



User Manual Document

MULTI FACTOR AUTHENTICATION (MFA)



Daftar Isi

1.	Dokumen Versi.....	3
2.	Pengertian Umum	3
2.1.	Pengertian Umum INSW	3
2.2.	Pengertian Umum Aplikasi INSW	3
3.	Pengguna Aplikasi.....	3
4.	Multi Factor Authentication (MFA)	4
4.1	Metode Multi Factor Authentication (MFA) dengan Email.....	5
4.2	Metode Multi Factor Authentication (MFA) dengan Passkeys.....	10
4.3	Metode Multi Factor Authentication (MFA) dengan Authenticator	23

Pendahuluan

Dokumen ini ditujukan untuk membantu pengguna dalam menjalankan proses pada aplikasi sesuai dengan prosedur yang ada. Dokumen ini diharapkan dapat dijadikan sebagai panduan untuk menyelesaikan masalah yang dihadapi dalam penggunaan aplikasi.

1. Dokumen Versi

Tanggal	Versi
3 Desember 2024	1.1

2. Pengertian Umum

2.1. Pengertian Umum INSW

Diatur dalam Peraturan Presiden Nomor 44 Tahun 2018, yaitu integrasi sistem secara nasional yang memungkinkan dilakukannya penyampaian data dan informasi secara tunggal, pemrosesan data dan informasi secara tunggal dan sinkron, dan penyampaian keputusan secara tunggal untuk pemberian izin kepabeanan dan pengeluaran barang sesuai dengan ketentuan peraturan perundang-undangan.

2.2. Pengertian Umum Aplikasi INSW

Sistem elektronik yang terintegrasi secara nasional, yang dapat diakses melalui jaringan internet (*public network*), yang akan melakukan integrasi informasi berkaitan dengan proses penanganan dokumen kepabeanan dan dokumen lain yang terkait dengan ekspor-impor, yang menjamin keamanan data dan informasi serta memadukan alur dan proses informasi antar sistem internal secara otomatis, yang meliputi sistem kepabeanan, perizinan, kepelabuhanan/kebandarudaraan, dan sistem lain yang terkait dengan proses pelayanan dan pengawasan kegiatan ekspor impor.

3. Pengguna Aplikasi

User Pengguna Jasa, Kementerian/Lembaga

Memulai Aplikasi

4. Multi Factor Authentication (MFA)

Multi-Factor Authentication (MFA) adalah mekanisme keamanan yang memverifikasi identitas pengguna menggunakan dua atau lebih faktor autentikasi dari kategori yang berbeda, seperti sesuatu yang diketahui (password), dimiliki (kode OTP, perangkat), atau sesuatu yang melekat (sidik jari, wajah). Cara kerjanya dimulai dengan pengguna memasukkan kredensial utama, seperti username dan password, lalu dilanjutkan dengan verifikasi tambahan seperti memasukkan kode OTP atau menggunakan biometrik. Jika semua faktor berhasil diverifikasi, akses diberikan, sehingga menambah lapisan keamanan dan mengurangi risiko akses tidak sah.

Terdapat 3 Metode Multi Factor Authentication (MFA) yaitu sebagai berikut :

1. **Email**

Pengguna akan menerima kode verifikasi melalui email yang terdaftar.

2. **Passkey**

Pengguna akan melakukan autentikasi melalui device yang terhubung (smartphone atau pc).

3. **Authenticator**

Pengguna dapat menggunakan aplikasi autentikator untuk memperoleh kode verifikasi.

Fitur Multi-Factor Authentication (MFA) memiliki dua opsi terkait masa berlaku sesi pada perangkat yang Anda gunakan. Berikut adalah panduan lengkap mengenai pengaturan masa berlaku MFA:

4. Mencentang “Trust This Device”

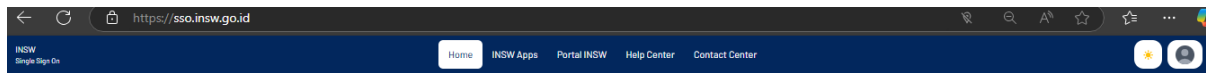
Opsi ini secara otomatis tercentang. Jika Anda membiarkan opsi ini tercentang, maka sesi MFA akan berlaku selama 14 hari ke depan pada perangkat tersebut. Selama periode ini, Anda tidak perlu melakukan autentikasi ulang setiap kali masuk. Centang opsi ini jika Anda menggunakan perangkat pribadi yang aman dan tidak ingin sering melakukan autentikasi ulang.

5. Tidak Mencentang “Trust This Device”

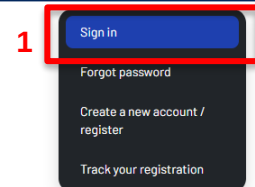
Jika Anda tidak mencentang opsi ini, maka sesi MFA akan berakhir pada tengah malam di hari yang sama. Setelah itu, Anda akan diminta melakukan autentikasi ulang saat login kembali ke aplikasi. Gunakan opsi ini saat login dari perangkat publik atau tidak aman, untuk meningkatkan keamanan akun Anda

4.1 Metode Multi Factor Authentication (MFA) dengan Email

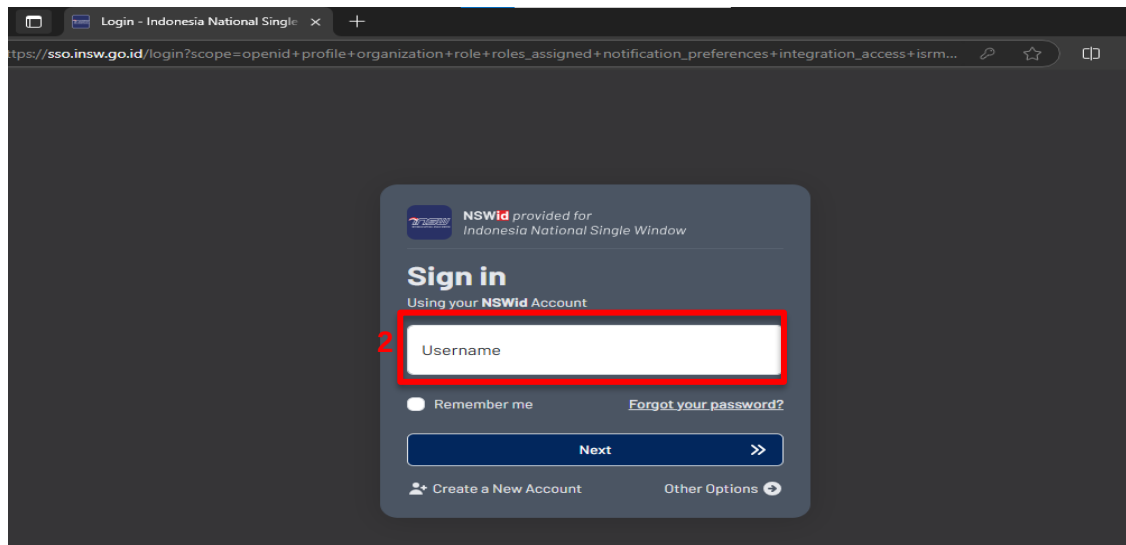
Multi Factor Authentication (MFA) dapat diakses melalui alamat <https://sso.insw.go.id> dengan tampilan awal berikut ini :



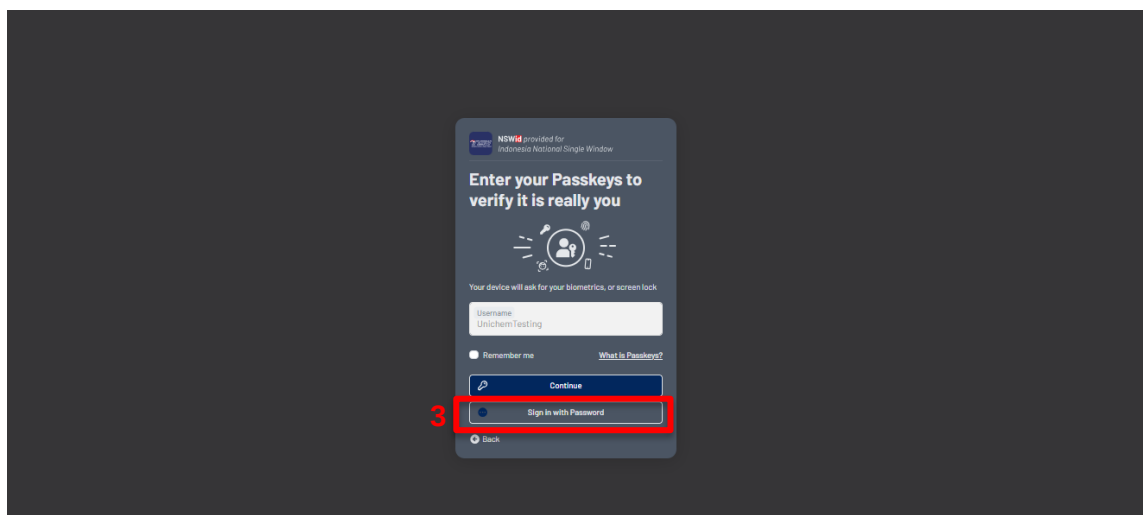
1. Klik icon user pada pojok kanan atas, kemudian klik “Sign In”.



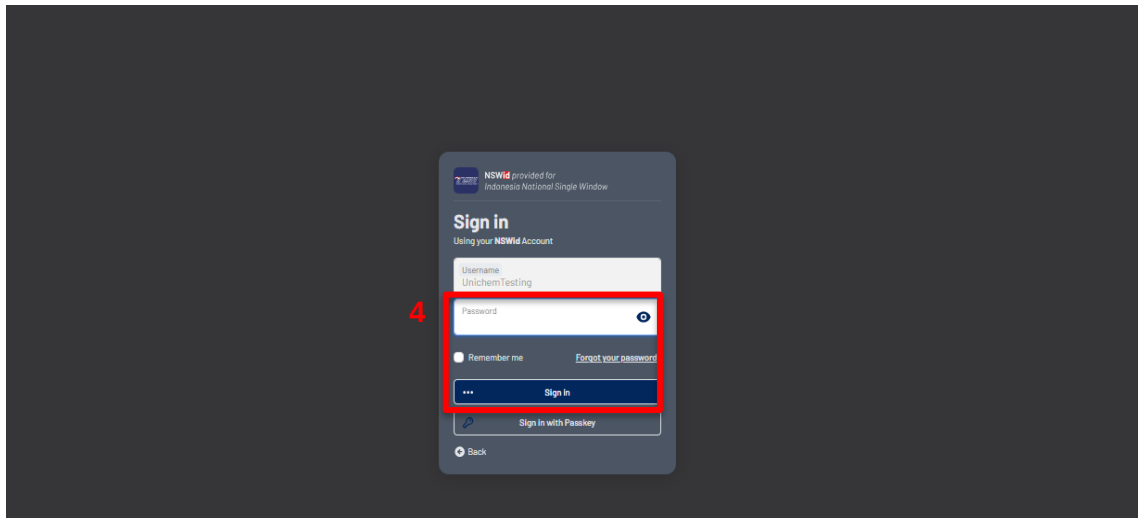
2. Untuk memulai aplikasi , Anda dapat memasukan **Username** lalu klik tombol next.



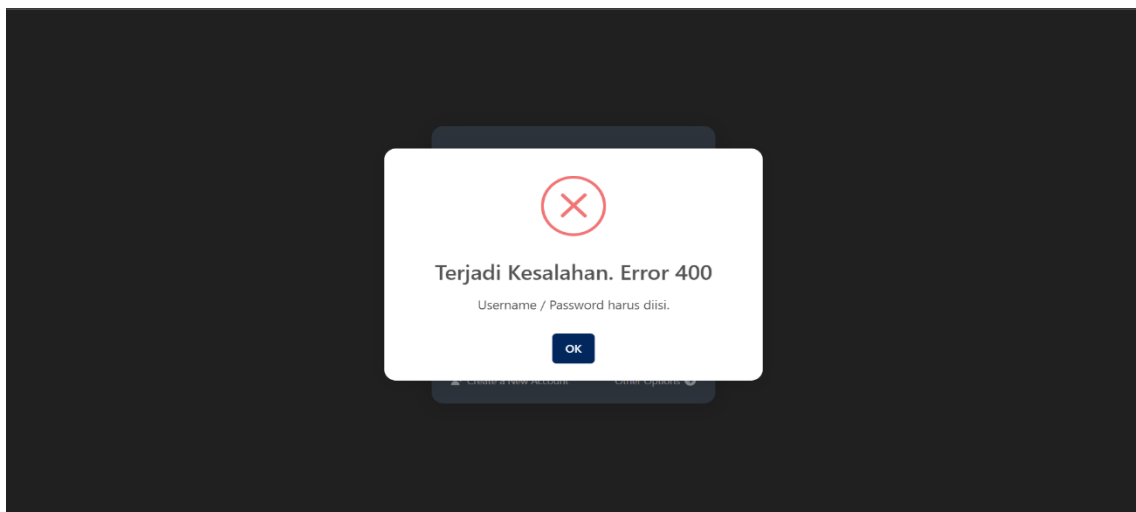
3. Lalu , klik tombol **Sign In With Password**.



