PERANCANGAN INFRASTRUKTUR KUNCI PUBLIK DENGAN IMPLEMENTASI PEMBUATAN KUITANSI DIGITAL PEMBAYARAN KURSUS BAHASA INGGRIS

Alwin Indra Fatra[*)], R. Rizal Isnanto, and Enda Wista Sinuraya

Jurusan Teknik Elektro, Universitas Diponegoro Semarang
Jl. Prof. Sudharto, SH, Kampus UNDIP Tembalang, Semarang 50275, Indonesia

[*)]*E-mail* : *alwin.indra@gmail.com*

Abstrak

Kuitansi dalam bentuk digital memiliki beberapa keuntungan dibandingkan kuitansi dalam bentuk fisik yakni kemudahan dalam hal penyimpanan, pemindahan dan pembuatan cadangannya. Namun Kesulitan melakukan pengesahan dan verifikasi serta kerentanan data digital untuk dimanipulasi menjadikan kuitansi digital masih jarang digunakan sekarang ini. Pada penelitian ini penulis membangun suatu infrastruktur kunci publik yang berfungsi untuk melakukan pengelolaan terhadap sertifikat digital. Sertifikat digital merupakan suatu data digital yang berisi informasi mengenai kepemilikan pasangan kunci publik dan kunci privat. Pengesahan kuitansi dilakukan dengan cara menandatangani kuitansi digital dengan kunci privat sedangkan proses verifikasinya menggunakan pasangan kunci publiknya. Dengan dilakukan penandatanganan diharapkan jika terdapat perubahan pada kuitansi digital dapat diketahui. Metode penelitian ini adalah menganalisis kebutuhan sistem, merancang sistem, membangun sistem, melakukan pengujian, menganalisis hasil pengujian serta menarik kesimpulan. Tujuan penelitian ini ialah meneliti pemanfaatan infrastruktur kunci publik untuk layanan pengesahan dan penjaminan informasi pada kuitansi digital. Hasil penelitian ini berupa suatu sistem terintegrasi untuk pembuatan dan penandatangananan kuitansi digital. Hasil pengujian menunjukkan sedikit saja perubahan pada kuitansi digital setelah ditandatangani menyebabkan status tandatangan menjadi tidak sah. Maka dapat ditarik kesimpulan bahwa tandatangan digital dapat mengesahkan dan mejamin integritas kuitansi digital. Penggunaan sertifikat digital dalam penandatanganan dapat memberikan informasi mengenai penandatangan.

Kata kunci:tanda-tangan digital,sertifikatdigital, kuitansi digital, servlet, jsp

Abstract

Receipts in digital form has several advantages over receipts in physical form in terms of the ease of storage, transport and manufacture of its reserves. But the difficulty of doing validation and verification as well as the vulnerability of digital data to be manipulated to make digital receipt is rarely used today.In this study, the authors construct a public key infrastructure which is used to take over management of digital certificates. Digital certificate is a digital data containing information on the ownership of a public key pair and a private key. Endorsement receipts done by digitally signing the receipt verification process, while the private key using the public key pair. By signing is expected if there is a change in the digital receipt can be known. This research method is to analyze system requirements, system design, system build, testing, analyzing test results and draw conclusions. The final aim is to investigate the use of public key infrastructure for authentication and assurance services information on the digital receipt The results of this study form an integrated system for the manufacture and penandatangananan digital receipt. The test results showed little change in the digital receipt is signed cause status after signature becomes invalid. It can be concluded that digital signatures can certify and assure the integrity of the digital receipt. The use of digital certificates in the signing can provide information about the signer.

Keywords:digital signature, digital certificate, digital receipt, servlet, jsp

1. Pendahuluan

Kuitansi umum digunakan sebagai tanda bukti dalam setiap transaksi yang terjadi sekarang ini. Namun Kuitansi yang ada sekarang ini umumnya memiliki dua kendala yang cukup serius yakni susah dilakukannya backup Kuitansi dan keretanan Kuitansi terhadap kerusakan. Salah satu cara penanggulangan kendala ini dengan cara mendigitalisasi Kuitansi.

