

# SafeNet Authentication Service Solution offers Multi-factor Authentication in Compliance with IT Security Guidelines (G3) Government Agency in Hong Kong

A Hong Kong government department deployed SafeNet Authentication Service Private Cloud Edition (SAS-PCE) to deliver a highly secure on-premises authentication solution in compliance with the multi-factor authentication (MFA) requirements in the Hong Kong IT Security Guidelines (G3).

## The Organization

The organization is a Hong Kong government department handling financial account information. The department is responsible for providing courteous and effective public service and in a cost effective manner while “promoting compliance through rigorous enforcement of law, education and publicity programmes.”

For this use case, the organization set an initial deployment for over 1,000 internal staff to be expanded to 3,000 more users in the future.

## The Business Need

### Following IT Security Guidelines: Two-Factor Authentication

As part of the Hong Kong government’s information and cybersecurity posture, the Office of the Government Chief Information Officer (OGCIO) has developed and maintained a comprehensive set of IT security policies and standards.

The [IT Security Guidelines \(G3\)](#) details the policy requirements and sets the implementation standard on the security requirements specified in the Baseline IT Security Policy (S17). Companies operating in Hong Kong are thus required to plan and facilitate effective information security practices to protect information systems and data assets.

Issued in March 2021, the G3 guidelines put emphasis on two-factor authentication, namely for access control, in which its stated requirements are “government bureaus, departments, and agencies (B/Ds) shall prevent unauthorised user access and compromise of information systems, and allow only authorised computer resources to connect to the government internal network.”

The points related to two-factor authentication are outlined under various access control scenarios that include user access management, system and application access control, and mobile computing and remote access.

## Challenge

The organization required a multi-factor authentication (MFA) solution that is simple, secure, and allowed for efficient integration. The organization also required a solution to be seamlessly integrated with their existing privilege account management (PAM), VPN, web-based applications, legacy directory services, as well the home-grown applications within the organization.



## Solution

With Thales strong authentication solutions and its ready out-of-box integration with hundreds of applications, as well as extensive APIs, the organization was able to deploy multi-factor authentication devices and management platforms that help verify user identities and guard against unauthorized access. SafeNet Authentication Service Private Cloud Edition (SAS-PCE) is an on-premises authentication solution that delivers fully-automated, highly secure authentication with the industry widest range of hardware, software and mobile token options tailored to the unique needs of your organization, substantially reducing the total cost of operation with granular security control while offering friendly end user access. SAS-PCE is also available for deployment as an appliance.

## Benefits

Thales delivered the capabilities that organization needed to strengthen security and comply with the IT Security Guidelines (G3) —while minimizing any end-user disruption or inconvenience.

As the government department handles critical data such as financial account information, timely, convenient access to these data is crucial. SAS-PCE is used by hundreds of commercial and governmental organizations and enterprises around the world as a core part of their Identity and Access Management strategy for these simple reasons:

- Strong authentication can be provided anywhere, to anyone where a password is used and through support of industry standards such as RADIUS and the availability of API's and agents for other applications
- Reduced IT management overhead - fully automated lifecycle administration of users, permissions and tokens, including provisioning, updates and revocation, and automated alerts and reporting
- We support the widest range of authentication methods providing the flexibility to choose the right token type for each individual's needs
- We support 3rd party tokens ensuring existing investment in tokens is maintained and providing a seamless migration for end users
- The comprehensive degree of automation drastically reduces the cost of management and administration, in some most cases leading to a TCO saving of up to 60%
- Tokens do not expire and can be re-issued to new users, further reducing costs and administrative burden
- Users can have more than one token with no extra charge beyond the cost of the token, providing support for users with multiple devices
- A comprehensive self-service portal allows users to carry out many functions that traditionally needed support from the help desk
- Extensive Use Case Coverage, with support for VPNs, VDI, cloud applications, local network access, and web portals as well as home-grown customized applications

## About Thales's SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

## About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.