4. Lalu Anda dapat memasukkan **Password** dan klik **sign in**.

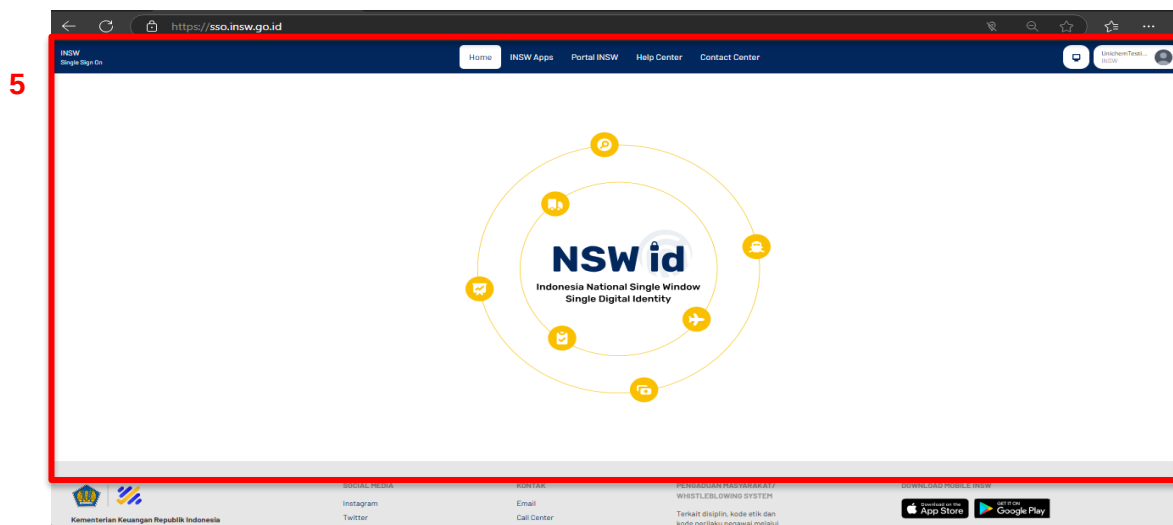


- a. Jika username dan password tidak sesuai maka akan tampil pesan seperti di bawah ini.

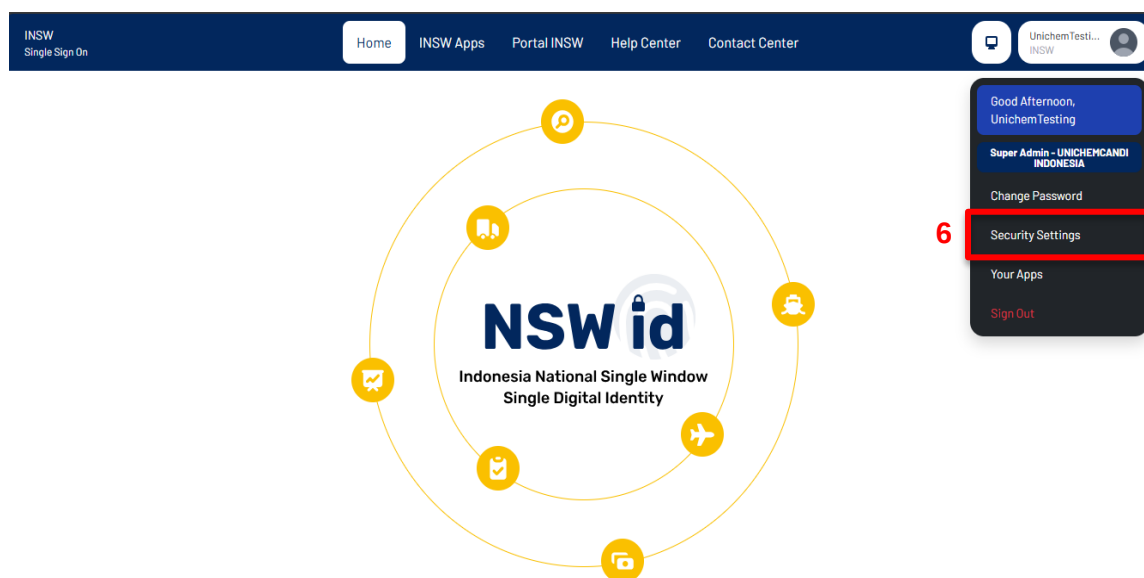


- b. Jika lupa password **Akun INSW**, klik **Lupa Password** dan masukkan **Email** dan **Username Akun INSW**.

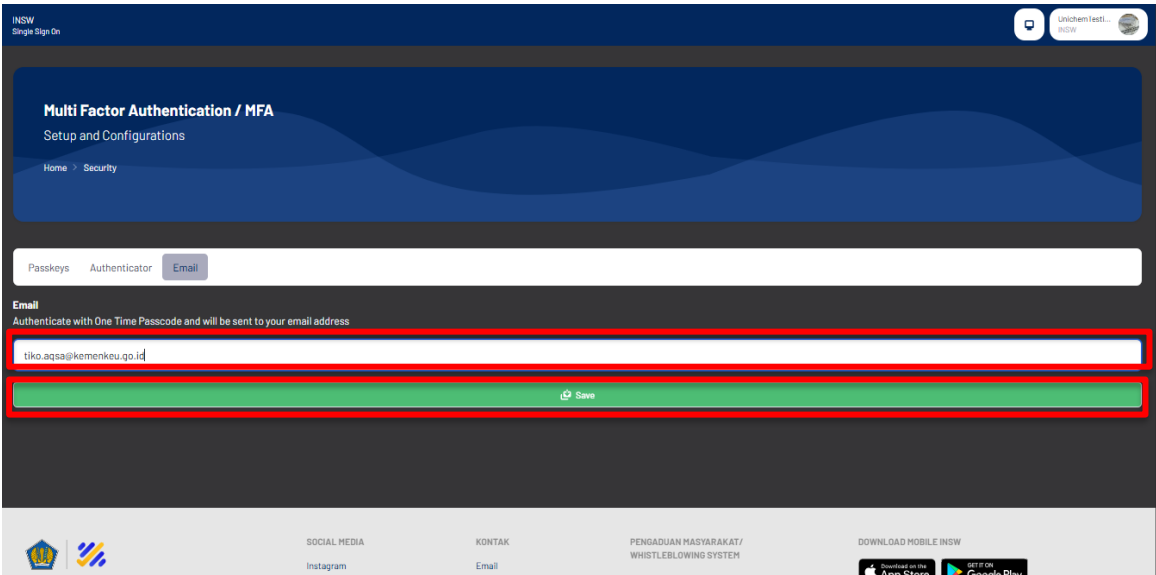
5. Setelah melakukan Sign-in, Anda akan masuk ke Home Single Sign On.



6. Klik **Security Settings** pada icon user pojok kanan atas.



7. Anda akan berada di halaman Multi Factor Authentication/MFA. Klik tab **Email** dan isi email pada kolom yang tersedia. Dalam proses pengaturan atau mengelola Multi-Factor Authentication (MFA), khususnya pada bagian yang berkaitan dengan email, pengguna memiliki fleksibilitas untuk mengubah alamat email yang terdaftar tanpa perlu meminta bantuan layanan pelanggan (contact center).
8. Klik **Save**.



INSW
Single Sign On

Multi Factor Authentication / MFA
Setup and Configurations

Home > Security

Passkeys Authenticator **Email**

Email
Authenticate with One Time Passcode and will be sent to your email address

7 tiko.agsa@kemenkeu.go.id

8 Save

SOCIAL MEDIA
Instagram

KONTAK
Email

PENGADUAN MASYARAKAT/
WHISTLEBLOWING SYSTEM

DOWNLOAD MOBILE INSW
Download on the App Store
GET IT ON Google Play

4.2 Metode Multi Factor Authentication (MFA) dengan Passkeys

Passkeys adalah cara baru untuk masuk ke aplikasi dan situs web. passkeys lebih mudah digunakan dan lebih aman dibandingkan kata sandi, sehingga pengguna tidak perlu lagi bergantung pada nama hewan peliharaan, tanggal lahir, atau “password123” yang terkenal sebagai password mereka. Sebaliknya, passkeys memungkinkan pengguna masuk ke aplikasi dan situs dengan cara yang sama seperti membuka kunci perangkat: dengan sidik jari, pemindaian wajah, atau PIN kunci layar. Dan, tidak seperti password, passkeys tahan terhadap serangan online seperti phishing, sehingga lebih aman dibandingkan kode OTP SMS. Passkeys adalah teknologi keamanan akun generasi berikutnya, dengan membandingkan *cryptographic secure key pairs* menjadikannya lebih aman dan dapat diandalkan, tidak seperti kata sandi yang bahkan diperkuat dengan autentikasi multi-faktor/MFA seperti One-Time Passcode (OTP). Agar fitur ini dapat berfungsi, Passkeys memerlukan perangkat dengan fungsi internet, wifi, dan Bluetooth.

Manfaat menggunakan metode Passkeys yaitu :

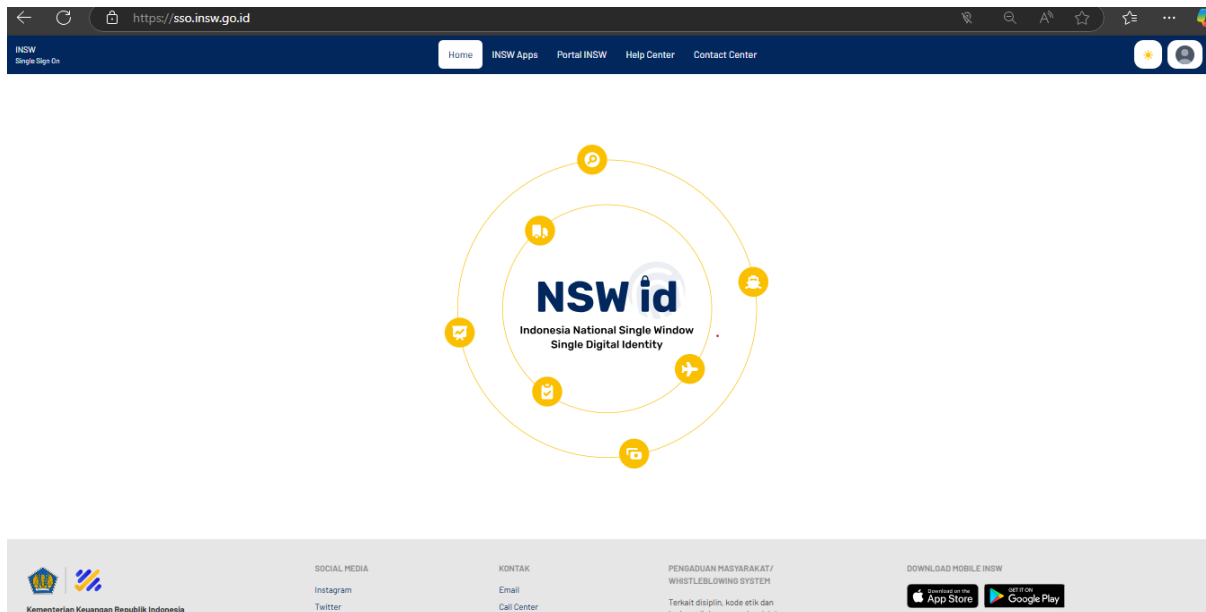
- Pengalaman yang lebih baik. Ucapkan selamat tinggal pada password yang rumit dan mengganggu serta MFA/OTP. Persyaratan keamanan kata sandi dan MFA/OTP dipenuhi oleh Passkeys.
- Kredensial yang kuat. Setiap passkeys didesain kuat. Mereka tidak pernah dapat ditebak, digunakan kembali, atau lemah.
- Aman dari phishing. Passkeys terpasang dengan aplikasi atau situs web tempat mereka dibuat, sehingga orang tidak akan pernah tertipu untuk menggunakan passkeys mereka untuk masuk ke aplikasi atau situs web palsu.

Untuk dapat menjamin keamanan akun Anda dalam penggunaan passkeys, perangkat yang Anda daftarkan harus memenuhi syarat sebagai berikut:

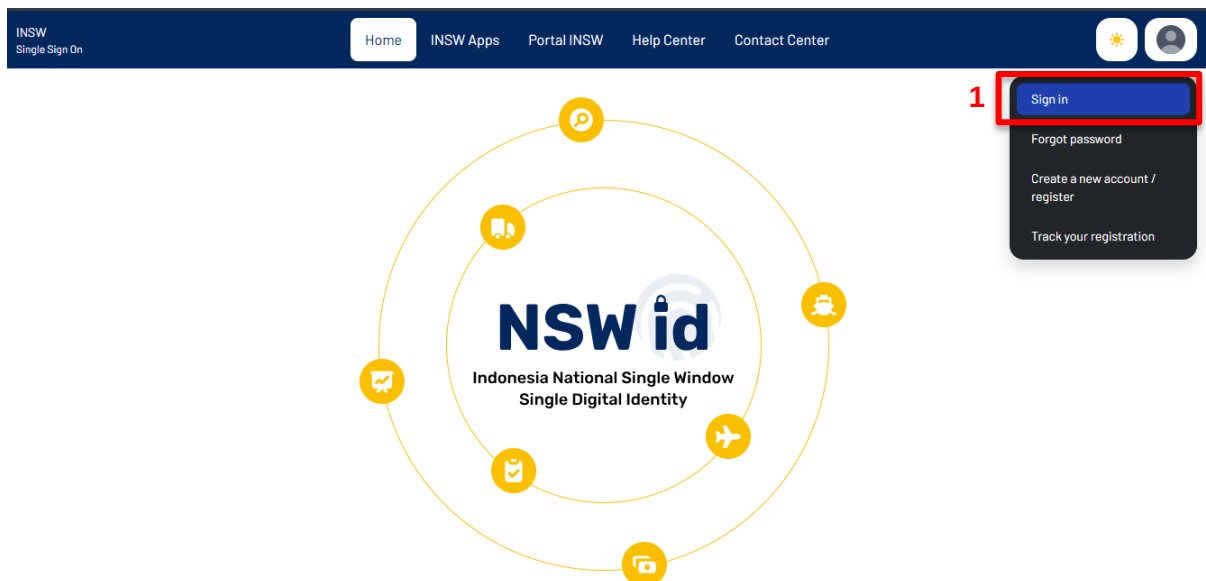
- Perangkat milik Anda atau perangkat kantor yang didelegasikan khusus kepada Anda, bukan perangkat yang dipakai bersama-sama.
- Perangkat Anda memiliki koneksi internet dan/atau bluetooth.
- Memiliki minimum versi sebagai berikut :

Jenis OS atau Perangkat Lunak	Versi Minimal
iOS/iPadOS/tvOS	16.0
macOS	13.0
Android	9.0 (Pie)
Windows	10
Semua Browser	Pastikan di versi terakhir/terupdate.

