SMS Based Authentication

Until recently two-factor authentication has been synonymous with the requirement for costly user token devices. Today's advances in mobile device technology and widespread availability of high speed networks means that the argument for choosing a token-based solution is no longer sustainable. Swivel's award winning technology enables organisations to leverage employees' existing mobile device functionality to support two-factor authentication across the full range of remote access environments including VPNs, Web sites, Cloud, and real/virtual desktops.

KEY BENEFITS

- OTC sent direct to mobile
- Can be used with or without PINsafe
- Easily configurable
- Reduced SMS costs with multiple OTC

The Swivel tokenless authentication platform works by sending security strings to you via SMS or mobile network. You are presented with a security string in a different channel from where you enter your OTC and is required as part of your normal application login process for authentication to take place.

SMS

Swivel provides organisations with a range of configurable SMS-based options for the delivery of the security string to the end user device, giving IT security manager's maximum deployment flexibility.

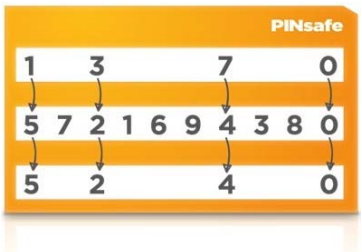
For all SMS implementations the format and wording of the messages is configurable.

One-Time-Code

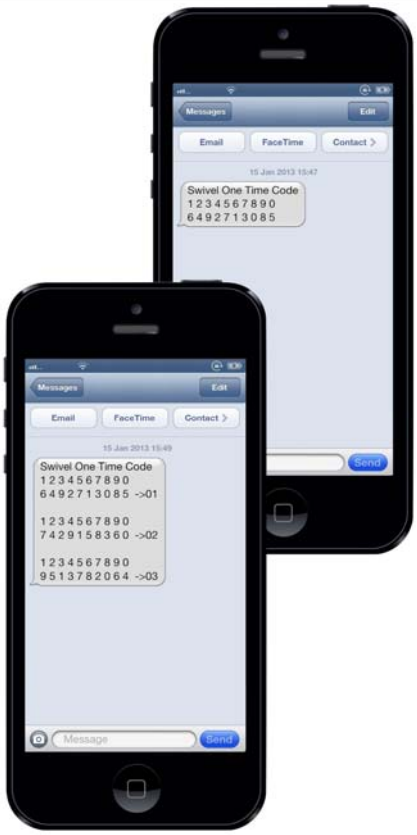
The Swivel solution can be used with or without Swivel's unique PINsafe extraction protocol. When the platform is configured without using the PINsafe protocol, you are sent a one-time-code via SMS. This code is then entered exactly as received as part of your login process.

PINsafe

A key and unique feature, of our authentication platform is our patented OTC extraction protocol PINsafe. PINsafe combines the use of registered PINs with random 10 digit security strings; you then combine these in your head to work out your unique OTC, putting you at the heart of the strong multi-factor authentication process. Utilising the PINsafe protocol provides users with additional level of security, should a phone be lost or stolen.



SWIVEL
the power of knowing



Advance SMS (Single)

The SMS containing the security string or OTC for the next login is sent immediately after an attempted authentication, meaning the user always has a security string ready for their next authentication attempt.

Advance SMS (Multiple)

The SMS contains multiple security strings or OTCs, which remain valid until used. The user is prompted by the login-form as to which string to use. The SMS is auto-refreshed after the last security string has been used. This has the benefit of reducing SMS costs and also means the user can have a number of security strings available to them even when they are out of coverage.

SMS On-demand

The user is sent an SMS containing the security string or OTC at the time of authentication.

SMS In-bound

The user texts the OTC to a known SMS number to complete the authentication challenge. This option ensures that the whole authentication process can be completed out-of-band for maximum protection from phishing, key-logging and man-in-the-middle attacks.

Technical Specs

Swivel's currently supported protocols and some providers are listed below. New SMS providers can be supported very quickly, normally at zero or nominal cost. Support for SMS overwrite is dependent on the SMS provider and network operator

Protocol	Provider
HTTP(s)	AQL, iTAGG, Clickatell, MACROKIOSK and many others,
SMTP Gateway	Various, including NHSMail
SMPP	SMPP Version 4. AQL, Vodafone, mobileStorm
GSM Modem	Serial AT Compatible (FASTRACK XTEND FXT003). USB and Ethernet modems also supported but require additional drivers