

## Two Factor Authentication Sistem Inventarisasi Barang dan Manajemen Dana Bantuan Operasional Sekolah Dinas Pendidikan Nasional

Neneng Nuryati<sup>1</sup>, Carolina Magdalena Lasambouw<sup>1</sup>, Djoni Djatnika<sup>1</sup>, Linda Lina Meilinda<sup>2</sup>, Farida Agoes<sup>2</sup>, Muhammad Rizqi Sholahuddin<sup>3</sup>, Maisevli Harika<sup>3,\*</sup>

<sup>1</sup>Jurusan Akuntansi, Politeknik Negeri Bandung, Bandung, Indonesia

<sup>2</sup>Jurusan Bahasa Inggris, Politeknik Negeri Bandung, Bandung, Indonesia

<sup>3</sup>Jurusan Teknik Komputer dan Informatika, Politeknik Negeri Bandung, Bandung, Indonesia

Email: <sup>1</sup>neneng.nuryati@polban.ac.id, <sup>1</sup>carolina.magdalena@polban.ac.id, <sup>1</sup>djoni.djatnika@polban.ac.id,

<sup>2</sup>lina.meilinda@polban.ac.id, <sup>2</sup>farida.agoes@polban.ac.id, <sup>3</sup>m.rizqi@polban.ac.id, <sup>3,\*</sup>maisevli@polban.ac.id

Email Penulis Korespondensi: maisevli@polban.ac.id

Submitted:23/09/2022; Accepted:29/09/2022; Published: 30/09/2022

**Abstrak**– Inventarisasi barang pada institusi besar merupakan kegiatan yang rumit, salah satu solusinya adalah dengan membuat sistem aplikasi web yang terstruktur dan dapat diakses dimana saja. Pada Dinas Pendidikan Nasional, bukan hanya pengelolaan inventarisasi saja yang menjadi masalah, namun juga mengelola manajemen Dana Bantuan Operasional Sekolah (BOS). Keamanan data harus menjadi prioritas, karena menyangkut jumlah dana yang besar dan dapat disalahgunakan oleh pihak yang tidak bertanggungjawab. Penelitian ini bertujuan untuk menerapkan Two Factor Authentication (2FA) pada Sistem Inventarisasi barang dan Manajemen Dana BOS. Tahap pertama adalah verifikasi oleh admin DISDIKNAS pada setiap tingkat Pendidikan. Selanjutnya, email verifikasi akan dikirimkan ke pendaftar untuk diverifikasi. Hasil penelitian menunjukkan, penggunaan 2FA tidak mengganggu performa web-based application maupun para penggunanya. Tingkat approval terhadap sistem adalah 97.4%. Penelitian ini memberikan kontribusi bagi penerapan keamanan website, dan dapat diterapkan pada sistem yang serupa.

**Kata Kunci:** Two Factor Authentication; Sistem Informasi; DISDIKNAS; Inventaris barang; Bantuan Operasional Sekolah

**Abstract**–Inventory of goods at large institutions is a complicated activity; one solution is to create a structured web application system that can be accessed anywhere. At the National Education Office, it is not only inventory management that is a problem but also the management of the School Operational Assistance Fund (BOS). Data security must be a priority because it involves significant funds and can be misused by irresponsible parties. This study aims to apply Two Factor Authentication to the Goods Inventory System and BOS Fund Management. The first stage is verification by the DISDIKNAS admin at each level of education. Next, a verification email will be sent to the registrant for verification. The results showed that the use of 2FA did not interfere with the performance of the web-based application or its users. The approval rate for the system is 97.4%. This research contributes to the implementation of website security and can be applied to similar systems.

**Keywords:** Two Factor Authentication; Information System; DISDIKNAS; Inventory of Goods; School Operational Assistance

### 1. PENDAHULUAN

Dinas Pendidikan dan Kebudayaan Nasional Kabupaten (DISDIKNAS) Kuningan pada tahun 2021 telah menggunakan sistem informasi berbasis *website* untuk mengelola aset mereka [1]. Aset yang tersebar pada sekolah-sekolah dalam wilayah kerja DISDIKNAS Kuningan dapat dicatatkan pada sistem informasi berbasis *website* tersebut. Tercatat 1.826 dari tingkat PAUD sampai SLTA berada pada wilayah kerja DISDIKNAS dengan total barang mencapai lebih dari 100.000 [1].

Pengembangan sistem informasi inventarisasi data barang DISDIKNAS Kuningan ini memungkinkan untuk menambahkan fitur baru walaupun sudah diimplementasikan (telah digunakan). Hal ini karena dari awal sistem informasi ini menggunakan metode pengembangan *Rational Unified Process* (RUP) [1]. Teknik RUP memungkinkan penyesuaian terhadap prototipe yang ada untuk menghasilkan sistem yang dapat diterima, dan perubahan yang terjadi dianggap sebagai bagian dari proses pengembangan itu sendiri [1]–[3]. Akan tetapi kekurangan pada *Software Development Live Cycle* (SDLC) ini sangat menyarankan aplikasi dikembangkan oleh pengembang yang sama [3].