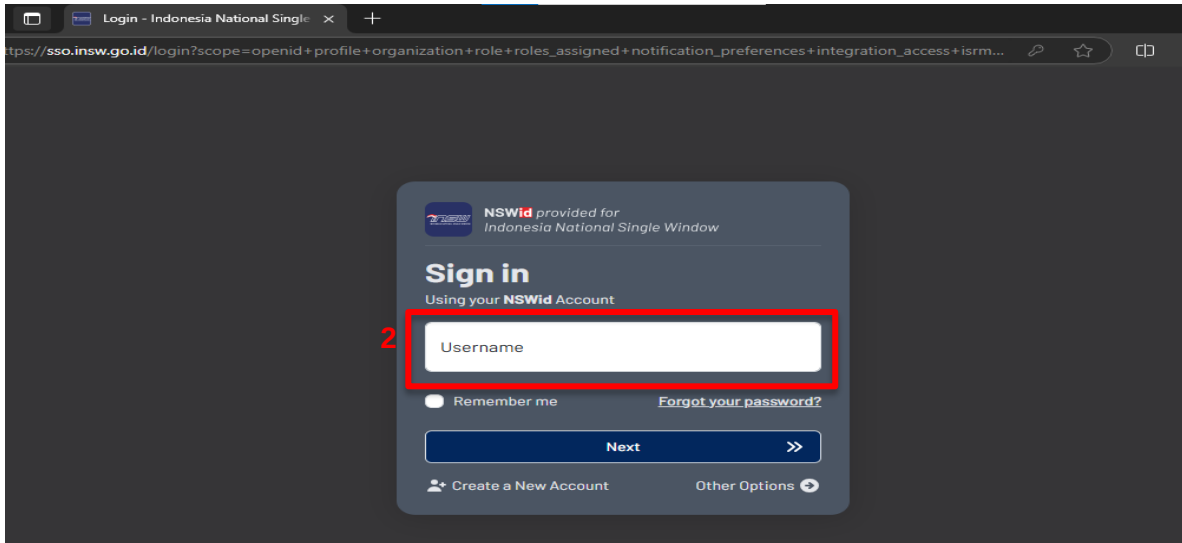
Multi Factor Authentication (MFA) dapat diakses melalui alamat <https://sso.insw.go.id>.
dengan tampilan awal berikut ini :



1. Klik icon user pada pojok kanan atas, kemudian klik **“Sign In”**.

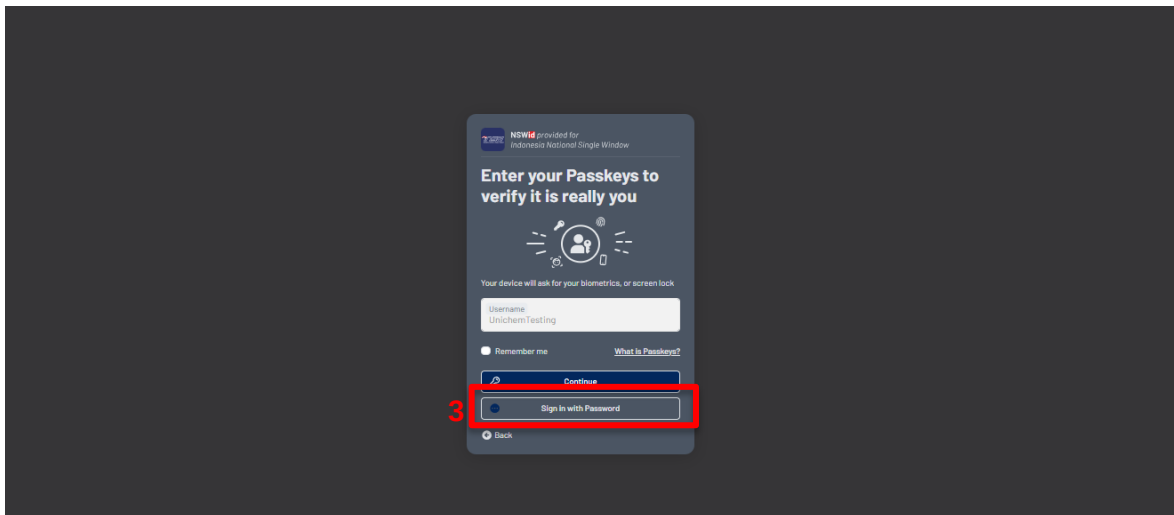


2. Untuk memulai aplikasi , Anda dapat memasukan **Username** lalu klik tombol next.



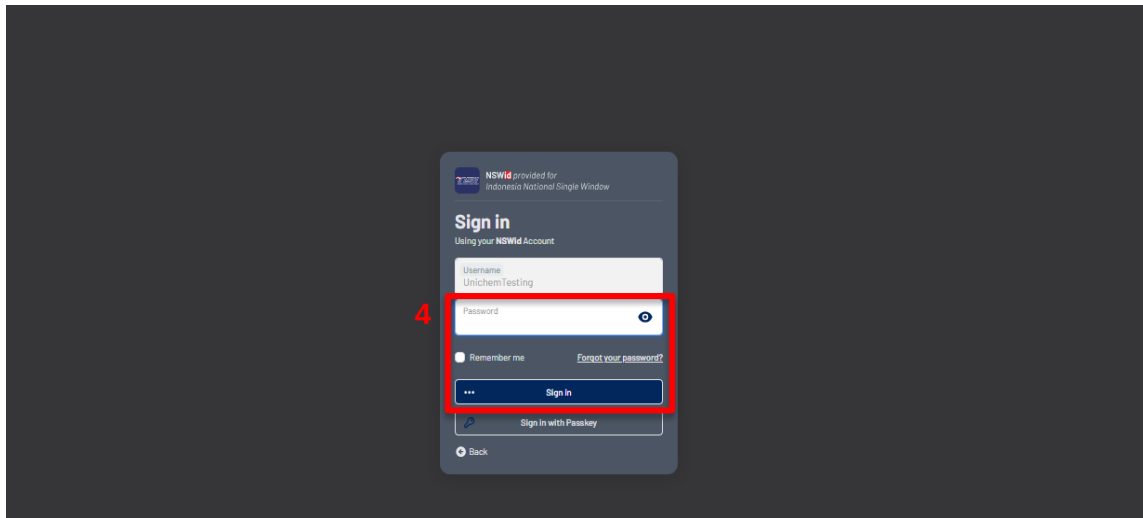
The screenshot shows a web browser window with the URL `https://sso.insw.go.id/login?scope=openid+profile+organization+role+roles_assigned+notification_preferences+integration_access+isrm...`. The page displays the "Sign in" form for the NSWid account. A red box highlights the "Username" input field, and a red number "2" is placed to its left. Below the input field are the "Remember me" checkbox, the "Forgot your password?" link, the "Next" button, and the "Create a New Account" and "Other Options" links.

3. Kemudian Anda klik **Sign in With Password**.

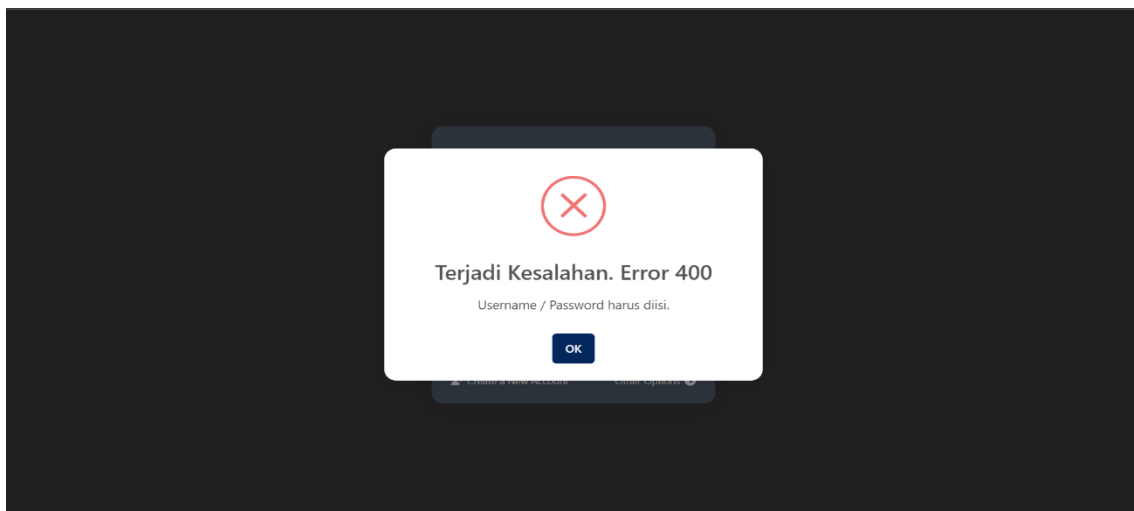


The screenshot shows the "Enter your Passkeys to verify it is really you" page. A red box highlights the "Sign in with Password" button, and a red number "3" is placed to its left. The page also displays the "Continue" button and the "Back" button. The "Username" field is pre-filled with "Unichem/Testing".

4. Lalu Anda dapat memasukkan **Password** dan klik **sign in** untuk masuk ke Home dari aplikasi.

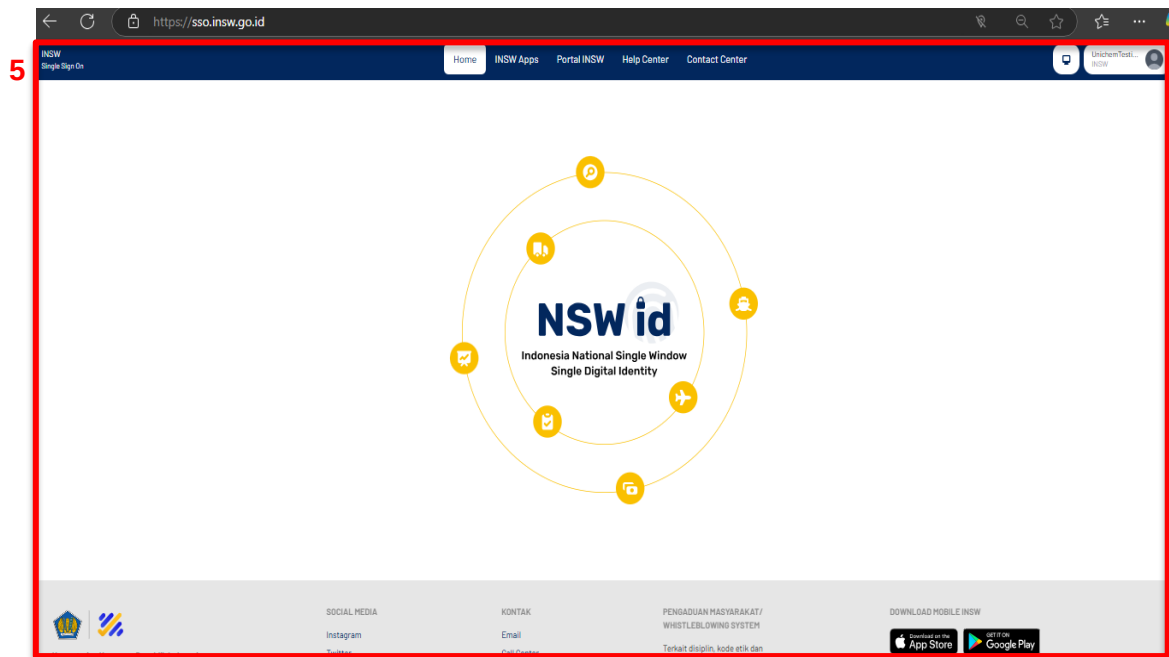


- a. Jika username dan password tidak sesuai maka akan tampil pesan seperti di bawah ini.

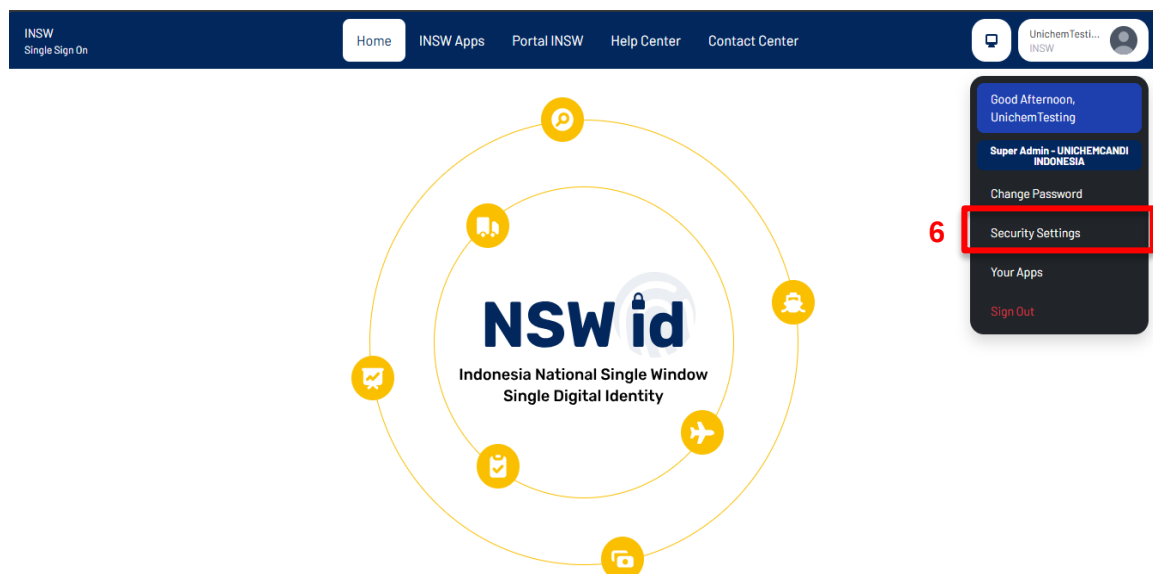


- b. Jika lupa password **Akun INSW**, klik **Lupa Password** dan masukkan **Email** dan **Username Akun INSW**.

