Computer Based Information System Journal

ISSN (Print): 2337-8794 | E- ISSN : 2621-5292
web jurnal : http://ejournal.upbatam.ac.id/index.php/cbis

PERANCANGAN INFRASTRUKTUR KUNCI PUBLIK DENGAN IMPLEMENTASI PEMBANGUNAN SISTEM UJIAN DARING BERBASIS WEB

Hermawan Setiawan, Adek Muhammad Zulkham Ristiawan Kertanegara
Politeknik Siber dan Sandi Negara, Indonesia.

INFORMASI ARTIKEL

Diterima Redaksi: Februari
Diterbitkan *Online*: Maret

KATA KUNCI

Public Key Infrastructure, Online Exam System, Covid-19

KORESPONDENSI

E-mail: hermawan.setiawan@poltekssn.ac.id

A B S T R A C T

During the Covid-19 pandemic, almost all educational institutions in Indonesia are implementing Distance Learning (PJJ). Like learning in general, in each semester an exam will be held, be it the Midterm Exam or the End of Semester Exam, and of course the exam takes place remotely. This has caused concerns from teachers to their students about the method of distributing exam questions and sending exam answer sheets. In other words, it is difficult for teachers to ensure the safety of the distribution of questions, as well as to carry out endorsements and verifications on the exam answer sheets collected by their students. In this study, the authors built a public key infrastructure implemented in a web-based online exam system with an approach to encryption and digital signatures. Encryption and digital signatures are two commonly used primitive cryptography that can provide security services, such as confidentiality, integrity, and authenticity of messages. It is hoped that with this research, we can find out the implementation of public key infrastructure in the web-based online examination system..

I. Latar Belakang

Ujian merupakan sebuah hal yang pasti dilaksanakan di seluruh lembaga pendidikan di Indonesia. Hal ini menjadi sangat krusial karena hasil ujian menentukan kemampuan siswa dalam memahami sebuah materi dan juga menentukan apakah siswa tersebut naik tingkat atau tidak ke semester selanjutnya[1]. Namun semenjak Covid-19 menyerang, ujian pun dilaksanakan secara jarak jauh atau daring[2]. Apalagi pemerintah Indonesia memberlakukan PSBB (Pembatasan Sosial Berskala Besar)

Berdasarkan survey yang dilakukan oleh KPAI [3], sebesar 12.9% responden tidak setuju ujian dilaksanakan secara daring, mereka mengusulkan ujian secara tertulis, yaitu semua soal diambil dan dikembalikan orangtua ke sekolah secara mandiri. Hal ini tentu menimbulkan permasalahan baru dari masalah sistem ujian daring yang sudah ada.

Salah satu masalah sistem ujian daring adalah susahnya pihak pengajar untuk memastikan apakah siswa mengerjakan soal tersebut dengan kemampuannya sendiri, alias

tidak mencontek. Masalah lain yang muncul adalah bagaimana cara pengajar memvalidasi bahwa lembar jawaban soal milik siswa asli dan belum pernah dirubah atau dimodifikasi oleh pihak-pihak yang tidak berwenang[4].

Pada penelitian ini, ditawarkan metode untuk mengatasi masalah sistem ujian daring, yaitu menggunakan enkripsi dan tanda tangan digital. Enkripsi dan tanda tangan digital adalah dua kriptografi primitif yang umum digunakan yang dapat memberi layanan keamanan, seperti kerahasiaan, integritas, dan keaslian pesan. IKP atau Infrastruktur Kunci Publik adalah infrastruktur yang mendukung pengoperasian kedua aplikasi kriptografi tersebut [5].

Penelitian ini ditujukan untuk merancang sistem ujian daring berbasis web menggunakan infrastruktur kunci publik.

II. Kajian Literatur

Salah satu implementasi dari infrastruktur kunci publik adalah penelitian oleh [6]. Pada penelitian tersebut Alwin beserta rekan rekannya merancang penggunaan kuitansi digital menggunakan infrastruktur kunci publik dengan studi kasus layanan bukti digital pembayaran kursus bahasa inggris. Infrastruktur kunci publik yang dibangun memanfaatkan metode tanda tangan digital, sehingga nota pembayaran yang bermula berbentuk nota fisik dapat berubah menjadi nota digital. Dengan menerapkan infrastruktur kunci publik diharapkan mampu melayani pembuatan maupun validasi tanda tangan digital sehingga dapat digunakan untuk layanan nota digital [7].

Pada penelitian [8] berjudul "E-Governance Public Key Infrastructure (IKP) Model", menjelaskan tentang implementasi infrstruktur kunci publik pada e-governance. Infrastruktur kunci publik yang menggunakan sertifikat digital X.509 dapat memberikan kerangka kerja yang bagus untuk menangani layanan pemerintah dan masalah dengan integritas tingkat tinggi. Rancangan infrastruktur kunci publik ini diharapkan mampu mempermudah penyampaian layanan kepada warga negara secara efisien dan dengan biaya yang terjangkau [9].

