MOF
MINISTRY OF FINANCE
SINGAPORE

iDA
SINGAPORE

FACT SHEET

SINGPASS

Singapore Personal Access (or SingPass) is a gateway to hundreds of e-services provided by more than 60 government agencies. Users only have to remember one password when connecting and transacting with the Government.

Launched in March 2003, SingPass now has more than 3.3 million registered users.

The following groups of users are eligible to apply for SingPass:

- Singapore Citizens and Permanent Residents
- Employment Pass and Personalised Employment Pass holders
- EntrePass holders
- S-Pass holders
- Dependant Pass holders (of EP, PEP, EntrePass and S-Pass holders)
- Selected Work Permit holders
- Long Term Visit Pass Plus (LTVP+) holders

On-going Security Measures

Managed by the Infocomm Development Authority of Singapore**,** the SingPass system is reviewed regularly and there are many on-going security enhancements to ensure that a secure SingPass service is delivered to its users.

Examples of some measures taken over the years to better protect users' personal information:

- Users will be prompted to change passwords to stronger ones every two years.
- Passwords of accounts that are inactive for more than three years will be reset to ensure that users with dormant accounts are not unnecessarily exposed to cyber threats.
- After three failed login attempts, users will be asked to key in a randomly-generated security code to mitigate brute force attacks on login.
- Any changes made to the account holder's key personal information will trigger a notification letter, which will be sent to the user's registered address to verify this change.

Launch of enhanced SingPass on 5th July 2015

The enhanced SingPass includes an improved user interface, mobile-friendly features and stronger security capabilities, such as 2-Step Verification (2FA) for government e-transactions, particularly for those involving sensitive data. (Refer to Annex A for the features of the enhanced SingPass)

With 2FA, users will be required to enter a One-Time Password (OTP) sent via SMS or generated through a OneKey token. This is in addition to their SingPass username and password, thus ensuring that their sensitive data is better protected.

As part of continuous effort to improve the system, the SingPass 2FA setup process was simplified such that users can register for 2FA via the SingPass website and activate their 2FA via SMS. Alternatively, they can log into Assurity's website using their NRIC and the password in the PIN mailer to activate their 2FA.

To enjoy the enhanced features, users simply need to complete the following steps:

1) Complete a one-time account update
For users who log into their SingPass account for the first time after 5th July 2015, they will automatically be prompted to:

   - ***Provide and verify their mobile number and email address***
     Users are to select their preferred mode of contact (SMS or email) so that they will receive SMS or email notifications whenever changes are made to their SingPass profile (e.g. password, mobile number, SingPass ID).

   - ***Set up security questions and answers***
     Users will be prompted to set up at least two security questions and answers. This is so that they can reset their passwords online easily by answering a security question correctly.

2) Set up their 2-step verification (2FA)
From 5th July 2016, all government e-services involving sensitive data will require SingPass 2FA to perform e-transactions. To set up their SingPass 2FA, users will need to:

   - ***Register for SMS or OneKey token via the SingPass website***
     Users can log into their SingPass account and click "Set Up 2-Step Verification (2FA) under the Quick Links section. They can choose to receive OTPs via SMS or generate them through a OneKey token.

     Upon successful registration, a PIN mailer will be sent to their registered address within seven working days for activation.

   - ***Activate 2FA using PIN mailer password***
     Users can send the activation code in the PIN mailer to 78111 via SMS, or log into Assurity's website (https://portal.assurity.sg/activate) using their NRIC and the password in the PIN mailer to activate their 2FA

     Upon successful activation, their SingPass 2FA setup is complete and they will go through a 2-step login process when performing sensitive government e-transactions.

(Refer to Annex B for visual illustration of how to set up SingPass 2FA)

For media clarifications, please contact:

Malini Nathan (Ms)
Assistant Director
Corporate and Marketing Communications Division, IDA
DID: (65) 6211 0660
Email: malini_nathan@ida.gov.sg

Jacklyn Chew (Ms)
Assistant Manager
Corporate and Marketing Communications Division, IDA
DID: (65) 6211 0708
Email: jacklyn_chew@ida.gov.sg

Annex A – Features of the enhanced SingPass

Improved Usability

1) **Simple One-Time Account Update**
Upon logging in to the enhanced SingPass for the first time, users simply need to provide their mobile number and/or email address, and set up a minimum of two security questions. This setup is required for users to access all online management features available in the enhanced SingPass.