Pemegang Kuitansi digital dapat membackup Kuitansinya cukup dengan menggandakan file kuitansi tersebut dan menyimpannya dibeberapa tempat seperti laptop, smartphone bahkan tempat pennyimpanan online. Sehingga bila salah satu file hilang atau rusak si pemegang Kuitansi masih memiliki cadangan file di tempat lain. Selain itu bila Kuitansi disimpan di tempat penyimpanan online maka pemilik Kuitansi dapat mengakses Kuitansinya dari manapun selama dia terhubung dengan internet.

Namun penggunaan kuitansi digital bukan berarti tanpa kendala. Kuitansi harus dapat diverifikasi oleh otoritas yang mengeluarkannya dan tidak boleh diubah. Sedangkan data digital rentan untuk diubah dan dimanipulasi sehingga sulit menjadikan dokumen digital sebagai suatu tanda bukti. Maka dibutuhkan suatu metode agar suatu Kuitansidigital tidak mudah diubah dan dapat diautentikasi keabsahan pembuatnya.

Tanda tangan digital merupakan salah satu solusi permasalahan ini. Dengan menggunakan tanda tangan digital maka pada sebuah data digital yang telah ditandatangani dapat dibuktikan telah terjadi perubahan atau tidak. Serta siapakah penandatangan data digital tersebut.

Secara umum terdapat dua komponen dalam tanda tangan digital yakni fungsi hash dokumen dan kriptografi kunci publik untuk mengenkripsi fungsi hash tersebut. Fungsi hash berfungsi sebagai penguji terhadap dokumen telah ada perubahan atau tidak. Sedang kriptografi kunci publikberfungsi memberikan informasi penandatangan data digital tersebut.

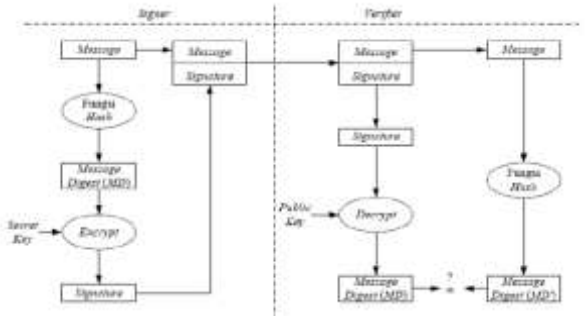
Pada kriptografi kunci publik yang digunakan dalam tanda tangan digital maka dibutuhkan suatu Infrastruktur Kunci Publik (IKP) yang berfungsi mengikat suatu kunci publik dengan pemilik kunci publik tersebut. Dengan adanya ikatan ini maka meyakinkan pemilik dokumen bahwa dokumen digital telah ditanda-tangani oleh pihak yang berwenang menandatangani.

Penelitian ini ditujukan untuk merancang penggunaan Kuitansi digital menggunakan infrastruktur kunci publik dengan studi kasus suatu layanan bukti digital pembayaran kursus bahasa inggris.
Tujuan penelitian ini adalah merancang suatu infrasturktur kunci publik yang mampu melayani pembuatan maupun validasi tanda tangan digital sehingga dapat digunakan untuk layanan nota digital yang menggantikan nota fisik.

2. Metode

2.1. Penandatanganan Dokumen Digital

Penandatanganan suatu dokumen digital terbagi atas tiga langkah yakni:
1. Menghitung nilai hash dokumen.
2. Mengenkripsi nilai yang di dapat menggunakan kunci privat pemilik tanda tangan.
3. Menambahkan tanda tangan pada file dokumen.



