THE UNITED REPUBLIC OF TANZANIA
PRESIDENT'S OFFICE
e-GOVERNMENT AUTHORITY
ISO 9001: 2015 Certified

NGAO PLATFORM
(Multi-Factor Authentication System)

User Manual

(GMS)

Published: July, 2025

Contents

1 Introduction

The Government Mailing System (GMS) is an official email platform for Tanzanian government institutions. To enhance its security, the GMS has been integrated with the NGAO Platform — a centralized Multi-Factor Authentication (MFA) solution developed by the e-Government Authority (e-GA). This integration ensures that only authorized users with proper authentication credentials can access sensitive government communication tools.

The NGAO Platform provides secure and flexible authentication options, including One-Time Passwords (OTP) via SMS or USSD, Time-based OTPs (TOTP) via the NGAO Authenticator App, and hardware-based tokens such as security keys. By enforcing MFA, the GMS ensures strong identity verification and reduces the risks of unauthorized access and data breaches.

1.1 Overview of NGAO Platform

The NGAO Platform is an authentication gateway designed by the Government to serve as the second layer of security across multiple government digital services. Its primary goals include:

- Strengthening access control through secure multi-factor authentication mechanisms.
- Supporting interoperability across various systems such as GMS, ERMS, e-Office, OSAT, and mGov.
- Allowing users to choose authentication methods that suit their preferences and technical environment.

Supported authentication methods on NGAO Platform include:

- **SMS OTP** – One-time passcode sent to the registered mobile number.
- **USSD OTP** – One-time passcode that can be accessed om USSD Menu *152*00*46# from a registered mobile number.
- **NGAO Authenticator App (TOTP)** – Time-based passcode generated on a mobile app.
- **Email OTP** – OTP sent to the registered institutional email.
- **Hardware Security Key** – Cryptographic security key such as YubiKey or similar.

1.2 Purpose of the Manual

This manual provides a step-by-step guide for users of the Government Mailing System (GMS) on how to:

- Register for Multi-Factor Authentication through the NGAO Platform.
- Authenticate login attempts using supported MFA options.
- Set up and use the NGAO Authenticator App for secure OTP generation.
- Manage and update their MFA settings within GMS.
- Troubleshoot common issues related to registration and authentication.

The guide is designed for end-users in government institutions who are required to secure their GMS accounts using NGAO. Whether using SMS, USSD, hardware keys, or the NGAO app, this manual ensures users can confidently navigate the secure login process.

2 Getting Started

2.1 Prerequisites for NGAO Platform Registration and Authentication

Before registering and authenticating with the NGAO Platform for GMS, ensure the following prerequisites are met:

1. **Valid GMS Account**
    - You must have an active GMS email account (e.g., name.surname@gms.go.tz or name.surname@gov.go.tz).
    - Ensure that you know your username and password for logging into the GMS portal.
2. **Mobile Device for OTP or USSD Authentication**
    - A mobile phone is required to receive authentication codes via SMS or to initiate verification via USSD menu. Make sure your number is active and reachable through Tanzanian mobile operators.
3. **NGAO Authenticator App** *(Optional but Recommended)*
    - For Time-based OTP (TOTP) generation, download and install the NGAO Authenticator App from the Play Store or App Store.
4. **Hardware Security Key** *(Optional)*
    - If you prefer physical authentication, ensure you possess a supported security key (e.g., YubiKey) compatible with the NGAO Platform.
5. **Internet Access**
    - A stable internet connection is required to access the GMS login portal and the NGAO Platform.

2.2 Accessing the GMS System

The Government Mailing System can be accessed via its official portal:

🔗 **GMS Portal URL**: https://mail.ega.go.tz *(example URL)*

Login Requirements:

- **Username**: Your government email (e.g., firstname.lastname@ega.go.tz)
- **Password**: The associated account password

If MFA registration has not yet been completed, you will be redirected to the NGAO Platform upon login to initiate registration.

2.3 Common Terminology

Term	Definition
OTP	One-Time Passcode used for authentication, valid for a short time
TOTP	Time-based OTP generated by the NGAO Authenticator App
MFA (Multi-Factor Authentication)	A login process requiring two or more verification steps
Hardware Key	A physical security device used for identity verification
SMS/USSD Verification	An authentication method involving code sent via SMS or verified over USSD
NGAO Platform	Central MFA system used across government platforms
GMS	Government Mailing System for official government email communication

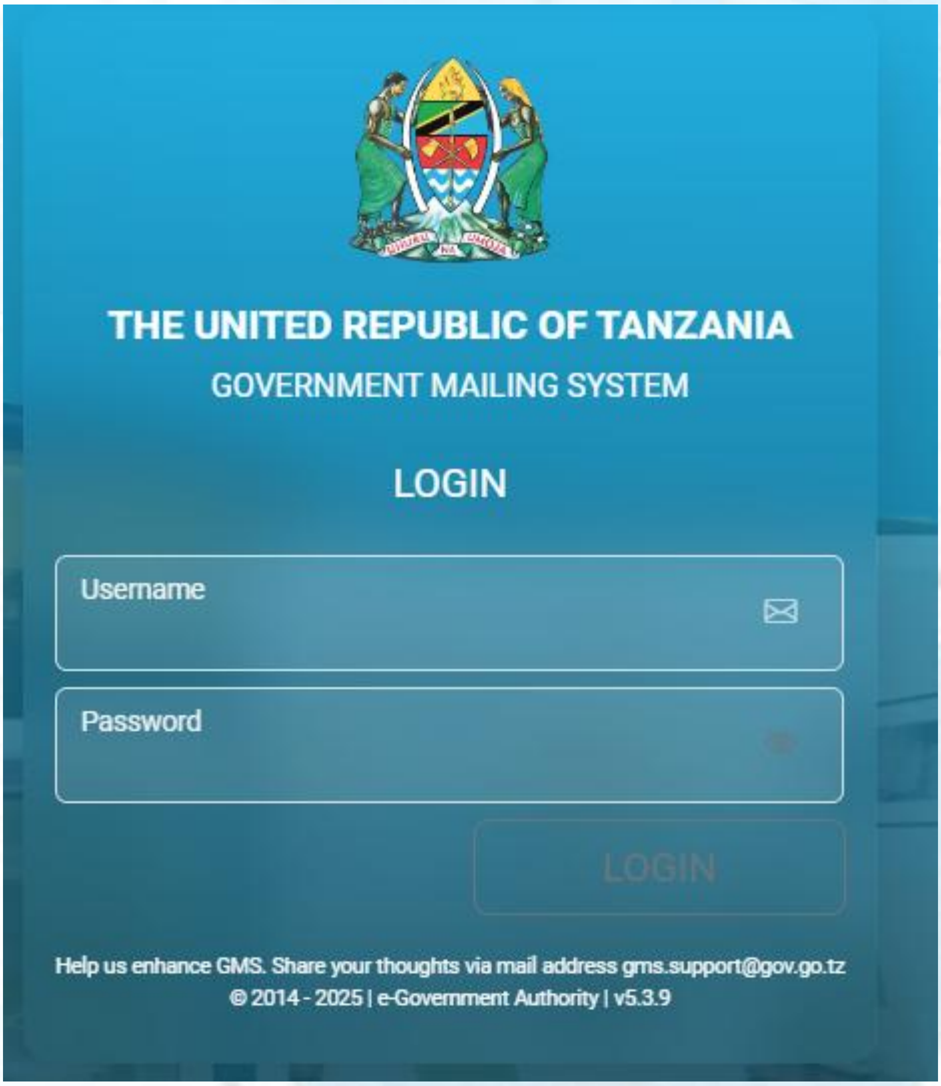
3 Registration into NGAO Platform

This section provides a detailed, step-by-step guide for registering your GMS account into the NGAO Platform for Multi-Factor Authentication (MFA).

3.1 Step 1: Logging into GMS

1. Open your preferred web browser.
2. Navigate to the GMS login portal:
   - 🔗 https://mail.ega.go.tz *(example placeholder)*
3. Enter your official government email (e.g., firstname.lastname@ega.go.tz) and password.
4. Click **Login**.

✅ If your account has not yet been registered with NGAO, you will be automatically redirected to the NGAO Platform to complete the MFA setup.