IKP adalah kerangka kerja yang terdiri dari perangkat keras, perangkat lunak, kebijakan, dan prosedur untuk mengelola kunci dan sertifikat[10]. Agar kerangka kerja ini berfungsi, Anda memerlukan berbagai komponen IKP. Komponen-komponen tersebut adalah [5]:

a. *Certificate Authority* (CA)

CA adalah pihak ketiga tepercaya yang mengotentikasi entitas yang mengambil bagian dalam transaksi elektronik[11]. Untuk mengotentikasi entitas, CA mengeluarkan sertifikat digital. Sertifikat ini adalah dokumen digital yang menetapkan kredensial entitas yang berpartisipasi dalam transaksi. Sertifikat digital yang dikeluarkan oleh CA berisi informasi, seperti nama pelanggan, kunci publik dan pribadi pelanggan, dan kunci publik CA yang menerbitkan. Informasi ini tergantung pada kebijakan perusahaan yang mengeluarkan sertifikat.

Sebelum menerbitkan sertifikat digital, CA memverifikasi permintaan sertifikat dengan Otoritas Registrasi (RA). Untuk memvalidasi permintaan sertifikat, CA menggunakan prosedurnya sendiri. Prosedur ini bergantung pada kebijakan organisasi dan infrastruktur yang tersedia untuk memvalidasi permintaan. Jika permintaan divalidasi, CA mengeluarkan sertifikat.

b. Registration Authority (RA)

RA bertanggung jawab atas interaksi antara klien dan CA[12]. Seringkali, karena banyaknya permintaan sertifikat, CA tidak mungkin menerima permintaan sertifikat, memvalidasi permintaan, dan menerbitkan sertifikat. Sehingga, RA bertindak sebagai perantara antara CA dan klien. Beberapa tugas RA adalah:

- Menerima permintaan entitas dan validasikan
- Kirim permintaan ke CA
- Menerima sertifikat yang diproses dari CA
- Kirim sertifikat ke entitas yang benar

c. IKP *Clients* (Entitas)

Entitas yang meminta CA atau RA untuk menerbitkan sertifikat biasanya disebut sebagai

IKP Clients. Semua komunikasi antara klien dan CA tetap aman. Selain itu, klien bertanggung jawab untuk memastikan keamanan kunci pribadinya. Ini karena jika kunci pribadi hilang, maka pesan terenkripsi tidak dapat didekripsi.

d. *Digital Certificate*

Komponen penting dari penyebaran IKP adalah sertifikat digital[13]. Sertifikat ini menjadi dasar penerapan solusi IKP. Sertifikat memastikan bahwa hanya kunci publik untuk sertifikat yang telah diautentikasi oleh otoritas sertifikasi yang bekerja dengan kunci privat yang dimiliki oleh suatu entitas[14]. Ini menghilangkan kemungkinan peniruan identitas.

Isi dari sertifikat digital[15] adalah :

- Nomor seri dari sertifikat digital
- Tanda tangan digital dari CA
- Public key entitas yang memiliki sertifikat digital tersebut
- Identitas entitas yang memiliki sertifikat tersebut
- Tanggal kadaluarsa sertifikat digital
- Identitas dari CA yang mengeluarkan sertifikat digital.

e. Certificate Distribution System atau Repository

Certificate Distribution System (CDS) mendistribusikan sertifikat kepada pengguna dan organisasi. Sertifikat ini dapat didistribusikan dalam dua cara tergantung pada implementasi IKP di organisasi[16]. Baik sertifikat dapat didistribusikan oleh pengguna sendiri atau mereka dapat didistribusikan oleh server direktori yang menggunakan LDAP untuk menanyakan informasi pengguna yang disimpan dalam database yang sesuai dengan X.500[17]. CDS mendistribusikan sertifikat bekerja sama dengan server layanan direktori.

Tujuan dari IKP adalah memberikan kepercayaan dan keamanan pada komunikasi elektronik. Pada IKP juga terdapat pasangan kunci untuk menjaga keamanannya [5].

Langkah-langkah yang terlibat dalam kerja IKP adalah[18] :

- Menghasilkan pasangan kunci
- Menerapkan tanda tangan digital untuk mengidentifikasi pengirim
- Mengenkripsi pesan
- Mengirimkan kunci simetris
- Memverifikasi identitas pengirim dengan menggunakan CA
- Mendekripsi pesan dan memverifikasi isinya.

Arsitektur IKP mencerminkan pengaturan CA dalam suatu organisasi dan hubungan antara masing-masing CA[19]. Maksudnya adalah bagaimana hubungan antara beberapa entitas atau CA untuk saling percaya terhadap sertifikat digital yang sudah dikeluarkan. Terdapat tiga jenis utama arsitektur IKP [20], yaitu:

- *Single CA Architecture*

Ini merupakan arsitektur yang paling dasar, yang mana hanya ada satu CA yang membuat serta mendistribusikan sertifikat. Sehingga masing-masing entitas saling mempercayai satu sama lain

- Arsitektur IKP Enterprise

Arsitektur IKP ini dapat diimplementasikan dalam dua cara, baik atasan-bawahan (hierarchial IKP architecture) atau *peer-to-peer* (mesh IKP architecture).

- Arsitektur IKP Hybrid

Ada tiga jenis arsitektur hybrid IKP, yaitu: Arsitektur Daftar Kepercayaan yang Diperluas; IKP perusahaan bersertifikat silang; dan Arsitektur jembatan CA[21].

Jalur sertifikasi (*certification path*) adalah rangkaian sertifikat, di mana entitas yang telah mengeluarkan sertifikat pertama adalah titik kepercayaan [5].