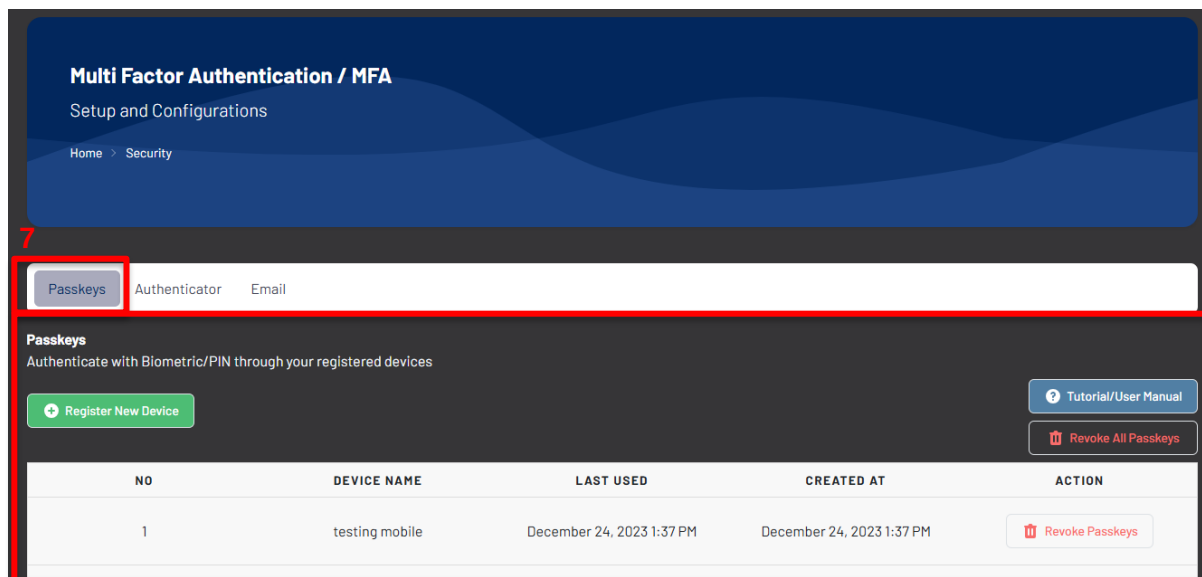
5. Setelah melakukan sign in, Anda akan masuk ke dalam Home Single Sign On



6. Klik **Security Settings** pada icon user pojok kanan atas.

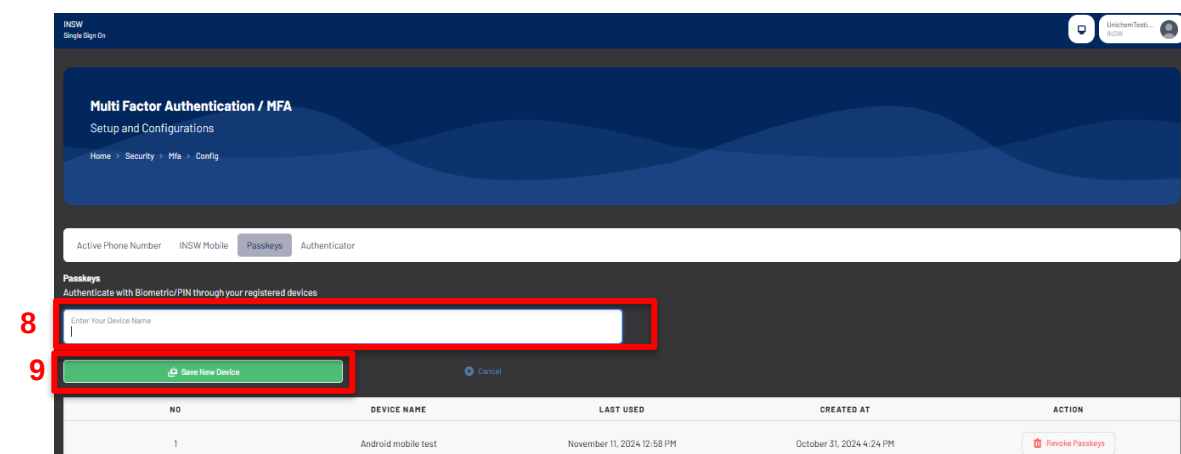


7. Anda akan berada di halaman Multi Factor Authentication/MFA. Klik tab **Passkeys** dan muncul tabel device nama yang telah terdaftar, jika Anda belum pernah mendaftarkan di Authenticator manapun anda dapat klik tombol **Register New Device**.

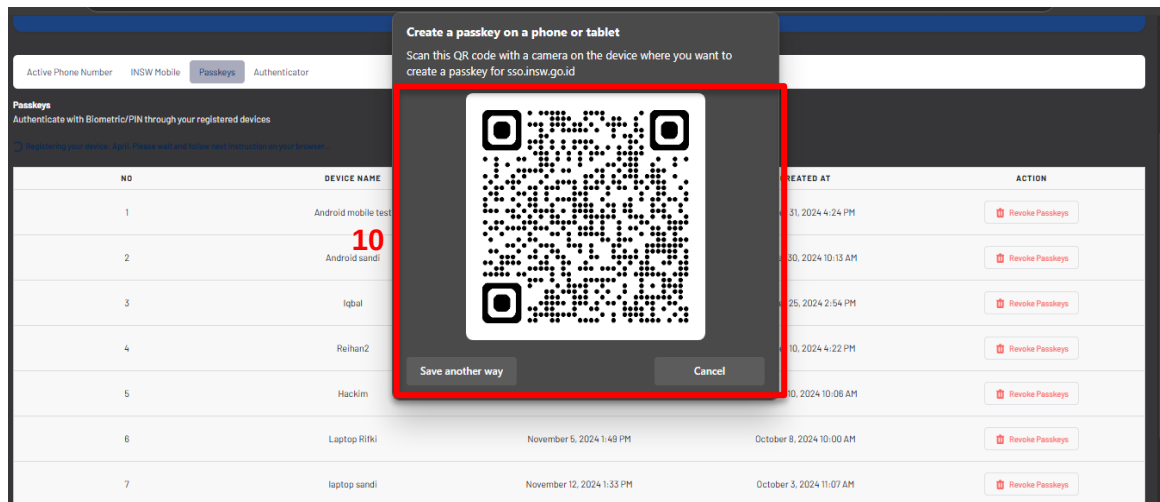


8. Isi nama device pada kolom yang tersedia.

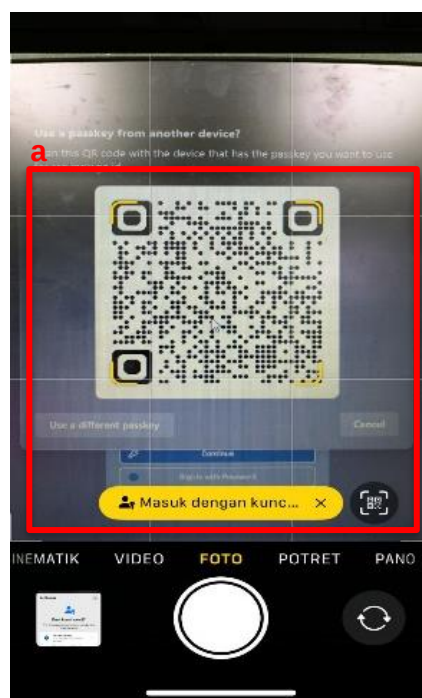
9. Kemudian, klik **Save New Device**



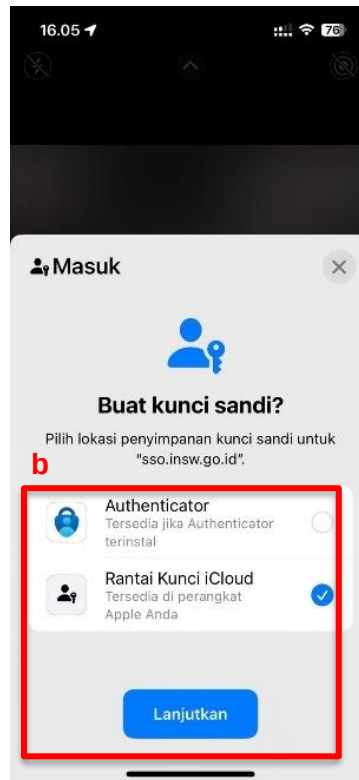
10. Langkah selanjutnya, akan muncul QR Code seperti di bawah ini. Untuk melakukan pendaftaran menggunakan Passkeys, Anda dapat membuka handphone Anda dan pastikan Anda telah memiliki aplikasi authenticator kemudian ikuti langkah – langkah berikut ini :



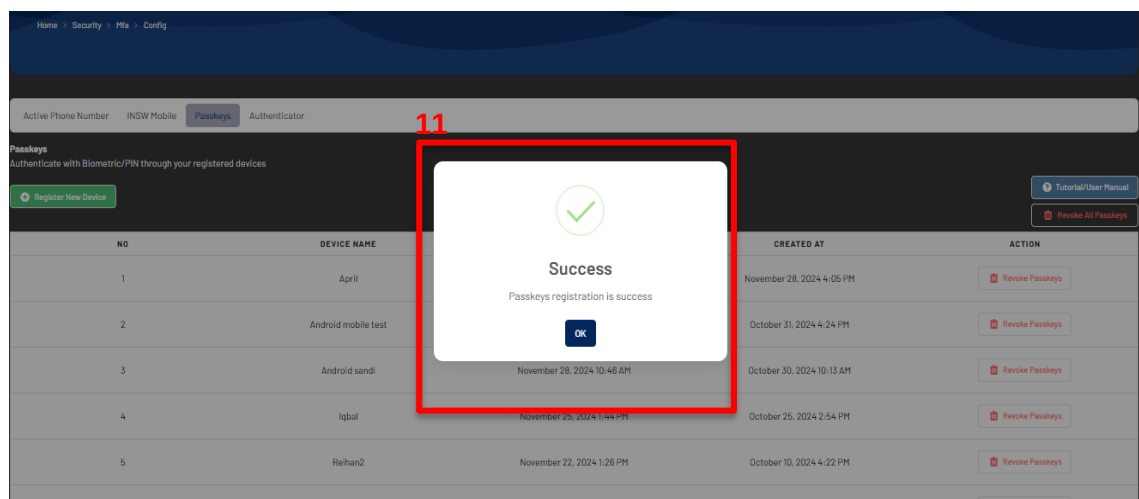
- a. Anda dapat membuka kamera handphone untuk melakukan Scan a QR Code yang ada di browser lalu klik tombol 'masuk dengan kunci' . Pastikan device yang akan didaftarkan berada di sekitar Anda.



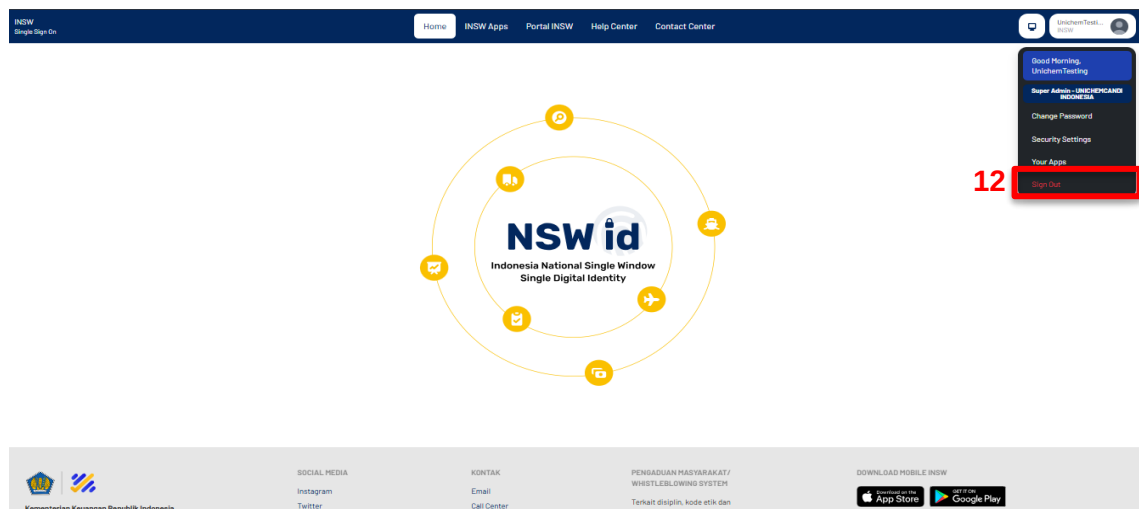
b. Klik rantai kunci icloud lalu klik lanjutkan.



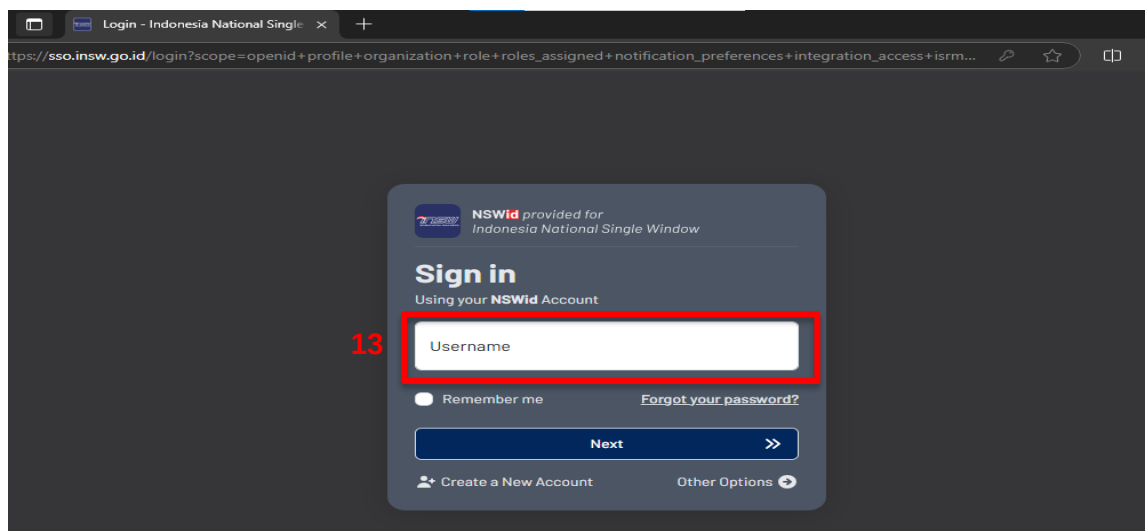
11. Kemudian, Anda dapat kembali pada halaman pengaturan authenticator di Browser Anda di tab Passkeys dan terdapat notifikasi pop-up pendaftaran passkeys berhasil dan nama Anda sudah berada di tabel nama-nama device.



