Industry Standard 2 Factor Authentication...without the plastic

A simple and feature rich tokenless OATH token

PIN pass

PINpass provides a simple to use and cost effective 2 factor authentication solution for organisations looking for a standards-based approach to logon security.

Strong logon security is as critical as ever for any business given today's threats, and IT security budgets are being stretched more than ever making defences harder to maintain. What if you could cut costs, reuse existing investments and more widely utilise strong logon security all at the same time? With PINpass you can!

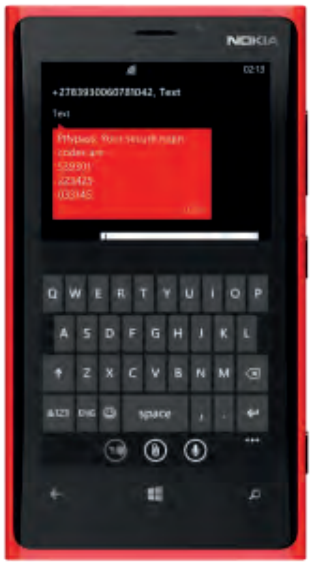
How it works

PINpass uses two unique and separate factors: The 'something you have' is in the form of a standards compliant (RFC 4226 & 6238) random One Time Pin (OTP) sent to the user's mobile device via SMS or email. The 'something you know' can either be a user selected static PIN number, or an existing Active Directory password which saves the user from having to remember yet another code.

The Authlogics server generates 6 to 8 digit OTP's which are delivered to users in Real-Time or Pre-Send configurations. Real-Time OTP's are sent one at a time, and only when the user needs to logon. Pre-Send OTP's are sent initially when the user is first enabled for PINpass, and subsequently after the last Pre-Send OTP has been used.

Pre-Send OTP tokens

Pre-Send OTP's help to overcome the limitations of inadequate mobile coverage or data connectivity for SMS or email delivery. Administrators can configure up to 10 Pre-Send tokens to be delivered in a single message to reduce delivery costs, and to ensure that the user has enough tokens on hand before requiring connectivity again. Administrators can also configure the life span of the Pre-Send OTPs on a per-user basis to strike the right balance between corporate security and a user's ability to logon.



Features and highlights

- NO hardware tokens!
- Securely logon on to Windows Desktops while in or out of the office
- Highly competitive pricing - especially compared to hardware solutions
- Emergency Override Access
- Secure access to internal & Cloud-based applications
- OATH, HOTP & TOTP (RFC 4226, 6238) compliant
- Real-Time or Pre-Send token delivery via SMS or email
- SMS flash and message overwrite functionality
- Active Directory or LDAP database storage (no schema extensions)
- RADIUS & Web Services interface for universal integration
- Rapid user provisioning (thousands in an hour)
- Web-based Operator portal for IT Helpdesk day-to-day operations
- Self service password reset
- Leverage existing Active Directory password or use a static PIN
- FIPS 198 & 180-3 compliant

Authlogics

Industry Standard 2 Factor Authentication ...without the plastic

Turn any mobile device into an OATH token

PINpass delivers industry standard OATH technology in a highly cost effective package by doing away with plastic key fobs and the hidden logistics costs - which can be greater than the initial purchase price.

Smart PIN placement - beyond just OATH

To simplify deployment, and to reduce the costs associated with user training, administrators can allow users to use their Active Directory password instead of a PIN. However for increased security the Password or PIN can be entered before or after the OTP. Furthermore the PIN can even be entered in the middle of the OTP, making it more difficult to differentiate between the OTP and the user's PIN by potential hackers.

Counting the cost

Batch sending one time codes greatly reduces the number of SMS messages sent, which can cut ongoing SMS delivery costs up to 90%. Furthermore, leveraging existing AD infrastructure and mobile devices requires no additional management overhead.

By utilising a Blackberry or ActiveSync infrastructure to deliver OTP's, the cost of delivery is reduced to zero while the security of sending an OTP is maintained, even over email. PINpass allows for Bring Your Own Device (BYOD) initiatives with minimal effort and without compromising security.

Deployment

PINpass is deployed as a component of the Authlogics product suite. Authlogics is built on 64bit .NET technology and can be deployed on a Windows 2008 x64 server in under 5 minutes. It has been designed to use an existing Active Directory as an accounts database without extending the schema, so there are no extra databases to backup and manage, and it is automatically highly available. A standalone LDAP directory is also available.

Authlogics includes a full RADIUS server for authentication and accounting to easily integrate with any 3rd party system. RADIUS proxy is also supported for coexistence or migration scenarios and RADIUS extensions can provide extra information about users to the authenticating device. If RADIUS isn't enough, an XML Web Services interface is also available for seamless integration into any application. SMS based OTPs are delivered via a choice of built in international SMS gateways (with sign-up assistance) while email based OTPs are sent via SMTP with optional Auth and TLS encryption.

Emergency Access

Freak weather conditions, terror alerts or a simple office move can mean that users are not able to get on with their day job. While rare, they can significantly impact business productivity. PINpass is here to help with the ability to use an emergency access licence key which allows for a much larger set of users to use PINpass than normal, but only for a short period of time. In addition, individual users can have their token overridden with a static code or password for a limited time or number of uses in an emergency situation.

"Thousands of users can be deployed in under 1 hour which is very reassuring for emergency situations."

The power of Authlogics

PINpass is one of the core components of the Authlogics product suite, an enterprise ready multi-factor authentication and management platform designed to easily fit into existing Active Directory environments, or as a standalone solution.

Authlogics has been designed to integrate with many systems from remote access solutions to application specific requirements via standard interfaces such as RADIUS and Web Services. It is quick to deploy, easy to maintain and manage with tools such as web based user self-service and helpdesk operation portals. Authlogics also includes Windows Desktop Logon functionality to allow for online and offline access to Windows PCs.

Harlow Enterprise Hub
Edinburgh Way, Harlow, Essex
CM20 2NQ United Kingdom
Email: intouch@digitalpathways.co.uk
Tel: +44 (0)844 586 0040

Digital Pathways