Penambahan fitur pengelolaan dana Bantuan Operasional Sekolah (BOS) merupakan hal yang sudah direncanakan pada saat pertemuan membahas kebutuhan sistem. Akan tetapi tidak langsung diimplementasikan pada sistem karena kebutuhan untuk inventarisasi barang lebih mendesak. Manajemen BOS ditambahkan pada tahun 2022. Pada manajemen BOS ini memudahkan penambahan anggaran oleh operator sekolah. Memudahkan melihat sisa anggaran belum terpakai, jenis anggaran terbesar, dan fitur-fitur sederhana untuk memudahkan *user* seperti *search*, otomatis terisi kode ketika barang dipilih. Terlepas dari kebutuhan awal terhadap sebuah sistem yang mampu mengelola aset dan dana BOS, DISDIKNAS Kuningan merasa perlu untuk mengamankan sistem yang berjalan. Hal ini berdasarkan banyaknya kasus peretasan terhadap *website* pemerintah [4]–[6].

Pada artikel-artikel tersebut disebutkan kalau sistem keamanan dari *website* pemerintah lemah [4]–[6]. Berdasarkan kesamaan celah pada *website* pemerintah yang sering dimanfaatkan oleh peretas. Penggunaan *password* sebagai satu-satunya pendekatan untuk penangkal peretas untuk masuk ke dalam aplikasi merupakan hal yang berisiko [7], [8]. Penyadapan bersifat aktif ataupun pasif sering terjadi dilakukan dalam jaringan. Pendekatan pengamanan tahun 2021 (aplikasi rilis pertama) adalah mengikuti *standard security protocol* [9] berdasarkan hasil *review* dari Alkudhayr et.al [10] untuk keamanan *web-based application*. Implementasi yang digunakan antara lain pada *layer*

TCP/IP menggunakan *protocol* HTTPS (*Hypertext Transfer Protocol - Secure*), dan SSL (*Secure Socket Layer*). Pendekatan ini telah digunakan semenjak pertama aplikasi *online* di Internet.

Bercermin pada kasus DROWN [11], HEARTBLEED [12], LOGJAM [13], POODLE [14], SmackTLS [15], dan Bjorka [16]. Implementasi HTTPS dan SSL saja ternyata tidak cukup. Dibutuhkan pengamanan lain seperti *Two Factor Authentication* (2FA) untuk *authentication* pengguna. 2FA menggunakan dua independen faktor dari tiga faktor untuk membuktikan keaslian identitas [7], [8]. Dengan menggunakan 2FA, jika *password* teretas akan tetapi masih ada *variable* lain yang harus dilengkapi untuk masuk ke dalam sistem. Perusahaan besar seperti Google juga telah menggunakan teknologi pengamanan dengan HTTPS ini sejak tahun 2010 [17], kemudian menerapkan 2FA [18]. Selain Google, Facebook [19], dan twitter [20] juga telah menerapkan 2FA untuk penggunanya.

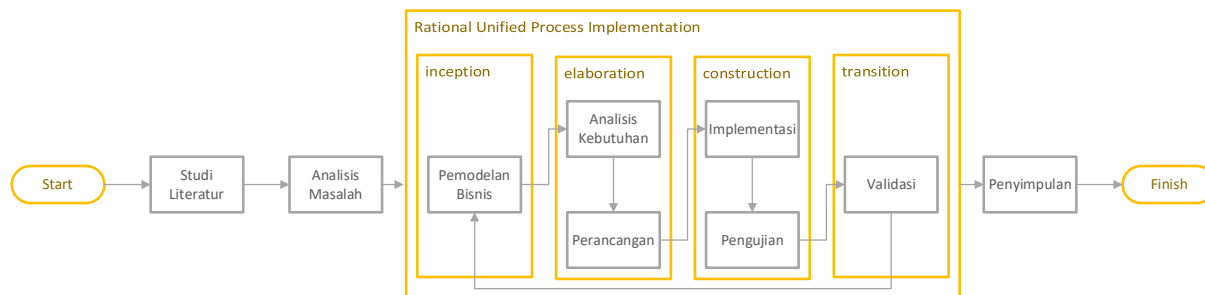
Implementasi 2FA untuk sistem informasi inventarisasi barang dan manajemen BOS ini kurang lebih sama. Menggunakan *username* dan *password*, kemudian kode unik akan dikirim via SMS (*Short Message Service*) atau menggunakan *email*, TOTP (*Time-based One Time Password*), *pregenerated code*, *push*, dan *Universal 2nd Factor* (U2F) [18]–[21]. Pada penelitian ini menggunakan SMS untuk mengirim kode unik, SMS dipilih karena harus diterima oleh nomor telepon yang bersifat unik ditambah telepon genggam tidak pernah bersifat personal dan pengguna cenderung bersama dengan telepon genggam.

Penelitian ini memiliki kontribusi dengan menunjukkan hasil penggunaan 2FA tidak mengganggu performa *web-based application* ataupun para penggunanya khususnya pada sistem inventarisasi barang dan manajemen dana BOS Kabupaten Kuningan. Hasil penelitian ini diharapkan dapat memberikan gambaran sederhana dokumentasi untuk mengamankan sistem bagi *stakeholder* sistem informasi pemerintahan.

## 2. METODOLOGI PENELITIAN

### 2.1 Tahapan Penelitian

Fokus penelitian ini adalah pada *authentication* pengguna pada sistem. Akan tetapi karena penelitian ini merupakan lanjutan dari penelitian sebelumnya [1] disebutkan ada beberapa fitur yang dikembangkan bersamaan dengan 2FA. Penambahan fitur baru berupa manajemen dana BOS, untuk perbaikan adalah perubahan fitur *login* dan registrasi pengguna. Fitur tambahan inilah yang menjadi latar belakang implementasi 2FA pada sistem. Arsitektur sistem yang dikembangkan masih menggunakan RUP dengan alur seperti Gambar 1.