2) **User-centric Interface**
The design of the enhanced SingPass is simple and easy to use, featuring clear and concise instructions, tool tips, updated security questions that are easy to remember and clearer security code.

3) **Additional Self Help Features**
How-to videos are introduced as part of the enhanced SingPass to provide users with an overview of the enhancements and easy-to-follow, step-by-step guides.

Greater Convenience

1) **Mobile Optimised**
Catering for a user landscape where mobile usage is proliferating, the enhanced SingPass is designed to be mobile optimised. When a mobile browser is detected, the screen display will be resized and key information and tasks will be prioritized for users to browse on-the-go.

2) **Faster Reset of Passwords Online**
With the enhanced SingPass, users who have forgotten their SingPass password can reset it online almost immediately via their mobile phones, instead of visiting a SingPass counter or submitting an online request to have the new password mailed to their registered address.

3) **Easy online account management**
The enhanced SingPass provides greater convenience by allowing users to view details of their previous transactions (e.g. password reset and e-service authentications) and update their SingPass profile (e.g. mobile number) easily online.

Improved Security

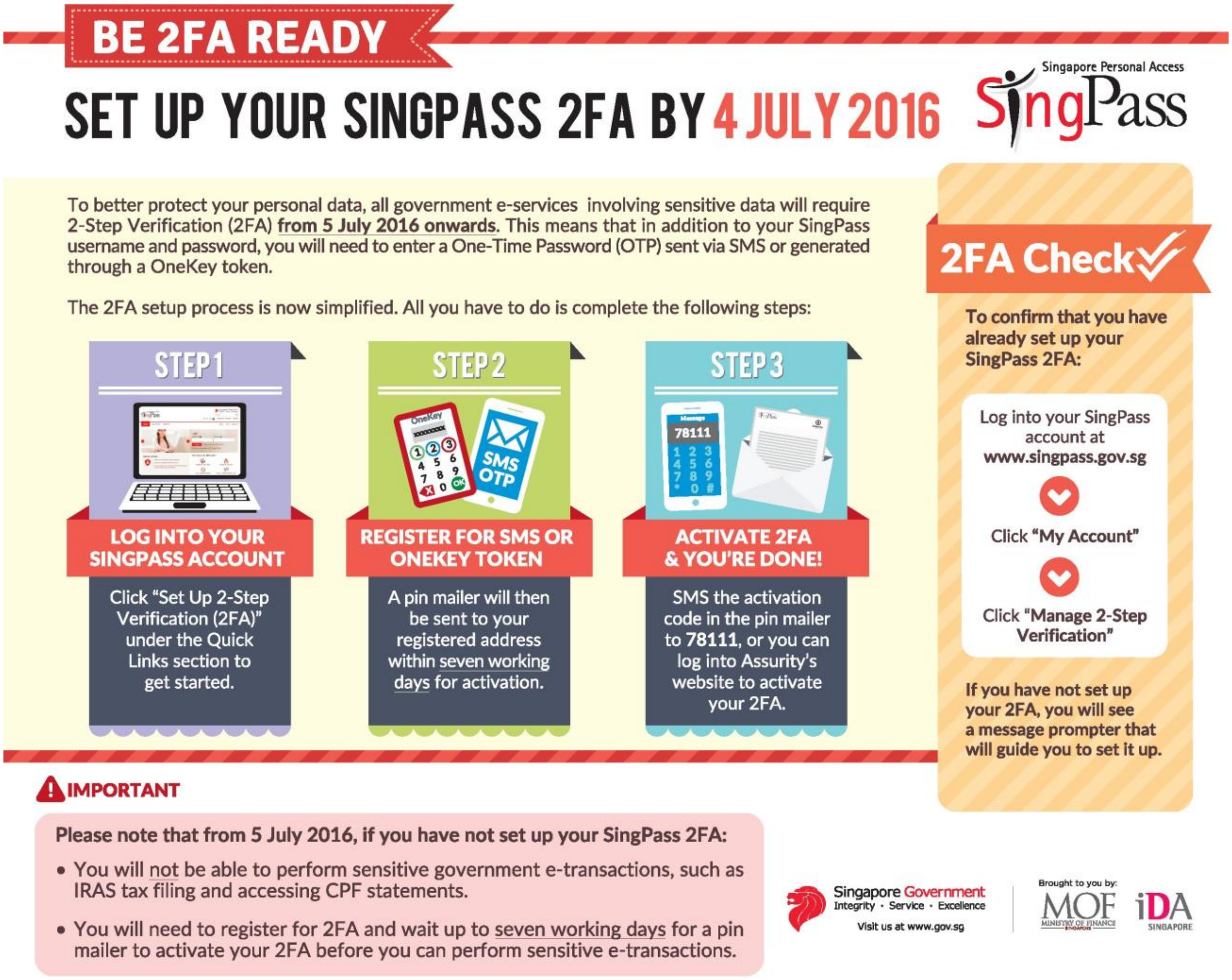
1) **Notifications through Short Messaging Service (SMS) and Email**
By providing their contact details and selecting their preferred mode of contact (SMS or email), users will be able to receive notifications for any key profile information changes.