THE UNITED REPUBLIC OF TANZANIA

GOVERNMENT MAILING SYSTEM

Help us enhance GMS. Share your thoughts via mail address gms.support@gov.go.tz

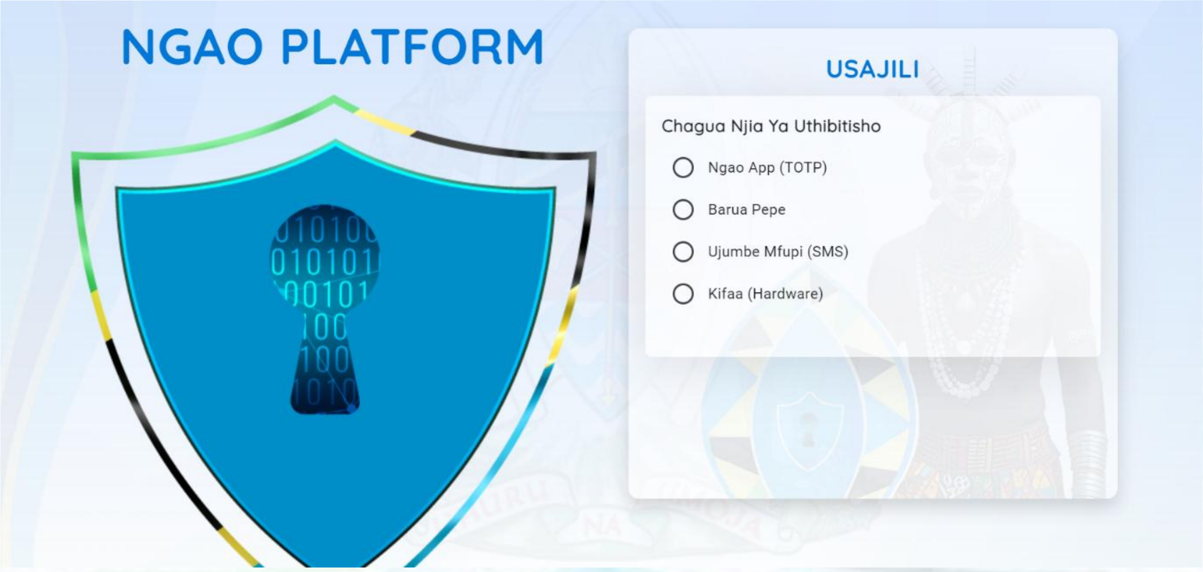
© 2014 - 2025 | e-Government Authority | v5.3.9

Figure 1 GMS Login Page

3.1 Step 2: Redirect to NGAO Platform for Registration

After successful login to GMS, you will be redirected to the NGAO Platform registration screen.

Here, you will be prompted to select your preferred authentication method(s) for MFA. You may choose one or more options depending on institutional policy and your device capabilities.



Chagua Njia Ya Uthibitisho

○ Ngao App (TOTP)

○ Barua Pepe

○ Ujumbe Mfupi (SMS)

○ Kifaa (Hardware)

Figure 2 NGAO Authentication Methods Options

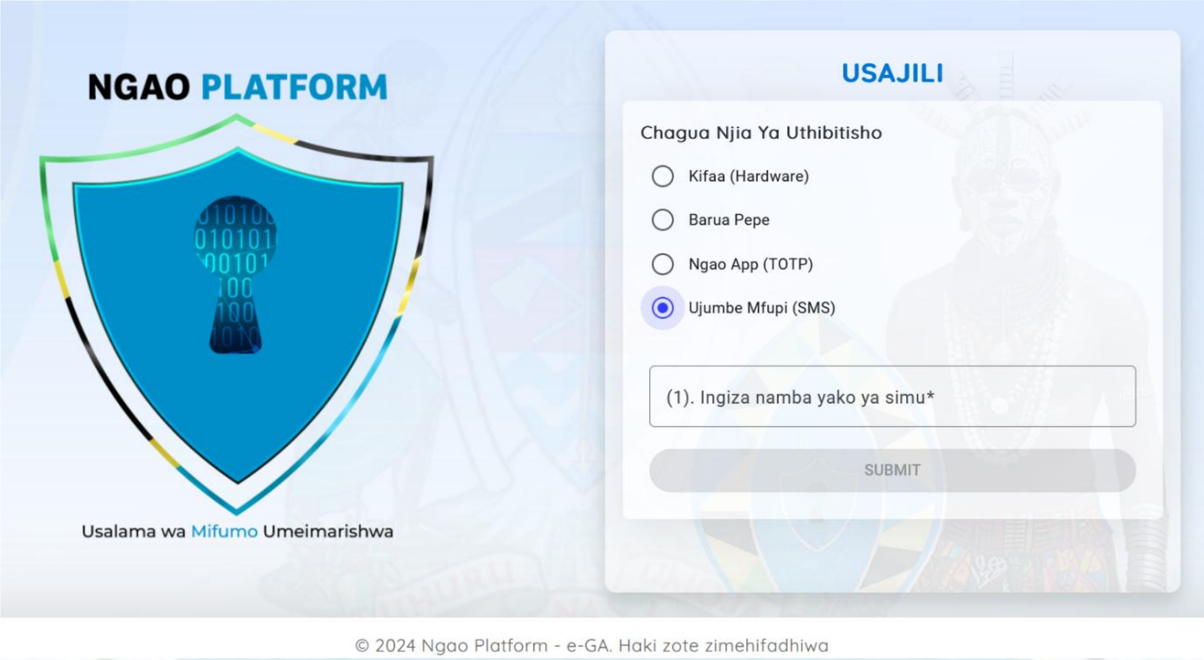
Step 3: Selecting Authentication Methods

NGAO offers the following authentication options:

Method	Description
SMS OTP	A 6-digit code sent via SMS to your registered phone number.
Email OTP	A one-time passcode sent to your registered email address.
TOTP (NGAO App)	A time-based OTP generated via the NGAO Authenticator App.
Hardware Key	A USB or NFC-based physical security device (e.g., YubiKey).
SMS/USSD Verification	A USSD prompt sent to your mobile number for authentication approval.

➤ **To Register:**

1. **SMS OTP**:
   - Enter your phone number.
   - You will receive a 6-digit code via SMS.



USAJILI

Chagua Njia Ya Uthibitisho

○ Kifaa (Hardware)

○ Barua Pepe

○ Ngao App (TOTP)

● Ujumbe Mfupi (SMS)

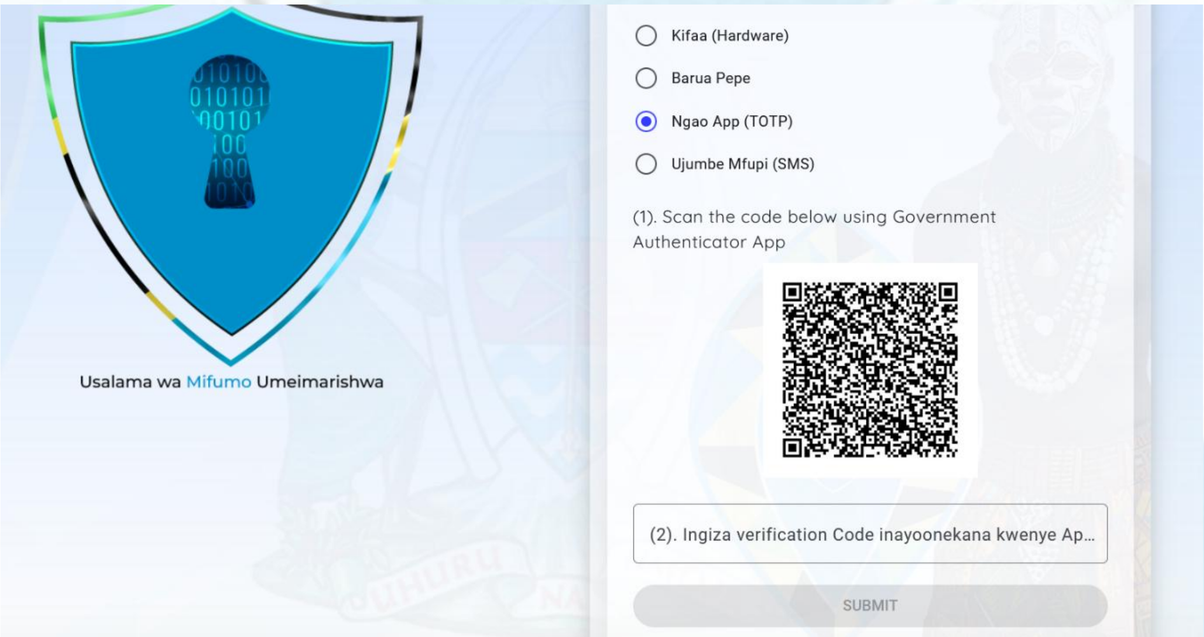
(1). Ingiza namba yako ya simu*

SUBMIT

© 2024 Ngao Platform - e-GA. Haki zote zimehifadhiwa

Figure 2 Registration of OTP Based SMS authentication Method

2. **USSD OTP**:
   - Enter Your Phone Number
   - From phone number you entered Dial ***152*00*46#** to view 6-digit code.
3. **NGAO App (TOTP)**:
   - Open the NGAO Authenticator App.
   - Scan the QR code shown on the registration screen.