Gambar 1. Alur Metodologi Penelitian [1]

Tahap awal penelitian ditandai dengan melengkapi pengetahuan mengenai fitur yang akan dikembangkan, menganalisis masalah, selanjutnya masuk ke *phase* RUP. Setelah beberapa kali spin (pada penelitian ini spin sejumlah fitur) dan selesai divalidasi untuk terakhir kalinya aplikasi di-*release*.

Studi literatur pada penelitian ini diperoleh dari wawancara awal dan temuan selama aplikasi digunakan pada tahun 2021. Temuan ini termasuk perilaku pengguna, dan perilaku sistem. Temuan-temuan ini dianalisis, hasil analisis pada tahap awal ini menghasilkan kesimpulan berupa aplikasi disempurnakan lagi dengan melengkapi fitur yang telah dijanjikan, serta penambahan 2FA pada sistem. Jadi total ada dua kali spin pada RUP sebelum ditarik kesimpulan untuk penyelesaian pengembangan sistem.

Rancangan model pada dokumentasi pengembangan menggunakan *Unified Modelling Language* (UML), diagram yang digunakan antara lain *use case* dan *sequence*. Fungsionalitas menggunakan *use case* dan *message* terhadap waktu interaksi antar objek di dalam dan di sekitar sistem.

### 2.2 Two Factor Authentication (2FA)

Metode *authentication* menggunakan faktor tambahan yang independen dari faktor utama (*password*). Faktor tambahan ini digunakan untuk membuktikan keaslian identitas dari pengguna yang masuk tersebut asli. Teknologi 2FA ini dimaksudkan untuk mengurangi risiko masuknya pihak lain yang bukan pengguna asli karena berhasil mendapatkan *password* dengan cara apa pun. 2FA membutuhkan pengguna untuk menyediakan beberapa faktor seperti [21]:

- Sesuatu yang diketahui oleh pengguna (*password*),
- Sesuatu yang dimiliki oleh pengguna (seperti *handphone* atau perangkat keras lain), dan

c. Sesuatu yang mencerminkan pengguna (*biometric* seperti *fingerprint*)

Lima metode yang paling umum untuk menggunakan 2FA antara lain: SMS, OTP, *pregenerated-code*, *push*, dan *Universal 2nd Factor*.

### 2.2.1 SMS (*Short Message Service*)

Metode 2FA paling populer adalah menggunakan SMS sebagai media mengirimkan kode uniknya [21]. Biasa terdiri dari enam digit kode unik. Idenya berawal dari 99% penduduk Amerika telah menggunakan *mobile phone* [22]. Metode ini biasanya server dihubungkan dengan *module* GSM untuk mengirimkan kode unik ke nomor pengguna yang berusaha login pada sistem.

### 2.2.2 TOTP (*Timed One Time Password*)

Metode ini biasanya dimulai dengan *synchronize* generator kode unik dari *provider* tertentu, contoh Google authentication [23] dan Microsoft authentication [24]. Aplikasi *authentication* ini menggunakan kombinasi potongan *timestamp*, nilai *hashing*, dan potongan kode dari *verification*. Keuntungan menggunakan metode ini pengguna tidak perlu jaringan selular lagi untuk *authenticating*.

### 2.2.3 *Pregenerated Code*

Kode tertentu yang digenerate oleh sistem dan tidak ada batas waktunya. Metode ini biasanya digunakan untuk *backup* 2FA saja karena risiko penggunaannya sama dengan risiko menggunakan *password*. Karena hal itulah penggunaan *pregenerated code* jarang ditemukan pada penelitian.