2) **Secure 2-step login for e-government transactions involving sensitive data**
Government e-Services that involve sensitive data will be required to implement 2FA. A one-time "second factor" password will be sent to users via Short Messaging Service (SMS) or generated from a OneKey token. To allow for a smoother transition for our users, there will be a 1-year transition period for users to choose to activate 2FA. After the transition period, users would need to go through a two-step login process for government e-services involving sensitive information

3) **Option to customise SingPass ID**
Users have the option to customise their SingPass ID, instead of using their NRIC/FIN number, to safeguard their SingPass login credentials. Please note that users can only customise their ID once and the change is permanent.

4) **Risk Based Authentication and Analysis**
A central logging facility uses analytics to analyse and identify unusual activities for further actions. Based on the risk level, the system may challenge the user to provide additional verification, such as answering a security question or entering a security code.

Annex B – Steps on how to set up SingPass 2FA



BE 2FA READY

SET UP YOUR SINGPASS 2FA BY 4 JULY 2016

Singapore Personal Access
SingPass

To better protect your personal data, all government e-services involving sensitive data will require 2-Step Verification (2FA) **from 5 July 2016 onwards.** This means that in addition to your SingPass username and password, you will need to enter a One-Time Password (OTP) sent via SMS or generated through a OneKey token.

The 2FA setup process is now simplified. All you have to do is complete the following steps:

STEP 1

LOG INTO YOUR SINGPASS ACCOUNT

Click "Set Up 2-Step Verification (2FA)" under the Quick Links section to get started.

STEP 2

REGISTER FOR SMS OR ONEKEY TOKEN

A pin mailer will then be sent to your registered address within seven working days for activation.

STEP 3

ACTIVATE 2FA & YOU'RE DONE!

SMS the activation code in the pin mailer to **78111**, or you can log into Assurity's website to activate your 2FA.

2FA Check✓

To confirm that you have already set up your SingPass 2FA:

Log into your SingPass account at **www.singpass.gov.sg**

Click **"My Account"**

Click **"Manage 2-Step Verification"**

If you have not set up your 2FA, you will see a message prompter that will guide you to set it up.

IMPORTANT

Please note that from 5 July 2016, if you have not set up your SingPass 2FA:

- You will not be able to perform sensitive government e-transactions, such as IRAS tax filing and accessing CPF statements.
- You will need to register for 2FA and wait up to seven working days for a pin mailer to activate your 2FA before you can perform sensitive e-transactions.

Singapore Government
Integrity • Service • Excellence
Visit us at www.gov.sg

Brought to you by:
MOF MINISTRY OF FINANCE SINGAPORE
iDA SINGAPORE

Updated as of 29 January 2016