



simplicity

security

freedom

connection and protection on the move

Business is going mobile. Today's agile organisations need to give their key people access to all their information and communication services, at any time, anywhere they happen to be. With voice, data, video and a world of additional resources converging onto unified networks, companies with true mobility are gaining sustainable competitive advantage.

How it was then

Mobility creates the need for strong security. In particular, user authentication processes - such as passwords - are often the weakest links in many secure access systems. Mobile access can create a trail of vulnerabilities, at worst opening the door to core systems. Traditional token-based solutions often are associated with hidden and rising costs resulting from the need to provide users with a device. In addition to the costs, the requirement to provision tokens can create a wasteful distraction for administrators and the solutions are often frustratingly complicated for users.

How it is now

Swivel is setting a new benchmark for authentication solutions, utilising technology based on 22 global granted patents.

Swivel offers a choice of tokenless multi-factor secure authentication solutions. It gives organisations of every size the control and freedom to focus on their core activities and future growth, rather than daily security concerns.

Secure, simple, multi-factor authentication made easy by the experts at Swivel - with complete freedom from tokens

- Freedom from ineffective complicated solutions and upgrades
- Freedom from the management of ID cards and tokens
- Freedom from hidden charges, such as re-licensing fees, or the cost of an actual security breach
- Freedom for users from the hassle of a token, and from complicated interfaces

Swivel's PINsafe solutions are reliable and resilient, delivering cost-effective authentication that is simple to deploy and to use.

The unique Swivel system combines the use of a registered PIN and a randomly generated security string. A one-time code (OTC) is extracted from the security string delivered to the user simply by "reading off" the digits that correspond to the position in the string of the numbers in the registered PIN.

For example if the PIN is 2-4-6-8 and the security string is 5173920648 the OTC would be the 2nd, 4th, 6th and 8th digits: 1-3-2-6.



Simple and Effective

- The user only ever needs to remember a simple 4 digit PIN
- The PIN number is never entered, reducing the risk of exposure
- The OTC changes with each authentication

Flexible

Swivel provides a full range of user interface options as standard, adaptable to the needs of each business for multi-channel and multi-factor solutions. The license is perpetual, eliminating the cost of re-licensing fees, and licences can be added and assigned to each user in line with corporate policies, and as access requirements change.

PINsafe solutions are easy to integrate into any environment. They can be deployed as software only, or as appliances that are fully compatible with Windows and Linux-based operating systems.

PINsafe - a total solution

The Swivel PINsafe solution provides VPN authentication for remote access to corporate or website applications, using mobile devices and web browsers. PINsafe is designed to combat threats ranging from skimming, phishing and spyware, to shoulder surfing, key logging, and social engineering. Its unique combination of registered PINs and randomly generated security strings delivered simply to the user makes it the safest, easiest, and most reliable and cost-effective authentication solution available.

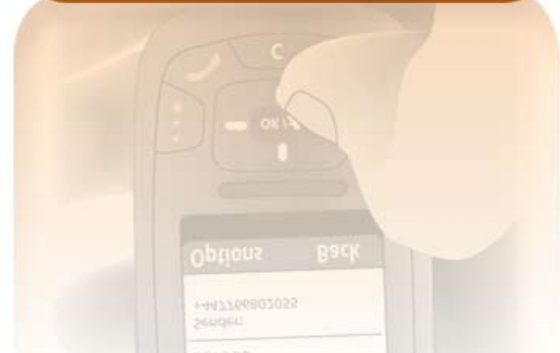
PINsafe has a full range of user interface options included in the license. They can be assigned to each user individually in line with corporate security policies and access authorisation requirements. With no tokens to manage, PINsafe allows for instant provisioning to end users. By removing the cost of individual tokens, and the cost and complications of administration, the overall budget requirements for implementing and maintaining the solution are significantly lowered as well, as are the costs of time and labour required to manage more demanding alternatives.

With flexibility built into its architecture for easy implementation, PINsafe is designed to accommodate the unique requirements of each individual organisation

- Users can be added and removed by managing the existing user repository; provisioning becomes part of the existing account creation process
- Proprietary PIN composition and PIN change policies can be set
- Self-care options include PIN change and PIN reset
- Logging features can be extended; logs can be routed to standard syslog server
- PINsafe scales easily. A single appliance, depending on configuration, can perform 50-100 authentications per

second, enough for most installations of up to 200,000 users. Multiple PINsafe appliances can be deployed within a single installation.

- One PINsafe server can work with multiple Active Directories, allowing the implementation of the solution across world wide geographical territories



mobile - solutions

Swivel PINsafe's SMS and Java solutions provide dual channel authentication, by allowing mobile devices to be used for the delivery of security strings. PINsafe sends the code to the mobile, both on demand or pre-sent, providing back-up should the user have no access to their mobile service.

SMS

The user receives their randomly generated security string by SMS. They then extract their OTC using their personal PIN, via a web browser or network interface. The two key elements of the authentication process are never transmitted on the same network.

Java

A simple Java application can be downloaded via GPRS onto compatible mobile devices. Up to 99 security strings can be downloaded and stored for extended periods of time outside a GPRS network, ensuring connectivity. With Swivlet, the generation of the OTC can also be automated, with the user entering their PIN via the keypad of the mobile device.