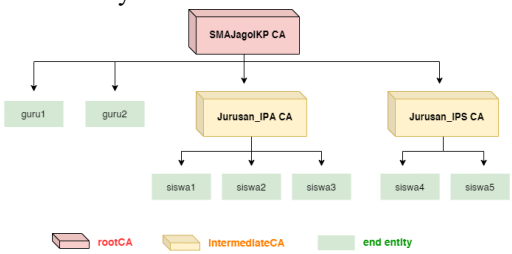
Validasi jalur sertifikat adalah proses yang melibatkan validasi setiap sertifikat di jalur sertifikasi untuk menentukan apakah kunci dalam sertifikat dapat dipercaya atau tidak [5].

III. Metodologi

3.1 Arsitektur IKP yang Digunakan

Arsitektur IKP yang digunakan pada penelitian ini adalah *Hierarchial IKP Architecture* atau

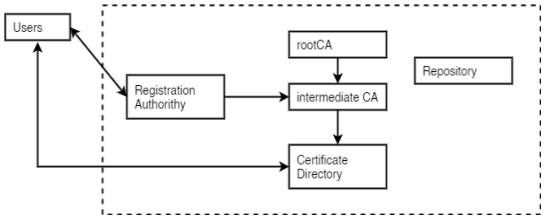
Arsitektur Hierarki[22]. Berikut skema arsitekturnya:



Gambar 1. Arsitektur IKP

Entitas tertinggi adalah rootCA bernama SMAJagoIKP.ca yang memiliki dua intermediateCA bernama Jurusan_IPA.ca dan Jurusan_IPS.ca dan juga merupakan CA yang mengeluarkan sertifikat milik guru yang diperbarui (*revoke*) setiap 5 tahun sekali dan atau dihapus ketika guru tersebut sudah tidak mengajar di sekolah terkait. Sedangkan pada setiap intermediateCA mengeluarkan sertifikat milik siswa dengan jadwal revoke setiap tahun dan atau dihapus ketika siswa tersebut sudah tidak menempuh pendidikan di sekolah terkait.

3.2 Komponen IKP dan Alur Pembuatan Sertifikat Digital



Gambar 2. Komponen IKP

Komponen IKP dari penelitian ini adalah *rootCA,* entitas CA tertinggi; *intermediateCA,* entitas CA yang di tanda tangani rootCA; *Certificate Directory*, tempat menyimpan semua sertifikat yang dikeluarkan; *Repository,* tempat penyimpanan sertifikat yang dicabut (pengarsipan); *Registration Authority (RA);* entitas untuk memastikan data user; dan *Users;* entitas akhir yang mana merupakan individu perorangan[23].

Alur proses pembuatan sertifikat digital berdasarkan gambar diatas terdiri atas lima langkah[24] yakni:

1) Users mengirimkan data diri lengkap kepada RA, yang mana RA merupakan pihak sekolah bagian Tata Usaha, untuk selanjutnya di cek dan diverifikasi kebenarannya.
2) RA juga membuatkan kunci privat milik user dan mengenerate kata sandi untuk penandatanganan. Selanjutnya kunci privat beserta sandi dikirimkan ke intermediateCA dan juga *Users*.
3) Semua data dari RA dikirim ke intermediateCA untuk dibuatkan *Certificate Signing Request* (CSR) berdasarkan data yang sudah ada.
4) Selanjutnya CSR ditandatangani oleh rootCA menggunakan kunci privat rootCA sehingga akan menjadi format .crt (sertifikat sesungguhnya)
5) Sertifikat yang sudah di tandatangani disimpan di database, dan sertifikat tersebut dapat diakses oleh seluruh Users. Sertifikat yang sudah dihapus akan disimpan pada *Repository*.

3.3 Alur Penandatanganan dan Verifikasi Dokumen Digital

Penandatanganan dokumen digital terbagi atas tiga langkah [6] yakni:

1) Menghitung nilai hash dokumen.
2) Mengenkripsi nilai yang di dapat menggunakan kunci privat pemilik tanda tangan, sehingga menghasilkan signature.
3) Menambahkan atau *concate* tanda tangan pada file dokumen.

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.
6.

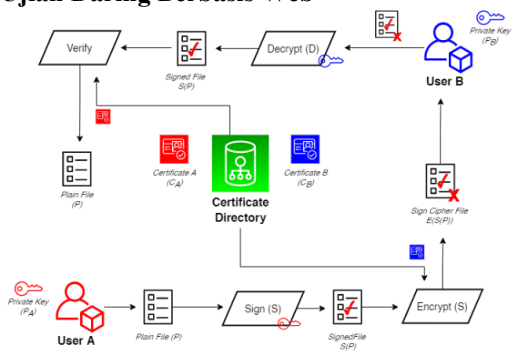
5.4 Alur Proses Enkripsi dan Dekripsi Dokumen Digital

Berdasarkan gambar diatas, proses enkripsi dilakukan oleh *Sender* menggunakan kunci publik milik *Receiver* sehingga menjadi file terenkripsi. Sedangkan di sisi *Receiver* akan mendekripsi pesan terenkripsi dari *Sender* menggunakan kunci privat miliknya.

5.5 Ilustrasi Penyediaan Layanan Antar Users

Sesuai gambar diatas, setiap user memiliki layanan yang sama, user dalam hal ini adalah guru dan siswa, yaitu Autentikasi, Enkripsi dan Dekripsi. Hal ini dilakukan pada penelitian ini karena antar user harus bisa saling mengirim dan mengautentikasi.

