TURing

KEY BENEFITS

- Easy to use
- No token to manage
- Easy to Integrate
- Simple and easy to understand
- Low cost of adoption

We all know that username and password is not enough but what do you do when you want to deploy stronger authentication but two factor authentication is over kill for lower risk environments?

Unlike many tokenless authentication solution providers, the Swivel platform can be used as a single-factor and/or two-factor authentication system, enabling organisations to tailor the solution using whatever combination they need to fit their security policies and compliancy regulations.

Single Factor Mode - How does it work?

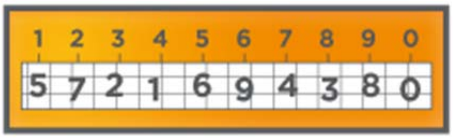
The Swivel tokenless authentication platform works by displaying a challenge to the user. The user is then required to respond with the correct response in order for authentication to take place.

In single-factor mode the user is presented with a security challenge on the same screen that they enter their one-time code. This is generally implemented within a browser, where an image is presented within the authentication dialogue.

This means that Swivel authentication can be applied no matter what device is being used to access the application and a token is not required to access the security string.

TURing

The TURing image is a single image used to represent the security string. The TURing image uses placeholders to help the user extract their One Time Code.



1	2	3	4	5	6	7	8	9	0
5	7	2	1	6	9	4	3	8	0

The user combines their PIN in their head with the security string and enters their OTC within the login screen.

In this example, a PIN of 4359 would produce a One Time Code of 1268. The TURing image is by far the most popular authentication interface especially with users.

SWIVEL
the power of knowing

Customisations

The TURing image can be customised in a number of different ways including:

- Fonts
- Background
- Boldness of characters
- Jiggling the characters so that they are not horizontally aligned
- Animation

Different colours and borders are available to allow you to select the “theme” for these images, e.g. monochrome only backgrounds. Use of different fonts and backgrounds make the TURing image more resistant to optical character recognition (OCR) attacks.

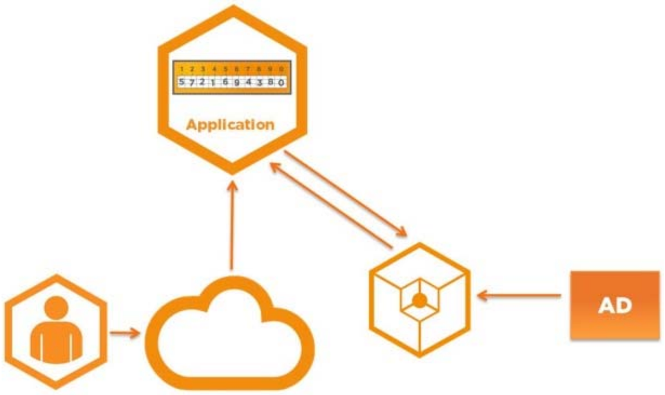
Animating the TURing image is a defence against screen capture type attacks. When the security string is animated only a subset of characters are visible at any one time meaning attacks that involve a screen shot or even low sample video will only get a partial result.

Integration

TURing integration requires the ability to present the challenge, the TURing image, to a user.

The TURing interface works across all browsers, and platforms including mobile. The TURing image is presented using a combination of HTML and JavaScript.

When a user accesses the sign-in page of an application, or VPN, they will be challenged with the TURing image. The code generated by the TURing image is sent to the Swivel core for validation. If the code is correct, they will be allowed past; failure will prompt for a new code.



TURing integration is available for most leading VPNs, web applications (OWA, SharePoint) and cloud solutions (Office365, Google, Salesforce.com). Please visit our knowledge base (kb.swivelsecure.com) for more information.