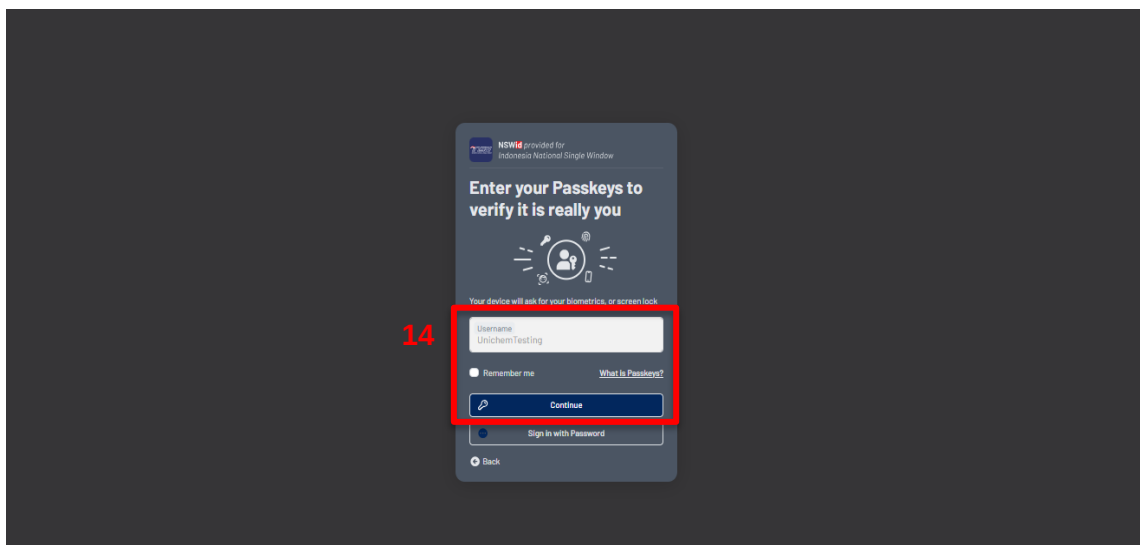
12. Setelah berhasil melakukan pendaftaran nama device di tab passkeys, Anda klik icon user di pojok kanan atas lalu klik **Sign Out** untuk keluar dari aplikasi. Kemudian Anda dapat sign in kembali menggunakan Sign in with passkeys



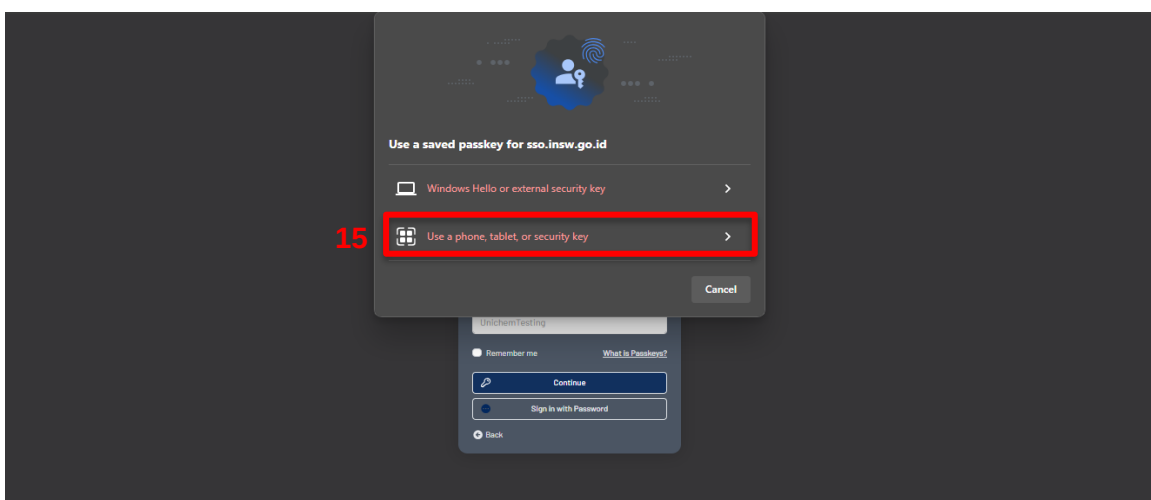
13. Silahkan Anda Isi username pada kolom yang tersedia, lalu klik tombol next



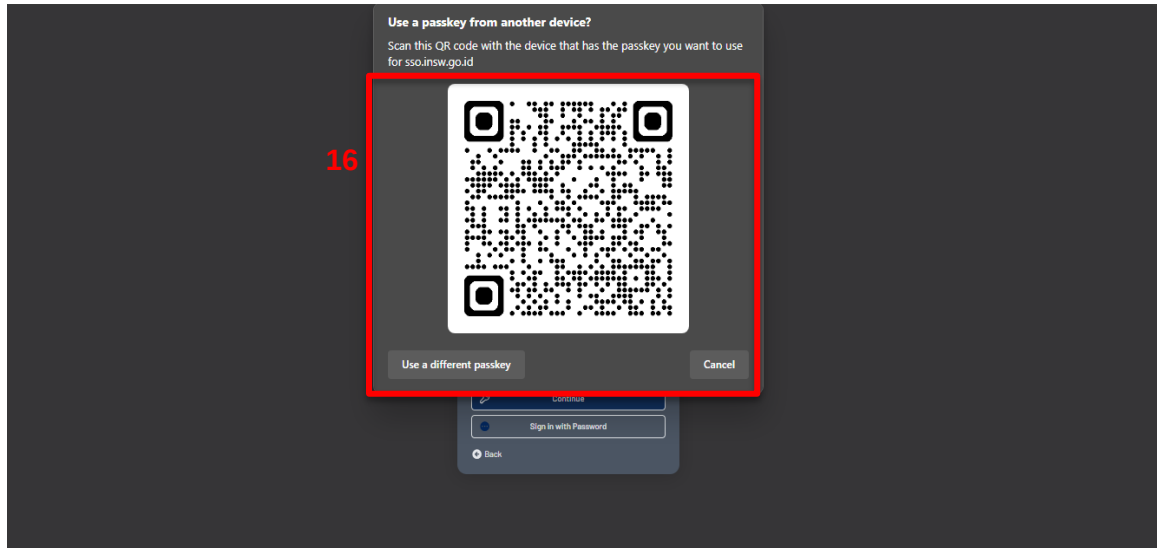
14. Kemudian Anda klik tombol **Continue**



15. Setelah itu Anda dapat klik **Use phone, tablet or security key**



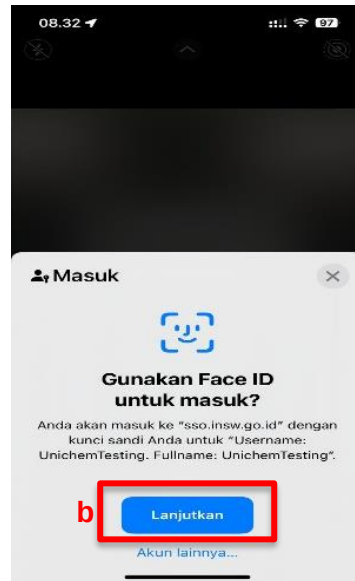
16. Berikutnya akan muncul QR Code. Anda dapat membuka handphone Anda dan ikuti langkah – langkah melakukan Scan QR Code berikut ini :



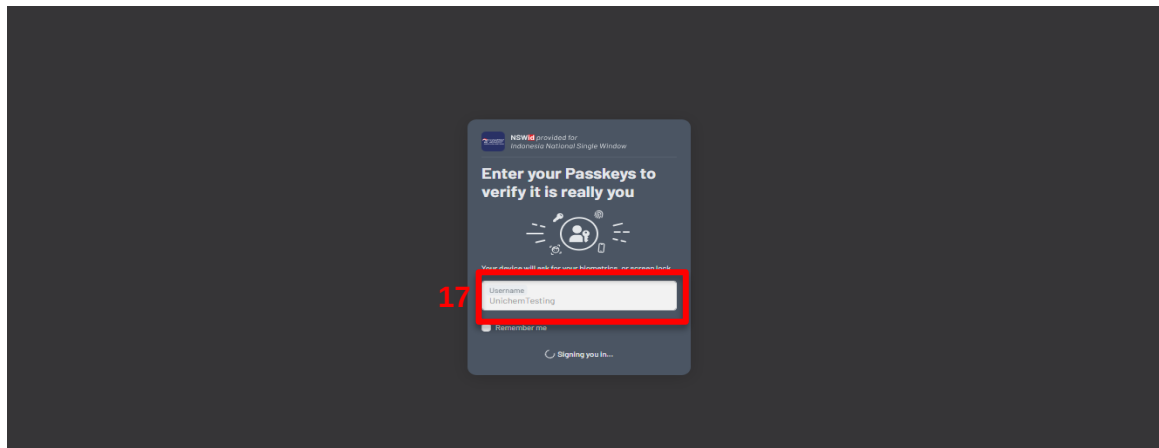
- a. Buka kamera yang ada di handphone Anda, lakukan scan QR Code yang ada di browser lalu klik tombol “masuk dengan kunci” seperti yang ada diatas



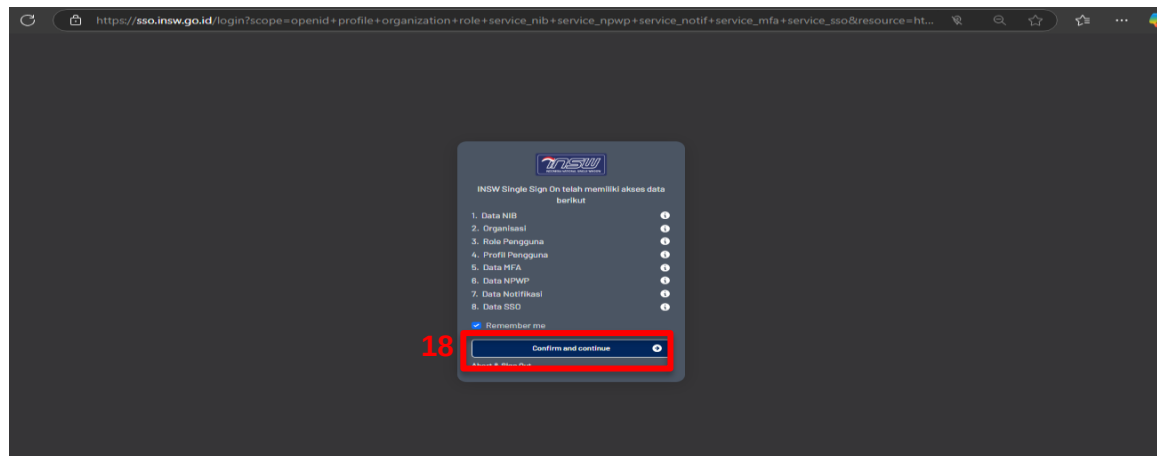
- b. Kemudian, klik **lanjutkan** untuk melakukan masuk ke dalam aplikasi.



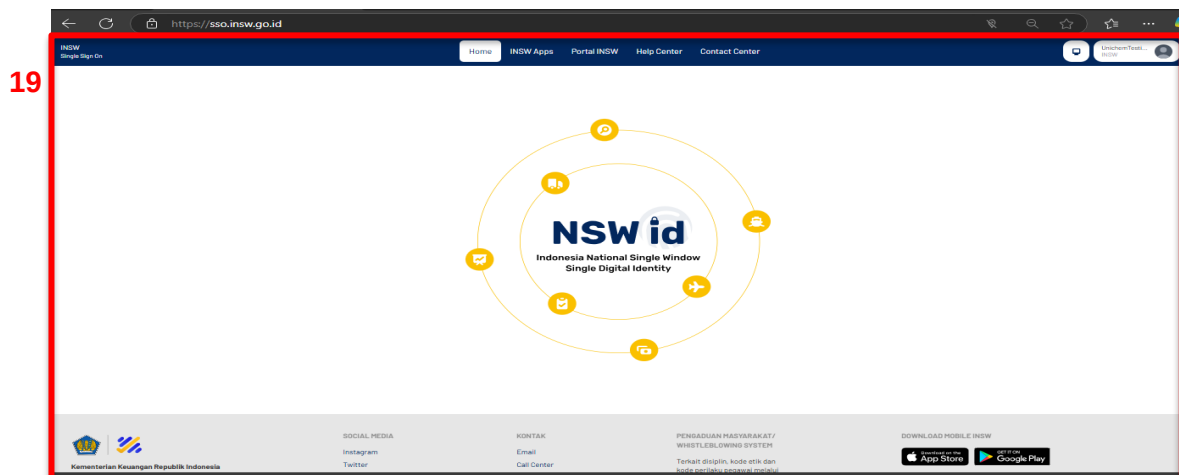
17. Setelah melakukan scan QR Code di handphone Anda, silahkan Anda kembali ke browser Anda dan melihat proses sign in seperti yang ada diatas.



