SMS PASSCODE® is the leading technology in adaptive multi-factor authentication, improving enterprise security and productivity through an easy to use and intelligent solution that ensures the safety of corporate networks and applications. SMS PASSCODE provides a superior user experience by taking full advantage of contextual information such as login behavior patterns and geo-location to assess the threat level and automatically adjust the level of user authentication needed.
WHY MULTI-FACTOR AUTHENTICATION?

A username and password are no longer enough to authenticate your users. Each day brings new stories of stolen identities and brands of all sizes falling victim to hackers. Weak or stolen user credentials are the preferred weapons used by hackers, and are behind approximately 76 percent of all network intrusions.

The threat is real, and it is growing fast. Stay safe with SMS PASSCODE.

WHY SMS PASSCODE?

Introducing an extra layer of user authentication into your environment is not always easy. Common challenges include:

1. How do you ensure user adoption and compliance?
2. How do you ensure hassle-free maintenance of the solution on a daily basis?
3. How do you add the strongest possible protection without breaking your IT budget?

SMS PASSCODE can help. With a track record of thousands of client installations around the world, we know what it takes to protect your remote access in a secure, flexible, and convenient way, no matter whether your users are logging in from London, New York, Berlin or Bangalore.

EVOLUTION OF AUTHENTICATION TECHNOLOGY

<table>
<thead>
<tr>
<th>80-90's</th>
<th>00's</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware Tokens</strong></td>
<td><strong>Mobile Based Solutions</strong></td>
<td><strong>Adaptive User Authentication</strong></td>
</tr>
<tr>
<td>+ Introduction of two-factor auth.</td>
<td>+ Real-time multi-factor auth.</td>
<td>+ Contextual intelligence layer</td>
</tr>
<tr>
<td>+ High cost on tokens</td>
<td>+ No hardware distribution</td>
<td>+ Policy-based trusted IPs</td>
</tr>
<tr>
<td>+ Distribution &amp; administration cost</td>
<td>+ Deployment of soft tokens / apps</td>
<td>+ Multiple OTP options</td>
</tr>
<tr>
<td>+ An extra thing to carry</td>
<td>+ Regional SMS delivery challenges</td>
<td>+ Location aware dispatching</td>
</tr>
</tbody>
</table>

ADAPTIVE USER AUTHENTICATION

SMS PASSCODE leverages the one thing users always carry with them – their mobile phone. The solution takes full advantage of contextual information such as login behavior patterns, geo-location, and type of login system being accessed. This provides some powerful benefits for your organization:

Maximize convenience for your users

For even greater user convenience SMS PASSCODE can be configured to dynamically change the level of security based on e.g where the users are located when logging in, what time they are logging in, and what network they are logging in from. For example, if the user is logging in from a trusted location such as the comforts of their home (where they have logged in from before), then they will not be prompted for an OTP (One-Time-Passcode) in order to authenticate. Whereas if they are attempting to log in while travelling i.e. from an airport lounge or hotel with public Wi-Fi then an OTP is mandatory to gain access.
Benefit from the market leading technology
All passcodes are generated in real-time and are locked to the session-ID of each particular login attempt for maximum security. No passcodes are stored on the user’s mobile phone. Advanced attacks such as real-time phishing or man-in-the-middle attacks are detected and the user is notified in the OTP message they receive.

Embrace flexibility as circumstances change
Circumstances change and you need a platform that you can rely on as your business requirements evolve. Through SMS PASSCODE’s advanced policy- and load balancing engine you have maximum flexibility to easily tailor the solution to your security needs while maintaining convenience for the users. This unique engine enables a secure, flexible, and convenient user authentication process that you can depend on anywhere and anytime.