5.6 Gambaran Umum Alur Kerja Sistem Ujian Daring Berbasis Web



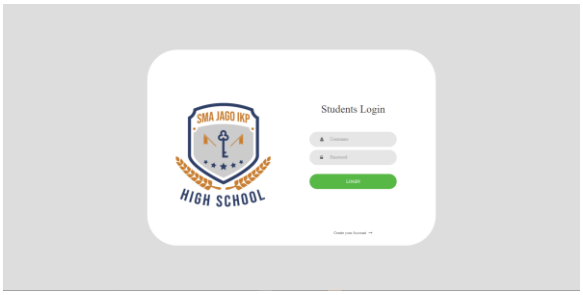
Gambar 3. Rancangan sistem IKP ujian daring

Sistem yang dibangun menerapkan layanan infrastruktur kunci publik sederhana sebagai penyokong layanan ujian daring berbasis web. Studi kasus dalam penelitian ini adalah pengembangan sistem enkripsi dan tanda tangan digital dari dokumen pada saat pengiriman maupun pengumpulan hasil jawaban ujian daring berbasis web. Skema proses kerja antar user dapat dilihat pada gambar diatas..

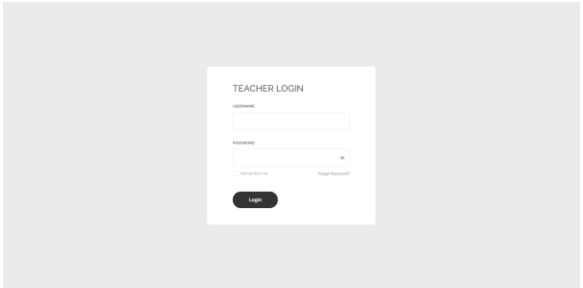
IV. Pembahasan

4.1. Tampilan Login Website

Nama dari website yang dibangun adalah "SMA JAGO IKP Learning System", wesbite dibangun menggunakan PHP 8 dan HTML. Terdapat dua website yaitu; sebagai siswa, dan sebagai guru.



Gambar 4. Halaman Login website siswa



Gambar 5. Halaman Login website guru

4.2. Menu Website

Pertama kali memasuki website, setelah berhasil login, kita akan langsung disuguhkan halaman awal yang berisi menu dari website ini.

Gambar 6. Halaman awal website siswa

Gambar 6 merupakan halaman awal ketika login pada laman siswa, langsung akan dipaparkan menu-menu dari website ini, yang terdiri dari:

- *Home*, menampilkan halaman awal website

- Download, untuk mendownload soal yang diberikan oleh guru.
- *Verify*, untuk memverifikasi dan dekripsi soal yang diberikan oleh guru
- *Upload*, untuk mengirim jawaban kepada guru yang bersangkutan, yang terlebih dahulu akan dienkripsi dan di tanda tangani
- *Cert Directory*, menu untuk Download sertifikat milik seluruh Civitas Akademika, baik siswa atau guru
- Logout.

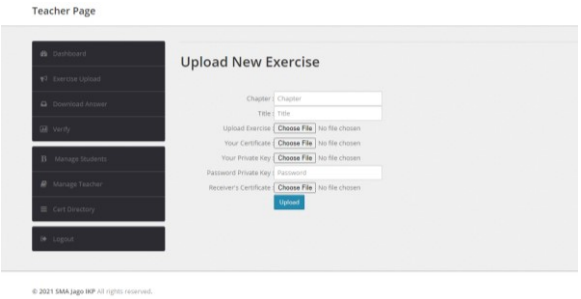
Gambar 7. Halaman awal website guru

Gambar 7 merupakan halaman awal ketika login pada laman guru, menu-menu yang diberikan hampir sama seperti pada laman siswa, yaitu Dashboard, Upload Exercise, Download Answer, Verify, Cert Directory, dan Logout.

Sedangkan fitur tambahan pada laman guru ini adalah Manage Student, yaitu menu untuk mengatur data murid atau siswa; dan Manage Teacher, untuk melihat dan mengatur data guru.

4.3 Proses Pengiriman Soal dan Jawaban

Ketika guru atau siswa ingin mengirim soal maupun jawaban, mereka harus masuk ke menu Upload di masing-masing laman. Untuk guru masuk ke menu Upload Exercise lalu tekan New, berikut tampilan pada laman guru ketika ingin menambahkan soal baru.



Gambar 8. Halaman upload soal baru

Akan ditampilkan beberapa inputan yang harus dimasukkan oleh guru, yaitu:

- *Chapter*, adalah nama atau jenis ujian, contoh : Ujian Akhir Semester
- Tittle, adalah judul ujian dan juga untuk siapa soal tersebut, contoh : matematika_adek
- *Upload Exercise*, berisi file soal yang akan di upload
- *Your Certificate*, berisi sertifikat (.crt) milik guru yang sebelumnya sudah dibagikan oleh bagian Tata Usaha atau dapat juga didownload pada menu Cert Directory
- *Your Private Key*, berisi file *private key* (.pem) milik guru yang sebelumnya sudah dibagikan oleh bagian Tata Usaha
- *Password Private Key*, adalah password dari file *private key* yang sudah diinputkan sebelumnya
- *Receiver Certificate*, berisi sertifikat (.crt) milik siswa, dalam ini adalah penerima, sertifikat dapat di download pada menu Cert Directory.