18. Berikutnya, klik **Confirm and Continue**.

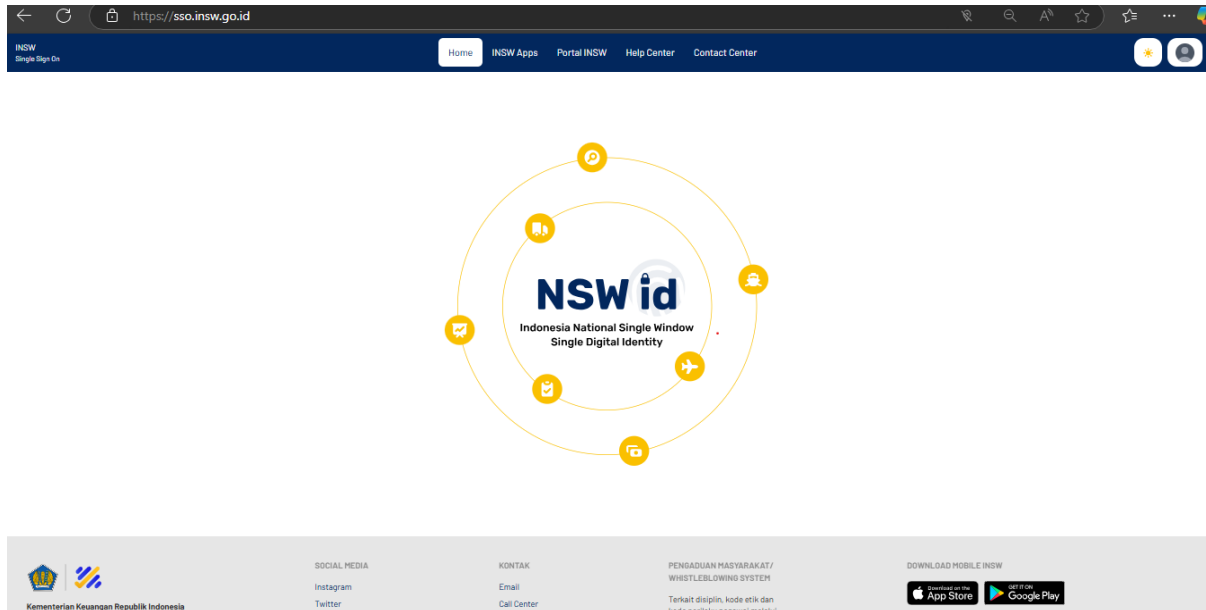


19. Setelah melakukan proses Sign in, Anda akan masuk ke Home dari aplikasi Single Sign On



4.3 Metode Multi Factor Authentication (MFA) dengan Authenticator

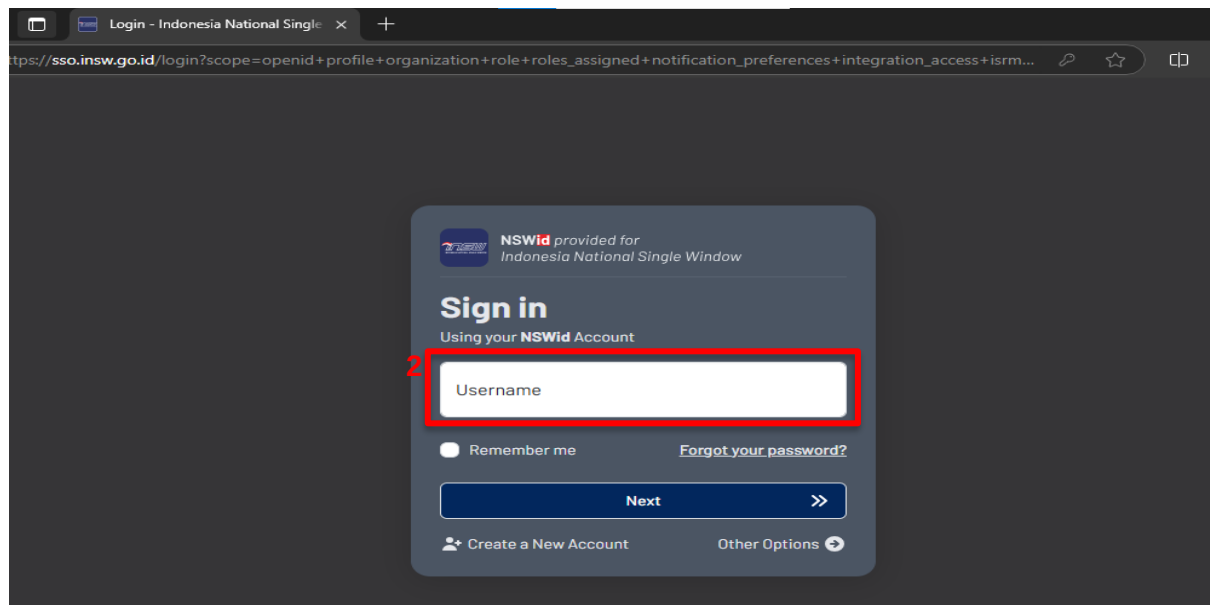
Multi Factor Authentication (MFA) dapat diakses melalui alamat <https://sso.insw.go.id> dengan tampilan awal berikut ini :



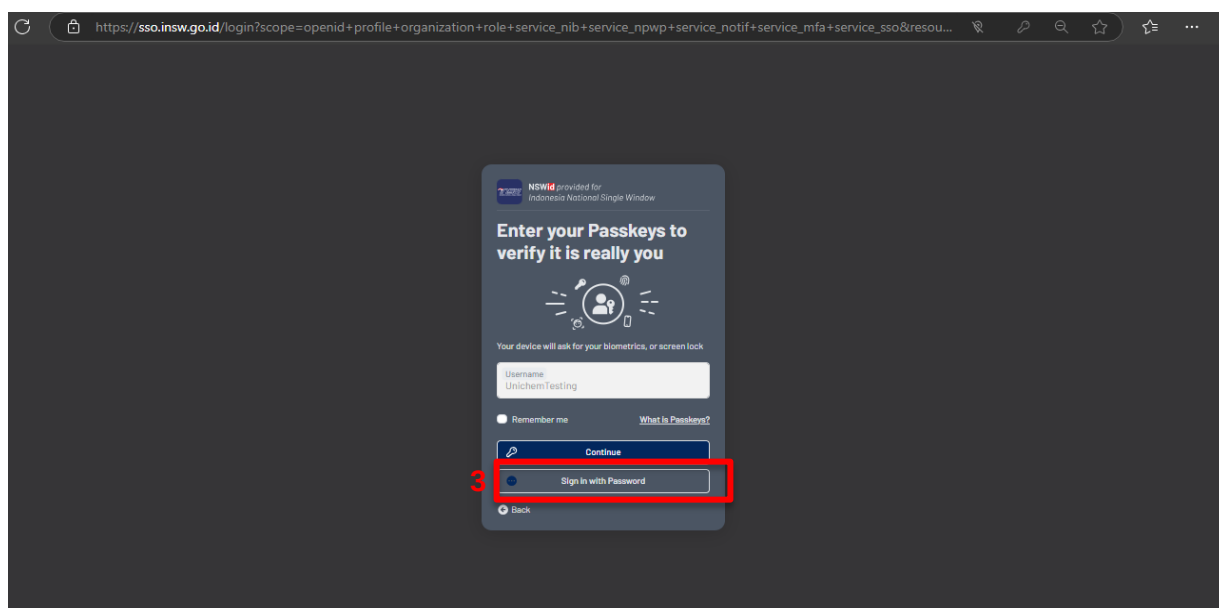
1. Klik icon user pada pojok kanan atas, kemudian klik **"Sign In"**.



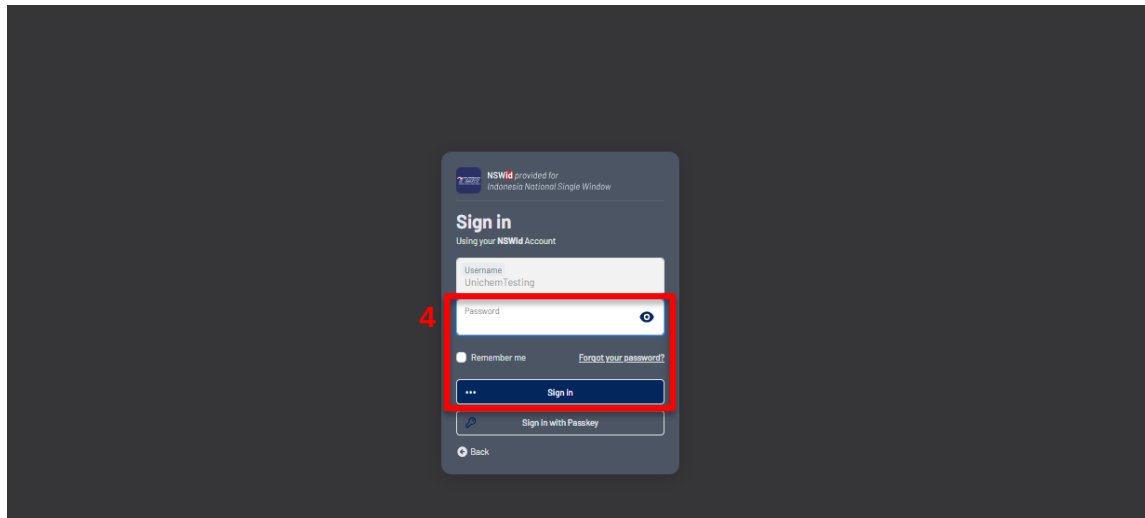
2. Klik icon user pada pojok kanan atas, kemudian klik **"Sign In"**.



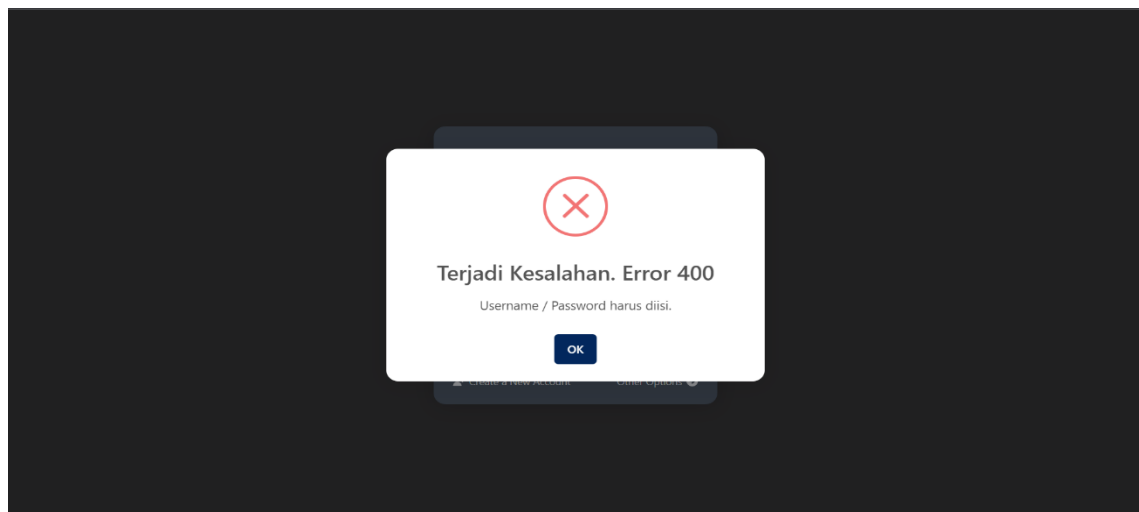
3. Untuk Kemudian Anda klik **Sign in With Password**.



4. Lalu Anda dapat memasukkan **Password** dan klik **sign in** untuk masuk ke Home dari aplikasi.

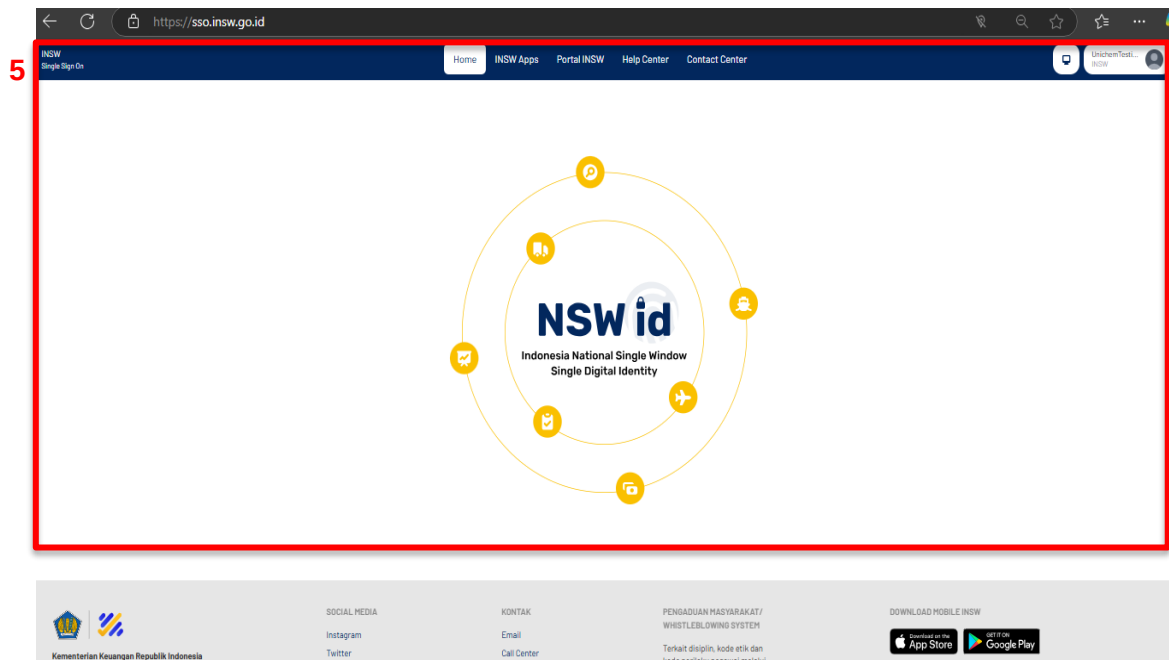


- a. Jika username dan password tidak sesuai maka akan tampil pesan seperti di bawah ini.



- b. Jika lupa password **Akun INSW**, klik **Lupa Password** dan masukkan **Email** dan **Username Akun INSW**.