IDENTIFY THREATS AND HACKING ORIGINS
SMS PASSCODE provides reporting and analytics capabilities so you can easily interpret login data to identify threats and monitor the overall setup performance. You can:

- Spot trends in login attempts and potential hacker attacks
- Understand which systems are being used remotely and from where
- Monitor failover services
- Identify high-risk locations

ENABLE SELF-ENROLLMENT OF ACTIVE SYNC DEVICES AND REDUCE BYOD COMPLEXITY
Managing the growing number of mobile devices accessing corporate data can be a challenging burden to your IT department. With SMS PASSCODE, users can onboard new devices easily and without contacting IT.

Secure Device Provisioning allows users to easily enroll new ActiveSync devices themselves without compromising security. Once a user activates ActiveSync on a device he/she will receive a quarantine email with a link to a Self-Service website where the user can approve the new device with a single click after being authenticated. You can also have the new device auto-approved if it is connected to a trusted network like the internal Wi-Fi within your organization, or your home IP.

Secure Device Provisioning is convenient for the users as they get easy access to data on their new device when and where they need it, and without having to contact IT to approve their new device. This frees the burden on IT departments and reduces complexity around supporting a mobile workforce with a growing amount of devices in a secure way.
PLATFORM OVERVIEW

EASY INSTALLATION AND DEPLOYMENT
Connect SMS Gateway modem(s), run plug-and-play installation of the SMS PASSCODE software, and the system is ready for use. No user deployed software is needed. SMS PASSCODE allows for one-click integration to Active Directory (AD) without schema changes or extensions.

HARDENED SECURITY KEEPS YOUR DATA SAFE
Our passcodes are cryptographically strong random generated OTPs using FIPS-140 validated crypto modules and all communication between components is AES 256bit encrypted. In addition SMS PASSCODE makes use of advanced brute force and denial-of-service attack detection and protection.

UNPARALLELED RELIABILITY
SMS PASSCODE’s mobile centered platform offers maximum flexibility and reliability through a number of realtime OTP delivery methods and a sophisticated automatic fail-over mechanism. In the unlikely event that the SMS does not arrive (e.g. in a country with under-developed GSM infrastructure) the user will automatically receive a new passcode via voice-call or secure e-mail.

In addition, SMS PASSCODE supports a broader range of OTP options, including traditional tokens and soft tokens from Microsoft or Google Authenticator. Secure e-mail using BlackBerry or ActiveSync provisioned mobile devices are other valid fail-over alternatives (if Outlook Web Access is secured). The SMS Gateway beats any SMS Service providers on reliability in every test case and is therefore still standard – but a combination is sometimes the answer in a global scale setup for a more cost effective solution.

PASSWORD RESET MODULE
Zero-deployment paired with the intelligent integration to login systems has made the SMS PASSCODE Password Reset Module unique and highly popular among enterprises throughout the world.

The solution detects if a user attempts to log in remotely using an expired or incorrect password and instantly notifies the user via SMS if a lock out occurs. The notification message includes a link to the password reset self-service website. From there the user can update the Active Directory password without having to contact the helpdesk.

The Password Reset Module is sold separately.
ADAPTIVE MULTI-FACTOR AUTHENTICATION

SMS PASSCODE delivers industry-leading value in four key areas:

Makes Security Hassle-Free and Painless for the User:
SMS PASSCODE improves security without sacrificing productivity. The offering is intuitive and so convenient that end users will happily maintain compliance. Using contextual information to assess the threat level, it automatically adjusts the level of authentication needed. Implemented worldwide, it works with all types of devices.

Easy for IT to Implement, Manage and Scale:
SMS PASSCODE is easy to install, deploy and administer. SMS PASSCODE offers flexible policy-driven administration, and protects multiple platforms on a global scale. SMS PASSCODE seamlessly integrates with both remote access systems and cloud applications.

Prevents Security Breaches with Contextual Intelligence:
SMS PASSCODE is realtime and session-specific, incorporating behavior such as login patterns and geo-location information to validate the user, thereby protecting against identity theft and modern Internet threats.

Reduces costs and improves ROI:
With a lower TCO (typically 50 percent lower TCO compared to traditional solutions) SMS PASSCODE offers an affordable multi-factor authentication solution that is highly secure, easy to deploy, manage and use. This keeps the TCO to a minimum, enhancing the ROI for customers while boosting organizational productivity gains.