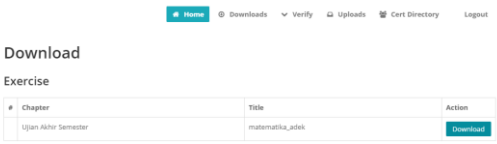
Lalu klik Upload untuk mengirim soal tersebut. Proses yang sama juga berlaku untuk siswa dalam hal mengirim jawaban kepada guru yang bersangkutan. Inputan yang dimasukkan sama, dikarenakan seluruh proses kirim mengirim pada website ini dilakukan dengan enkripsi dan tanda tangan digital[25].

4.4 Proses Download dan Verifikasi Soal dan Jawaban

Sebelumnya sudah dipaparkan bagaimana proses mengupload soal dan jawaban, sekarang adalah proses untuk mendownload dan memverifikasi

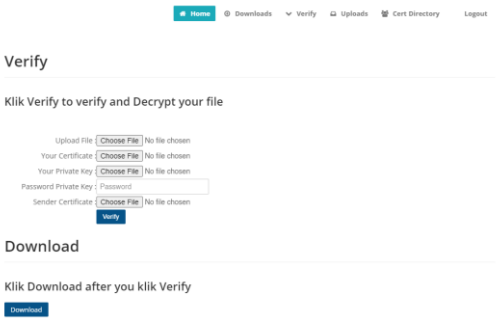
soal maupun jawaban tersebut. Perlu kita ingat bahwa seluruh file yang dikirim di website ini akan melalui proses enkripsi dan tanda tangan digital, sehingga jika kita ingin dapat membaca isi file tersebut, kita harus memverifikasi dan mendekripsi file tersebut.

Ketika guru atau siswa ingin mendownload soal maupun jawaban, mereka harus masuk ke menu Download di masing-masing laman, sedangkan untuk verifikasi dapat masuk ke menu Verify. Untuk siswa dapat masuk ke menu Download dengan tampilan seperti berikut



Gambar 9. Halaman Download soal

Ketika siswa ingin mendownload soal, dia dapat mencari soal miliknya yang bersesuaian, lalu tekan Download, dan otomatis file terdownload ke komputer siswa. Sedangkan untuk verifikasi dapat masuk ke menu Verify pada gambar 10.



Gambar 10. Halaman verifikasi

Tampilkan beberapa inputan yang harus dimasukkan oleh siswa, yaitu:

- Upload File, berisi file soal yang sudah di download pada menu Download sebelumnya
- Your Certificate, berisi sertifikat (.crt) milik siswa yang sebelumnya sudah dibagikan oleh bagian Tata Usaha atau dapat juga didownload pada menu *Cert Director.y*
- Your Private Key, berisi file *private key* (.pem) milik siswa yang sebelumnya sudah dibagikan oleh bagian Tata Usaha
- Password *Private Key*, adalah password dari file *private key* yang sudah diinputkan sebelumnya.
- *Sender Certificate*, berisi sertifikat (.crt) milik guru, dalam hal ini adalah pengirim, sertifikat dapat di download pada menu Cert Directory.

Lalu klik *Verify*, jika sudah maka otomatis website akan melakukan verifikasi dan mendekripsi file tersebut. Setelah itu tekan Download, untuk mendownload file yang sudah dapat dibaca. Proses yang sama juga berlaku untuk guru pada menu *Verify* di laman guru.

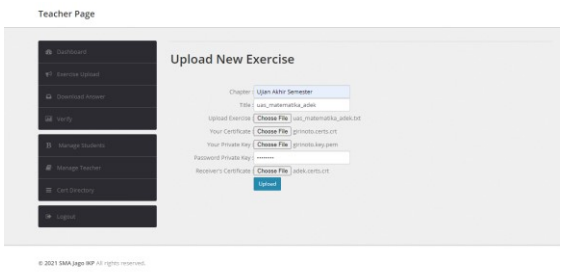
4.5 Ilustrasi

Kita akan mencoba melakukan ilustrasi proses ujian daring antara guru dan siswa pada website SMA Jago IKP Learning System. Sebagai contoh, guru dalam hal ini adalah Bapak Hermawan , Siswa adalah adek, Chapternya adalah Ujian Akhir Semester, dan mata pelajaran adalah matematika.

Pertama tama ini adalah isi file soal yang akan dikirim dengan judul uas_matematika_adek.txt

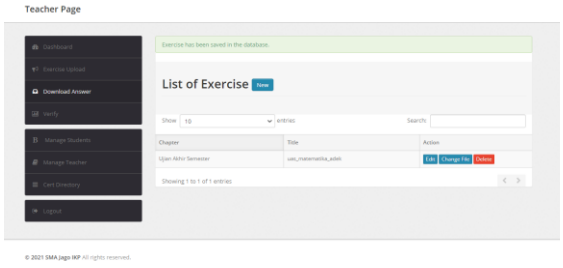
Gambar 11. Soal plaintext dari guru

Selanjutnya, tambahkan soal melalui menu Upload Exercise di laman guru, dan masukkan data-data lain yang diperlukan. Dan tekan Upload



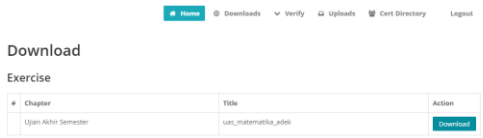
Gambar 12. Proses Upload Soal oleh guru

Cek pada menu Exercise Upload di laman guru, apakah soal sudah masuk atau belum.

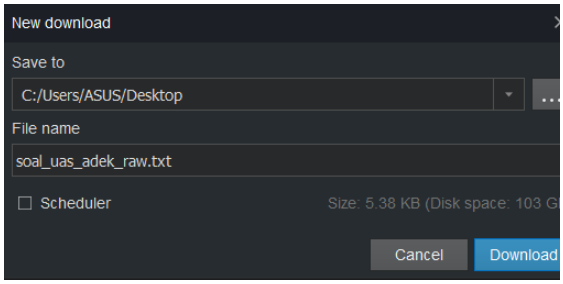


Gambar 13. Periksa soal sudah terkirim atau belum

Jika sudah, sekarang kita masuk ke laman siswa pada menu Download. Cari file soal yang sesuai untuk siswa yang dituju, jika sudah ditemukan tekan Download.



Gambar 14. halaman Download siswa

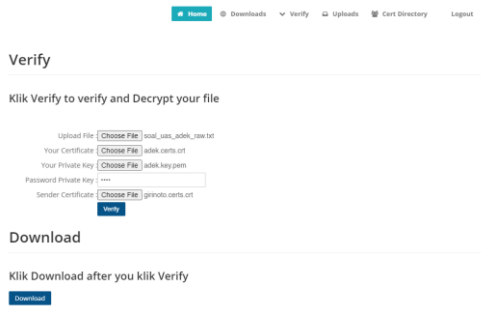


Gambar 15. Proses Download

Coba kita buka file tersebut.

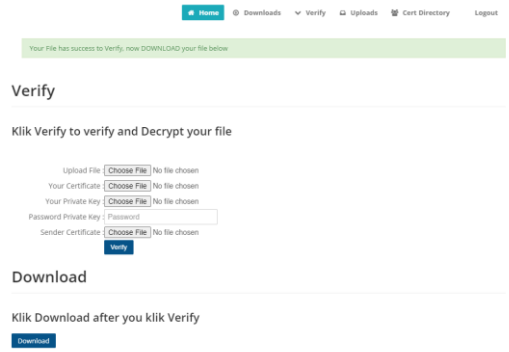
Gambar 16. Isi file yang baru di Download

Isinya akan nampak seperti itu, untuk dapat membacanya, maka kita harus melakukan verifikasi beserta dekripsi file tersebut pada menu Verify.

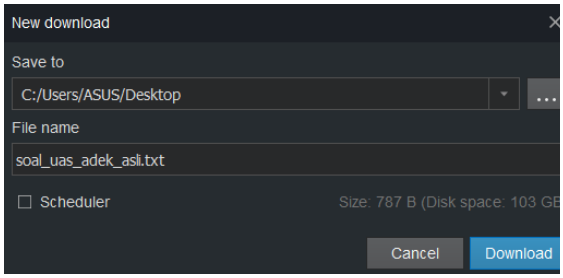


Gambar 17. Proses Verifikasi pada laman siswa

Isi data-data pada menu Verify sesuai yang dibutuhkan, jika sudah tekan Verify. Lalu akan muncul notifikasi seperti gambar dibawah ini. Dilanjutkan dengan tekan Download untuk mendownload file yang sudah diproses melalui proses verifikasi dan dekripsi.

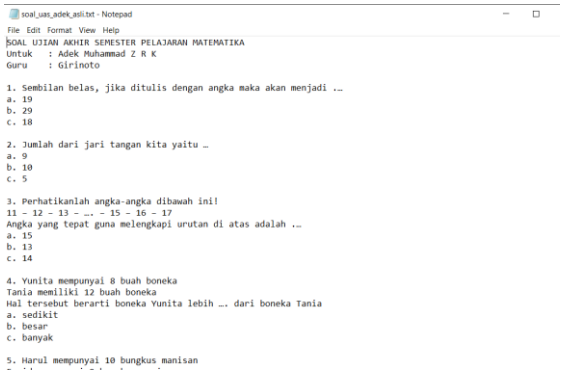


Gambar 18. Notifikasi bahwa soal sudah di verifikasi



Gambar 19. Proses Download soal hasil verifikasi

Dan sekarang coba kita buka file soal_uas_adek_asli.txt.



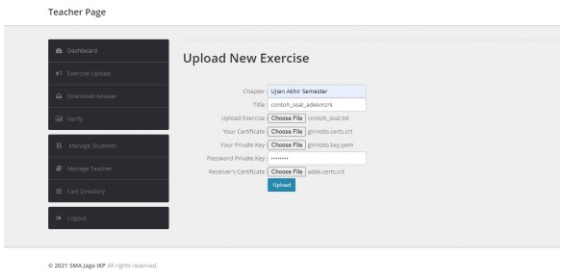
Gambar 20. Isi file soal hasil verifikasi

Berhasil. Soal dapat kita terima dengan baik dan dengan tingkat keamanan yang dapat dipastikan.

Setelah ini siswa dapat langsung mengerjakan soal ini, lalu mengirimkan jawabannya melalui laman siswa dengan metode dan proses yang sama dengan proses diatas. Dan untuk guru pun baru akan bisa membaca jawaban tersebut ketika melakukan verifikasi dan dekripsi pada menu Verify.

