

FACT SHEET

SINGPASS

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

Launched since 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 in July 2015

The enhanced SingPass will be launched on 5 July 2015 and it will include an improved user interface, mobile-friendly features and stronger security capabilities, such as Two-Factor Authentication (2FA) for e-government transactions, particularly for those involving sensitive data. This will be a one-time "second factor" password generated through an OneKey token or sent via Short Messaging Service (SMS). (Refer to Annex A for the features of the enhanced SingPass)

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

1) Update their SingPass account

- ***Provide and verify 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

- ***Register for SMS or OneKey token***

Users are to select their preferred mode of verification (SMS or OneKey token). This is to ensure that users' personal information and sensitive data are better protected with an additional layer of security. Upon successful registration, users will receive a pin mailer password/token within five working days.

- ***Activate using pin mailer password***

After users have received their pin mailer password/token, they are to follow the instructions in the mailer to activate the 2-step verification function.

- ***Link with SingPass account***

Once activated, users will be prompted to link their mobile number/OneKey token with their SingPass account.

For media clarifications, please contact:

Malini Nathan (Ms)

Senior Manager

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 that require additional layer of verification.

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.

Updated as of 1 July 2015