OneSpan

FAQ

MULTI-FACTOR AUTHENTICATION SOLUTIONS

SWIFT Mandatory Security Controls:

4.2 Multi-factor Authentication – Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.

5.2 Token Management – Ensure the proper management, tracking, and use of connected hardware authentication tokens (if tokens are used)

MULTI-FACTOR AUTHENTICATION SOLUTIONS COMPLIANT WITH SWIFT CSP

Which OneSpan's solutions answer the MFA requirement of the SWIFT CSP?

We provide both server-side and client-side solutions to comply with the MFA requirement:

a) Server-side

OneSpan Authentication Server is a comprehensive, centralized, and flexible authentication platform designed to deliver complete authentication lifecycle management via a single, integrated system. It offers secure and seamless access to a variety of corporate resources and applications from SSL VPNs to the SWIFT network. It supports OneSpan's entire range of authentication solutions and simplifies authentication management for both administrators and end users. OneSpan Authentication Server also meets SWIFT's requirement for managing and tracking the authentication tokens.

b) Client-side

Authentication on a workstation connecting to the SWIFT network involves using a separate device – a software or hardware token. OneSpan offers the following solutions:

- Hardware tokens (One-button, Transaction Data Signing tokens, PKI USB keys)
- Cronto code hardware tokens
- Mobile Authenticator app: Mobile Authenticator generates a one-time password and supports additional PIN protection, fingerprint recognition, FaceID, and device binding capabilities to ensure the highest level of security.
- Mobile Authenticator Studio app: This solution offers authentication capabilities combined with enhanced built-in application security.
- Mobile Authenticator SMS:Mobile Authenticator SMS sends one-time passwords via SMS or email. This solution can be used as a primary authentication method or as a back-up in case an authentication device is lost or unavailable.

Which mobile operating systems do your software tokens support?

OneSpan's mobile tokens can be used both on Android and iOS devices.

Can we use one token for multiple users?

Each token can only be linked to a single user for security purposes. In its Security Conformance Requirements, SWIFT states: "The authentication factors presented are individually assigned and support individual accountability of access to the messaging interface."

FAQ | MULTI-FACTOR AUTHENTICATION SOLUTIONS

Is MFA required to access all SWIFT services or only selected ones?

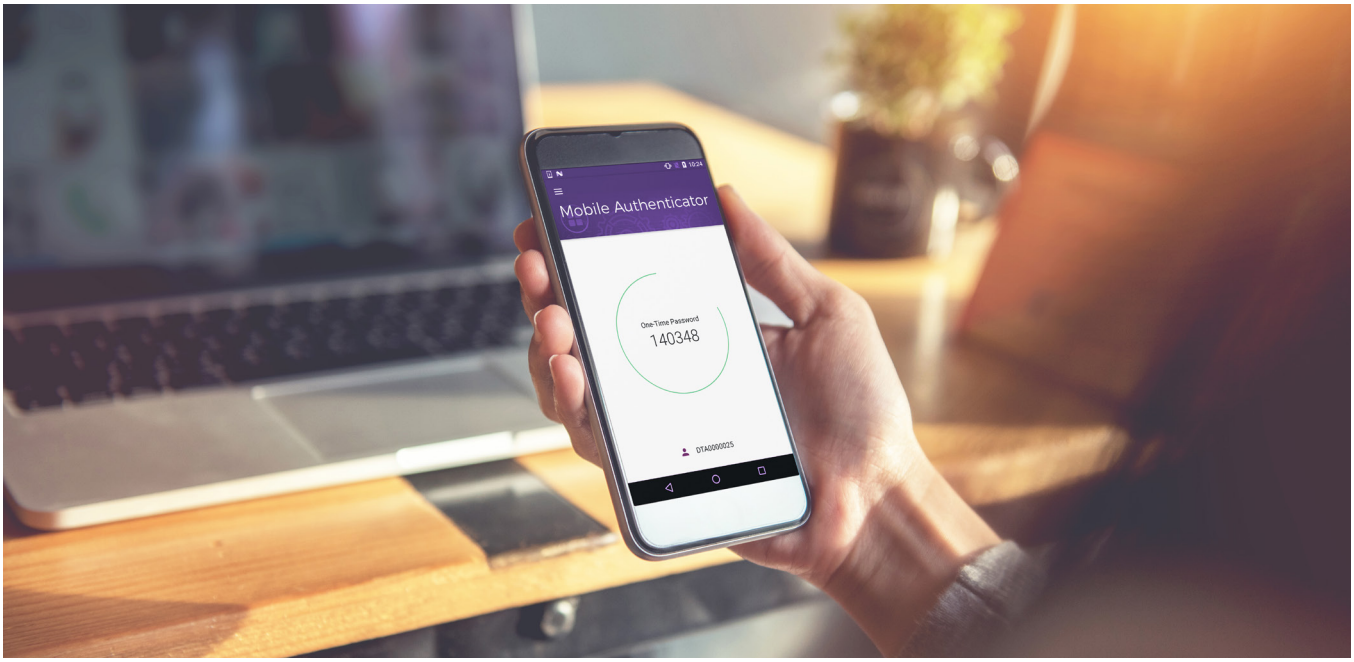
Access to any SWIFT service can be compromised. Therefore, we suggest securing access to all services with MFA solutions.

Is MFA required for users of all permission levels or only for administrators?

SWIFT requires that you secure access for all users, which means that each individual user is required to use MFA to access any of the elements of the SWIFT network.

Do you have experience with authentication solutions to secure access to SWIFT?

Yes, we have several examples of successful implementations of authentication solutions to the SWIFT network. Please contact our sales representative for more information.



OneSpan

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
www.OneSpan.com