemen keamanan. Hasil rancangan spesifikasi keamanan dapat dijadikan sebagai acuan bagi pengembangan layanan sistem informasi di lingkungan instansi pemerintah, khususnya yang terkait keamanan kontrol akses.

Penelitian selanjutnya dapat dilakukan proses pembangunan SISINFO sesuai dengan perancangan spesifikasi keamanan kontrol akses yang telah dibuat pada penelitian ini.

DAFTAR PUSTAKA

AUSANKA-CRUES, RYAN, 2011. Methods for Access Control: Advances and Limitations, California: Harvey Mudd College.

COMMON CRITERIA, 2017. Common Criteria for Information Technology Security Evaluation (REV 5) [online] Tersedia di: < https://www.commoncriteriaportal.org/cc/> [Diakses 9 Oktober 2018]

ERL, THOMAS, 2005. Service-Oriented Architecture: Concepts, Technology, and Design. New Jersey: Prentice Hall.

KEMENTERIAN KOMUNIKASI DAN INFORMATIKA, 2011. Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik, Jakarta.

MENEZES, dkk, 1997. Handbook of Applied Cryptography. Florida: CRC Press.

OFFERMANN, PHILIPP, 2009. Outline of a Design Science Research Process, 4th International Conference on Design Science Research in Information Systems and Technology.

PATIL, AKSHAY dan PROF. B. B. MESHRAM, 2012. Database Access Control Policies, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp.3150-3154.

REYNOLDS, JIM dan CHANDRAMOULI, RAMASWAMY, 1998. Role-Based Access Control Protection Profile version 1.0, 1998.

SALUNKE, DIPMALA, dkk, 2013.A survey paper on Role Based Access Control, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3.

SCHNEIER, BRUCE, 1996. Applied Cryptography, Second Edition. New York: John Wliey & Sons Inc.

UNDANG-UNDANG NOMOR 14, 2008. Keterbukaan Informasi Publik.