IDENTITY ASSURANCE

Balancing security, cost and customer experience for Microsoft Azure and Office 365

Prove user presence and non-repudiated access to Azure and Office 365.

Allow users to self-create and manage their accounts.

Ensure access by authorised users only.

Block account takeover.

TokenOne provides organisations using Active Directory, and users of Azure or Office 365, a strong two-factor authentication security solution that assists them in meeting their legal and industry compliance obligations.

Compared to other approaches for multi-factor solutions (such as soft tokens), TokenOne Authentication is a genuine, strong two-factor solution where both factors are strong. TokenOne Authentication is:

- Simple and easy to deploy en masse
- Allows users to continuously and securely manage their own digital identity
- Proving users are present at the transaction (not just the token).

TokeOne Authentication is not just simple and secure, it is also less expensive to deploy, manage and administer than traditional two-factor solutions.

Challenges of deploying strong two-factor authentication across Azure & Office 365

- Verifying new users without delay and at a business justifiable cost
- Ensuring convenience and simplicity for the user
- One solution for all access points, including Microsoft Azure, Office 365 accounts and services
- Passwords and simple OTP solutions like SMS may not meet an organisation's legal and industry compliance obligations

Solutions

- TokenOne delivers a strong two-factor authentication solution that enables increased security at scale for Azure and Office 365
- TokenOne enables organisations to deploy a cost effective authentication solution that meets both, security AND compliance requirements
- TokenOne Authentication scales easily across cloud based infrastructure while allowing a single user experience regardless of the backend infrastructure

Outcome

- Simple to register, manage and use
- Easily and cost effectively deployed solution
- Strong two-factor authentication for specific services or across the whole environment
- Non-repudiated access to key Microsoft services and sites
- High value application data (compliance)
- Single branded solution for users regardless of distribution of backend infrastructure

Using TokenOne Authentication

A TokenOne user's PIN is never entered, transmitted or stored anywhere!

User proves their identity to start the registration process.

TokenOne Authentication One time pad (KeyMap) allows the user to convert their PIN for registration and ongoing authentication.

The user's PIN is mentally converted, using the KeyMap, into a different code every time.

The user enters their one time code to prove they "know" their secret PIN without ever revealing it.

Registration

Authentication

Azure and Office 365 Use Case

The key differentiator with other authentication services such as RSA, Vasco, Google Authenticator, Authy etc. is that TokenOne Authentication proves user presence. We provide genuine strong two-factor authentication, as both factors are strong.

There are three (3) accepted factors in Authentication:

1. Something you know - the knowledge factor
2. Something you have - the possession factor
3. Something you are - the inherence factor

With TokenOne Authentication you never enter or reveal your secret PIN – so the knowledge factor is kept strong and safe. Other solutions require users to prove knowledge of their secret (their password) by entering it. TokenOne Authentication sets a new standard for the knowledge factor by enabling proof of the knowledge factor without ever revealing it. This makes the TokenOne PIN a "zero knowledge password proof" and sets a new standard for authentication.

The second factor, the possession factor, is your smart device. This has been profiled and must also be present to prove you are an authorised User.

With TokenOne Authentication both factors are strong. TokenOne Authentication proves who is accessing your site or service. This is vital not only for the security of sensitive information but also for compliance.