○ Kifaa (Hardware)

○ Barua Pepe

● Ngao App (TOTP)

○ Ujumbe Mfupi (SMS)

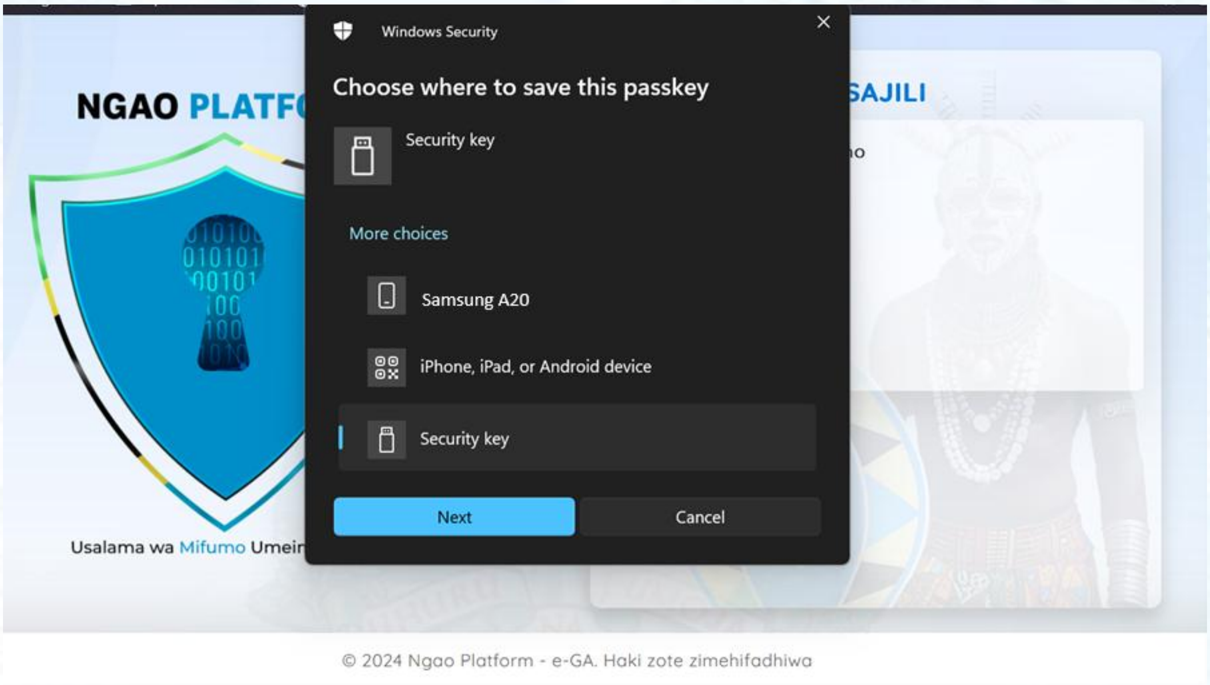
(1). Scan the code below using Government Authenticator App

(2). Ingiza verification Code inayoonekana kwenye Ap...

SUBMIT

Figure 3 QR Code for scanning during Mobile App Registration

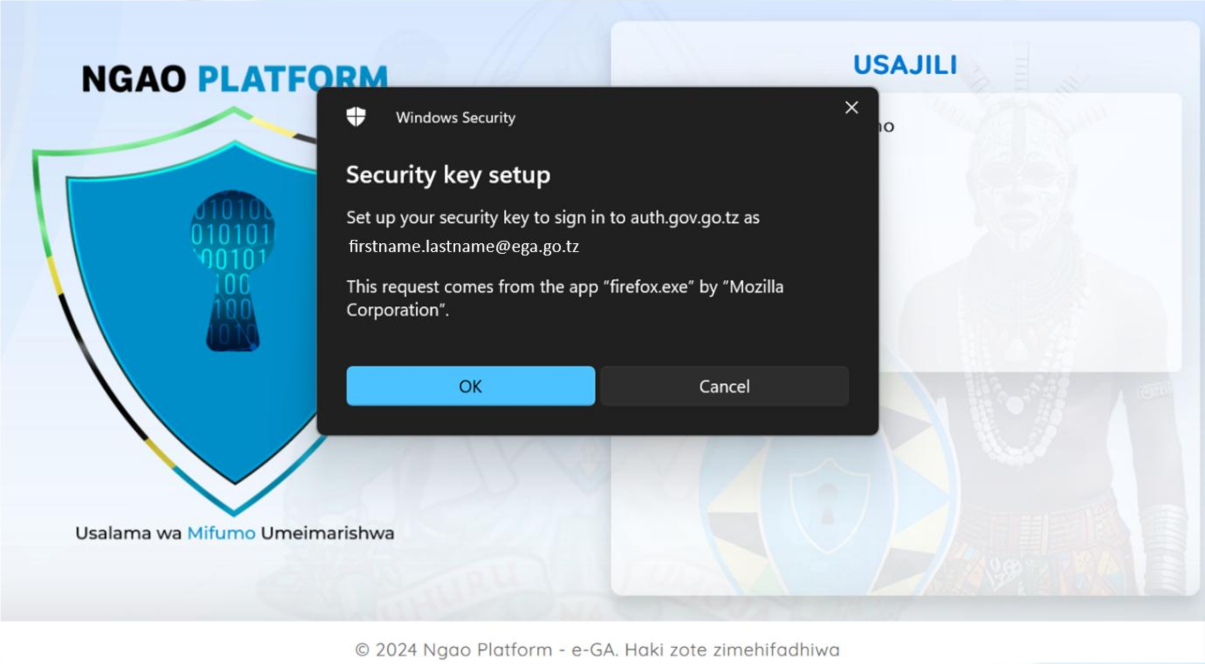
4. **Hardware Key**:
    - Insert your key into the USB port when prompted.
    - Follow the on-screen instructions (enter key password, touch the device, etc.).



Windows Security

Choose where to save this passkey

Figure 4 Registering Hardware as Authentication Method



Windows Security

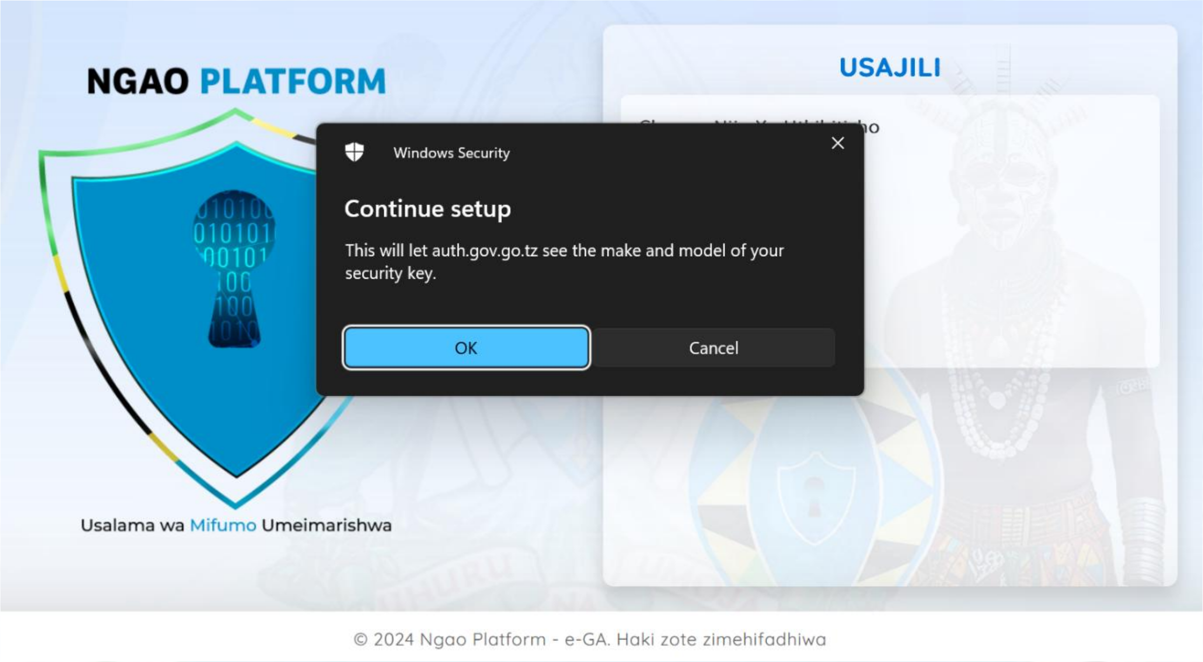
Security key setup

Set up your security key to sign in to auth.gov.go.tz as firstname.lastname@ega.go.tz

This request comes from the app "firefox.exe" by "Mozilla Corporation".