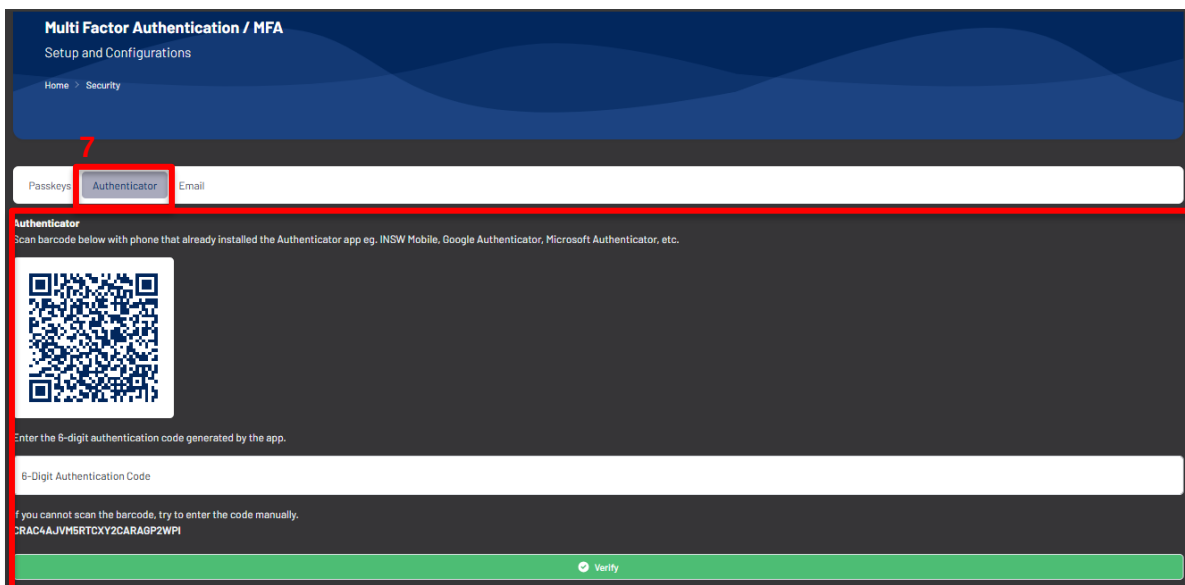
5. Anda akan masuk ke dalam Home Single Sign On.



6. Klik **Security Settings** pada icon user pojok kanan atas.

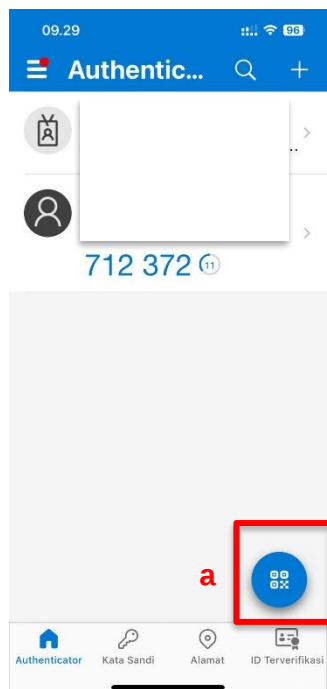


7. Anda akan berada di halaman Multi Factor Authentication/MFA. Klik tab **Authenticator** dan akan muncul QR Code jika Anda belum pernah mendaftarkan di Authenticator manapun.

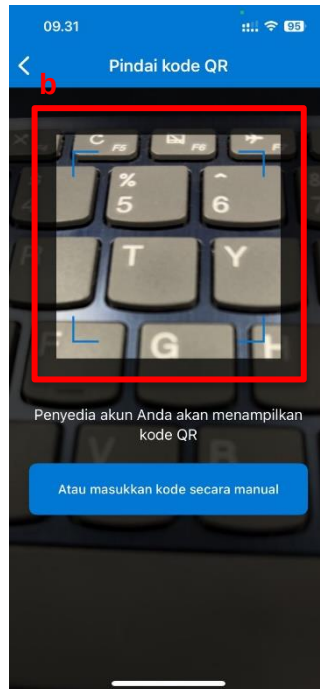


Untuk melakukan pendaftaran, Anda membutuhkan handphone yang sudah terinstal aplikasi authenticator untuk melakukan scan barcode dan memasukan kode unik. Berikut adalah langkah-langkahnya :

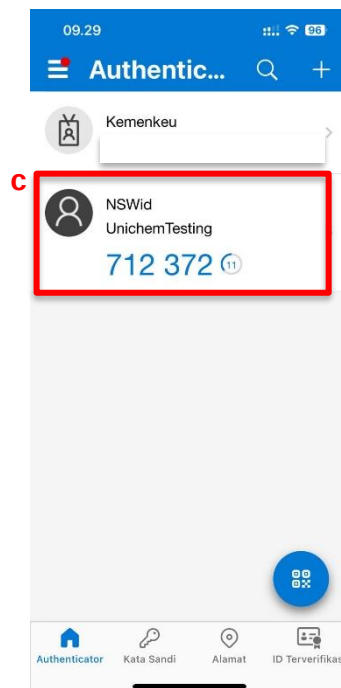
- a. Buka aplikasi authenticator. Anda dapat menggunakan Google Authenticator atau Microsoft Authenticator. Gambar diatas merupakan contoh Microsoft authenticator, Klik tombol di pojok Kanan Bawah, kemudian muncul pilihan diatas.



- b. Selanjutnya , scan dengan QR Code yang telah tersedia sebelumnya dalam browser

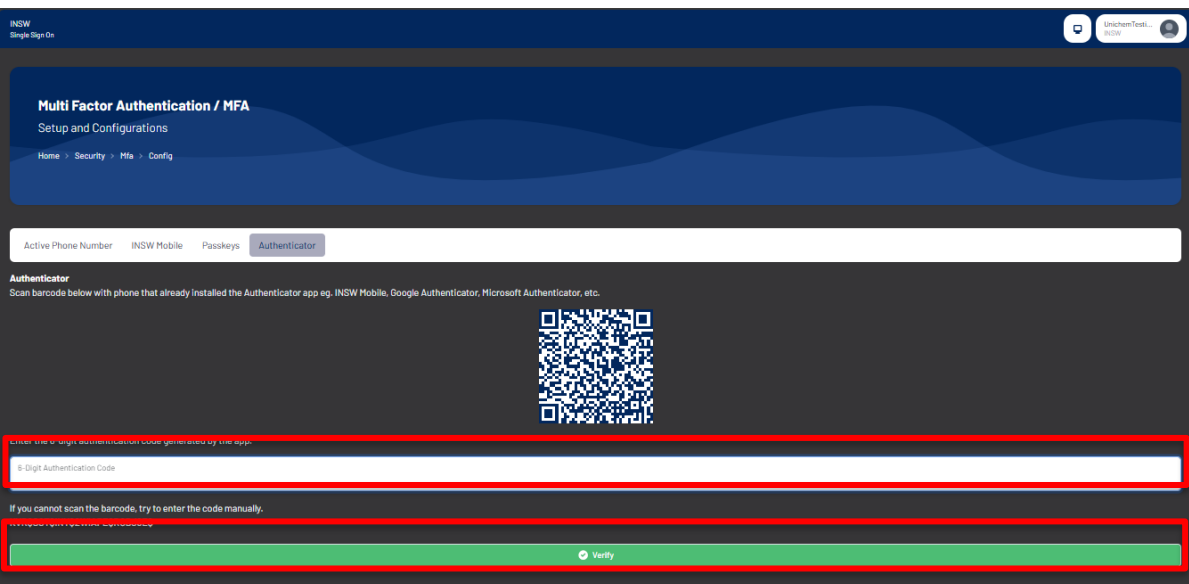


- c. Jika sudah berhasil melakukan scan a QR Code, akan muncul ke list Authenticator Anda **NSWid: <<USERNAME ANDA>>**

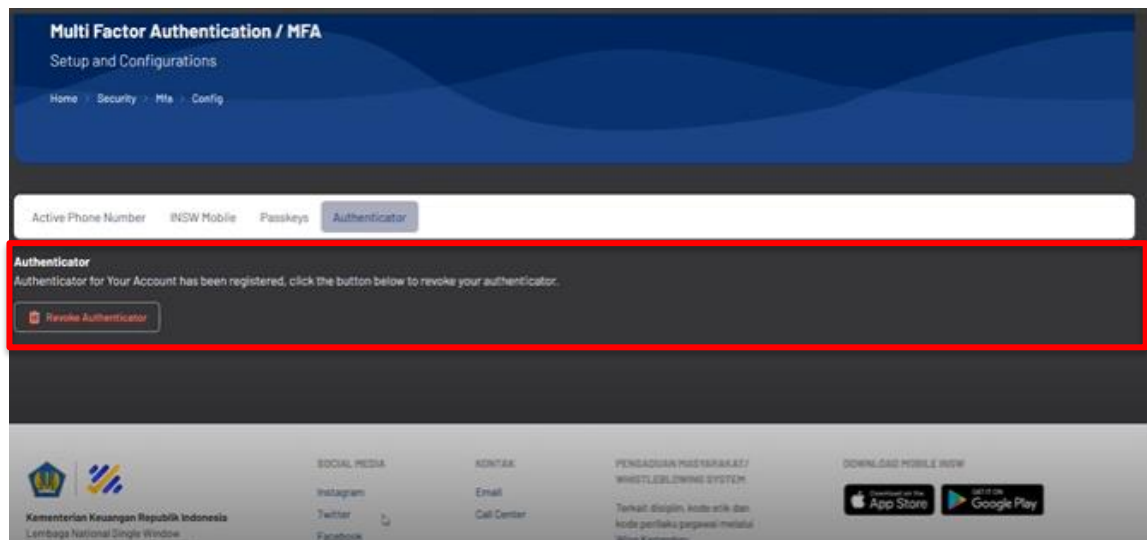


8. Setelah Anda melakukan scan QR Code dan mendapatkan list authenticator, Anda dapat kembali pada halaman pengaturan authenticator di Browser Anda. Kemudian masukan 6 Digit Kode pada kolom yang tersedia sebelum batas waktu nya habis (batas waktu 6 Digit Kode adalah 30 detik) , jika sudah mendekati waktu expired, disarankan tunggu hingga tergenerate kode baru.

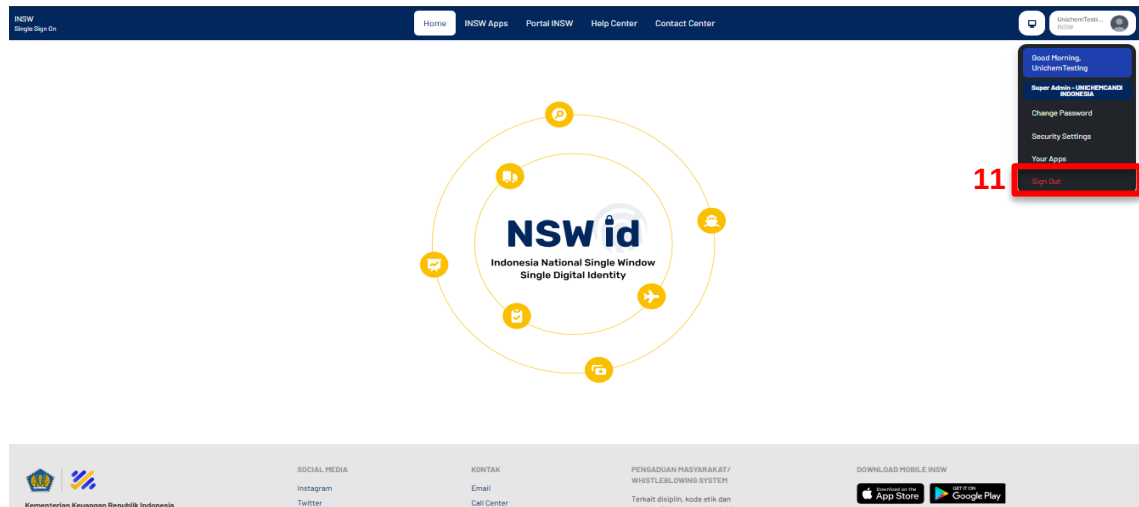
9. Klik **Verify**.



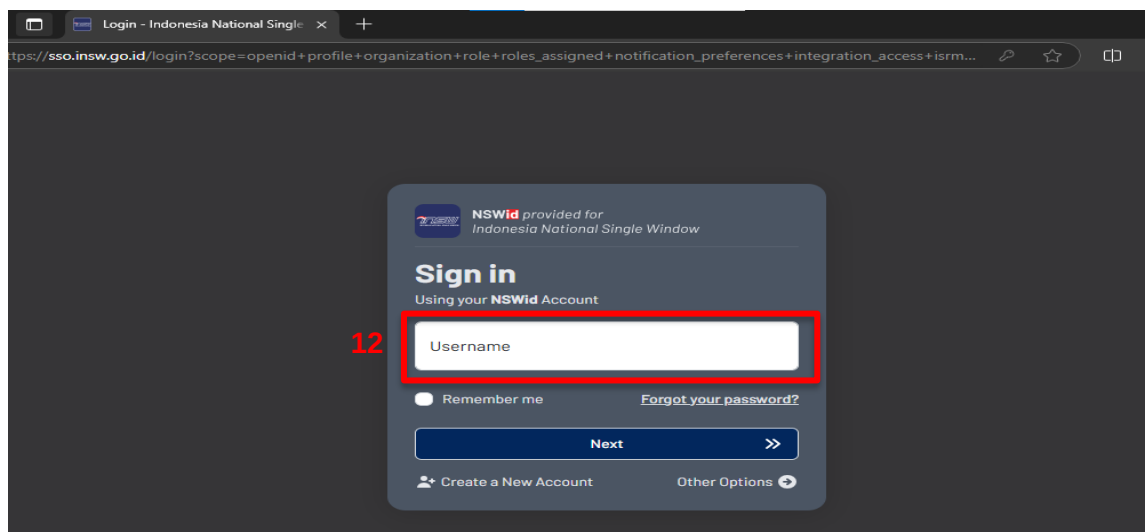
10. Setelah melakukan **verify** , akun Anda telah terdaftar authenticator



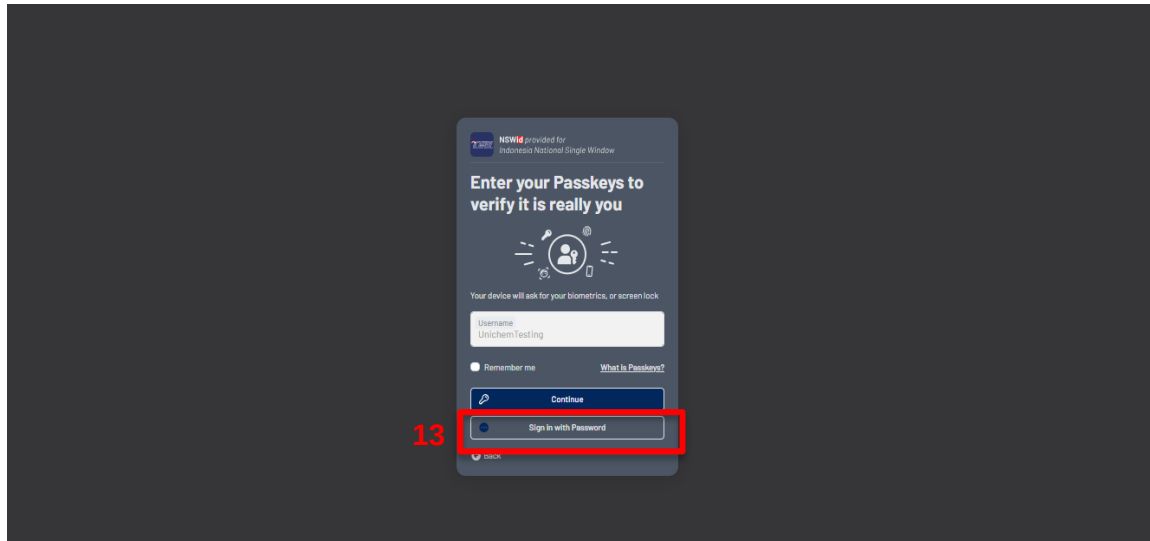
11. Setelah berhasil melakukan pendaftaran di authenticator, Anda klik icon user di pojok kanan atas lalu klik **Sign Out** untuk keluar dari aplikasi. Kemudian Anda dapat sign in kembali menggunakan Sign in with **authenticator**.



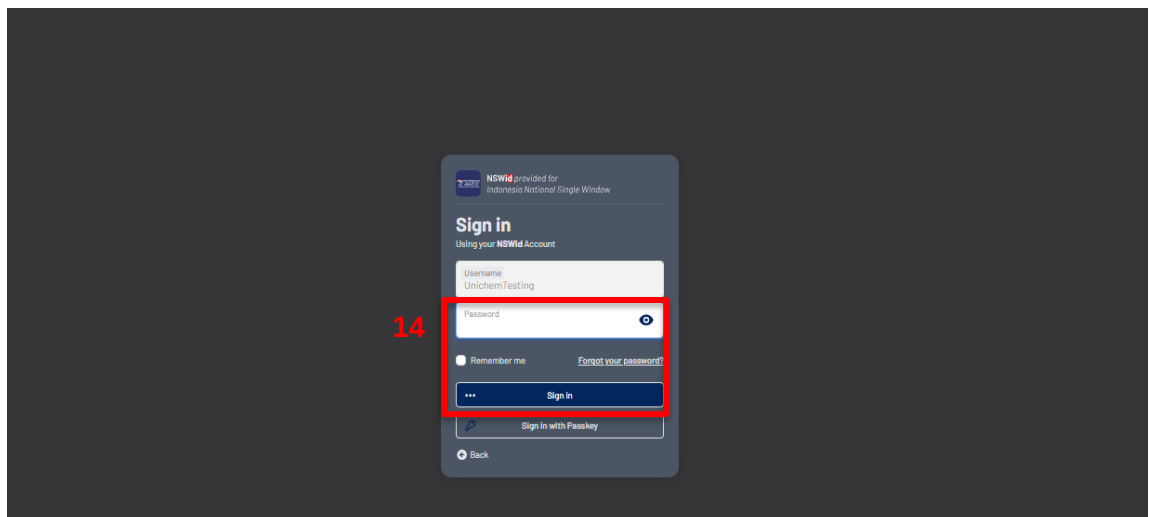
12. Silahkan Anda Isi username pada kolom yang tersedia, lalu klik tombol next



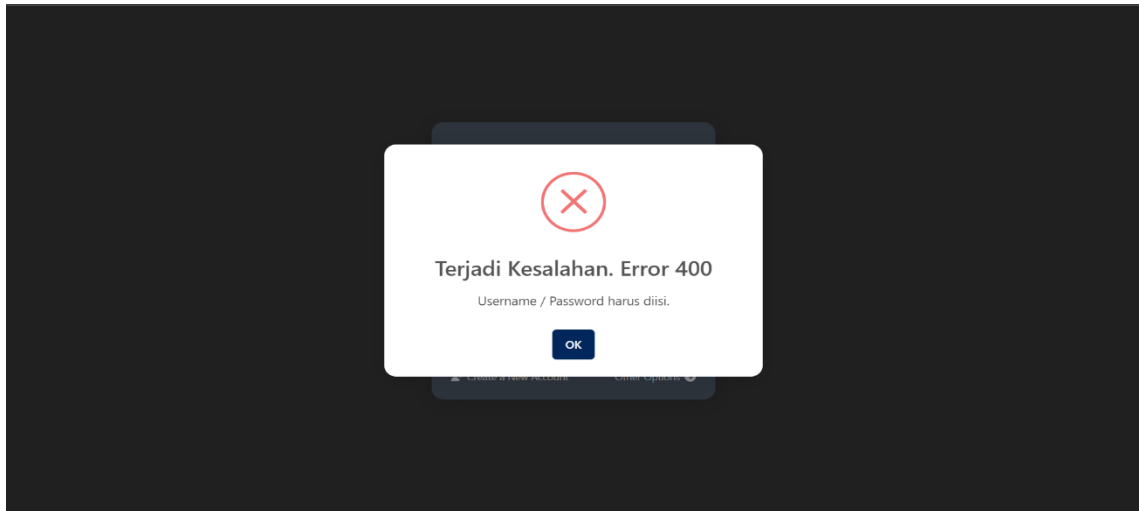
13. Kemudian Anda klik tombol **Sign With Password**



14. Lalu Anda dapat memasukan **Password** dan klik **sign in**.

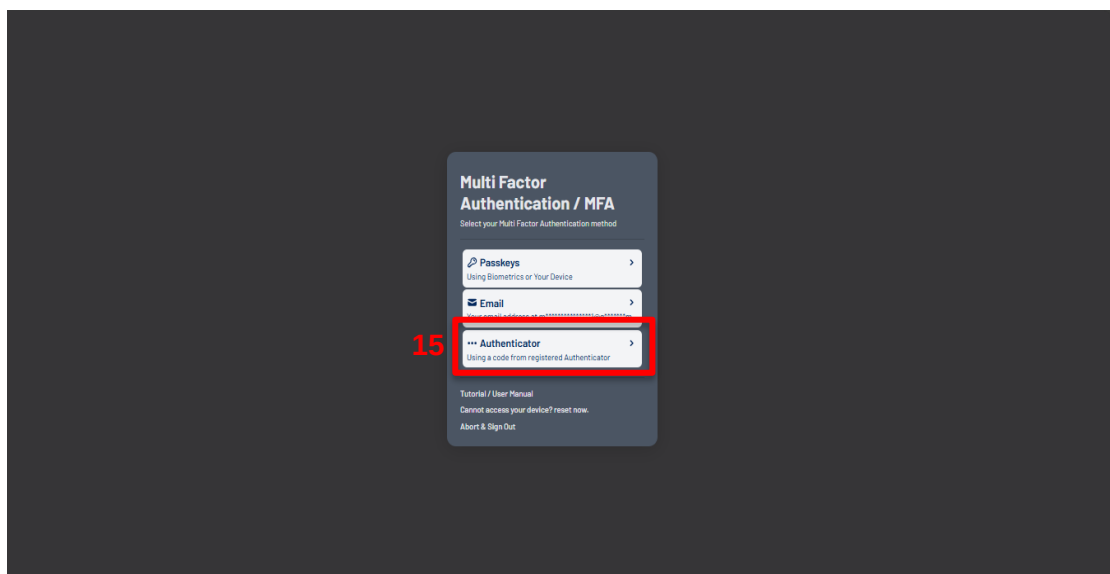


- a. Jika username dan password tidak sesuai maka akan tampil pesan seperti di bawah ini.



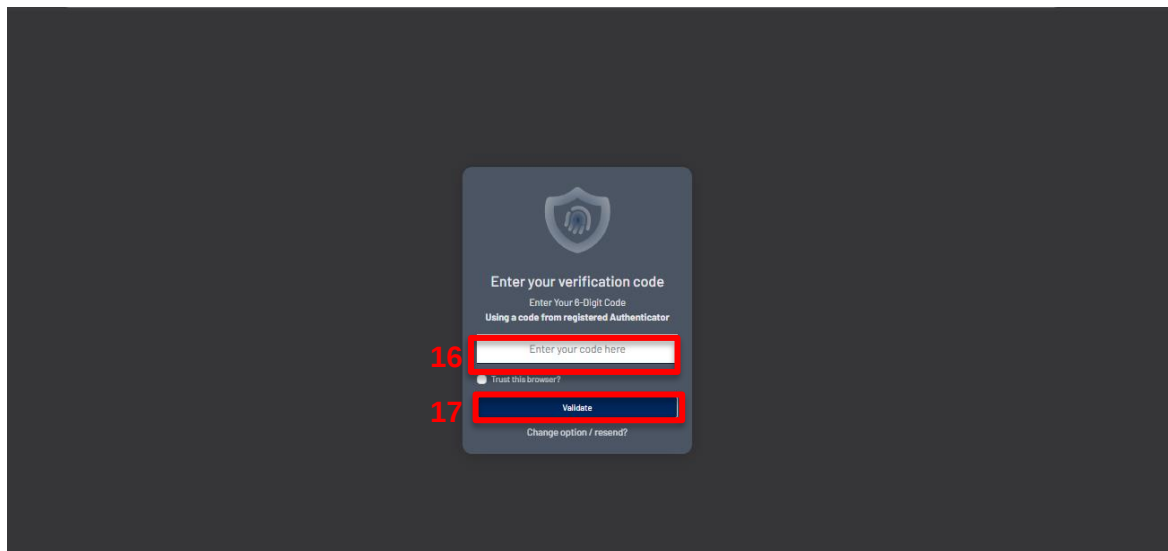
- b. Jika lupa password **Akun INSW**, klik **Lupa Password** dan masukkan **Email** dan **Username Akun INSW**.

15. Sebelum Anda masuk ke dalam Home, Anda akan mendapatkan pop-up berupa form multi factor authentication (MFA). Klik metode **Authenticator**.

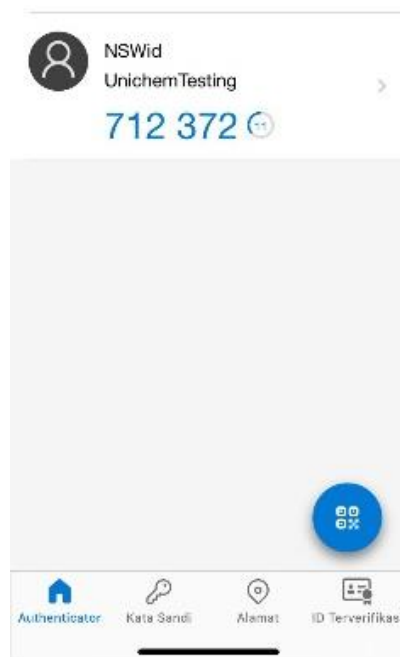


16. Anda akan diminta untuk memasukkan kode unik. Silahkan Anda cek aplikasi authenticator yang ada di handphone Anda dan akan mendapatkan list kode authenticator. Kemudian masukan 6 Digit Kode sebelum batas waktu nya habis (batas waktu 6 Digit Kode adalah 30 detik) , jika sudah mendekati waktu expired, disarankan tunggu hingga tergenerate kode baru.

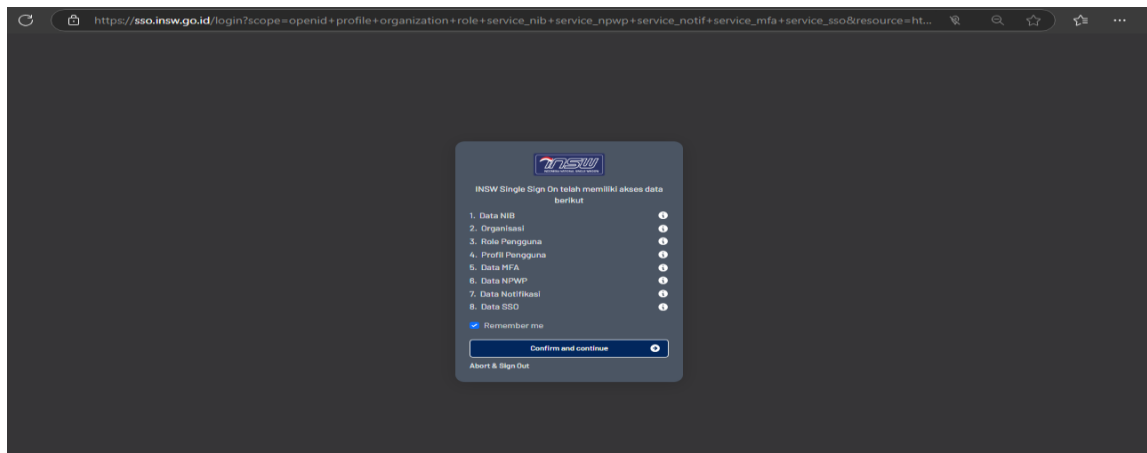
17. Klik **Validate**.



Contoh kode yang masuk dapat dilihat dibawah ini



18. Berikutnya, klik **Confirm and Continue**



19. Setelah berhasil melakukan proses sign in Anda akan masuk ke Home dari aplikasi Single Sign On

19

