Swivel Accessibility in Authentication

Contents

Introduction

Swivel Secure is a vendor of Strong and Two Factor Authentication. This document details how Swivel allows authentication for those who have various forms and degrees of disability.

The flexibility of Swivel means that a solution can be deployed in a variety of methods where the user can select which authentication method suits them and is available for all users.

Architecture

Swivel is usually located at the entry point to a VPN or website, where the correct determination of a user is required. Typically this will be in the form of a username, one time code, and optionally a static password.

Swivel Protocol

Swivel optionally provides additional security to One Time Codes used for authentication by PIN protection. Security measures applied to the PIN include:

- PIN extraction provides additional security.
- PIN length 4-10 numbers, increasing the length increases the security with a trade off against users ability to remember a longer PIN.
- Optionally PIN distribution may be by a different method to security string distribution and is defined by transport (SMS, Email, Postal Delivery).
- PIN security warning to users to never reveal their PIN?s and avoid social engineering.
- PINless option for use with dual channel authentication. The One Time Code is the Security String.

Vendor Integration

Swivel provides a variety of delivery methods that integrate in a number of different ways with partner vendors. When integrations are carried out it is important to ensure that accessibility options are provided by the access device vendor, these may include:

- Clear fonts
- Ability to increase font size
- Text for use with text to speech readers
- Clearly defined user input fields
- Ability for speech to text readers to input information
- ALT Tags with text for embedded images
- Ability to TAB between fields
- Clear method of obtaining assistance
- Ability to use varying input devices such as on screen keyboard, accessibility keyboards

Security String Delivery

Security Strings may be provided to the user in a number of ways. In this section we look at each in turn and examine how they can be used and in some cases modified for greater accessibility. Some methods inherently allow greater accessibility than other methods, and may be suitable for particular groups of users. Swivel supports a mix of authentication methods where appropriate.

Swivel Single Channel ? Embedded Images

Swivel currently provides three types of single channel authentication images for strong authentication, by default all use obfuscation to reduce the chance of automated character recognition, with customisable fonts and backgrounds the images can be selected to allow easier recognition. The Single Channel image requested by the user is provided as an SSL image in their web browser, it is a unique GIF based upon the username, the request (image) has a configurable lifespan (default 120 seconds) to provide a security string that can be refreshed by user demand.

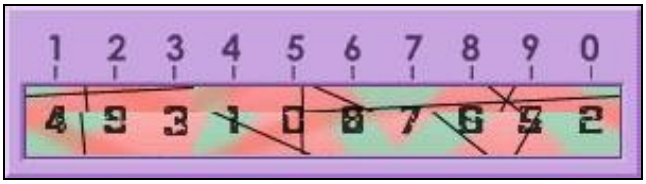
Some features of Swivel Single Channel embedded image accessibility include

- Fully customizable fonts
- Fully customizable backgrounds
- Fully customizable border

- Ability to generate new images on demand
- Ability to work with existing technologies such as screen magnifiers

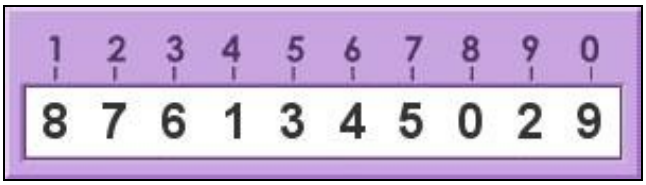
TURing

Standard Turing showing standard font, background and border



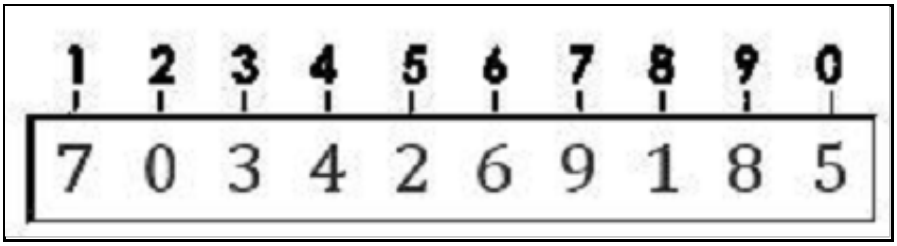
Where the font is difficult to read, Swivel can be modified to display clearer fonts and backgrounds without patterns and an increased contrast

Modified Turing with easy to read font and clear background coloured border

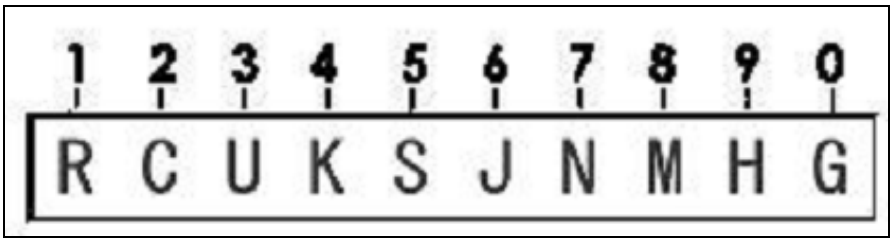


The border can be changed to make the contrast between numbers and background greater