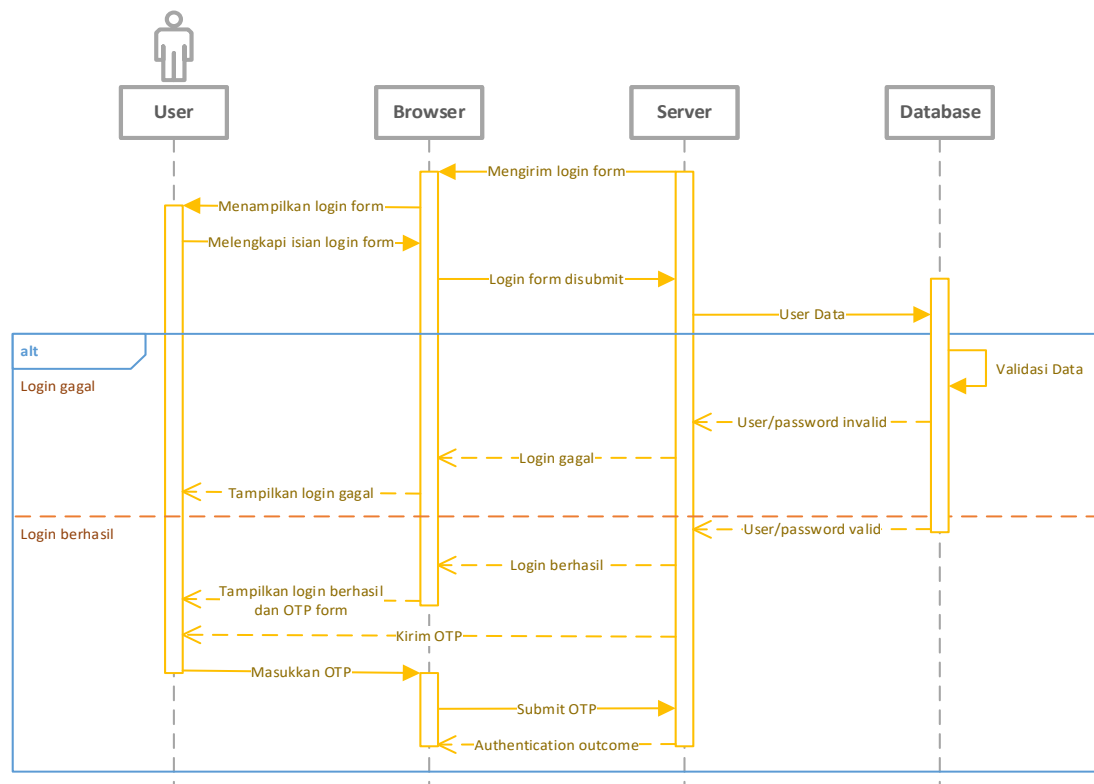
### 2.2.4 *Push*

Metode *push* ini merupakan implementasi teknologi *push notification*. Biasanya notifnya ada dua pilihan “Approve” atau “Deny” percobaan *login* ke sistem. *Push authentication* tidak membutuhkan ruang simpan yang eksplisit untuk *secret key*, akan tetapi server harus mampu memastikan *push* notif dikirim ke *device* yang tepat.

### 2.2.5 *Universal 2nd Factor*

Dikembangkan oleh Google dan Yubico. U2F ini menggunakan USB *hardware device* (*security key*) untuk *authenticate* pengguna. Pada proses *authenticate* pengguna harus terhubung ke *security key* melalui USB *port* pada *device*-nya.

Secara garis besar konsep 2FA yang diimplementasikan pada web dapat dilihat pada Gambar 2, pada gambar ini dapat dilihat perbedaan mencolok antara penggunaan satu faktor saja dengan menggunakan dua faktor untuk *authentication*.



Gambar 2. Sequence diagram overview 2FA pada website

Dapat dilihat pada Gambar 2, secara umum pemanfaatan 2FA pada *website* dengan OTP menggunakan generator OTP yang ditanam pada server atau dihubungkan ke perangkat lain sebagai media pengiriman (seperti modul GSM untuk SMS OTP).

### 2.3 User Acceptance Test (UAT)

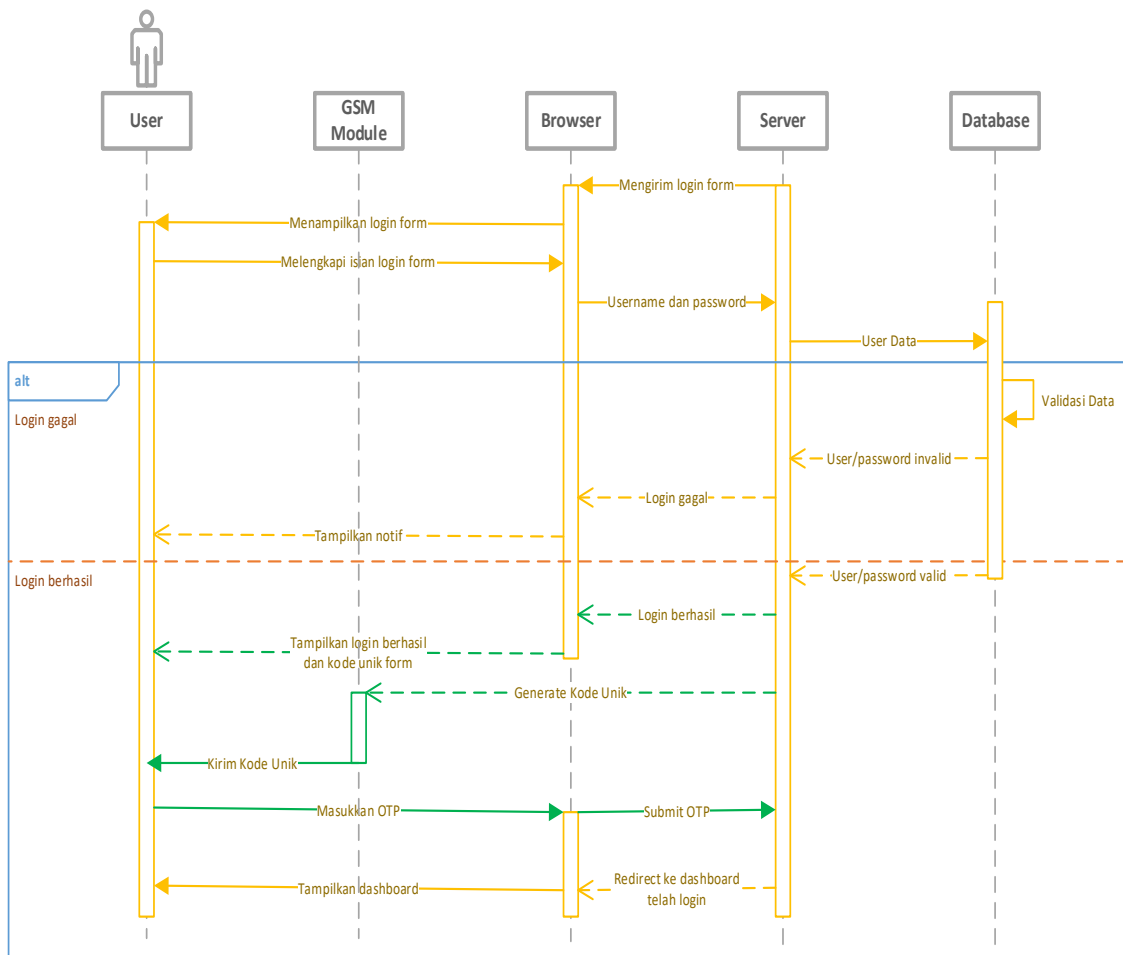
UAT merupakan validasi solusi yang dipilih untuk mengatasi masalah apakah diterima untuk *user* [25]. Proses ini sangat penting dalam mengembangkan aplikasi. Untuk pengujian salah satu pendekatannya adalah menggunakan kuesioner. Perhitungan diperoleh dengan persentase dari total skor dibandingkan dengan skor tertinggi. Pada UAT penelitian ini digunakan lima kategori dimulai dari 1 – 5 dengan keterangan sangat tidak setuju, tidak setuju, netral, setuju, dan sangat setuju.

