

## EXECUTIVE SUMMARY

**Business Objective**

Enable remote employees to access corporate resources and applications securely

**The Problem**

The bank needed a scalable and proven high-security solution that preserved customer acceptance and usability

**The Solution**

- Digipass® GO 3
- OneSpan Authentication Server Framework

**Results**

- Reduced exposure to core systems through password misuse
- Prevents access to confidential information by unauthorized users
- Maintains data integrity and document confidentiality
- High user acceptance

# SOUTH AFRICAN BANK ELIMINATES REMOTE ACCESS SECURITY CONCERNS

Standard Bank Group is a leading South African banking group. Outside the African continent, Standard Bank Group operations span to 16 countries, including the United Kingdom.

In a time of ever-growing internet security threats, the bank realized that traditional static passwords were inadequate to secure remote access for its branch offices worldwide. By deploying OneSpan authentication technology, the bank's employees have real-time access to corporate resources and applications, anywhere at any given time.

Standard Bank's Corporate and Investment Banking division is a leading global emerging markets corporate and investment bank and offers its clients banking, trading, investment, risk management and advisory services in developing economies throughout the world. It has specific sector expertise in industries relevant to its global footprint, with strong sector value propositions in mining and metals; oil, gas and renewables; telecommunications and media; power and infrastructure; and financial institutions. The group is represented in 33 countries.

## Static Passwords Too Vulnerable for Secure Access

Local branch offices connect to the bank's central network through a SSL/VPN connection. This remote access method has yielded far-reaching productivity benefits, but security risks have increased. To secure remote access to its network for London-based employees, the bank realized they needed a more robust security solution than traditional static passwords.

Single-factor authentication is inadequate for remote use as it poses huge identity theft risks.



“We were looking for a cost-effective and scalable solution with the flexibility to grow with the Group's authentication needs. OneSpan's Digipass technology met all of our security requirements.”

**James Atkins**

Network and Security Engineer  
Standard Bank

“Organized cybercrime has increased substantially over the past decade,” says James Atkins, Network and Security Engineer at Standard Bank. “Fraudsters will continue to exploit vulnerabilities in corporate IT systems. Conventional static passwords can be easily obtained or hacked by third parties, gaining them unauthorized access to core systems and confidential information. They do not offer sufficient protection against fast growing forms of online fraud like phishing, key loggers and Trojans. We therefore decided to implement a high-security solution that bypasses the weaknesses of static passwords in order to maintain data integrity and document confidentiality.”

### OneSpan’s Two-factor Authentication Offers High Return on Investment

Two-factor authentication is a far more robust security solution than traditional password authentication, as it requires two separate security elements. Intruders not only need to obtain a password or PIN code, but would also need the physical authentication device in order to access the corporate network and its applications.

In a side-by-side trial, Standard Bank evaluated several two-factor authentication solutions from different vendors. Solution offerings were compared on key areas such as initial setup cost, cost over lifetime, user-friendliness, average lifetime of the authentication devices and ease of setup and management. The solution needed to provide a user-friendly environment for employees as well as IT staff to access the network from any location. Business-critical data held on the server and corporate network needed to remain confidential and unauthorized access to corporate applications had to be prevented at all cost.

“We were looking for a cost-effective and scalable solution with the flexibility to grow with the Group’s authentication needs,” James Atkins states. “OneSpan’s Digipass technology met all of our security requirements. Additionally, the fee per device is very reasonable and the average battery lifetime of seven years and beyond offers a high return on investment.”

### Up And Running In No Time

Standard Bank deployed OneSpan’s Digipass technology together with the software suite, which was installed on two redundant servers. Implementation was simple. The software installation went swiftly and the system was up and running in no time.

“The manual assignment of the authentication devices to each individual user took up most of the time and was quite a lengthy process,” James Atkins tells us. “It was, however, user crucial that we would complete this task first as it allowed us to disable alternative access methods that no longer complied with our security policies. Now, a year later,

we have over eight hundred employees actively using this service.”

Currently the bank is looking to upgrade to the OneSpan Authentication Server. It offers a complete web-based administration interface and provides a built-in SOAP API so that authentication and transaction validation functions can be integrated into existing web-based applications. One Digipass GO 3 device could then be used to secure several applications.



“We were looking for a cost-effective and scalable solution with the flexibility to grow with the Group’s authentication needs. OneSpan’s Digipass technology met all of our security requirements. Additionally, the fee per device is very reasonable and the average battery lifetime of seven years and beyond offers a high return on investment.”

**James Atkins**  
Network and Security Engineer  
Standard Bank

### Secure Access With Dynamic Passwords

Thanks to OneSpan, the bank’s employees now have full access to the corporate network and its applications without the need for any client-based software to be installed on their PC.

Standard Bank’s employees in London are now able to connect to the VPN/ firewall and use their Digipass GO 3 to authenticate themselves and access the corporate network. They log-on with a dynamic password, generated by the stand-alone authentication device Digipass GO 3. The server software verifies all authentication requests. Only when there is a positive proof of identity, access to the bank’s network and its applications is granted.

As passwords are neither directly or indirectly exposed over the internet or stored on the employee’s PC, they cannot be compromised by phishers. Furthermore, the Digipass-password changes default every 32 seconds.

Batch processing of username/ password combinations or keystroke logging becomes therefore virtually impossible as the time-limit forces fraudsters to operate in real-time. “Two-factor authentication enabled us to severely reduce exposure to our core systems through password misuse,” James Atkins adds.

## CASE STUDY | STANDARD BANK

The use of OneSpan authentication was readily accepted by the business. Digipass GO 3 is a one-button authenticator and its use is very intuitive, resulting in a high user acceptance. In the last twelve months, Standard Bank noted a 100% increase in the amount of VPN accounts created.

### Client Overview

Standard Bank is a leading African banking group focused on emerging markets globally. It has been a mainstay of South Africa's financial system for over 145 years, and now spans 17 countries across the African continent. Its international expansion has taken it to 16 countries outside Africa including Brazil, Russia and China. Its headquarters are in Johannesburg and it is listed on the Johannesburg Stock Exchange.



OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

#### CONTACT US

For more information:

[info@OneSpan.com](mailto:info@OneSpan.com)

[OneSpan.com](https://www.OneSpan.com)



Copyright © 2018 OneSpan North America Inc., all rights reserved. OneSpan™, DIGIPASS® and CRONTO® are registered or unregistered trademarks of OneSpan North America Inc. and/or OneSpan International GmbH in the U.S. and other countries. All other trademarks or trade names are the property of their respective owners. OneSpan reserves the right to make changes to specifications at any time and without notice. The information furnished by OneSpan in this document is believed to be accurate and reliable. However, OneSpan may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use. Last Update May 2018.