OK
Cancel
NGAO PLATFORM
Usalama wa Mifumo Umeimarishwa
USAJILI
© 2024 Ngao Platform - e-GA. Haki zote zimehifadhiwa

Figure 5 Steps on registration of Hardware Method for Authentication

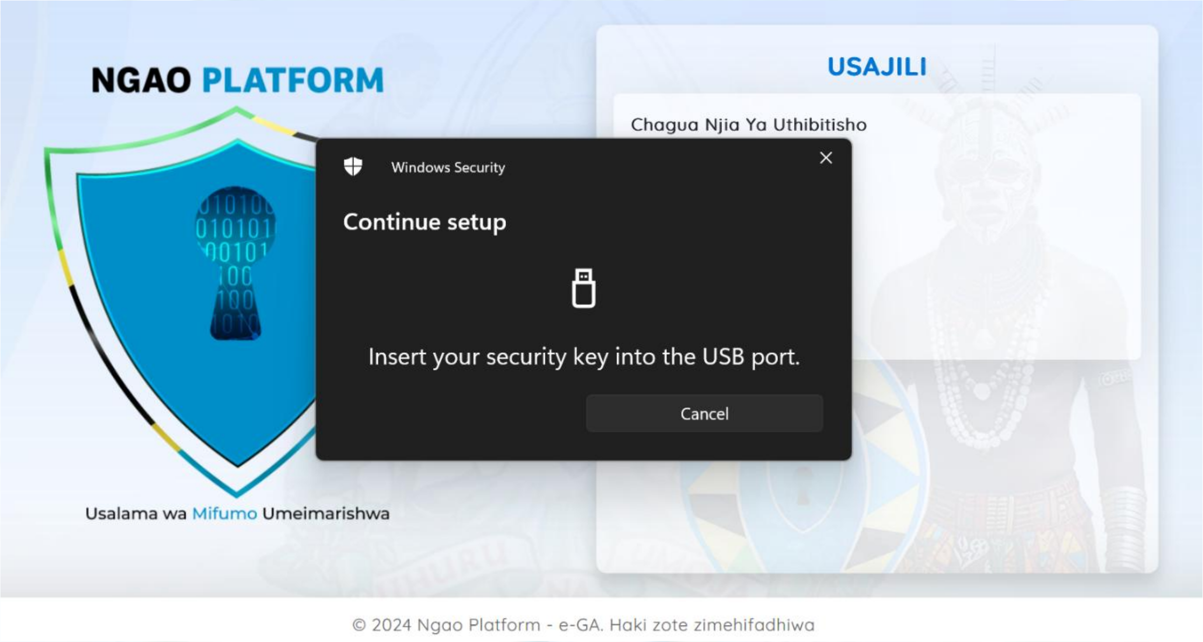

NGAO PLATFORM
Usalama wa Mifumo Umeimarishwa
USAJILI
Windows Security

Continue setup

This will let auth.gov.go.tz see the make and model of your security key.

OK
Cancel
© 2024 Ngao Platform - e-GA. Haki zote zimehifadhiwa

Figure 6 Steps on registration of Hardware Method for Authentication

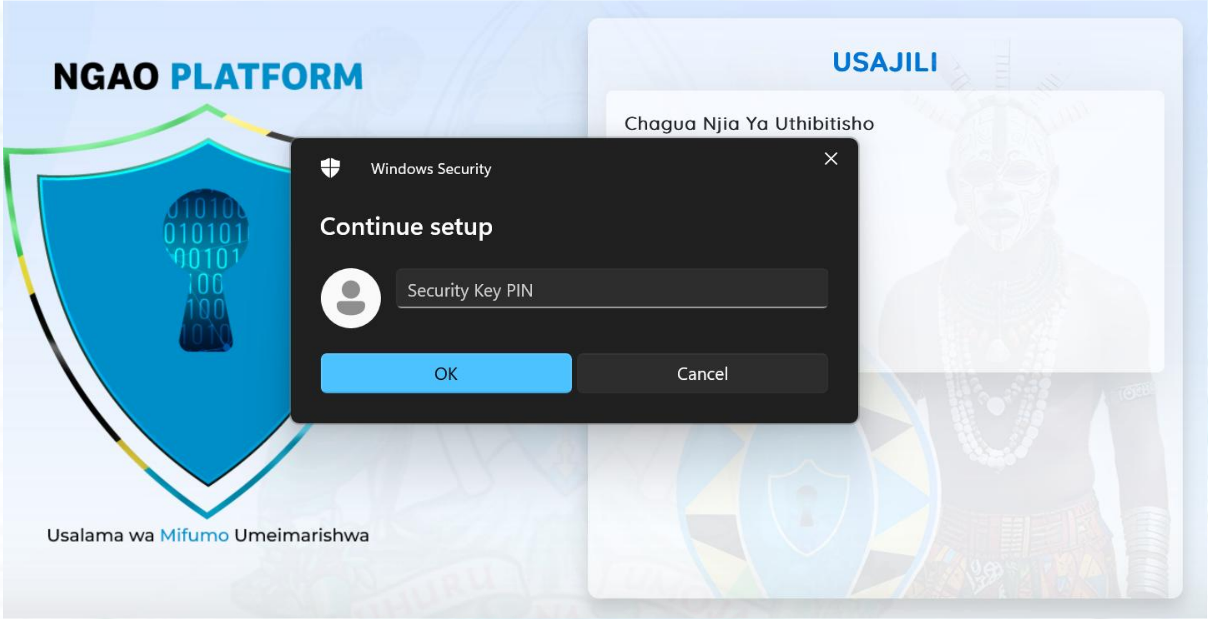

NGAO PLATFORM
Usalama wa Mifumo Umeimarishwa
USAJILI
Chagua Njia Ya Uthibitisho
Windows Security

Continue setup

Insert your security key into the USB port.

Cancel
© 2024 Ngao Platform - e-GA. Haki zote zimehifadhiwa

Figure 7 Steps on registration of Hardware Method for Authentication – At this stage you should insert security key



NGAO PLATFORM

Usalama wa Mifumo Umeimarishwa

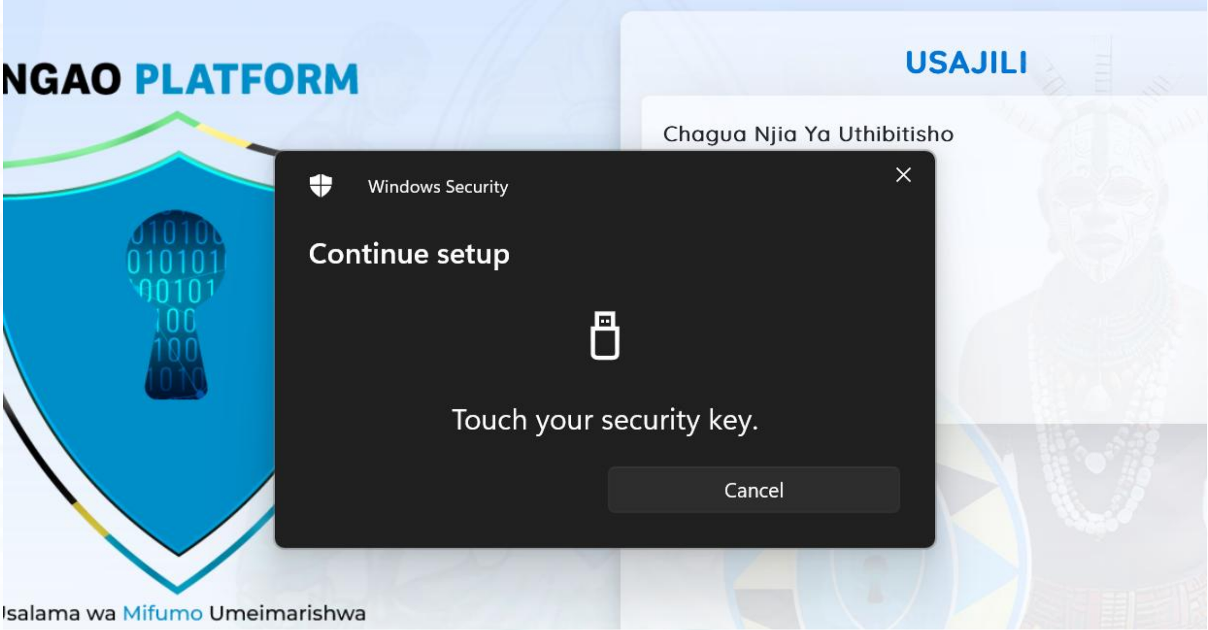
USAJILI

Chagua Njia Ya Uthibitisho

Windows Security

Continue setup

Figure 8 Steps on registration of Hardware Method for Authentication - At this stage you should input password of security key