## 3. HASIL DAN PEMBAHASAN

Implementasi 2FA pada penelitian ini pada dua fitur utama sistem, pertama pada fitur *login* dan kedua pada fitur registrasi. Pada bagian ini dibahas bagaimana implementasi pada kedua fitur tersebut secara detail.

### 3.1 2FA Login

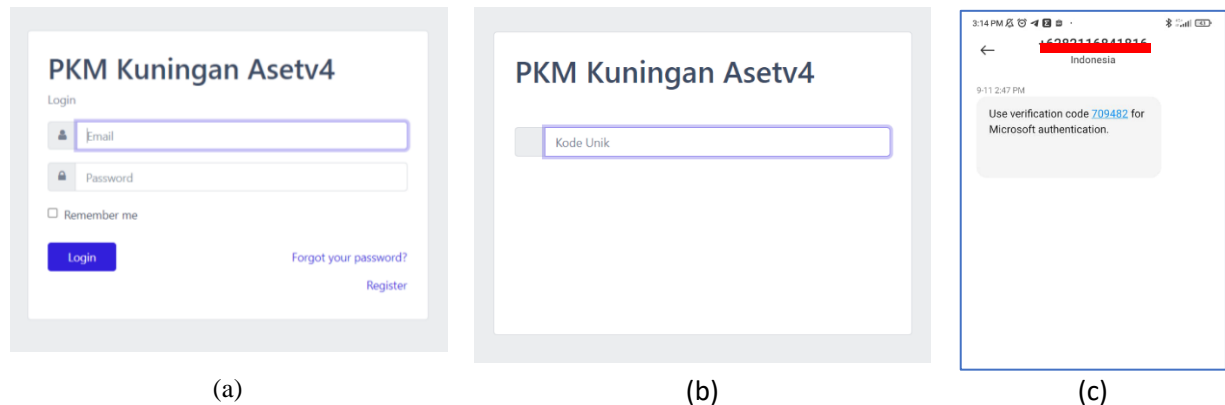
Model untuk *login* ke dalam sistem setelah implementasi 2FA dapat dilihat pada Gambar 3.



**Gambar 3.** Sequence Diagram Masuk ke Sistem Setelah 2FA diimplementasikan

Gambar 3 merupakan *sequence* diagram untuk masuk ke sistem informasi setelah menggunakan 2FA. Untuk tahap awal sama dengan *login* pada sistem sebelumnya. Masukkan *username* dan *password*, kemudian sistem akan memvalidasi apakah *user* terdaftar atau tidak. Jika *user* valid, *user* dikirim (*redirect*) ke halaman *dashboard*. Setelah penambahan 2FA ada *message* baru yang muncul (ditandai dengan warna hijau).

Tampilan halaman *login* dapat dilihat pada Gambar 4.a. Setelah memasukkan *username* dan *password* yang valid sistem akan menampilkan halaman *input* kode unik seperti Gambar 4.b. Masukkan OTP yang dikirim via SMS (Gambar 4.c) untuk *login* ke sistem.



