Overview

The OneKey token is one of the two-factor authentication (2FA) methods for SingPass log in to government digital services.

As announced in March 2020, the Government will progressively cease the use of the OneKey token and users have one year to switch to an alternative 2FA method before 31 March 2021.

If you're still using the OneKey token for logins, we highly encourage you to switch to any of the following Two-Factor Authentication (2FA) methods now!

The following pages will detail the alternative methods and how you can adopt them depending on which suits you best.

This information is also translated here in: Chinese, Malay and Tamil.

Do you have a smartphone?

Download the SingPass Mobile app!

If you have a smartphone, you can download and set up the SingPass Mobile app from the official app stores.

For iOS users:
https://go.gov.sg/spm-app-store

For Android users:
https://go.gov.sg/spm-play-store

This easy and convenient application helps you to log in to digital services using your fingerprint, face or a 6-digit passcode.

For detailed instructions on how to set up your SingPass Mobile app, you may visit go.gov.sg/singpass-2FA-guides or refer to the iOS instructional guide or Android instructional guide. The instructional guides are also available in Chinese, Malay and Tamil.

Do you have a phone that cannot download apps?

Sign up for SMS 2FA!

With this, you can use the SMS One-Time Password (OTP) sent to your mobile number to log into SingPass.

1. Visit www.Singpass.gov.sg
2. Log in with your OneKey token
3. Select "Set Up 2FA"
4. Select 'Register SMS 2FA'
5. Enter and verify your mobile number

Note: You can choose your preferred mode of verification by selecting 'Manage 2FA'.

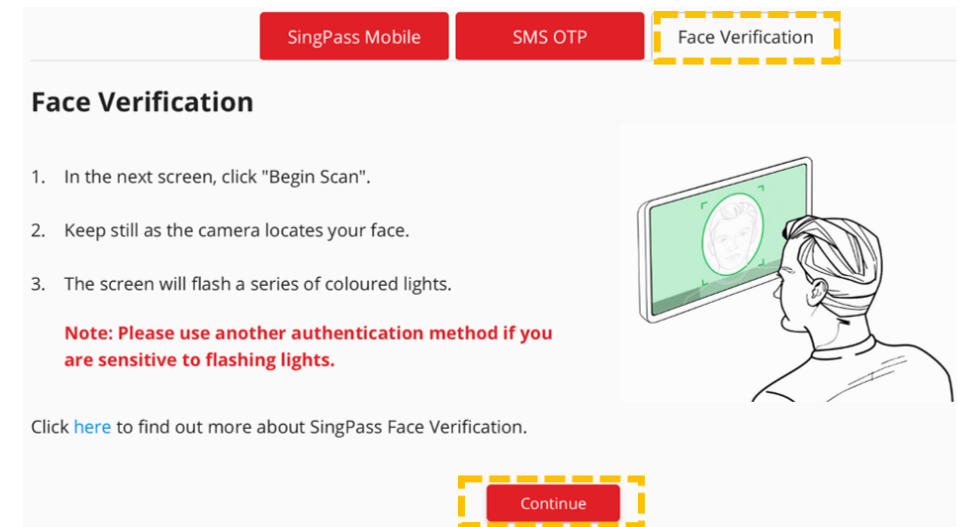This service is only available for locally-registered numbers.

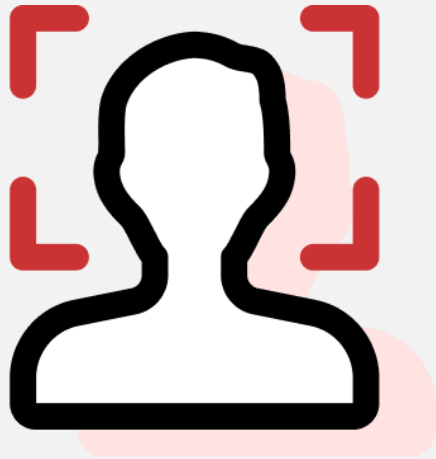SingPass

I have a computer with a web camera

Face Verification

Log in to a digital service with your SingPass ID and password, followed by scanning your face on a computer with a web camera, or a smartphone with a front-facing camera. No prior registration is required to use Face Verification as a 2FA mode.

Alternatively, you may also use the SingPass Face Verification kiosks located at CPF Service Centres, IRAS Taxpayer and Business Service Centre, Our Tampines Hub's Public Service Centre, Geylang East Public Library, and Assurity Customer Care Centre.

SingPass Mobile   SMS OTP   Face Verification

Face Verification

1. In the next screen, click "Begin Scan".

2. Keep still as the camera locates your face.

3. The screen will flash a series of coloured lights.

Note: Please use another authentication method if you are sensitive to flashing lights.