NGAO PLATFORM

Usalama wa Mifumo Umeimarishwa

USAJILI

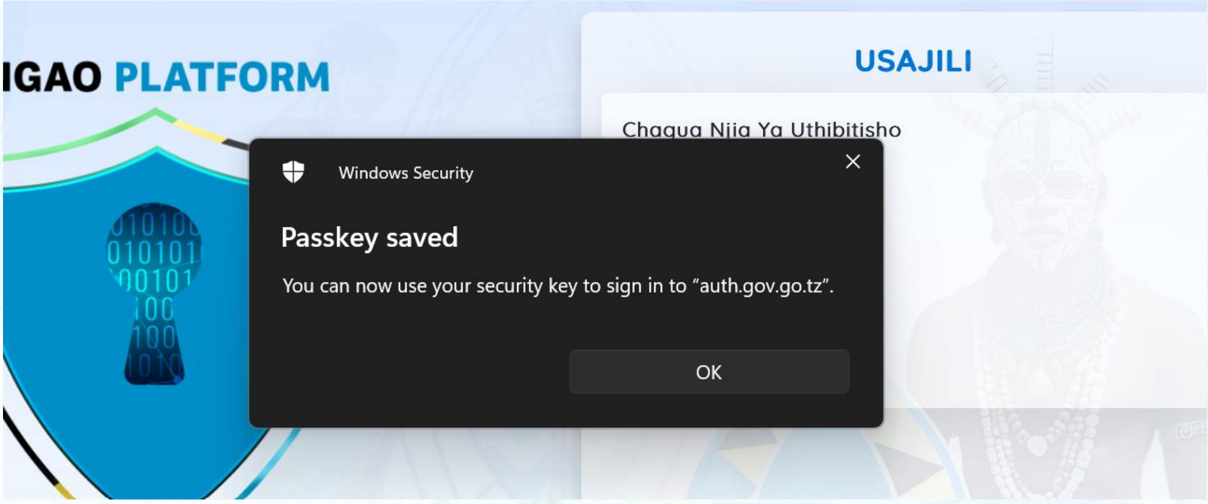
Chagua Njia Ya Uthibitisho

Windows Security

Continue setup

Touch your security key.

Figure 9 Steps on registration of Hardware Method for Authentication - At this stage you should touch the security key



Passkey saved

You can now use your security key to sign in to "auth.gov.go.tz".

Figure 10 Steps on registration of Hardware Method for Authentication - At this stage registration process is completed

Step 4: Completing Registration

You will now be asked to confirm the authentication method:

- For **SMS OTP**, enter the received code and click **Verify**.
- For **USSD OTP**, input the 6-digit code shown after dialling ***152*00*46#.**
- For **TOTP**, enter the 6-digit code shown in the NGAO App.
- For **Hardware Key**, complete the device validation.
- For **SMS/USSD**, respond to the mobile prompt to authorize.

After successful validation, you will see a confirmation that your GMS account is now registered with the NGAO Platform.

✅ **Summary of Registration Process:**

1. Login to GMS.
2. Get redirected to NGAO Platform.
3. Select and configure your preferred MFA method(s).
4. Validate the selected method(s) using OTP, TOTP, hardware, or USSD.
5. Complete registration.

You are now ready to authenticate securely with NGAO each time you access the GMS.

4 Authentication Process

Once you have completed registration into the NGAO Platform, each subsequent login to the Government Mailing System (GMS) will require Multi-Factor Authentication (MFA). This section explains how the authentication process works and provides step-by-step guidance for each supported method.

4.1 Logging into GMS

1. Open your browser and go to the GMS login page:
   🔗 https://mail.ega.go.tz (*use link to your institution GMS*)
2. Enter your government email and password.
3. Click **Login**.

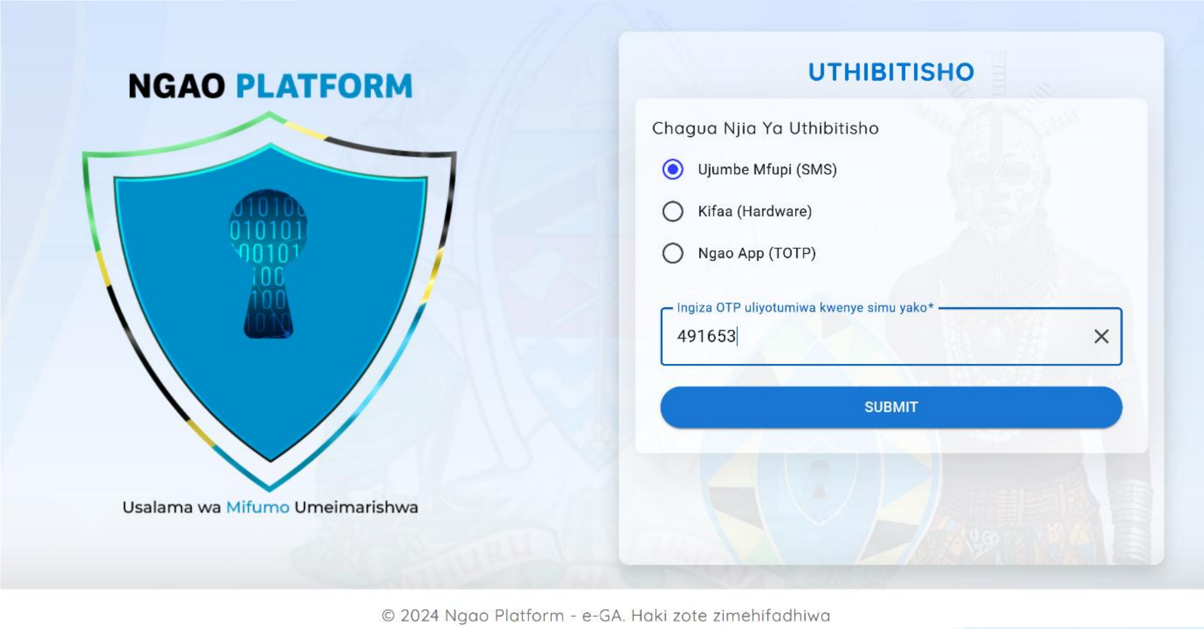
✅ If your credentials are correct, you will be redirected to the NGAO Platform to complete the authentication step using your previously registered method(s).

4.2 Step-by-Step Authentication Process via NGAO Platform

Depending on the authentication method you selected during registration, the NGAO Platform will prompt you to authenticate using one of the following options:

4.2.1 Method 1: SMS OTP

1. A 6-digit OTP will be sent to your registered mobile number.
2. Enter the OTP in the input field on the NGAO authentication page.
3. Click **Submit**.



UTHIBITISHO

Chagua Njia Ya Uthibitisho

● Ujumbe Mfupi (SMS)
○ Kifaa (Hardware)
○ Ngao App (TOTP)

Ingiza OTP uliyotumiwa kwenye simu yako*: 491653

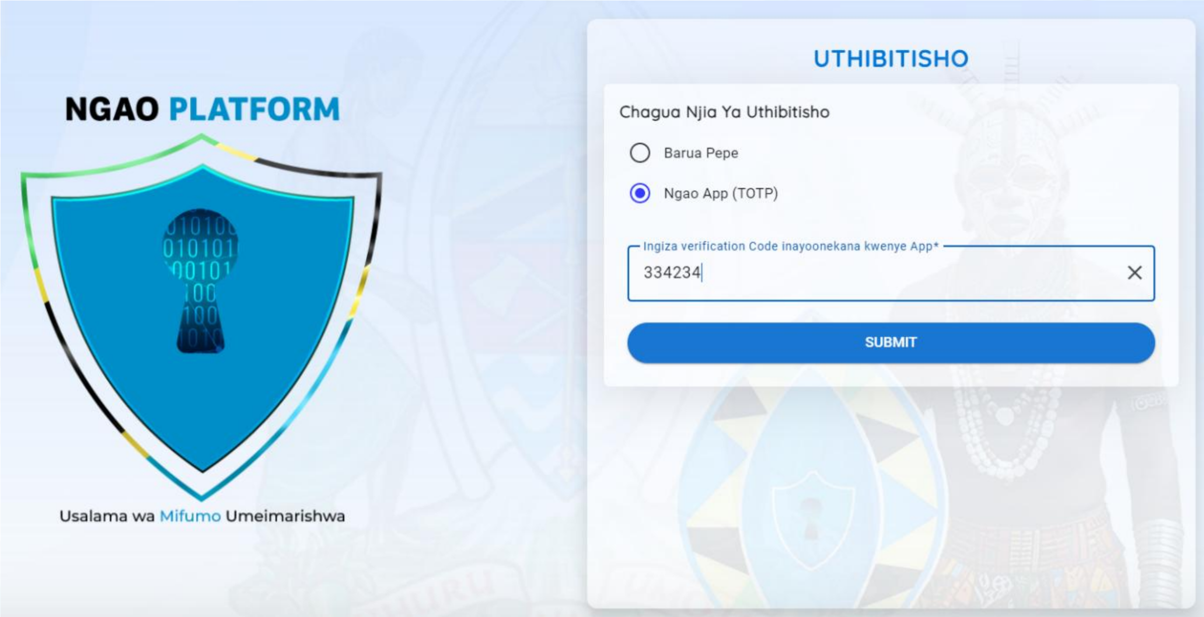
© 2024 Ngao Platform - e-GA. Haki zote zimehifadhiwa