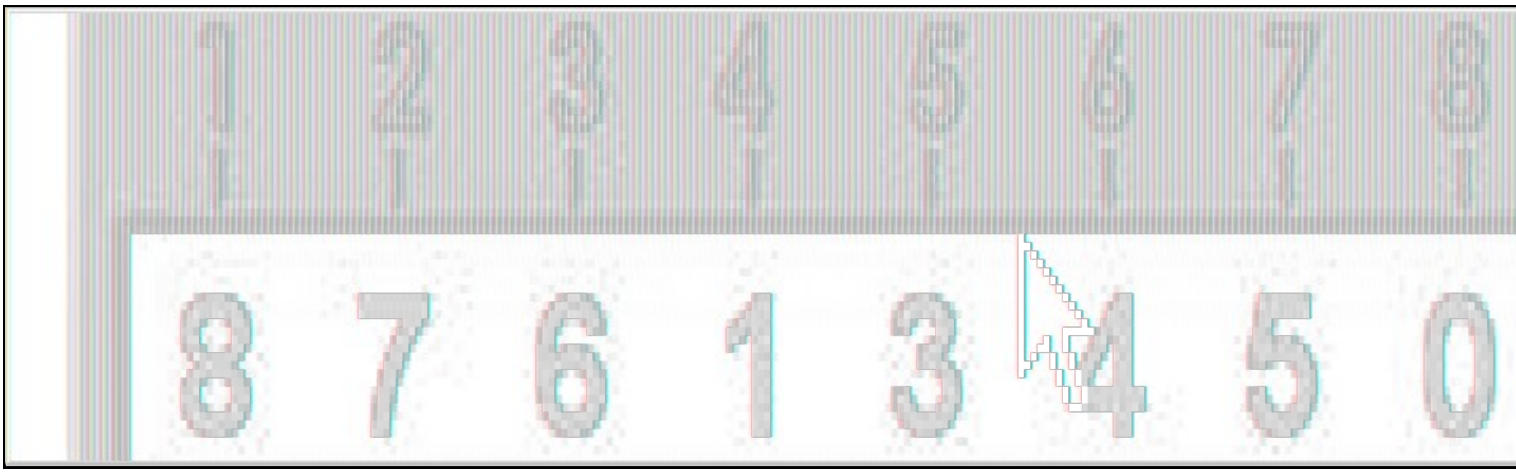
Modified Turing with easy to read font and clear background and border



Modified Turing with easy to read upper case letter font and clear background and border

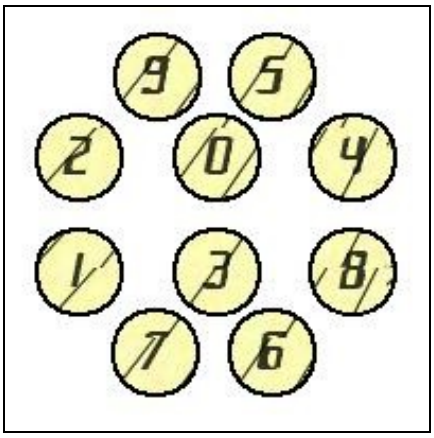


The images can be viewed through a variety of tools such as the Windows Magnifier:

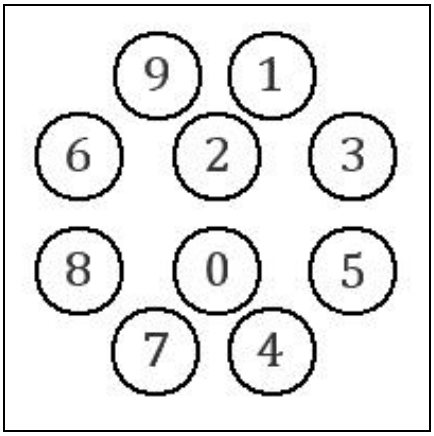


PATtern

This provides additional security as a PIN is not used but instead a pattern, it is not related to the Pinpad.

