Schlumberger

Azure Active Directory

Schlumberger Single Sign On process.

On April 22, the following SIS applications aligned their customer registration and sign on processes with www.delfi.slb.com. This change enables single-sign-on for our customers across the following sites, once they have authenticated with a valid email address and password:

- www.software.slb.com
- www.nexttraining.net
- www.ocean.slb.com

Customers were also asked to supply additional information to add a multi-factor authentication check (2FA), which sends a verification code to their mobile device for additional security compliance.

What is today's solution?
The new service leverages MS Azure AD B2C Identity Service and is the underlying technology that manages the identity of any customer who wishes to register for customer support or DELFI Services.

Why do we need 2FA?
Additional layers of security through the implementation of multi-factor authentication (2FA) has been configured by default to protect our customers data from cybercriminals. Hacking a password is extremely easy. However, gaining access to a physical device that generates the second code is not as simple, which is why 2FA is one of the most effective security approaches available.

The generation of a one-time-password (OTP) is supported by SMS and Call Me options with the Schlumberger use case.

Furthermore, 2FA effectively secures mobile devices which is an increasingly common way of accessing online Schlumberger resources, or company owned data like shared documents.

I cannot use 2FA
If you are unable to use 2FA for any reason, we can bypass the 2FA stage by supporting the federation of your customer credentials into Azure. This relies on your company managing your identity profile, and you therefore align with your company's IT policies.

Next steps
If you are interested in Azure AD Customer Federation, please contact your Schlumberger account manager who can start these conversations on your behalf with our engineering teams.

Version 1.0 – August 2020