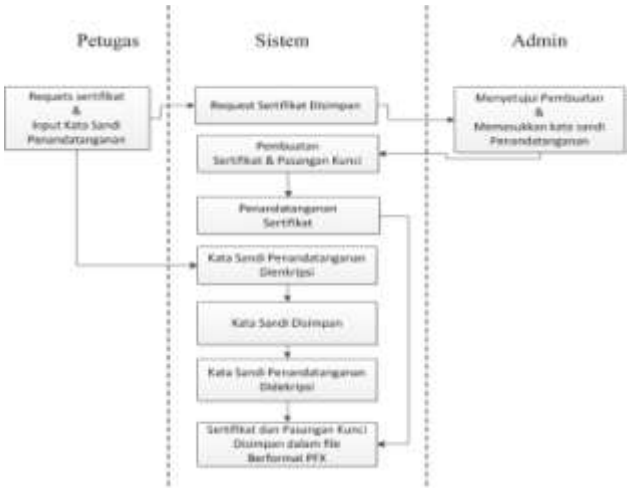
Gambar1. Alur Proses Penandatanganan dan Pemeriksaan Tanda Tangan Digital

Sedang proses pemeriksaan keabsahan suatu tanda tangan digital dapat dilakukan dalam lima langkah yakni:
1. Memisahkan dokumen asli dan tanda tangan dari file digital.
2. Mendekripsi tanda tangan sehingga dihasilkan nilai hash tanda tangan.
3. Menghitung nilai hash dokumen sehingga dihasilkan nilai hash perhitungan.
4. Membandingkan nilai hash tanda tangan dengan nilai hash perhitungan jika sama maka dokumen tak pernah diubah sejak ditandatangani.
5. Jika langkah 4 telah dilalui dengan baik maka periksa status dan lembaga penjamin tanda tangan.

Gambaran alur proses penandatanganan dan pemeriksaan tanda tangan digital dapat dilihat pada Gambar 1.

2.2. Pembuatan Sertifikat Digital

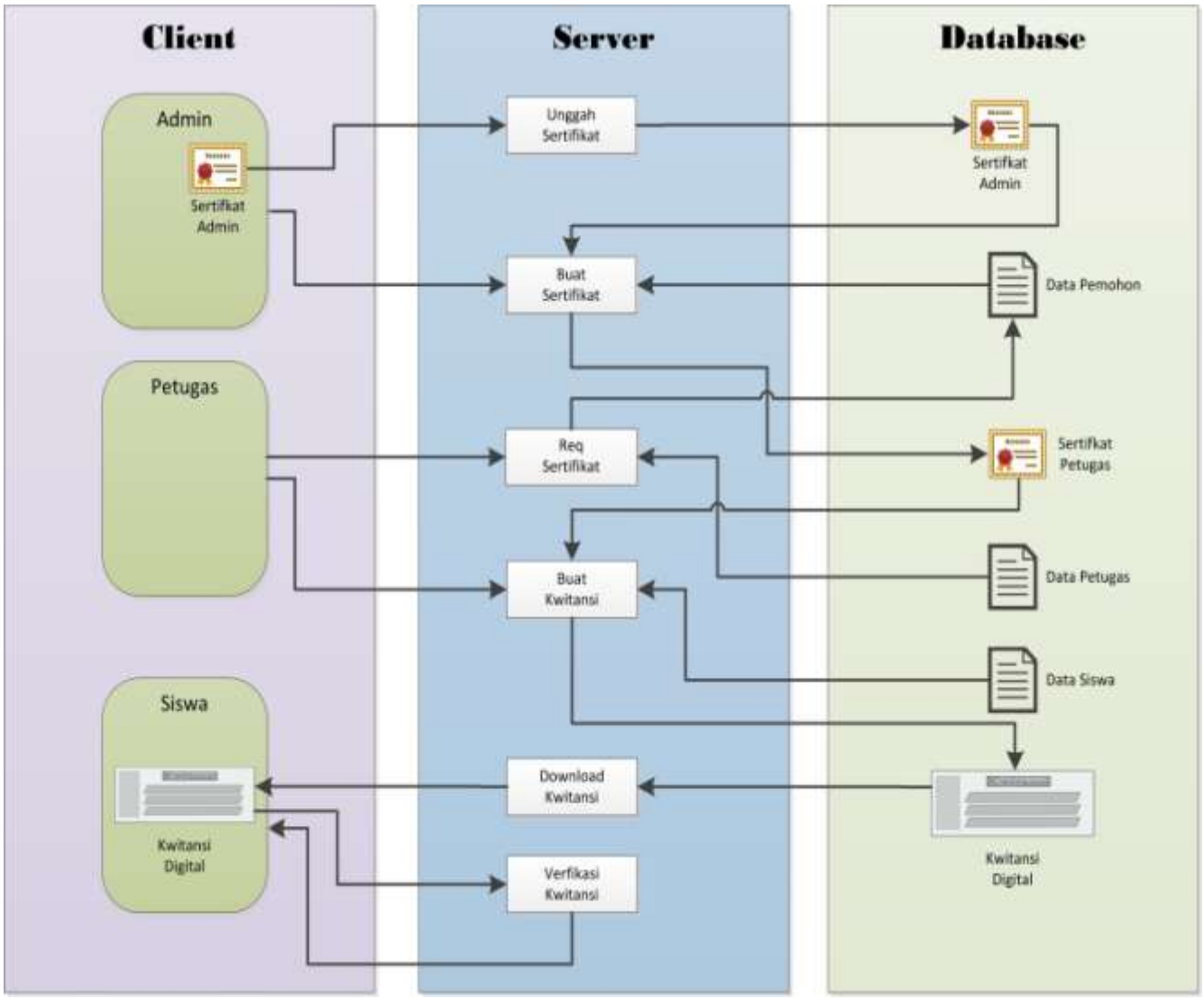
Alur proses pembuatan sertifikat digital untuk petugas tata usaha oleh admin terdiri atas empat langkah berikut:



1. Permintaan pembuatan sertifikat dari petugas tata usaha beserta penyertaan kata sandiyang akan digunakan untuk penandatanganan.
2. Pengenkripsian kata sandi yang telah dimasukkan petugas oleh sistem.
3. Pembuatan dan penandatanganan pasangan kunci publi-kunci privat beserta sertifikat digital petugas oleh admin.
4. Penyimpanan kunci publik-kunci privat beserta sertifikat digital petugas ke dalam file pfx yang diamankan menggunakan kata sandi yang telah dimasukkan petugas

Gambaranalur proses pembuatan sertifikat digital dapat dilihat pada Gambar 2.

Gambar2. Alur Proses Pembuatan Sertifikat Digital Petugas



Gambar 3. Gambar Umum Alur Kerja Sistem

2.3. Pembuatan Kuitansi Digital

Alur proses pembuatan kuitansi digital oleh petugas tata usaha terdiri atas tiga langkah berikut:

1. Pemasukan informasi untuk kuitansi sekaligus kata sandi untuk melakukan penandatanganan.
2. Sistem membuat kuitansi dalam bentuk pdf bedasarkan informasi yang telah dimasukkan
3. Sistem melakukan penandatanganan pada kuitansi yang telah dibuat.

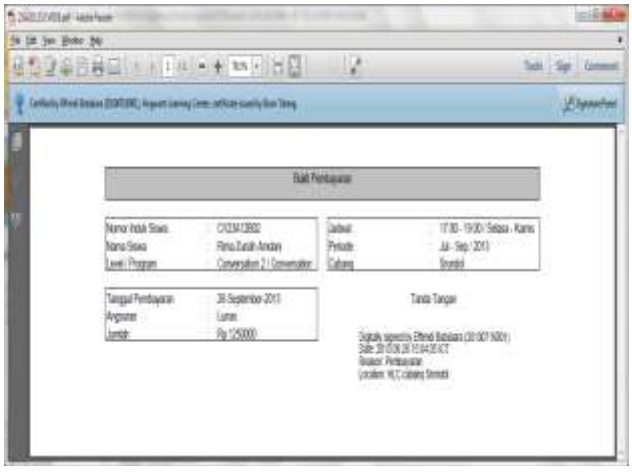
2.4. Gambaran Umum Alur Kerja Sistem

Sistem yang dibangun merupakan suatu layanan infrastruktur kunci public sederhana sebagai penyokong utama layanan tanda pembayaran digital atau kuitansi digital. Studi kasus dalam penelitian ini adalah pengembangan system tanda pembayaran digital suatu lembaga kursus bahasa inggris. Terdapat tiga actor utama dalam system yakni admin, petugas tata usaha dan siswa. Skema hubungan antara admin, petugas dan siswa dapat dilihat pada Gambar 3.