Figure 11 Authenticate by using OTP from SMS

4.2.2 Method 2: NGAO App (TOTP)

1. Open the NGAO Authenticator App on your mobile device.
2. Locate the 6-digit OTP corresponding to the GMS account.
3. Enter the code into the NGAO Platform prompt.
4. Click **Submit**.

✅ TOTP codes change every 30 seconds, so ensure timely entry.



UTHIBITISHO

Chagua Njia Ya Uthibitisho

○ Barua Pepe

● Ngao App (TOTP)

Ingiza verification Code inayoonekana kwenye App*: 334234

Figure 12 Authenticate using TOTP from NGAO App

4.2.3 Method 3: Hardware Security Key

1. Plug your security key (e.g., YubiKey) into a USB port or use Mobile/Tablet device if supported.
2. When prompted, touch the device or enter the key's password if required.
3. The NGAO Platform will validate the key and automatically proceed with authentication.

⚠ For best results, use supported browsers like Firefox or Chrome.

4.2.4 Method 4: USSD Verification

1. From phone number you entered Dial ***152*00*46#** to view 6-digit code.
2. Enter the code into the NGAO Platform prompt.
3. Click **Submit.**

📶 Ensure you have network signal to access USSD Menu and you are using same mobile number as registered to access USSD Menu.

4.3 Successful Authentication

After entering the correct OTP or completing the hardware/USSD verification:

- The NGAO Platform will authenticate your session.
- You will be redirected to the GMS inbox or dashboard.
- You can now use GMS services securely.

✅ **Summary of Authentication Flow:**

1. Login to GMS with username and password.
2. Redirected to NGAO Platform.
3. Authenticate using:
   - SMS OTP
   - Email OTP
   - NGAO App (TOTP)
   - Hardware Security Key
   - SMS/USSD Verification
4. Access GMS system securely.

5 Using the NGAO Authenticator App

The NGAO Authenticator App is a mobile application used to generate secure, time-based one-time passcodes (TOTP) for Multi-Factor Authentication (MFA). It works even without an internet connection, making it one of the most secure and reliable options for authentication when accessing GMS.

5.1 Installing and Setting Up the NGAO Authenticator App

To start using the app, follow the steps below to install and configure it for your GMS account.

5.1.1 Steps to Install the NGAO Authenticator App

➤ **For Android Users:**

1. Open the **Google Play Store** on your Android device.
2. Search for **NGAO Authenticator**.
3. Tap **Install**, then wait for the download and installation to complete.

➤ **For iOS Users:**

1. Open the **Apple App Store** on your iPhone or iPad.

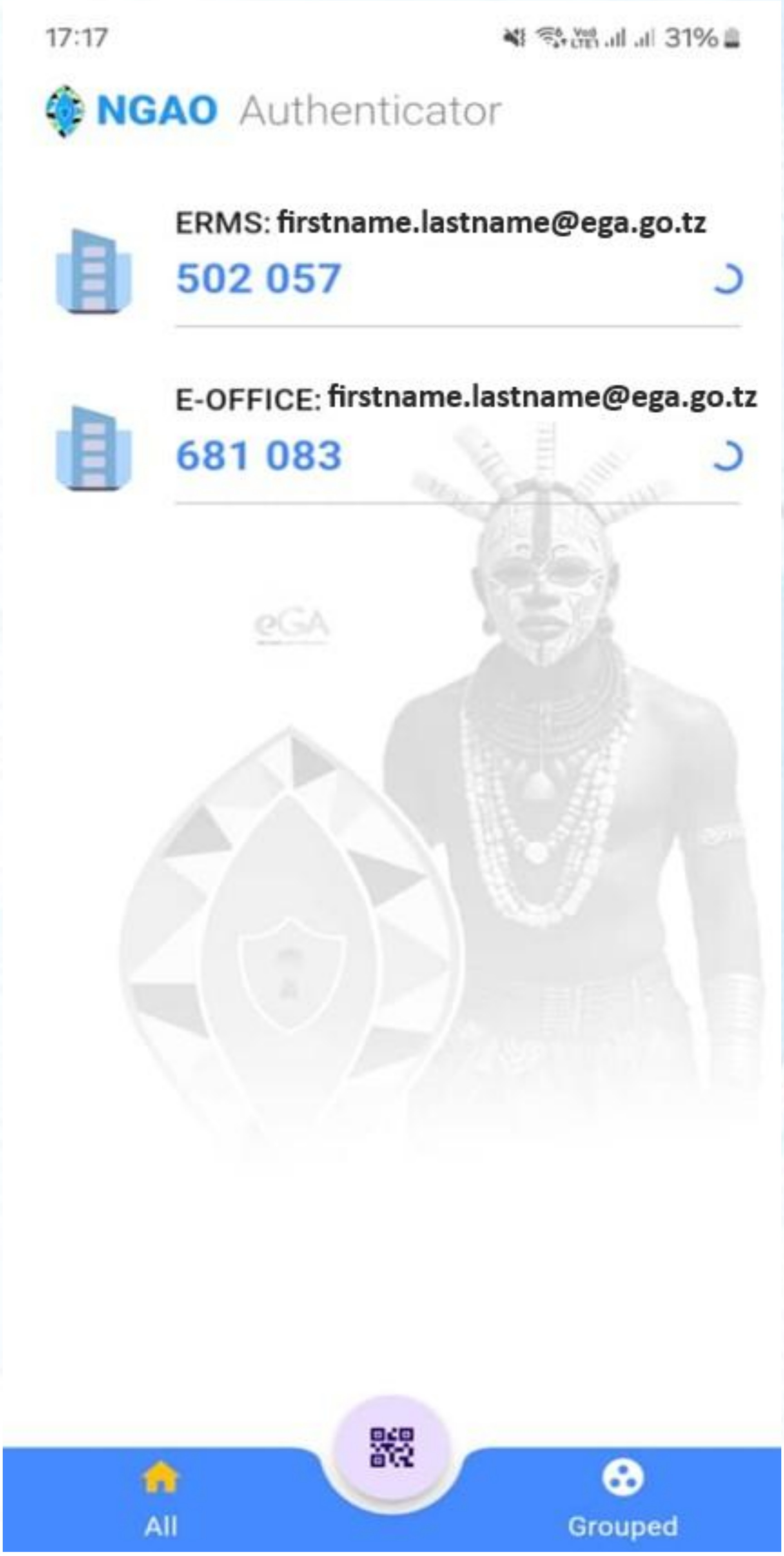
2. Search for **NGAO Authenticator**.
3. Tap **Get**, then allow the app to install.

5.1.2 Setting Up the NGAO Authenticator App

Once the app is installed:

1. Open the NGAO Authenticator App.
2. On the NGAO Platform registration screen (during MFA setup), select **TOTP – NGAO App**.
3. A QR code will be displayed.
4. In the app, tap **Scan QR Code** and point your camera at the screen to scan.
5. The GMS account will be added automatically, and a 6-digit TOTP will be generated.

🔒 Each account listed in the app will display a time-sensitive OTP, which refreshes every 30 seconds.


17:17

31%

NGAO Authenticator

ERMS: firstname.lastname@ega.go.tz

502 057

E-OFFICE: firstname.lastname@ega.go.tz

681 083

Figure 13 TOTP Generated per system registered in NGAO App

5.2 Generating OTP for GMS System

After setup, use the NGAO Authenticator App to generate OTPs every time you log into the GMS system.