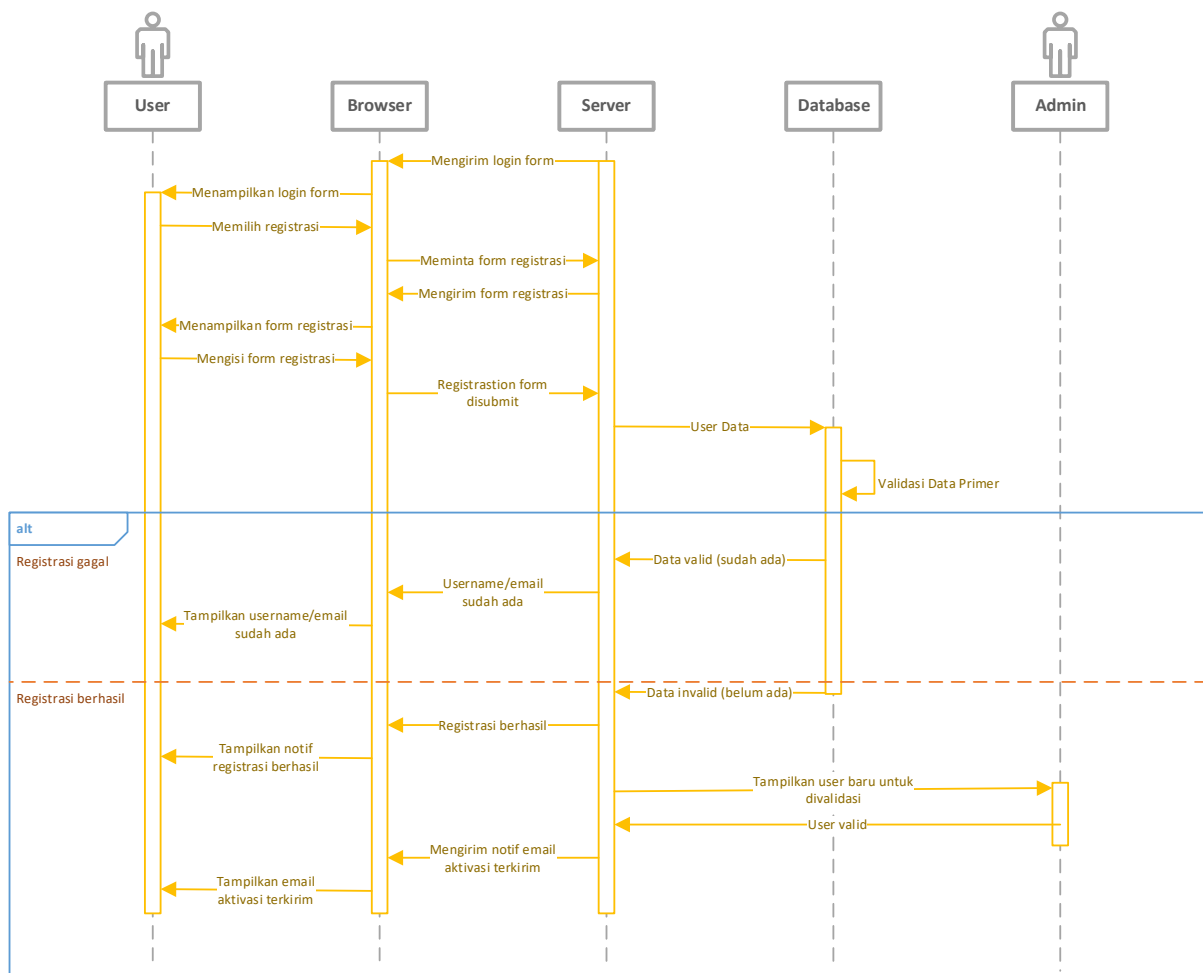
Gambar 4. a. Halaman login, b. Halaman input kode unik, dan c. Kode unik yang terkirim ke user

### 3.2 2FA Registration

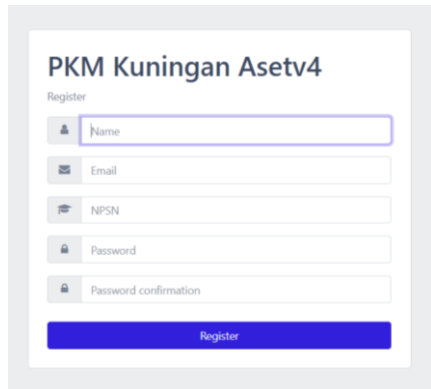
Pada sistem lama tidak ada model registrasi pengguna karena pada wawancara user di-assign oleh admin DISDIKNAS. Akan tetapi ada beberapa kasus seperti penggantian operator di sekolah dan ada sekolah yang operatornya per kecamatan. Perbedaan kasus pada sekolah-sekolah ini memunculkan kesulitan admin DISDIKNAS untuk penanganan registrasi pengguna baru. Untuk itu dibuatkan menu registrasi untuk user baru.

Pengguna baru meminta form registrasi dengan mengklik tautan pada login form. Sistem akan mengirimkan form registration, setelah diisi sistem akan memvalidasi username dan atau email belum pernah digunakan. Jika salah satu pernah digunakan maka sistem akan menampilkan notifikasi kalau registrasi gagal dengan tambahan username/email sudah ada. Sebaliknya jika username dan email baru maka registrasi berhasil. Admin akan memvalidasi user baru ini sebelum email aktivasi dikirimkan sistem ke pengguna baru.

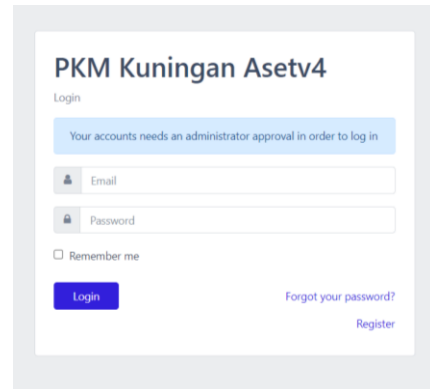
Cara kerja 2FA pada registrasi ini adalah user baru divalidasi oleh admin DISDIKNAS, hal ini ditampilkan lebih jelas pada activity diagram pada Gambar 5.



Gambar 5. Sequence diagram registrasi dengan 2FA



(a)



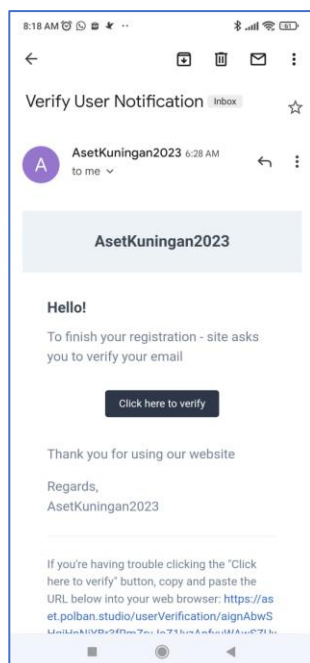
(b)

