

MPASS™

Multi-factor authentication
for effective protection from
cybersecurity breaches



**INNOVATIVE
SOLUTIONS**

mPass Stay Fraud Free!

Enhanced security against fraud with multi factor authentication via SMS to authorize or access to sensitive corporate data. mPass Factor with SMS can provide guarantees against the risk of attack from malicious software or phishing attacks. **mPass** is a multi factor authentication system based on something you know and something you have.





Secure Your Network and Stay Fraud Free!

mPass enhances the level of trust between the end users and enterprise applications by enabling Strong authentication between the entities

Today, enterprises are embracing cloud and ever increasing mobility to empower user access to corporate data anytime, anywhere. With ever changing landscape of security threats pertaining to web, mobility and cloud offerings, enterprises understand the threats and therefore demand stronger security to ensure protection of their corporate data

Traditional user login method of simple username and password is not secure enough anymore and pose high risk to corporate data. Multi factor authentication reduces such risk by introducing the dynamic password generated using industry standard OATH (Open Authentication) event-based or time based algorithms



Password and User ID cannot protect you from being hacked!

Traditionally every application uses a "single factor user authentication" by username and a password. But there is a high security risk involved in this approach because system cannot identify if it's a real user or an attacker. A simple scenario is where an attacker can just guess or use advanced random password tools to compromise your password there by gaining instant access to your online account and information.

Stronger authentication uses more than one factor; not only do you have to know something like your password, but you have to have something like your smartphone or any unique thing like your fingerprint. mPass is the answer for this problem, it delivers the one time password on user's mobile device through SMS or can be generated on a user's mobile application (Soft Token). This process ensures the credibility of the user's identity and minimize the risk of being fraud or hacked.

mPass for Multiple Applications



mPass allows you to create OATH-compliant strong authentication with multiple delivery channels to users on their mobile handsets.



mPass is easy to integrate with various applications within enterprise from remote VPN access to mail servers and web portals and cloud based applications



mPass can be smoothly integrated with leading technology providers such as Juniper, Cisco, Citrix, PaloAlto Networks, F5, Oracle and Microsoft



Event-based Tokens



Integration APIs



VPN / SSL VPN



Time-based Tokens



RADIUS



Citrix Access Gateway



SMS OTP



SOAP / XML



Microsoft OWA



LDAP Integration



Enterprise Web Applications



UNIX / Linux

mPass is Suitable for all industries

mPass is suitable for all kinds of industries to reduce the odds of exploitation. If user password is stolen or intercepted, it alone will not be enough to take over their account. Below are the few examples from some sample industries where mPass can create a fraud free business for you and for your online users



Security in Government Portals

- Private networks and their security
- E-Government public services where public identity verifications are involved



Banks and Financial Sector's Security Verifications

- OTP (One time password) for accessing online portal and secure dashboards
- Fraud financial transaction



Any public or private organizations

- mPass can be used by any organization regardless of their industry type
- Ensuring fraud free cyber environment is the responsibility of each organization which can secure your business and its future

mPass for Multiple Applications



Web based Configuration

The configuration system is available as a web based user dashboard



Auto Account Status

Automatic enabling and disabling of user accounts



User Portal

Secure User Portal for self management of tokens



Standards and Compliant

OATH compliant OTP Generation (HOTP, TOTP)



SMS Token on Mobile

With the integration of any SMS gateway a secure SMS OTP token can be delivered on the phone based on OAuth



Administrator in Control

Administrator defined time release and length of session



Soft Token on Mobile

For soft token mPass Mobile App is available in following platforms (Android, Windows and IOS platforms)



Secure Dashboard

SSL enabled user application dashboard available for any gateway configuration



Zero-Footprint

Nothing required by the client side to install on SMS Token



Standard Reports

Audit user login reports and sessions



Always update

Delivers robust support to current and evolving authentication needs



API and Integration flexibility

mPass can be integrated with any application through SOAP APIs

mPass Use Cases



Enabling Strong authentication for leading VPN's and Firewall solutions



Strong authentication for Windows Logon



Enabling Strong authentication for In house developed Applications



Re-Set Password Applications



OWA Strong authentication




ERP portals

MPASS™



Your
Business.
Secured!


Head Office

 P. O. Box 69328, Al-Uruba Road
Al-Wurud, Podium Building, 2nd Floor
Riyadh 11547, Saudi Arabia

 +966 11 2931501

 info@is.com.sa


Dubai, UAE

 P. O. Box 414067, Office No. 606
6th floor, Building 12, Bay Square,
Business Bay, Dubai

 +971 4 221 7197

 dubai@is.com.sa

Abu Dhabi, UAE

 P.O. Box 32672, 1st Zayed Road
Abu Dhabi Island, Abu Dhabi,
United Arab Emirates

 +971 2 634 0128

 dubai@is.com.sa

Branches

Jeddah | Al Khobar

 @InnovativeSolutionsSA

 @IS_Arabia

 @Innovative Solutions SA

 @IS_Arabia

www.is.com.sa