5.2.1 Steps to Generate OTP using NGAO Authenticator App

1. Open the NGAO Authenticator App on your mobile device.
2. Find the entry for your GMS account.
3. Note the 6-digit OTP displayed.
4. Enter this OTP into the NGAO authentication screen when prompted during GMS login.
5. Click **Submit**.

⏱ Make sure to enter the OTP within the 30-second window before it refreshes.

5.2.2 Important Notes

- The NGAO Authenticator App **does not require internet** to generate OTPs during or after setup.
- If you uninstall the app or lose your phone, you will need to re-register the app via the NGAO Platform (contact your IT support).
- Avoid sharing screenshots of your QR code during setup, as it can compromise your account.

5.3 Using the Grouped View for OTPs

The app supports a **Grouped View** feature for users managing multiple systems (e.g., GMS, ERMS, e-Office).

Steps to Use Grouped View:

1. Open the NGAO Authenticator App.
2. Tap the **Grouped View** or **Grouped** tab at the bottom.
3. OTPs will be shown grouped by category or system name (e.g., GMS, e-Office).
4. Use this view to quickly locate and manage your authentication codes.

📲 This feature is particularly useful for users who access more than one government system with NGAO MFA.

6 Multi-Factor Authentication (MFA) Setup – Self Service

The NGAO Platform allows users to manage their Multi-Factor Authentication (MFA) preferences directly within the GMS system. Through this self-service interface, users can add, update, or remove MFA methods such as SMS OTP, TOTP via the NGAO Authenticator App, hardware security keys, and SMS/USSD.

6.1 Overview of MFA Options in GMS

The GMS system, integrated with NGAO, supports several authentication methods to enhance security. Users may configure one or more of the following:

Method	Description
SMS OTP	Receives a one-time passcode via SMS for login.
Email OTP	Receives a one-time passcode via email.
NGAO App (TOTP)	Generates a time-based passcode through the mobile NGAO Authenticator App.
Hardware Key	A physical device used for secure login.
USSD OTP	Receives a one-time passcode on USSD Menu at ***152*00*46#** to view 6-digit code for login.

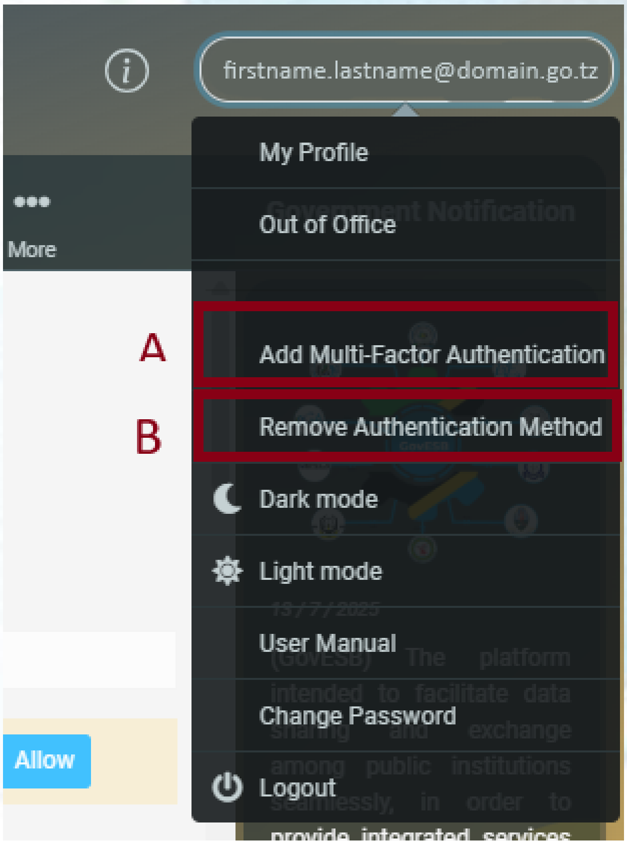

firstname.lastname@domain.go.tz
More
My Profile
Out of Office
A
Add Multi-Factor Authentication
B
Remove Authentication Method
Dark mode
Light mode
User Manual
Change Password
Logout
Allow

Figure 14 MFA Management in GMS

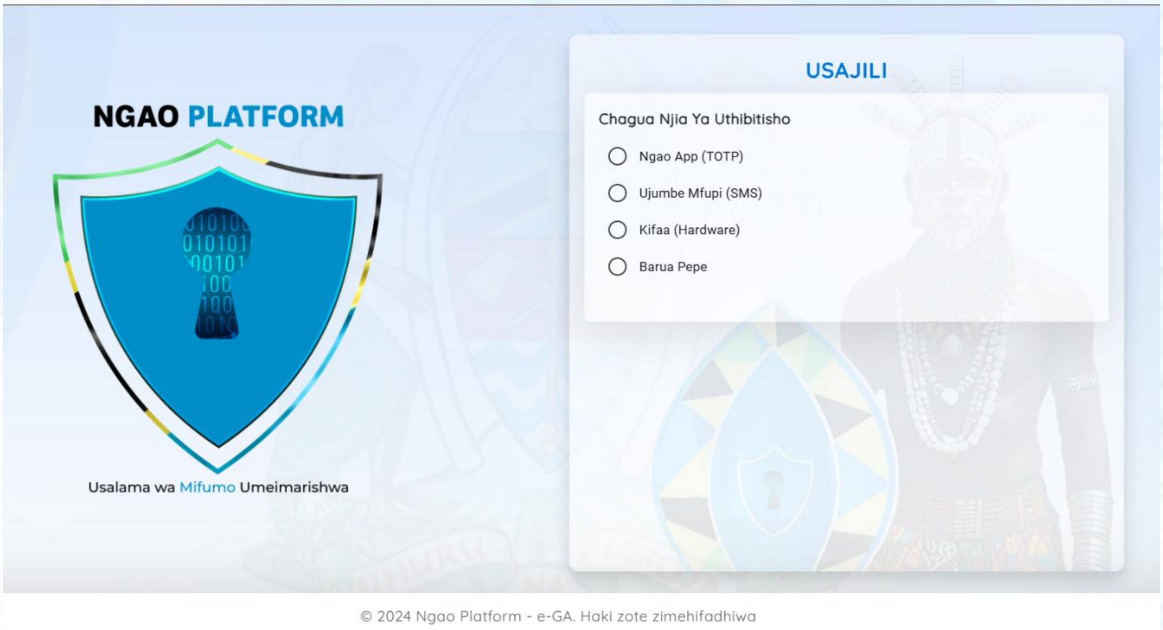
6.2 Register Additional MFA Method in GMS

Users can add more authentication methods anytime by accessing the MFA settings section within the GMS web interface.

6.2.1 Steps to Register Additional MFA Method:

1. **Login to GMS**
    - Navigate to: https://mail.ega.go.tz
    - Enter your email and password.
2. **Navigate to MFA Settings**
    - Go to **Quick Settings option by Clicking on your mail address** then select required option Add Multifactor **Authentication Methode** or **Remove Authentication Method.**
3. **Add Additional Method**
    - Choose a method to register:
        - **SMS OTP**: Enter and verify your mobile number.
        - **Email OTP**: Enter your email address and verify with received code.
        - **NGAO App (TOTP)**: Scan the QR code using the NGAO Authenticator App.
        - **Hardware Key**: Insert and register your USB/NFC key.
        - **SMS/USSD**: Provide your mobile number; verify via USSD Menu or SMS confirmation.
4. **Verification**
    - Complete the verification step for the selected method (enter OTP, scan QR etc.).
5. **Save**
    - Click **Save** to apply the changes.

🔐 Multiple methods can be registered for fallback or increased flexibility.