**Gambar 6.** a. Halaman registrasi, dan b. Notifikasi setelah registrasi kompliti

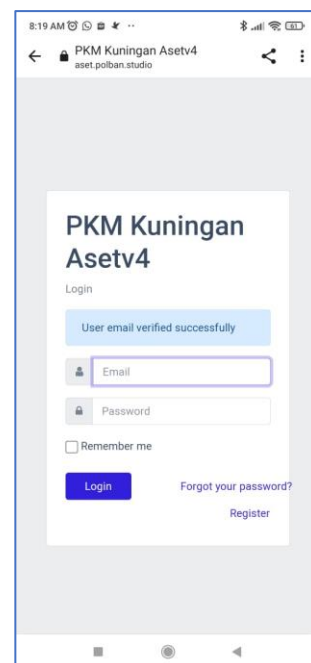
Halaman form input yang harus diisi pada saat registrasi ditampilkan pada Gambar 6.a dan redirect setelah approval oleh admin Gambar 6.b. Gambar 7 merupakan tampilan halaman validasi oleh admin. Setiap user yang sudah ditandai “Verified” akan dikirim email aktivasi oleh sistem. Setelah pengguna baru mengeklik tautan pada email barulah user aktif dan ditandai “Approved” oleh sistem. Pada saat inilah pengguna baru dapat mengakses sistem.

ID	Name	Email	Two-Factor Auth	Approved	Verified	Roles	NPSN
17	Mochamad Saipul	sd01.mekarjaya@gmail.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ad	20212703
16	Naufal Muhammad	admin.sd02mekarja@gmail.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ad	20212702
15	Aceng Rohmat Admin SD Mekarmulya	aceng.adminmekarmulya24@gmail.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ad	20212701
14	Diana Setiawati	diana.moet_90@gmail.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ad	20212700
13	Muhammad Imron SD 2 Pagundan	imron.operator.sdn02pagundan@gmail.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ad	20212669
12	Ica Humaira	icahu_20212668@gmail.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ad	20212668
11	Asep M. Aviana	asep-osde_02.padareki@gmail.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ad	20212667

**Gambar 7.** Halaman approval oleh admin



(a)



(b)

**Gambar 8.** a. Email verifikasi user baru, dan b. Notifikasi email sudah diverifikasi

Operator sekolah dan operator kecamatan ketika *login* maupun registrasi memiliki penanganan yang sama. Perbedaan antara kedua user ini level penggunaannya, operator kecamatan hanya ada pada sekolah dasar saja. Operator kecamatan ada satu tingkat di atas operator sekolah, operator ini bertugas memvalidasi anggaran dan hal lainnya sebelum finalisasi oleh operator sekolah. Penanganan ini tidak berpengaruh ke implementasi 2FA ini.

### 3.3 Analisis Hasil

Berdasarkan hasil dari sebaran kuesioner dari user yang akan terlibat di tahun 2022, dengan rinci empat admin di DISDIKNAS untuk masing-masing tingkatan sekolah (TK, SD, SMP, dan SMA), dan sampel 15 operator dari sekolah di wilayah DISDIKNAS Kuningan. Dengan pertanyaan sesuai dengan tabel 1.

**Tabel 1.** Daftar pertanyaan kuesioner

No.	Pertanyaan
1	Apakah kode unik diperoleh?
2	Apakah <i>login</i> dapat dilakukan dengan kode unik yang diperoleh?
3	Apakah penggunaan kode unik berpengaruh dengan keamanan sistem?
4	Apakah penggunaan kode unik mengganggu penggunaan aplikasi?
5	Apakah aplikasi sesuai dengan kebutuhan?

Hasil kuesioner dengan pertanyaan sesuai tabel 1 diperoleh nilai dengan persentase 100%, 100%, 90.5%, 95.7%, dan 100%. Berdasarkan hasil tersebut dapat disimpulkan secara tidak langsung 97.24% penggunaan sistem 2FA untuk sistem informasi inventarisasi barang dan manajemen dana BOS untuk Dinas Pendidikan Nasional Kabupaten Kuningan.

## 4. KESIMPULAN

Penelitian implementasi *two factor authentication* untuk sistem informasi inventarisasi barang dan manajemen dana BOS di DISDIKNAS Kuningan Jawa Barat ini berhasil dilakukan. 2FA tidak hanya digunakan pada fitur *login* akan tetapi juga pada fitur registrasi. Secara keseluruhan pengguna menunjukkan tanggapan yang baik terhadap penggunaan aplikasi ini. Persentase pengguna setuju adalah sebesar 97.4%. Terbukti bermanfaat dan memudahkan pengamanan data pada sistem informasi tersebut. Selanjutnya model ini dapat menjadi contoh untuk *website* pemerintah lainnya untuk mengamankan sistemnya. Kekurangan yang sangat terasa adalah penggunaan modul GSM untuk pengiriman SMS. Penggunaan SMS menggunakan pulsa, sedangkan sistem belum punya *monitoring* khusus untuk pengawasan penggunaan pulsa. Kemungkinan pulsa habis dan sistem tidak memberitahukan admin sangat tinggi. Penggantian ke teknologi sosial media seperti WhatsApp atau Telegram sangat memungkinkan, akan tetapi belum dapat dipastikan seluruh pengguna setuju. Perlu dilakukan *survey* tersendiri untuk hal ini. Ada kemungkinan penggunaan salah satu ataupun penggunaan kedua *social* media tersebut. Penelitian lanjutan mengenai implementasi WhatsApp atau Telegram pengganti modul GSM perlu dilakukan, selain itu penelitian untuk bukti 2FA dapat mengamankan aplikasi *web-based* seperti ini dapat dilakukan. Caranya dengan mengawasi apakah ada *attacker* yang mencoba meretas sistem. Masih sehubungan dengan aplikasi web penelitian yang mungkin dilakukan untuk meningkatkan kinerja sistem adalah mengukur performa sistem, *user experience* (UX), dan lainnya.

