



# Idenprotect Passport

## Financial Services Case Study

### Swiss Wealth Management giant removes complexity, increases security and trust by using Idenprotect Passport

Headquartered in Zurich, Switzerland, this leader and household name in Financial Services wanted to ensure its workforce would be secure, efficient and productive no matter where they were located or which type of device they were using. The customer had embarked on a global project that included a strategic solution for remote and flexible working for their Wealth Management employees. An essential requirement of this new strategy was to enable their employees to have access to their highly sensitive documents and information from their mobile and tablet devices.

IT needed to deliver a seamless authentication experience to satisfy the needs of its mobile Wealth Management workforce whilst addressing the inherent risks and challenges of securing many different types of devices in many locations.

The project wanted to achieve the productivity benefits associated with modern working practices, cloud computing and mobile technology whilst maintaining the highest levels of security and reducing cost.

#### THE CHALLENGE

To provide a strategic authentication solution that is context-based for risk management purposes, integrates with complex environments and is able to meet the most stringent of security controls whilst delivering a world-class, passwordless user experience that is resistant to phishing on both corporate and Bring Your Own (BYO) managed devices.

Additionally, the organisation also wanted to:

- Have the ability to use the solution within their own custom mobile applications using a Software Development Kit (SDK).
- Have the capability to remove hardware-based authenticators, pre-shared secrets or passwords
- Find a strategic authentication and identity management solution aligned to their security ethos that would provide flexibility, trust and usability.
- Leverage their existing IT investments. Like many other financial services organisations, they had heavily invested in Public Key Infrastructure (PKI) as the main trust and security backbone.

#### THE EXPECTATION

Clear expectations were agreed between the project sponsors and Idenprotect. The project had to deliver:

- A world-class and seamless user experience that was consistent across different use cases.
- Authentication and Identity Management with the ability to integrate with systems and services that support the management of mobile workforces.
- A single and centralised solution that would support both corporate-owned and BYO.
- A solution that would provide self-service features for its users, automated workflows and the flexibility to easily integrate with other applications and systems that were used within the organisation.

## THE SOLUTION

After a very detailed and competitive process, Idenprotect, a leader in phishing-resistant, passwordless access security, was selected for its innovative approach and its ability to bring cohesion within complex environments through the use of Idenprotect Passport.

In addition, the ability to use existing infrastructure, without changing operational and business processes, was seen as highly beneficial as it would not add further strain to an already complex environment. Existing services within the enterprise, such as Databases, Certificate Authorities, Directory Servers and other components would therefore still be used. This flexibility would then allow many parts of the business to implement Idenprotect Passport within their own applications.

From the users' perspective, Idenprotect Passport would provide a simple and trusted process that would allow them to seamlessly enrol, activate and authenticate. The solution would also ensure that trusted staff, contractors and other authorised users could be on-boarded simply and quickly.

The phishing-resistant, passwordless capabilities provide a zero-touch for its users by allowing access to documents without having to remember or use a password, reducing the complexities and frustrations normally experienced with using multiple passwords to access multiple systems. The phishing-resistance that Idenprotect Passport provides ensures assurance and piece of mind for senior management in that none of their staff will fall victim to a phishing or credential theft attack. Finally, the solution is expected to significantly free up time for users to allow them to work on more important things.



The bank required a technology that would satisfy the needs of the business by:

- Enabling secure access to the corporate email system and to multiple applications so that corporate data could be accessed whilst on the move.
- Supporting multiple platforms on multiple networks using different authentication mechanisms and single sign-on.
- Facilitating appropriate and accurate user identity validation and device trust to prevent unauthorised access.
- Preventing any external parties from having any type of control or ability to re-construct business sensitive cryptographic key material that may be generated on user devices.
- Protecting the private keys of each user by using a segregated secure execution environment in hardware.
- Being resistant to tampering, reverse engineering, application attacks and cloning.
- Enabling location awareness policies for remote access and to ensure compliance with local and international laws on privacy.

## THE RESULT

Idenprotect Passport has been a huge success for our customer and especially for the daily users of the technology. The user experience is significantly enhanced as users no longer have to repeatedly input their passwords to their mobile devices to access documents or nor do they have to resynchronise their passwords once they have been through a password reset process.

Flexibility within the solution has allowed system owners and administrators to adopt Idenprotect Passport without changing significant parts of their network. The flexibility has been extended further by enabling other parts of the organisation to use Idenprotect Passport in securing their own bespoke applications while simply and quickly meeting internal governance, compliance and external regulatory obligations.

Cost and time savings have been delivered by facilitating trusted access to sensitive data via BYO devices, not just via corporate-owned devices. Further cost savings have been made through integration with new web-based services that automate helpdesk activities. Indirect savings will also be realised through increased user productivity and a reduction in IT support calls for password resets and account unlocks.



[sales@idenprotect.com](mailto:sales@idenprotect.com)  
+44 (0) 20 3900 2704  
[www.idenprotect.com](http://www.idenprotect.com)

### About Idenprotect

Idenprotect enables security-conscious businesses that want to control who can access their digital resources, whether on-premise or in the cloud, without friction or complexity. Led by experienced leaders within the cyber security field and expertise in enterprise security and access technology, Idenprotect's passwordless and phishing-resistant technology is a proven solution within large and small enterprises, securing some of the worlds best-known and largest brands.