Click here to find out more about SingPass Face Verification.

Continue

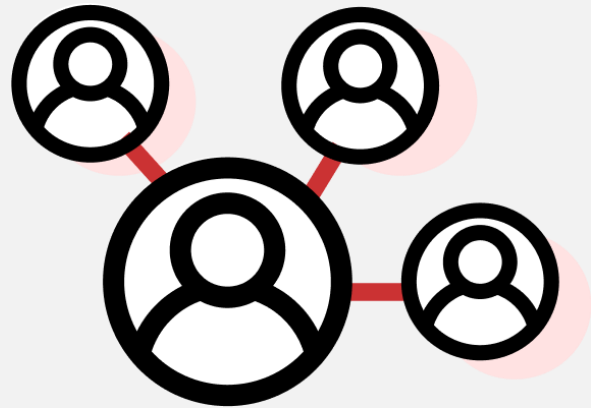SingPass

I have a computer with a web camera

FAQ: Face Verification

QN: Why is my SingPass Face Verification unsuccessful?

There may be several possible reasons for this. For ways to improve the success of Face Verification, you should ensure that:

- Your face is not covered

- You keep still while scanning is in progress

- Your environment is not too dark

- There is no strong lighting in the background

- You use a minimum resolution of 2 megapixels for the camera

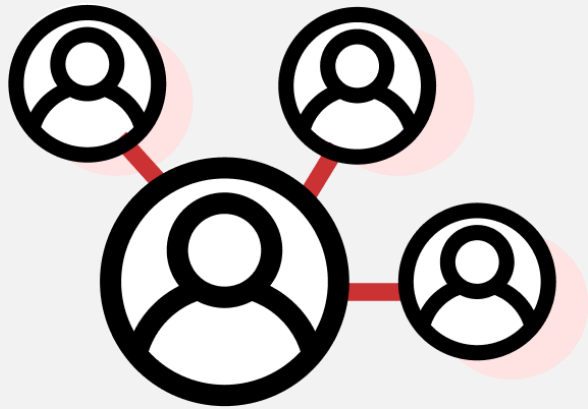**SingPass**

I need help when transacting online

Multi-User SMS 2FA

If a family member or trusted individual is helping you with your digital transactions, you can give your one-time explicit consent to link your SingPass account to his/her mobile number for the purpose of receiving the SMS-OTP.

Both parties are required to be present to activate this option at any of the SingPass counters islandwide (for locations, check go.gov.sg/singpass-counters).

If you have difficulties being physically present, please contact our SingPass Helpdesk at +65 6643 0555 / support@singpass.gov.sg.

SingPass

I need help when transacting online

FAQ: Multi-User SMS 2FA

QN: Is Multi-User SMS 2FA only for family members to use?

No. This alternative 2FA method seeks to support older, or less tech-savvy SingPass users who require assistance transacting with the Government. They may be assisted by a trusted caregiver who may or may not be a family member.

QN: How many users can be linked with the Multi-User SMS 2FA?

A primary user's mobile number may be linked with 5 additional SingPass accounts. A secondary user may be linked with only one account holder's mobile number.

SingPass

💡 TIPS: How to keep your SingPass account safe

- **Do not share login information**: Keep your SingPass ID, password and 2FA details confidential.

- **Do not re-use passwords**: Certain websites that you access may not be secure. Login information may be stolen from these sites and used to hack your SingPass account.

- **Change your passwords regularly**

- **Use strong passwords**: Strong passwords are alphanumeric and contain 8 to 24 characters.

- **Beware of phishing sites**: There may be sites that look like government websites to trick you in disclosing your personal details. To verify if it is not a phishing website, always check that the URL is correct (www.singpass.gov.sg), and there should be a 'lock' icon in the address bar.

If you think that you been scammed or suspect that your account has been hacked,

we strongly advise you to take the following actions:

- **Reset your SingPass password immediately** to prevent unauthorised access to your account.

- **Lodge a police report** at any Neighbourhood Centre/Post, or via the Electronic Police Centre website.

- **Email GovTech at info@tech.gov.sg** to highlight your case to the Administrator

SingPass

THANK YOU

If you have further questions on the various 2FA methods, visit go.gov.sg/singpass-2fa-methods
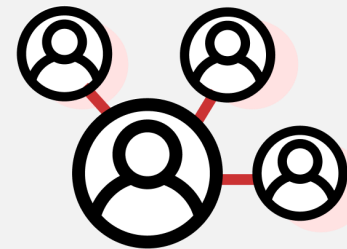
Or write in to support@singpass.gov.sg

SingPass
Mobile app

SMS 2FA

Face
Verification

Multi-User
SMS 2FA