3. Hasil dan Analisis

3.1. Hasil Pembuatan Kuitansi Digital

Hasil pembuatan kuitansi digital dapat dilihat pada Gambar 4. Pada gambar tersebut telihat pita berwarna biru pada pojok kanan atas. Pita tersebut mengindikasikan bahwa kuitansi digital belum pernah dilakukan peubahan semenjak ditandatangani serta lembaga penjamin keabsahan tanda tangan digital merupakan lembaga yang terpercaya.

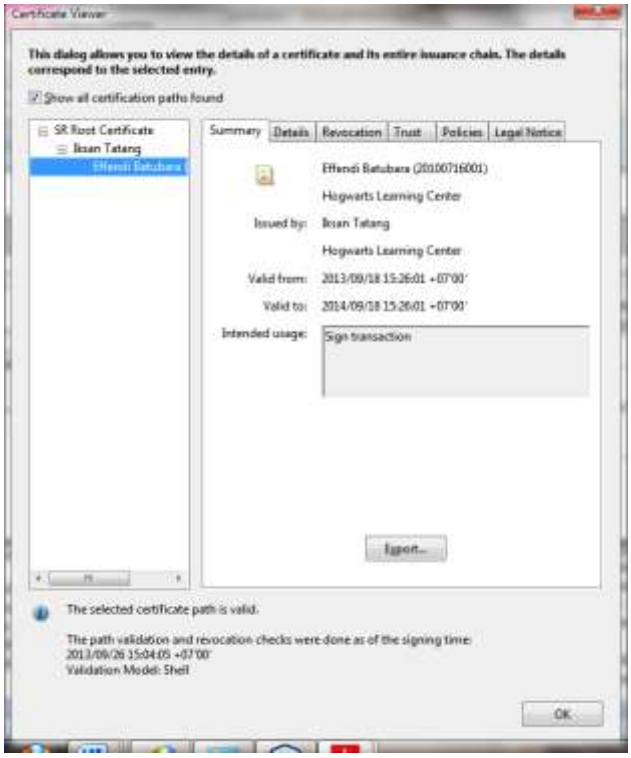


Gambar 4. Tampilan Kuitansi Digital yang Absah

Untuk melihat informasi mengenai penandatangan dapat dilakukan klik kiri pada area tanda tangan maka akan muncul sertifikat digital yang menyimpan informasi mengenai penandatangan beserta penjaminnya seperti terlihat pada Gambar 5.

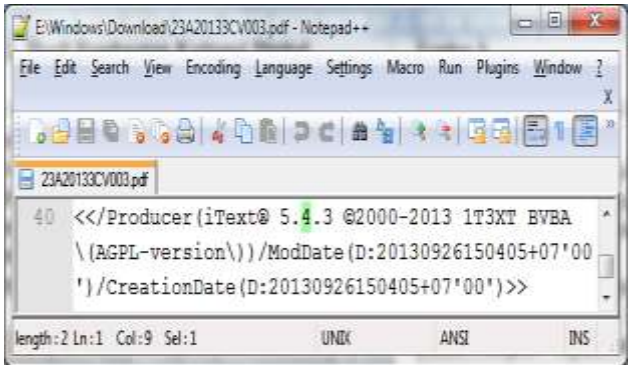
3.2. Percobaan Pengubahan Kuitansi

Percobaan pengubahan kuitansi dilakukakan untuk melihat reaksi yang terjadi pada kuitansi bila dilakukan pengubahan data pada kuitansi.