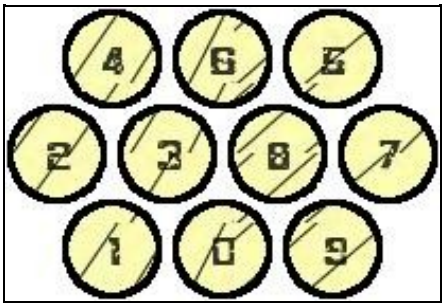


Modified PATtern with easy to read font and clear background

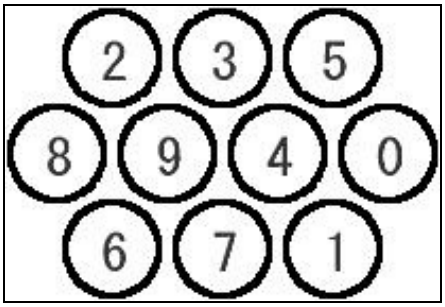


PATtern 2

This provides additional security as a PIN is not used but instead a pattern, it is not related to the Pinpad.

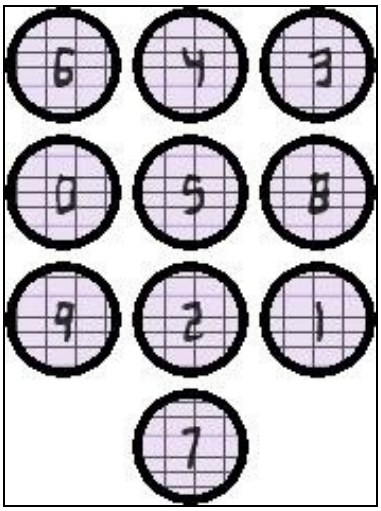


Modified PATtern with easy to read font and clear background

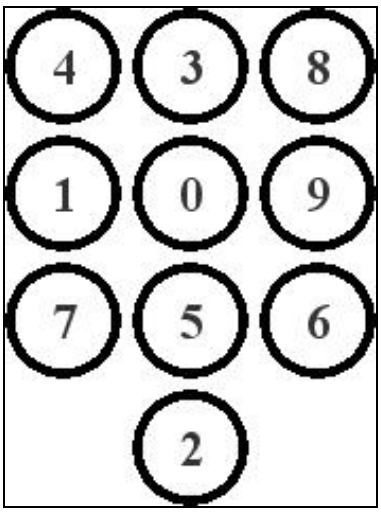


BUTton

Is styled as a telephone keypad. It is not related to the Pinpad.

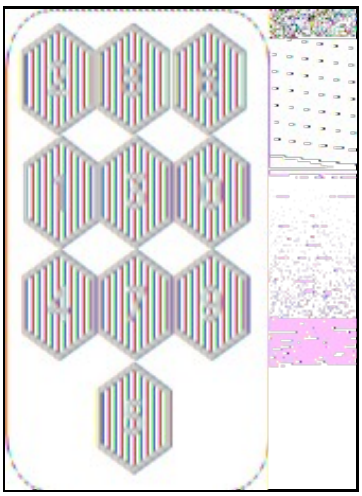


Modified BUTton with easy to read font and clear background



PINpad

This allows the PIN number to be clicked on



Swivel Single Channel Security ? Spoken security string

Swivel has developed the ability for Swivel to provide security strings by an audio message.

Swivel Single Channel Security ? Clear text security string

Swivel has developed the ability for Swivel to provide security strings by text in a web browser.

Swivel Single Channel Security ? Taskbar

Swivel has developed the ability for Swivel to provide security strings by Turing in a pop box. This could further be developed for audio or text or other method, if other accessibility programs have API?s.

Where a PC has been customized for the specific needs of accessibility for an individual or group, then this may be a suitable method of providing authentication strings.

Swivel Dual Channel Authentication ? SMS

Using SMS turns the users mobile phone into a token for authentication, and has become an accepted form of two factor authentication.

Some features of Swivel Dual Channel SMS accessibility include

- Uses commonly available devices
- Existing SMS accessibility tools can be used
- User can request new security string
- PINless option

With SMS there is the option for PINless authentication as an acceptable method for providing users with a One Time Code for authentication. The security string is sent in the clear, without the need of a PIN to extract a OTC.

Existing technology for reading the text message can be employed by mobile phone users. In addition some SMS providers support text to voice so the user would receive a voice call of the security string or One Time Code.