USAJILI

Chagua Njia Ya Uthibitisho

○ Ngao App (TOTP)

○ Ujumbe Mfupi (SMS)

○ Kifaa (Hardware)

○ Barua Pepe

© 2024 Ngao Platform - e-GA. Haki zote zimehifadhiwa

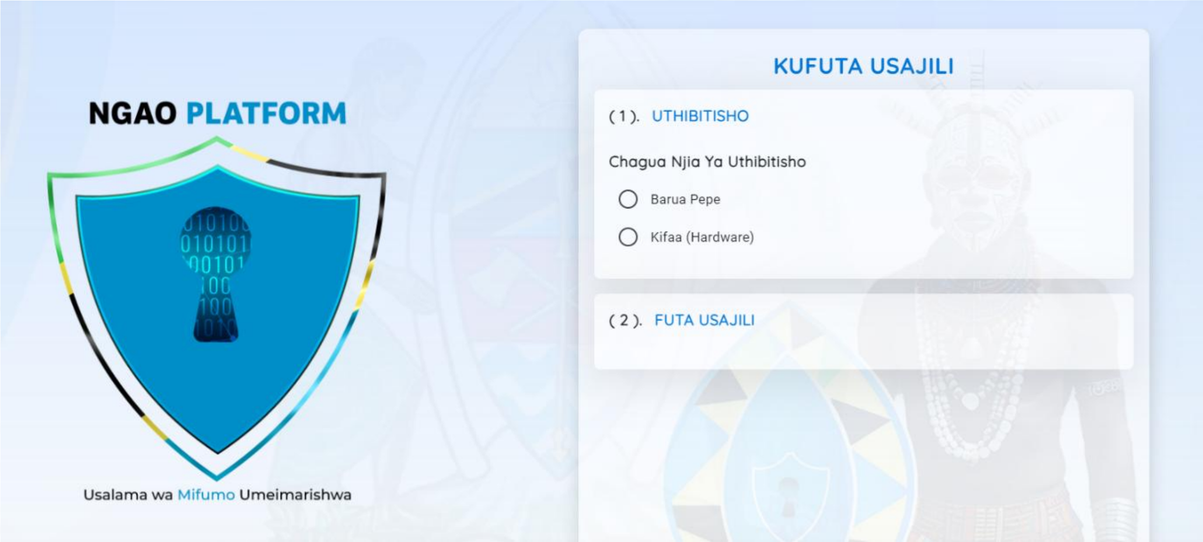
Figure 15 NGAO Authentication Management in mGov 2.0

6.3 Managing and Changing MFA Options

Users can update their MFA settings at any time using the same self-service interface. This includes changing mobile numbers, adding backup options, or removing outdated devices.

6.3.1 Steps to Manage MFA:

1. **Log in to GMS**.
2. Go to **Settings > NGAO Authentication**.
3. In the MFA management section, you can:
   - **Update mobile number or email**.
   - **Rescan QR code** to link a new phone.
   - **Replace or unregister a hardware key**.
   - **Enable or disable SMS/USSD login confirmation**.
4. **Authenticate Before Changes**
   - You will be required to verify your identity before making changes (via existing method).
5. **Save and Confirm**
   - After updating your MFA preferences, click **Save**. Changes will take effect immediately.



KUFUTA USAJILI

(1). UTHIBITISHO

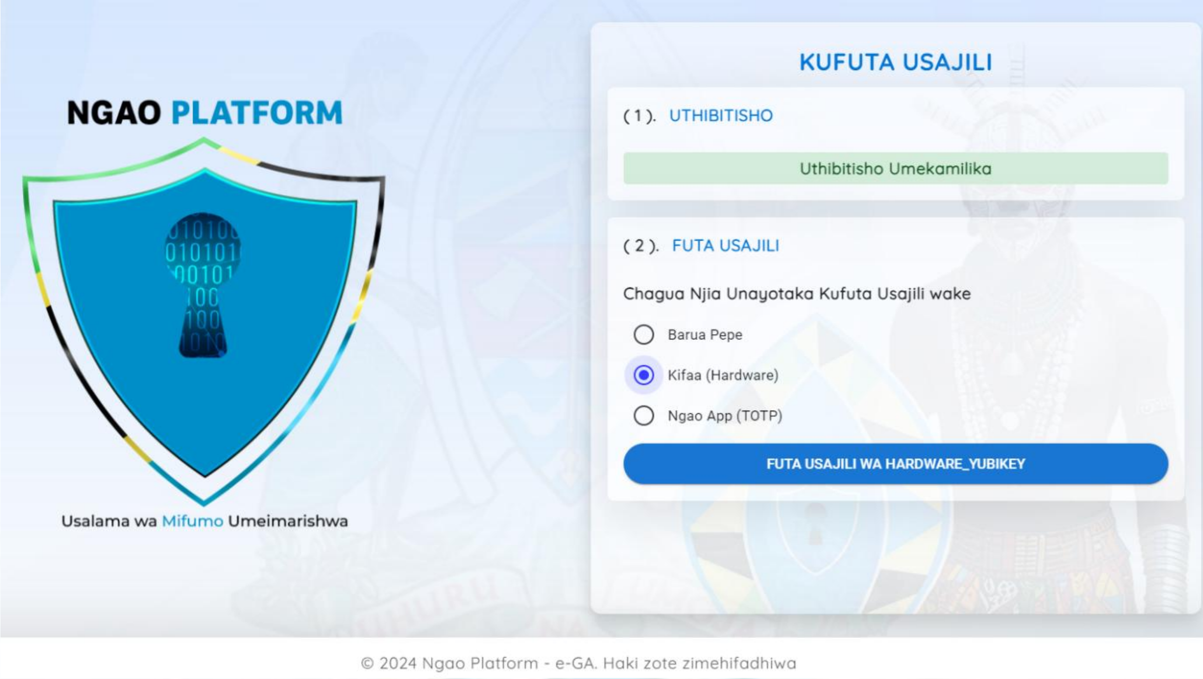
Chagua Njia Ya Uthibitisho

○ Barua Pepe

○ Kifaa (Hardware)

(2). FUTA USAJILI

Figure 16 Removing Authentication Method by authenticating first - self service


NGAO PLATFORM
Usalama wa Mifumo Umeimarishwa
FUTA USAJILI WA HARDWARE_YUBIKEY
© 2024 Ngao Platform - e-GA. Haki zote zimehifadhiwa

KUFUTA USAJILI

(1). UTHIBITISHO

Uthibitisho Umekamilika

(2). FUTA USAJILI

Chagua Njia Unayotaka Kufuta Usajili wake

○ Barua Pepe

● Kifaa (Hardware)

○ Ngao App (TOTP)

Figure 17 Removing Authentication Method selection - self service

7 Troubleshooting

This section outlines common issues users may encounter when using the NGAO Platform with the Government Mailing System (GMS), along with recommended solutions. It also provides answers to frequently asked questions (FAQs) related to the NGAO Authenticator App and multi-factor authentication (MFA).

7.1 Common Issues During Registration and Authentication

7.1.1 Issue 1: Not Receiving OTP via SMS

Possible Causes:

- Mobile network delays
- Incorrect phone number

Solutions:

1. Refresh Page and select SMS Option again on the NGAO screen.
2. Ensure your phone has good signal reception.
3. Contact your IT helpdesk if the problem persists.

7.1.2 Issue 2: OTP Expired

Possible Causes:

- Time delay during entry
- Device clock out of sync

Solutions:

1. Request or regenerate a new OTP.
2. If using the NGAO App, ensure your phone’s date/time is set to automatic or synchronized with the network.

7.1.3 Issue 3: Unable to Scan QR Code for NGAO App (TOTP)

Possible Causes:

- Camera not functioning or blocked
- App lacking camera permissions

Solutions:

1. Check and enable camera access for the NGAO Authenticator App.
2. Clean your camera lens or improve lighting.
3. Try using a different device to scan the QR code.

7.1.4 Issue 4: Hardware Security Key Not Detected

Possible Causes:

- Key not properly inserted
- Incompatible or unsupported browser
- USB port issues

Solutions:

1. Reinsert the security key and try again.
2. Use a supported browser such as **Firefox** or **Chrome**.
3. Try a different USB port or device.
4. Ensure the key is properly registered and not corrupted.

7.1.5 Issue 5: Cannot Access NGAO Platform

Possible Causes:

- Internet connection issues
- Blocked site or firewall restrictions
- Browser cache problems

Solutions:

1. Confirm that your device is connected to the internet.
2. Clear your browser's cache and cookies.
3. Try accessing the NGAO Platform from a different browser.
4. Contact your IT support to check for firewall or proxy restrictions.

7.2 FAQ on Using NGAO Authenticator App

Q1: Can I use the NGAO Authenticator App on multiple devices?

No, each device must be registered with separate user account for the application, you can't use one user account on different devices so to use them interchangeably.

Q2: What happens if I lose my phone with the NGAO Authenticator App installed?

You will lose access to TOTP codes. Contact your system administrator or IT helpdesk to reset your MFA configuration. You can then re-register a new device. If you have other method for MFA, you can login on GMS and re-register new device.

Q3: Can I use both a hardware security key and the NGAO Authenticator App?

Yes, you can register multiple MFA methods. This provides backup options in case one method fails or is unavailable.

✅ **Summary of Troubleshooting:**

Problem	Recommended Action
OTP not received	Resend, check contact info, verify signal
OTP expired	Regenerate OTP, sync device time
Can’t scan QR	Check camera access or use another device
Hardware key not detected	Check USB port, browser compatibility
Access issues with NGAO Platform	Clear cache, check network, try another browser