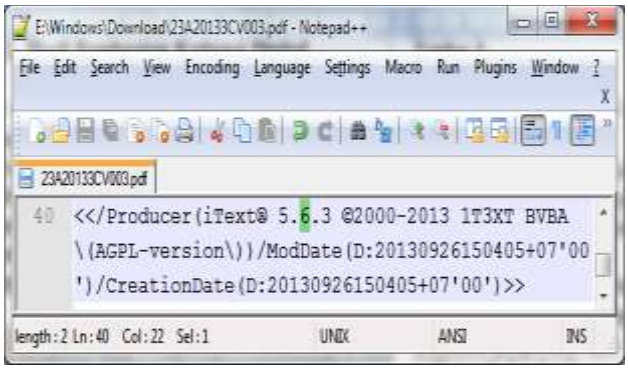
Gambar 5. Tampilan Sertifikat Digital

Gambar 6 memperlihatkan baris keempat puluh kuitansi digital yang dibukan dengan program Notepad++. Dilakukan pengubahan data melalui Notepad++ seperti terlihat pada Gambar 7.

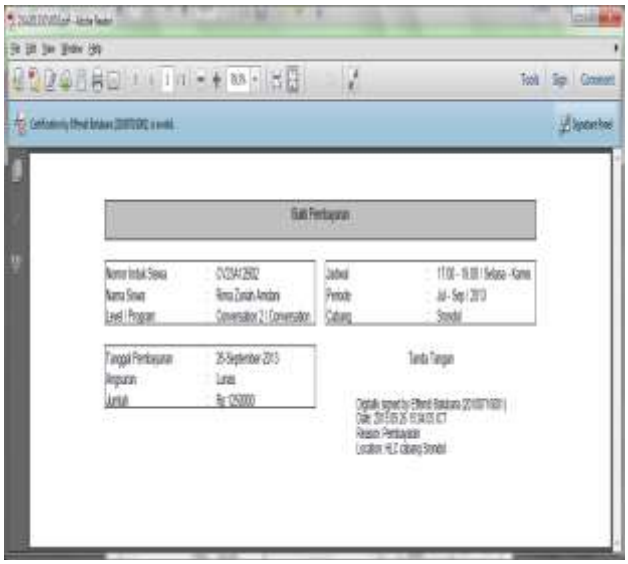


Gambar 6. Tampilan Baris ke-40 Kuitansi Digital

Bila kuitansi yang telah diubah dibukan menggunakan program Adobe Reader maka terlihat tanda pita biru di pojok kiri atas telah berubah menjadi tanda dokumen yang disilang seperti terlihat pada Gambar 8.



Gambar 7. Tampilan Pengubahan Baris ke-40 Kuitansi Digital



Gambar 8. Tampilan Kuitansi Digital yang Tidak Absah

3.3. Analisis

Pada dasarnya konsep tandatangan digital merupakan suatu algoritma yang digunakan untuk menjamin bahwa dokumen yang telah ditandatangani tidak pernah diubah setelah penandatanganan. Selain itu tandatangan digital juga menjamin bahwa dokumen ditandatangani oleh pemilik kunci privat.

Hasil pada percobaan mengindikasikan bahwa dengan menggunakan sertifikat digital maka informasi mengenai penandatangan serta lembaga penjamin dapat diketahui seperti pada Gambar 5 serta bila ada pengubahan sedikit saja pada dokumen digital yang telah ditandatangani maka tanda tangan digital yang disertakan tidak lagi absah seperti terlihat pada Gambar 8.

Dua hal ini mengindikasikan tanda tangan digital yang disertai sertifikat digital dapat menjamin keabsahan kuitansi digital karena identitas penandatangan serta indikasi adanya perubahan pada kuitansi dapat diketahui.