## REFERENCES

- [1] N. Nuryati, C. M. Lasambouw, D. Djatnika, and ..., "Sistem Inventarisasi Barang Dinas Pendidikan Nasional Kuningan Jawa Barat," *JURIKOM (Jurnal ...)*, vol. 8, no. 6, pp. 392–400, 2021, doi: 10.30865/jurikom.v8i6.3574.
- [2] G. Blokdyk, *Rational Unified Process A Complete Guide*, 2020 Editi. 5STARCOoks, 2020.
- [3] M. Sudarma, S. Ariyani, and P. A. Wicaksana, "Implementation of the Rational Unified Process (RUP) Model in Design Planning of Sales Order Management System," *INTENSIF J. Ilm. Penelit. dan Penerapan Teknol. Sist. Inf.*, vol. 5, no. 2, pp. 249–265, 2021, doi: 10.29407/intensif.v5i2.15543.
- [4] Kominfo, "50 Porsen Situs Pemerintah Diserang Hacker!," *Kominfo.Go.Id*, p. 1, 2012. [Online]. Available: <https://kominfo.go.id/content/detail/1493/50-porsen-situs-pemerintah-diserang-hacker/0/berita>
- [5] Can/fjr, "Situs Pemerintah Mudah Diretas, Data Warga Dijual Bebas," *cnnindonesia.com*, 2021. [Online]. Available: <https://www.cnnindonesia.com/teknologi/20211122123922-185-724359/bssn-ungkap-sebab-situs-pemerintah-rentan-diretas>
- [6] A. Al Faqir, "Situs Pemerintah Sering Diretas, Sri Mulyani: Tingkatkan Cyber Security," *merdeka.com*, 2022. [Online]. Available: <https://www.merdeka.com/uang/situs-pemerintah-sering-diretas-sri-mulyani-tingkatkan-cyber-security.html>
- [7] A. Q. Chen and W. Goh, *Two factor authentication made easy*, vol. 9114. 2015. doi: 10.1007/978-3-319-19890-3\_29.
- [8] M. Stanivlav, *Two-Factor Authentication*. O'Reilly, 2015.
- [9] J. M. Kizza, *Guide to Computer Network Security*, vol. 39, no. 1. 2015. [Online]. Available: <http://dx.doi.org/10.1016/j.compeleceng.2012.04.015%0Ahttp://link.springer.com/10.1007/978-1-4471-6654-2%0Ahttp://link.springer.com/10.1007/978-1-4471-6654-2>
- [10] F. Alkhudhayr, S. Alfarraj, B. Aljameeli, and S. Elkhdiri, "Information Security: A Review of Information Security Issues and Techniques," *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, 2019, doi: 10.1109/CAIS.2019.8769504.
- [11] N. Aviram *et al.*, "Drown: Breaking TLS using SSLv2," in *Proceedings of the 25th USENIX Security Symposium*, 2016, pp.



689–706.

- [12] “Heartbleed Bug,” 2014. <https://heartbleed.com/> (accessed Jun. 22, 2022).
- [13] D. Adrian *et al.*, “Imperfect forward secrecy: How diffie-hellman fails in practice,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2015, vol. 2015-October, pp. 5–17. doi: 10.1145/2810103.2813707.
- [14] B. Möller, T. Duong, and K. Kotowicz, “This POODLE Bites: Exploiting The SSL 3.0 Fallback,” *Security Advisory*, 2014. <https://www.openssl.org/~bodo/ssl-poodle.pdf>
- [15] B. Beurdouche *et al.*, “A messy state of the union: Taming the composite state machines of TLS,” in *Proceedings - IEEE Symposium on Security and Privacy*, 2015, vol. 2015-July, pp. 535–552. doi: 10.1109/SP.2015.39.
- [16] “Apakah Bjorka Hacker atau Cuma Pengepul Data?,” *cmindonesia.com*, 2022. <https://www.cnnindonesia.com/teknologi/20220914154148-192-847818/apakah-bjorka-hacker-atau-cuma-pengepul-data> (accessed Jun. 22, 2022).
- [17] Z. Ait and G. Illyes, “HTTPS as a ranking signal,” *Google Search Central*, 2014. <https://developers.google.com/search/blog/2014/08/https-as-ranking-signal> (accessed Jun. 22, 2022).
- [18] “Advanced sign-in security for your Google account,” 2011. <https://gmail.googleblog.com/2011/02/advanced-sign-in-security-for-your.html> (accessed Jun. 22, 2022).
- [19] Facebook, “Introducing Login Approvals,” 2011. <https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920/> (accessed Jun. 22, 2022).
- [20] J. O’Leary, “Getting Started With Login Verification,” 2014. <https://blog.twitter.com/2013/getting-started-login-verification>.
- [21] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, “A usability study of five two-factor authentication methods,” in *Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019*, 2019, pp. 357–370.
- [22] J. Poushter, “Mobile Fact Sheet,” 2017. [Online]. Available: <http://www.pewinternet.org/fact-sheet/mobile/>
- [23] I. Wigmore, “Google Authenticator.” <https://play.google.com/store/search?q=google+authenticator+apps&c=apps> (accessed Jun. 22, 2022).
- [24] Microsoft Corporation, “Microsoft Authenticator,” 2013. <https://play.google.com/store/search?q=microsoft+authenticator+apps&c=apps> (accessed Jun. 22, 2022).
- [25] R. Kohlman, *User Acceptance Test (UAT) Planning Guide*. Majik Moments, 2020.