

## Tokenless, Two-Factor Authentication

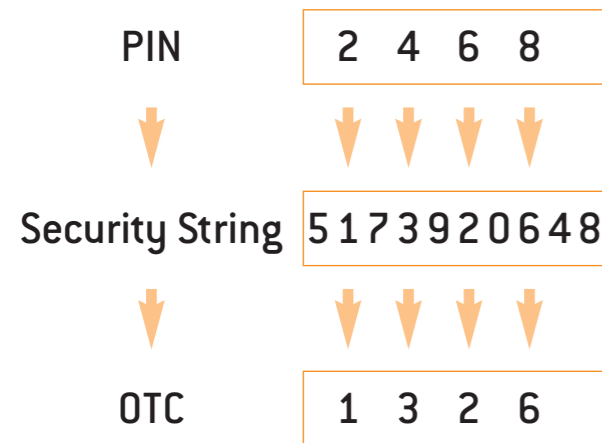
### User Interface Options

Swivel's PINsafe two-factor authentication technology has been developed to provide a secure, flexible and cost effective solution for a wide range of remote network access applications including SSL VPN systems.

### The Swivel Protocol

This patented algorithm involves the use of a registered PIN and a security string delivered to the user. PINsafe leverages the full functionality of the cellular network infrastructure and internet technology to provide a range of client interface options that eliminates the need to distribute hardware or software tokens to large numbers of authorised users.

A one-time code (OTC) is extracted from the string by 'reading' off the digits corresponding to their registered PIN. In the example below if the PIN is 2-4-6-8 the OTC would be the 2nd, 4th, 6th and 8th digits i.e. 1-3-2-6



Included as standard options within the set-up and configuration workbench, PINsafe offers three choices for the user interface that can be assigned to each user in line with corporate security policies and access authorisation requirements. Each interface enables the user to either generate the OTC necessary automatically or manually extract the OTC to complete the authentication process.

### Cellular Short Message SMS

For organisations that have large numbers of employees or customers who have cell phones PINsafe includes an option for the security string to be delivered to the user via a SMS text message. Using the SMS option the user always has an active security string stored on the phone and ready for use at the point of authentication.

This ensures that the user is not prevented from access by the lack of a cellular network signal or delays in the relay of SMS traffic between networks. Once the security string has been used the server sends out the next SMS, which overwrites the previous message to avoid user confusion and unnecessary inbox management.



In practice the user needs only to extract the OTC from the SMS using the same procedure as described above and then enter it via a Web browser or network interface. This means that the two key elements of the authentication process are never transmitted on the same network making them virtually impossible to capture by Trojan spyware.

The SMS option is particularly aimed at organisations whose users need remote anytime, anywhere access from any end-point device including from a hotel business centre or cyber café for travelling executives.

## Tokenless, Two-Factor Authentication

### Java Application

PINsafe can also be deployed using a Java-enabled mobile device including cell phones and PDAs with cellular connectivity. Using this option a simple Java application can be downloaded to the device via a GPRS connection.



This option offers a range of additional features not available using the TURing or SMS interface.

Firstly the system includes the option to store multiple security strings on the device to allow for extended roaming periods outside a GPRS network area.

Secondly the generation of the OTC is automated with the user entering their PIN on the mobile device's keypad. The OTC is displayed on the screen of the device and includes two check digits to synchronize the security string with the authentication server. The system allows for up to 99 strings to be stored on the phone which can be replenished at anytime convenient to the user.

### The TURing Interface

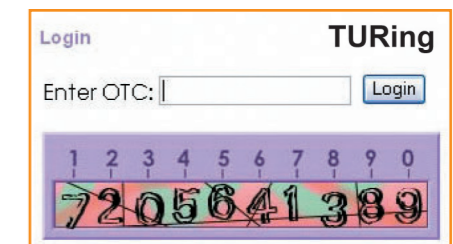
The TURing interface, named in honour of the World War II code breaker, uses an obfuscated image to display the security string served as a web page once the login session has been initiated.

The obfuscation of the image and the generation of the GIF are designed to ensure that the security string is protected from Trojan OCR software during the delivery from the server and display on the client PC. This is particularly important if the user is accessing the system from an untrusted device and also provides additional protection where up to date anti-virus software is running, which would be our normal recommended approach.

A special feature of the system ensures that each time a new image is displayed the appearance is different. By using a combination of randomly selected irregular font and patterned backgrounds the chances of any undetected OCR software compromising the string over an extended period of time will also be significantly reduced.

As an extra security feature, during the authentication process the user is never required to enter their registered PIN at a keyboard (only the OTC is typed) ensuring that it cannot be captured by spyware such as key loggers, further protecting the ID of the user.

The TURing interface can be easily integrated with existing web sites of SSL VPN technologies to replace weak username and password authentication or as an alternative to costly token based systems. Alternatively with Windows based systems the TURing image can be stored on the user's Active Desktop and integrated within a range of standard business applications.



Patent information: Single/Dual Channel; UK patent no 2 366 966 US patent applications 2002/0029342 and 2002/0059146 International patent application WO 02/21463, nationalised in 14 countries including: European patent application 1 316 076. Company No. 4068905