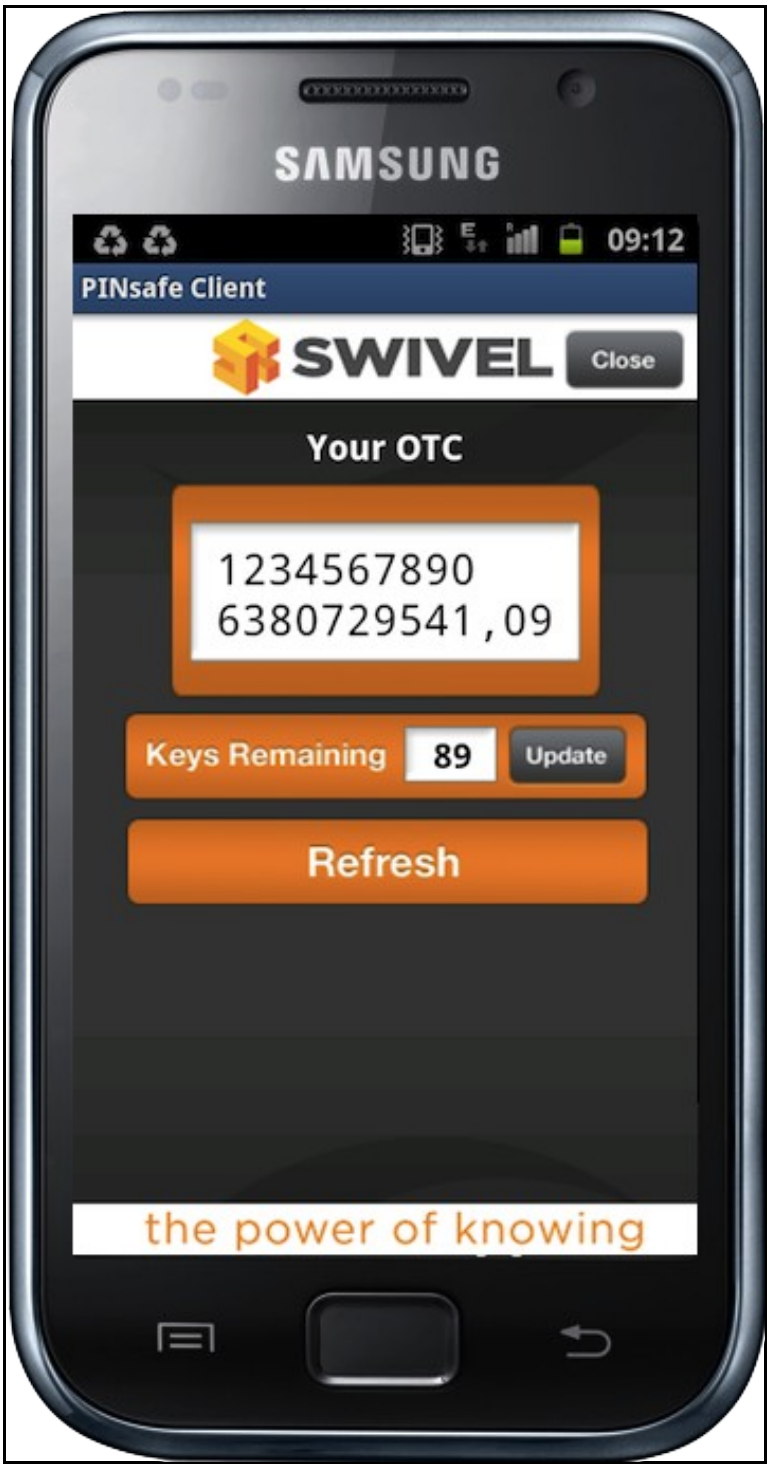
Additional tools may be of use such as the Nokia Braille reader: http://betalabs.nokia.com/apps/nokia-braille-reader

Swivel Dual Channel Authentication ? Mobile Phone Authentication

The Mobile Phone Apps download and holds up to 99 security strings on the mobile phone. The PIN number is never stored on the mobile, so cannot be extracted. The security strings are downloaded by GPRS/3G/4G.

A proof of concept has been made of the speaking version of the Java applet and provides an ideal way of providing the One Time code for authentication, although the user needs to start the application, select enter OTC and enter the PIN. Further development of this application could perhaps have the PIN box appear upon starting the application.

Where a mobile telephone has been customized for the specific needs of accessibility for an individual or group, then this may be a suitable method of providing authentication strings.



Swivel Dual Channel Authentication ? Voice Authentication

Swivel can be configured to call a telephone number, such as landline or a mobile number and then the user may authenticate themselves, the following configurable options are available for a user to authenticate themselves entirely out of band:

- Accept call by pressing # on phone keypad
- Enter OTC on phone keypad
- Enter PIN on phone keypad

Swivel Single/Dual Channel Authentication - Email

Email may be used as two factor authentication when requested by a user that receives emails by GPRS/3G to a mobile device, but can also be single channel when received on the same PC used for authentication. Existing tools for reading emails could be utilised.

Security and Accessibility

For every single user, there is an accessibility trade off in all security implementations, and is determined by the company security policy. Care must be taken where security may be lowered to allow greater ease of use. Where this is a particular subset of users then that form of access may be allowed for only a group of users rather than for general use, or where policy dictates, it may be mandated that the authentication methods are usable by all. Security measures that can be deployed are:

- Limited login attempts to prevent brute force attacks
- Combining authentication technologies
- ChangePIN functions using a variety of Single and Dual channel authentication methods