“SMS PASSCODE is a great hassle-free product and does exactly what we need it to.”
John Owen, IT Manager, Day Group
SOLUTION HIGHLIGHTS

**Seamless Integration:** The SMS PASSCODE platform integrates seamlessly to login systems, for an intuitive and user-friendly remote access login experience.

**Adaptive Authentication:** Balance high security and strong user compliance with a solution that automatically adapts the level of authentication needed based on the threat level.

**Status Feedback:** SMS PASSCODE provides unrivaled status feedback enabling the user to follow the login progress. Status feedback inspires user confidence and reduces the number of helpdesk calls.

**Flash SMS:** By default, passcodes are sent as Flash SMS, which automatically pop up on the user’s mobile phone without any user action, and the Flash SMS is not stored on the cell phone. Regular SMS is supported as an option.

**Location and Behavior Aware:** SMS PASSCODE takes full advantage of contextual information such as login behavior patterns and geo-location information to effectively grant or deny user access.

**Secure Device Provisioning:** Secure device provisioning allows users to easily enroll new ActiveSync devices by themselves without compromising security.

**Password Reset Module:** The password reset module offers integrated Active Directory password reset via an easy to use 24/7 self-service site, secured by SMS PASSCODE Multi-Factor Authentication. No deployment needed.

**MemoPasscodes™** Makes innovative use of letter combinations to provide users with easy-to-read passcodes, that support the intuitive login process of SMS PASSCODE.

**Range of OTP Delivery Methods:** With SMS, voice-call, cloud keys, secure e-mail, or hard- / soft tokens as delivery methods SMS PASSCODE can support your business requirements now, and in the future.
SUPPORT FOR LEADING REMOTE ACCESS SYSTEMS

SMS PASSCODE supports a broad set of login systems used for remote access. The platform is designed to integrate seamlessly into any of the third party systems listed below, to ensure a secure login process that is intuitive to the end-user.

The following systems are supported:

**RADIUS VPN/SSL VPN Clients:**
- Check Point
- Cisco ASA
- Netscaler Gateway & Citrix Access Gateway (CAG)
- Juniper
- Microsoft Forefront (UAG)/Direct Access
- Barracuda SSL VPN and NG firewalls
- VMware Horizon View
- Microsoft SharePoint Portal Server
- Any other RADIUS client supporting challenge/response

**Internet Information Services (IIS) Web Sites:**
Support for the following types of web sites:
- Web Sites using Basic / Integrated Windows Authentication
- Web Sites using Custom / SAML based Authentication

**Microsoft ISA/TMG Server & Web Sites:**
Support for Microsoft ISA/TMG published web sites:
- Terminal Service / Remote Desktop Service (Windows Server 2008 / 2012)
- Microsoft SharePoint Portal Server
- IIS Web Sites using Basic or Integrated Windows Authentication
- Any Web Site not requiring Authentication Delegation

**Windows Logon, Remote Desktop/Terminal Services:**
Support for the following Servers and Services:
- Remote Desktop / Terminal Services (RDP Connections)
- Windows Servers 2003 / 2008 / 2008R2 / 2012 / 2012R2
- Windows XP, Vista, Windows 7 (incl. Single-Sign-On), Windows 8 and Windows 8.1
- VMware Virtual Desktop Portal & Client Access

**Citrix Web Interface**

**Microsoft Active Directory Federated Services 2.x proxy plug-in for multi-factor authentication**

**Transparent support Cloud Applications such as Salesforce.com, Microsoft Office 365, Google Apps etc.**

---

(1) Protection of SharePoint Portal Server using RADIUS is only supported, if the SharePoint Portal server is published through an Application Gateway, which will ensure that the user is only required to authenticate once during the initial logon. E.g. using the Microsoft IAG/UAG, Citrix Access Gateway configured to make use of persistent cookies. (2) Configuration required.

www.smspasscode.com