

Level up security

SMS PASSCODE Version 2018
Modern adaptive user authentication





”Users see Security as desert-walks, so we needed the right partner.”

JØRGEN DINESEN

IT DIRECTOR, COPENHAGEN ZOO



SMS PASSCODE Multi-Factor Authentication (MFA) **combines strong security and ease of use.** Version 2018 introduces Hybrid MFA – On Prem with Cloud Services.

A username and password are no longer adequate to verify the identity of your users. The traditional hard and soft-token solutions no longer provide sufficient protection against modern threats. In addition, they are expensive to manage - both from a roll out and maintenance perspective, and they are a challenge to the users.

With SMS PASSCODE MFA 2018, the solution can now be delivered both as pure On-Prem (the traditional) and now also as Hybrid, which is On-Prem combined with SMS PASSCODE's Cloud Service for sending one-time passcodes by APP, SMS, E-mail or telephone calls. This means that, unlike at present, you do not need modems or your own SMS service providers.

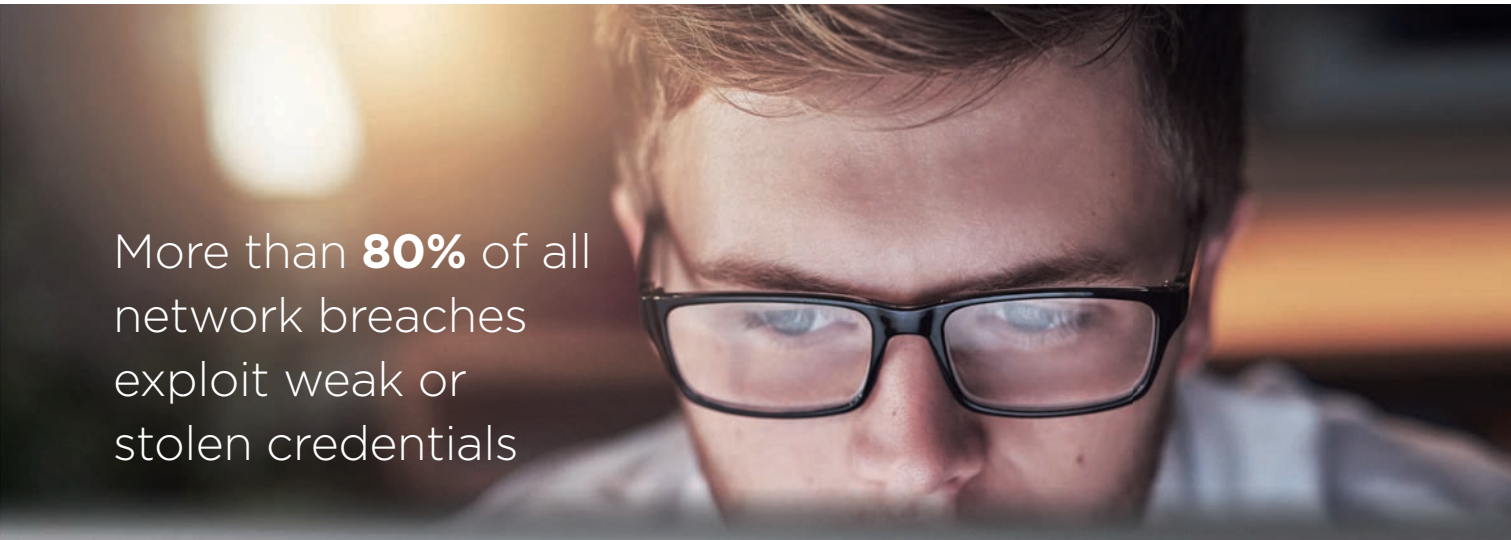
With SMS PASSCODE MFA 2018, we are also introducing our new Secure Device Provisioning, which allows protection of Office365-associated ActiveSync devices, without having to establish an MDM solution, that is usually costly and difficult to roll out to the many private mobile phones and tablets, which often have ActiveSync e-mail and calendar today.

With GDPR, the interest in data protection of Webmail/ Office365 with MFA has received a boost, and only SMS PASSCODE MFA can cover ActiveSync as part of this security, without having to implement an MDM project.

SMS PASSCODE is pioneering a new generation of more intelligent and user-optimized authentication that allows you to increase remote access security without compromising user-friendliness. With a track record of thousands of client installations worldwide, we know what it takes to protect your systems and cloud applications, whether your users are logging in from Aarhus, New York, Berlin or Bangalore.

SMS PASSCODE MFA authenticates users by looking at their login history and requesting a one-time passcode when necessary. In that case, a session-specific OTP (One-Time-Passcode) is sent in real time to the user's mobile phone as an App notification, SMS, e-mail, or phone call.

SMS PASSCODE MFA delivers industry-leading value in four key areas: Security, convenience, easy of administration and returns.



More than **80%** of all network breaches exploit weak or stolen credentials

Prevent security breaches with contextual intelligence

SMS PASSCODE MFA works in real time and uses session-specific OTPs and multiple factors to validate users. The solution thereby protects against identity theft and modern threats, such as Ransomware and APT.

Cyber threats have escalated dramatically and hackers have tools at their disposal that are more advanced than ever before. Underestimating these threats can have a devastating impact on your organisation.

Weak or stolen user credentials is the preferred weapon used by hackers, and is exploited in more than 60% of all network breaches. The threat is real and it is growing fast. With multi-factor authentication from Entrust Datacard, however, you can effectively disarm the hackers of their preferred weapon.

MORE FACTORS WORKING TO YOUR ADVANTAGE

SMS PASSCODE MFA involves several factors relating to each login. These factors include: geo-location, network IP, the system being accessed, time of login, etc. Together, these factors provide a picture of the context the user is in, helping to determine the validation requirement for each login and whether or not the user should be allowed access.

REAL-TIME AND SESSION-SPECIFIC PASSCODE

For maximum security, all OTPs are generated in real-time and are locked to the session-ID of each particular login attempt. There are no predefined passcodes or seed files that can be hacked and no passcodes are stored on the user's mobile phone.

ADVANCED PROTECTION AGAINST HACKER ATTACKS

Innovative use of contextual information, such as the geo-location, enables SMS PASSCODE MFA to detect and alert a user if an advanced attack, like real-time phishing, is taking place. The system can be configured e.g. to not allow logins from specific areas and countries, or to notify the user in the OTP message itself.

CRYPTOGRAPHICALLY STRONG OTPS

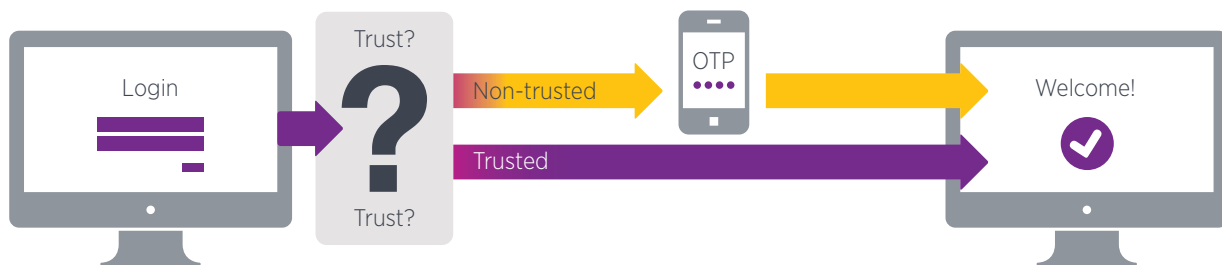
The OTPs are randomly generated via a cryptographically strong, FIPS-140 validated random generator, and all communication between components is 256-bit AES encrypted. In addition, SMS PASSCODE MFA offers advanced brute force and denial-of-service attack detection and protection.

Make security convenient and painless for your users

SMS PASSCODE MFA improves security without compromising the user experience. The solution is so intuitive that the employees will love using it.

By leveraging the one thing that users always carry with them, their mobile phone, the solution provides an unrivalled user experience that incorporates contextual information. The platform can be configured to utilize this information to assess the threat level and dynamically adjust the level of user authentication required.

For example, if a user logs in from a known location, such as from their own home (from which the user has previously logged in), no OTP will be requested for authentication. However, if the user attempts to log in while travelling, for example, from an airport lounge or a hotel's public Wi-Fi, an OTP is mandatory in order to gain access. In addition to the adaptive login process, other components also contribute to the great user experience that SMS PASSCODE MFA is known for:



UNMATCHED RELIABILITY

SMS PASSCODE MFA's advanced OTP delivery platform and automatic failover mechanism ensure that OTPs always reach the users, regardless of where and when they log in.

LOCATION-BASED MESSAGE DISPATCHING

SMS PASSCODE MFA can be configured to automatically select the most suitable OTP delivery method based on the user's login context.

For example, if a user on a business trip in Singapore, the solution can be configured to deliver the OTP through a local service provider, so costs are kept to a minimum. In the event that a user is in an area with poor cellular coverage the solution will deliver the OTP via the SMS PASSCODE app or any of the available secondary delivery methods.

STATUS FEEDBACK

SMS PASSCODE MFA provides status feedback that enables the user to follow the login process as it progresses. Status feedback inspires user confidence and reduces the number of help desk calls.

FLASH SMS

By default, OTPs are sent as Flash SMS, which are automatically displayed on the user's mobile phone. No user action is required. An additional advantage is that Flash SMS is not stored on the mobile phone. Common SMS is supported as an option.

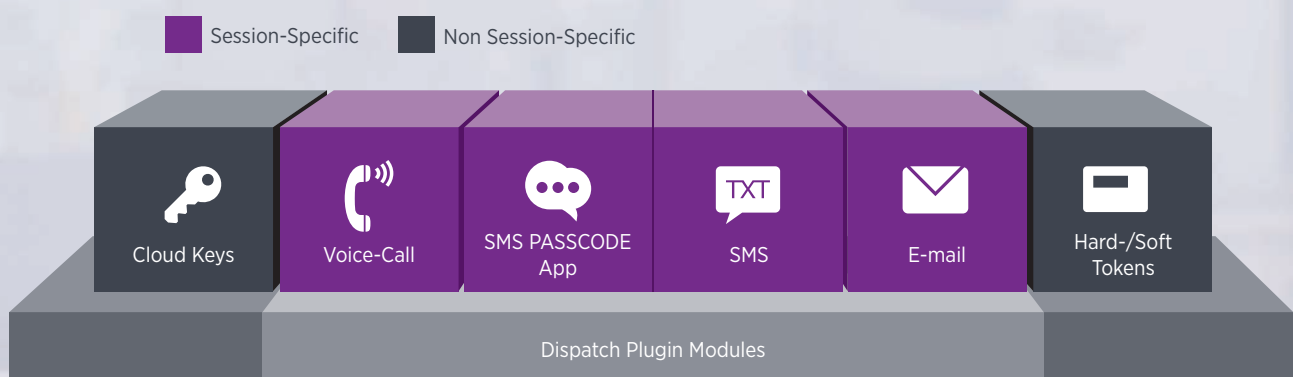
MEMOPASSCODES™

SMS PASSCODE MFA makes innovative use of letter combinations to provide users with easy-to-read, easy-to-remember passcodes that help support the intuitive login process.

Should we share the assignment? Introduction of SMS PASSCODE Hybrid MFA

SMS PASSCODE MFA can be implemented as an "all-behind-the-firewall" version or as Hybrid, where SMS PASSCODE is responsible for operating the App, SMS or phone call service.

The SMS PASSCODE MFA platform allows you to complete the setup and get online in minutes. Run the plug-and-play installation of the MFA software, point to an AD user group and the system is ready to use. The roll-out requires no software installation by the users and no training of the employees is required. SMS PASSCODE MFA comes with 1-click integration to Active Directory and LDAP Directories.



USER MANAGEMENT

Users are synchronized from Active Directory and/or general LDAP Directories like OpenLDAP or AD LDS. Users can be imported by selecting a specific user group, or by use of an LDAP filter. It is even possible to import users from multiple domains, or let users self-enrol. This is particularly helpful in large enterprises and hosting environments.

USER GROUP POLICIES


Every user is assigned to a User Group Policy and automatically inherits the specified permissions. A permission change affects every user in the group. Multiple

User Group Policies can be defined. This means that you can define different permission sets for individual groups of employees, external consultants, etc. The day-to-day maintenance of permissions can conveniently be handled in Active Directory.

SMS PASSCODE MFA HYBRID

With Hybrid, SMS PASSCODE MFA is installed "on-premise", with the benefits this has, while we also assume responsibility for dispatching OTPs via SMS, app and phone call. A support agreement is also contained for the purpose of the cooperation.





Expenses are usually only
50% of other solutions due
to ease of administration

Reduce costs and increase productivity

With an MFA solution that the users accept, multiple systems can be protected and opened to more employees, reducing TCO and boosting ROI.

The introduction of Office365, Salesforce, Workday and other cloud services means that virtually all users will be remote users. By choosing a solution that is cheaper and easier for users to use and understand, all access systems can be protected, for the benefit of everyone who now has access to being productive.

EFFECTIVE BREACH PREVENTION

The implementation and maintenance costs of SMS PASSCODE MFA, relative to the increased security level that it provides, is marginal compared with the tidal wave of costs associated with your systems being compromised.

EMPOWERED WORKFORCE

After implementing SMS PASSCODE MFA, customers typically experience an increase in the use of remote access. This means that more employees access more data and more applications on a regular basis, which is a good indicator for productivity gains. Offering employees the opportunity to work from home, or allowing external consultants access to relevant systems, yields a significant increase in productivity.

REDUCED ADMINISTRATIVE COSTS

Customers moving from another authentication solution to SMS PASSCODE MFA have typically saved about 50%. The Password Reset solution also reduces the help desk costs by allowing users themselves to manage password switching, etc.

UNPROBLEMATIC IMPLEMENTATION

Despite the many advantages of SMS PASSCODE MFA, the installation has only a minimal impact on the existing infrastructure. The system is self-contained, which is a great advantage in terms of ROI because the life-cycle of the installation is almost independent of the supporting systems and processes. An installation can run side-by-side with a token-solution during migration and just a single license covers all your systems.

Solution Highlights



Seamless integration: The SMS PASSCODE MFA platform integrates seamlessly with login systems and cloud solutions for an intuitive and user-friendly remote access experience.



Adaptive Authentication: Balance high security and strong user-friendliness with a solution that automatically adapts the level of authentication based on the user's current circumstances.



Automatic failover: It is possible to establish highly flexible failover mechanisms to ensure that the OTPs always arrive. The solution can even switch between transmissions, depending on the user's current login context.



Broad Directory Support: Users can be synchronized from Active Directory and general LDAP Directories like OpenLDAP or AD LDS. Users can be imported by selecting a specific user group, or by use of an LDAP filter.



Real-Time Protection: All OTP codes are generated in real-time at the point of login. There are no pre-issued passcodes or seed files that could be hacked. At the same time, real-time is a prerequisite for delivering session-specific OTPs.



Session-Specific: For maximum security, all OTPs are locked to the session-ID of each particular login attempt. The system detects advanced attacks and the users are notified in the OTP message they receive.



PowerShell: SMS PASSCODE MFA supports PowerShell. Administrators can use PowerShell scripting to create role-based access, integrate to other systems, or automate daily tasks such as checking license availability or country-specific logins.



Status Feedback: SMS PASSCODE MFA provides unrivalled 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, OTPs are sent as Flash SMS, which are automatically displayed on the user's mobile phone, without any user action. The Flash SMS is not saved on the mobile phone. Common SMS is supported as an option.



Location and Behaviour Aware: SMS PASSCODE MFA takes full advantage of contextual information such as login behaviour patterns and geo-location information to effectively grant or deny user access in an easier and more efficient way. Geo-fencing, allows admins to white- and blacklist based on systems and locations. E.g. limit access through Citrix NetScaler from certain countries.



Secure Device Provisioning: This functionality allows users to quickly and easily enrol new ActiveSync devices by themselves without compromising security and without having to contact the help desk for assistance.



MemoPasscodes™: SMS PASSCODE MFA makes innovative use of letter combinations to provide users with easy-to-read and easy-to-remember passcodes that support the intuitive login process. Passcodes and notifications alike can be customized to your specific needs.



OTP Delivery Methods: With plug-ins and standard OTP delivery methods like apps, SMS, voice-call, secure e-mail, cloud keys, and hard- / soft tokens, SMS PASSCODE MFA can support your business requirements now and in the future.



Advanced database auditing: SMS PASSCODE MFA includes advanced auditing capabilities to help customers comply with strict industry regulations and meet audit control requirements.

Protect your systems and applications

Regardless of whether you want to protect cloud applications, VPN, Webmail, VDI or similar, SMS PASSCODE MFA offers all the integration and scalability that you need.

The solution supports a broad set of login systems for remote access and cloud services. The platform is designed to integrate seamlessly to the most popular third party systems to ensure a secure and intuitive login process for end-users.

For a full list of supported systems, please see the back page.





SMS PASSCODE app

The SMS PASSCODE app is available for iOS and Android smartphones.

As an existing licence-holder, your end-users have free access to the SMS PASSCODE app (except for possible data traffic charges when using the app on a smartphone). Obtaining and installing the app is very simple and straightforward. The SMS PASSCODE app also has the following advantages:

Greater security: Messages are sent encrypted, end-to-end from the SMS PASSCODE MFA installation to the SMS PASSCODE app. All app installations use their own auto-generated encryption key, which means that only the intended recipients of the message can decrypt it.

Supported Systems

SMS PASSCODE MFA 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. This is in order 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
- Juniper
- Direct Access
- Barracuda SSL VPN and NG firewalls
- VMware Horizon View
- Microsoft SharePoint
- Other RADIUS clients (challenge/response)
- Palo Alto
- F5 BIG-IP
- NCP VPN

Microsoft TMG Server & Websites

Support for Microsoft TMG published websites:

- Outlook Web Access 2003 / 2007 / 2010 / 2013
- Remote Desktop Web Access (Windows Server 2008 R2 / 2012 R2 / Windows Server 2016)
- Microsoft SharePoint
- IIS Websites using Basic or Integrated Windows Authentication
- Websites that do not require Authentication Delegation

Windows Logon, Remote Desktop Services

Support for the following Servers and Services:

- Remote Desktop Services (RDP Connections)
- Windows Servers 2008 R2 / 2012 / 2012 R2 / 2016
- Windows 7, Windows 8, Windows 8.1 and Windows 10
- VMware Virtual Desktop Portal & Client Access

Microsoft AD FS Protection

- AD FS 2.0 plug-in for multi-factor authentication
- AD FS 3.0/4.0 adapter for multi-factor authentication

Multi-factor authentication support for:

- Access to cloud applications such as Salesforce.com, Microsoft Office 365, Google Apps, etc. (AD FS 2.0/3.0/4.0)
- Access to websites published through Microsoft Web Application Proxy (AD FS 3.0/4.0), such as Outlook Web Access
- Approval of devices in connection with workplace joins (AD FS 3.0/4.0)

Internet Information Services (IIS) Websites

Support for the following types of websites:

- Outlook Web Access 2010 / 2013 / 2016
- Remote Desktop Web Access (Windows Server 2008 R2 / 2012 R2 / 2016)
- Websites using Basic or Integrated Windows Authentication

Secure Device Provisioning

Protection for ActiveSync devices on the following systems:

- Exchange 2010
- Exchange 2013
- Exchange 2016
- Exchange Online

(1) Protection of SharePoint 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 login. For example, using the Citrix Netscaler configured to make use of persistent cookies.

Entrust Datacard A/S

Park Allé 350 D, DK-2605 Brøndby

Phone: +45 70 22 55 33

www.entrustdatacard.com