Mobile Swivel - the key benefits

- Utilises business tools that are already in use - mobile phones
- Fast to deploy
- Reduces management costs
- Nothing to buy
- Nothing to distribute or reclaim
- If people lose or break their phones, they address the problem immediately



web-based - solutions

PINsafe's single channel web-based solution is ideal for protecting Web pages, OWA or SSL VPNS. It is simple to integrate with SSL VPN technologies, and is an effective alternative to vulnerable username and password authentication. PINsafe uses TURING or PATtern to secure access, with no ongoing cost for authentication. The PIN is never entered, so it is immune to keyboard loggers.

TURING

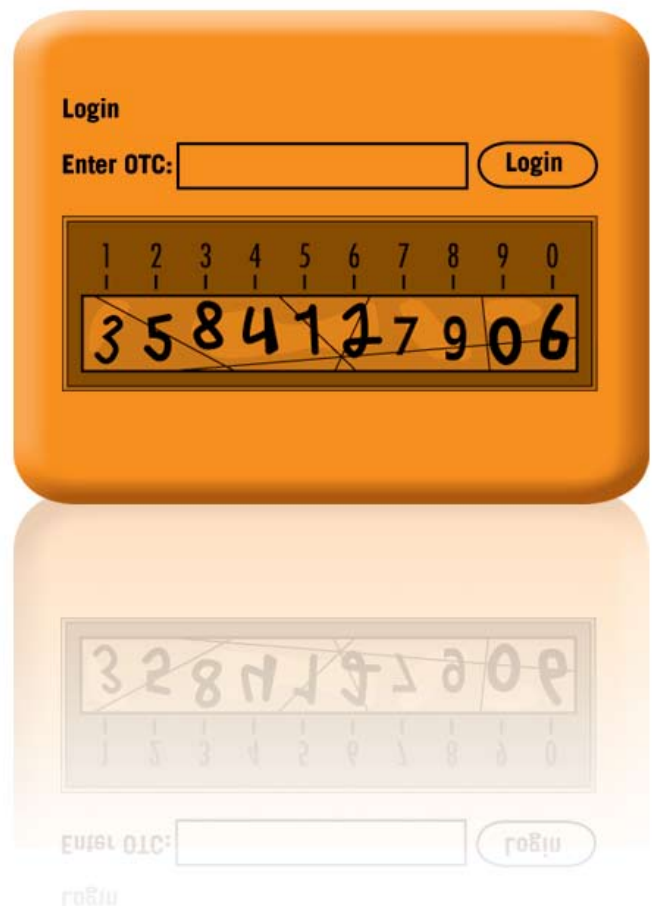
With this technique an obfuscated image is used to display the security string. It is served as a web page once the login session has been initiated. The randomly selected irregular fonts and patterned backgrounds ensure each new image appears differently, minimising detection.

Randomly generated GIF sent via HTTPS

This is a mix of numbers and letters, which may be case sensitive or insensitive, and may employ an irregular font and patterned background. It is immune from OCR software.

PATtern

As an alternative to a numeric based PIN, PATtern allows users to base their PIN on the position of the digits. Security is strengthened by using a location to pinpoint the OTC, with the security string extending to numbers, upper and lower case letters, or a combination.



PositiveID, a third party tool, can be integrated with PINsafe to add another factor of authentication to the single channel solutions. PositiveID creates a unique digital fingerprint for a device such as a PC, laptop or PDA, using up to 15 different elements to create a dedicated profile for each user. Users can be restricted to specific devices, or several devices can be registered to a single user.

integration



PINsafe has an in-built Radius server that allows integration with a range of remote access products including:

Array Networks
Aventail
Bluecoat
Checkpoint
Cisco
Cisco ASA
Citrix
Co-Sign
Cyber Ark
F5
Fortinet
Juniper
Microsoft IAG
Microsoft IIS
Microsoft ISA Sever
Microsoft Outlook Web Access
Nortel
Netilla
Other Radius technologies

PINsafe integrates with existing LDAP based repositories such as Windows Active Directory, allowing membership to be managed as part of an enterprise user management process. Remote access can be specifically configured to allow VPN access for home and remote corporate users, both trusted and un-trusted. Access can also be allowed for selected third parties, using either their own internal databases to store user data, or an existing database infrastructure.

Use of PINsafe - OWA

IIS OWA runs on IIS server

PINsafe can provide authentication for access to IIS

ISA 2004 or 2006 ISA can allow access to OWA

PINsafe can provide authentication in a single page

Other Portal (IAG, Juniper, Aventail, Citrix, etc)

PINsafe can allow access to OWA through SSL

VPN authentication

Deployment

Compatible with Windows and Linux based operating systems PINsafe can be deployed as:

Software Only

Simple standalone appliance

HA Active/Active option on appliance

HA Active/Active option available with additional DR appliances

HA Active/Passive option on appliance

Software Only or VM solution

Depending on the requirement additional site-resilience and disaster recovery can be built into the solution.

Established in 2000 and a member of the worldwide Marr Group of companies, Swivel is pioneering network security solutions. Based on patented technology, Swivel's multi factor authentication solution, PINsafe, is successfully providing peace of mind to organisations of all shapes and sizes.

Our distributors and resellers support a global reach; current clients include leading financial, retail, engineering and legal companies as well as government and health organisations.

Head Office

Swivel Secure Limited
Equinox 1, Audby Lane
Wetherby LS22 7RD UK

Tel: +44 (0) 1937 582020
sales@swivelsecure.com
www.swivelsecure.com



SWIVEL®
Authentication Solutions