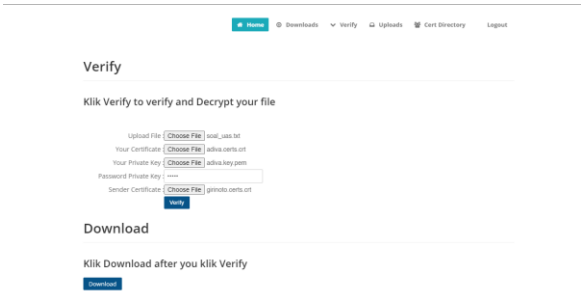
4.6 Percobaan Kegagalan Verifikasi

Percobaan kegagalan verifikasi dilakukan untuk melihat reaksi ketika file soal maupun jawaban yang sudah dikirim tidak di verifikasi oleh entitas yang benar.



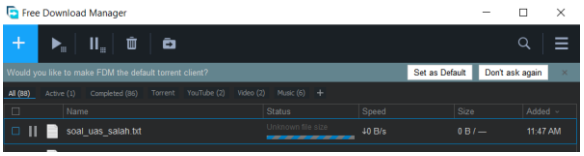
Gambar 21. Proses Upload soal oleh guru

Gambar diatas menunjukkan bahwa soal ditujukan kepada murid bernama “Adek”, dan dikirim oleh “Pak Hermawan ”



Gambar 22. File soal coba diverifikasi oleh murid lain

Gambar diatas menunjukkan bahwa soal yang dikirim sebelumnya akan diverifikasi oleh “Adiva” menggunakan sertifikat dan kunci privat miliknya.



Gambar 23. File soal hasil verifikasi tidak bisa di download

Dan inilah yang terjadi, kita tidak bisa mendownload file tersebut dikarenakan file tersebut kosong, yang menandakan bahwa file soal gagal diverifikasi.

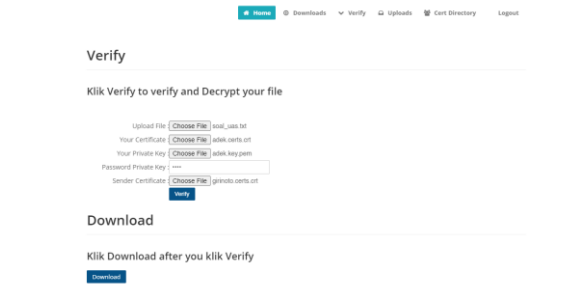
4.7 Percobaan Pengubahan Soal dan Jawaban

Percobaan pengubahan soal dan jawaban dilakukan untuk melihat reaksi ketika file soal maupun jawaban diubah oleh entitas yang tidak bertanggung jawab, lalu coba diverifikasi oleh murid yang asli.

Gambar 24. Soal yang belum diedit

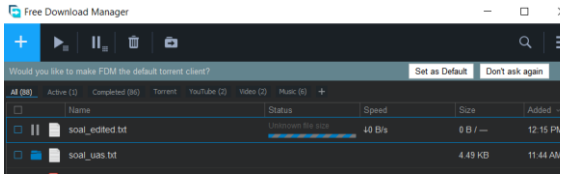
Gambar 25. Soal yang sudah diedit

Dua gambar diatas menunjukkan soal yang dikirim oleh guru, sebelum dan sesudah diedit entitas tidak bertanggung jawab.



Gambar 26. Murid yang asli coba verifikasi

Lalu dari gambar diatas, dapat dilihat bahwa murid yang asli akan mencoba membaca dan verifikasi soal yang sudah diberikan oleh guru, yang mana file sudah diedit.



Gambar 27. File soal hasil verifikasi tidak bisa di download

Sama seperti percobaan sebelumnya, file soal hasil verifikasi tidak bisa di download dikarenakan file tersebut kosong, yang menandakan bahwa soal tersebut telah terjadi perubahan sebelumnya.

.

V. Kesimpulan

File yang dienkripsi dan ditanda tangani hanya bisa dibuka dan dibaca ketika tidak terjadi anomali, baik perubahan isi file maupun percobaan verifikasi entitas yang berbeda. Jika selama proses berjalan sesuai yang sesungguhnya, maka dapat dipastikan terjaminnya keabsahan dari file yang dikirim dan diterima. Media website merupakan media yang sangat cocok untuk mengimplementasikan metode enkripsi dan tanda tangan digital pada sistem ujian daring ini. Terbukti bahwa penerapan enkripsi dan tanda tangan digital melalui media file sharing terjamin keamanannya.

Ucapan Terima Kasih

Terima kasih kepada semua pihak yang telah membantu selesainya tulisan ini termasuk reviewer yang banyak membantu.

Daftar Pustaka

[1] nanda nadia et all Elisa, “penerapan zachman framework pada arsitektur sistem informasi ujian online berbasis web,” *JURNAL REKAYASA TEKNOLOGI NUSA PUTRA*, vol. 1, no. 1, 2019.

[2] S. Kaddoura, D. E. Popescu, and J. D. Hemanth, “A systematic review on machine learning models for online learning and examination systems,” *PeerJ Comput Sci*, vol. 8, 2022, doi: 10.7717/PEERJ-CS.986.

[3] S. Penilaian, J. J. Berbasis, and P. Kpai, “"SurveI Pelaksanaan Pembelajaran Jarak Jauh (PJJ) dan.”

[4] A. Bangun Priambodo, “Sistem Informasi Ujian Berbasis Web Pada SD Islam Teratai Putih Global Bekasi,” *INFORMATICS FOR EDUCATORS AND PROFESSIONALS*, vol. 1, no. 1, pp. 109–123, 2016.

[5] S. Choudhury, *Public Key Infrastructure implementation and design*. New York: M&T Book, 2002.

[6] A. I. Fatra, R. R. Isnanto, and E. W. Sinuraya, “PERANCANGAN INFRASTRUKTUR KUNCI PUBLIK DENGAN IMPLEMENTASI PEMBUATAN KUITANSI DIGITAL PEMBAYARAN KURSUS BAHASA INGGRIS,” *Transient*, vol. 2, no. 3, 2013.

[7] A. I. Fatra, R. R. Isnanto, and E. W. Sinuraya, “PERANCANGAN INFRASTRUKTUR KUNCI PUBLIK DENGAN IMPLEMENTASI PEMBUATAN KUITANSI DIGITAL PEMBAYARAN KURSUS BAHASA INGGRIS.”

[8] W. Agangiba, M. Kontoh, and A. Kwansah Ansah, “E-governance public key infrastructure (PKI) model,” *Int. J. of Electronic Governance*, vol. 6, pp. 133–142, Nov. 2013, doi: 10.1504/IJEG.2013.058360.

[9] A. W. Akotam, M. S. Kontoh, and A. K. Ansah, “E-governance public key infrastructure (PKI) model,”

International Journal of Electronic Governance, vol. 6, no. 2, pp. 133–142, 2013, doi: 10.1504/IJEG.2013.058360.

[10] V. Lozupone, "Analyze encryption and public key infrastructure (PKI)," *Int J Inf Manage*, vol. 38, pp. 42–44, Nov. 2018, doi: 10.1016/j.ijinfomgt.2017.08.004.

[11] A. Garba, Z. Chen, Z. Guan, and G. Srivastava, "LightLedger: A Novel Blockchain-Based Domain Certificate Authentication and Validation Scheme," *IEEE Trans Netw Sci Eng*, vol. 8, no. 2, pp. 1698–1710, Apr. 2021, doi: 10.1109/TNSE.2021.3069128.

[12] A. Albarqi, E. Alzaid, F. Alghamdi, S. Asiri, and J. Kar, "Public Key Infrastructure: A Survey," *Journal of Information Security*, vol. 06, pp. 31–37, Nov. 2015, doi: 10.4236/jis.2015.61004.

[13] R. Hunt, "PKI and digital certification infrastructure," Nov. 2001, pp. 234–239. doi: 10.1109/ICON.2001.962346.

[14] S. Sakhreliya, N. Pandya, and A. Professor, "Public Key Infrastructure (PKI) using Symmetric Key Cryptography (SC) in VANETs," *International Journal of Computer Science and Information Technologies*, 2014, [Online]. Available: www.ijcsit.com

[15] T. D. Hedberg, S. Krima, and J. A. Camelio, "Embedding X.509 Digital Certificates in Three-Dimensional Models for Authentication, Authorization, and Traceability of Product Data," *J Comput Inf Sci Eng*, vol. 17, no. 1, Mar. 2017, doi: 10.1115/1.4034131.

[16] F. B. Manolache and O. Rusu, "Automated SSL/TLS Certificate Distribution System," in *2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Nov. 2021, pp. 1–6. doi: 10.1109/RoEduNet54112.2021.9637722.

[17] F. Muchtar, A. Saheed, M. H. Abd Wahab, and S. Z. Syed Idrus, "Query Operation in Trader Service: LDAP Directory versus Database," *IOP Conf Ser Mater Sci Eng*, vol. 917, p. 12052, Nov. 2020, doi: 10.1088/1757-899X/917/1/012052.

[18] P. Danquah and H. Kwabena-Adade, "Public Key Infrastructure: An Enhanced Validation Framework," *Journal of Information Security*, vol. 11, no. 04, pp. 241–260, 2020, doi: 10.4236/jis.2020.114016.

[19] R. Prodanovic and I. Vulic, "Failure points in the PKI architecture," *Vojnotehnicki glasnik*, vol. 65, pp. 771–784, Nov. 2017, doi: 10.5937/vojtehg65-11144.

[20] Choudhury, *Public Key Infrastructure implementation and design*. New York: M&T Books, 2002.

[21] C. Satizabal, R. Paez, and J. Forne, "PKI trust relationships: from a hybrid architecture to a hierarchical model," in *First International Conference on Availability, Reliability and Security (ARES'06)*, Apr. 2006, pp. 8 pp. – 570. doi: 10.1109/ARES.2006.93.

[22] C. Satizábal, J. Forné, J. Hernández-Serrano, and J. Pegueroles, "Building hierarchical public key infrastructures in mobile ad-hoc networks," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006, vol. 4325 LNCS, pp. 485–496. doi: 10.1007/11943952_41.

[23] T. Fadai, S. Schrittwieser, P. Kieseberg, and M. Mulazzani, "Trust me, I'm a Root CA! Analyzing SSL Root CAs in Modern Browsers and Operating Systems," Nov. 2015, pp. 174–179. doi: 10.1109/ARES.2015.93.

[24] M. Piščević and D. Simić, "Reducing E-commerce risks using digital certificates," *Yugoslav Journal of Operations Research*, vol. 19, Nov. 2009, doi: 10.2298/YJOR0901185P.

[25] W. Sardjono, W. Priatna, Pardiyo, G. R. Putra, and H. Juwitasary, "The use of digital signatures in the business world in the industrial revolution 4.0 era," *ICIC Express Letters, Part B: Applications*, vol. 12, no. 11, pp. 987–993, Nov. 2021, doi: 10.24507/icicelb.12.11.987.