4. Kesimpulan

Berdasarkan perancangan, implementasi, dan pengujian penelitian yang berjudul ”Perancangan Infrastruktur Kunci Publik Dengan Implentasi Layanan Bukti Digital Pembayaran Kursus Bahasa Inggris”, maka dapat diambil beberapa kesimpulan sebagai berikut. Kuitansi digital dapat digandakan beberapa kali tanpa merubah validitas kuitansi. Perubahan pada isi kuitansi menyebabkan tidak validnya tanda tangan pada kuitansi. Tingkat kepercayaan terhadap tandantangan digital semakin tinggi bila dikeluarkan oleh otoritas penyedia layanan tandantangan digital yang terpercaya. Pembubuhan informasi identitas penandatangan dan aturan penggunaan tanda tangan dapat dilakukan dengan menyertakan sertifikat digital saat penandatanganan. Layanan infrastruktur kunci publik berfungsi untuk menerbitkan, mengelola dan menarik sertifikat digital. Saran penulis kedapannya dapat digunakna protokol penanda waktu dan ocsp untuk lebih menjamin keamanan dari kuitansi digital maupun sertifikat digital yang ditandatangani.

Referensi

[1] Siegfried Weinmann, 2006, Digital Documents Does our saved knowledge have a safe future?, London Metropolitan University, London.
[2] Ir. Rinaldi Munir M.T., Otentikasi dan Tandatangan Digital, ITB, Bandung
[3] Klaus Schmeh, 2003, Cryptography and Public Key Infrastructure on the Internet, John Wiley & Sons, Chichester, West Sussex, England.
[4] Ivan Wibowo , Budi Susanto, Junius Karel T, 2009, Penerapan Algoritma Kriptografi Asimetris Rsa Untuk Keamanan Data Di Oracle, Jurnal Informatika.
[5] Aditya Pratama, 2010, Studi Perbandingan dan Implementasi Kombinasi Fungsi Hash dan Kriptografi Kunci-Publik, ITB, Bandung.
[6] Ricky Gilbert Fernando, 2007, Penggunaan Fungsi Hash Dalam Kriptografi Penggunaan Fungsi Hash DalamKriptografi, ITB, Bandung.
[7] Muhamad Zaki Riyanto, Sistem Kriptografi Kunci Publik Multivariat, UGM, Yogyakarta.
[8] FIPS PUB 186-1, 1998, Digital Signature Standard (DSS), U.S. Department Of Commerce.
[9] Lala Septem Riza , 2006, Digital Timestamping: Suatu Tinjauan Komprehensif dan Usulan Model Skema Implementasi, ITB, Bandung.
[10] Amir Manzoor, 2010, E-Commerce: An Introduction, Lap Lambert Academic Publishing, Saarbrucken, Germany.
[11] Riyanto, Suprapto, Hendi Inderlarko, 2008, Tuntunan Praktirs Pengembangan Aplikasi Manajemen Database dengan Java 2 (SE/ME/EE), Gaya Media, Yogyakarta.
[12] Nur Widiyanto, 2010, Aplikasi Java Enterprise dengan Arsitektur Model View Controller (MVC), Penerbit Andi, Yogyakarta.
[13] Sri Hartati Wijono S.Si, B Herry Suharto, Matius Soesilo Wijono, 2007 Pemrograman Java Servlet dan JSP dengan Netbeans, Penerbit Andi, Yogyakarta.
[14] The Java EE 5Tutorial, Oracle.

[15] Glend S. Maatita, Febriliyan Samopa, Radityo Prasetianto Wibowo, Pengembangan Aplikasi Manajemen Proyek Perangkat Lunak Berbasis Spring : Modul Core System Dan Manajemen Source Code , ITS, Surbaya.
[16] Febrian Setiadi , XML Digital Signature pada wireless Web services, ITB, Bandung.
[17] Jon Ellis, Linda Ho, Maydene Fisher, 2001, JDBC 3.0 Specification, Sun Microsystems, Inc.
[18] Abdul Kadir, 2009, Dasar Perancangan & Implementasi Relasional, Penerbit Andi, Yogyakarta.
[19] Janet Valade, 2010, PHP & MySQL(R) For Dummies(R), 4th Edition, Wiley Publishing, Inc. Indianapolis, indiana, USA.
[20] Rosa A.S., M. Shalahuddin, 2011, Modul Pembelajara Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi