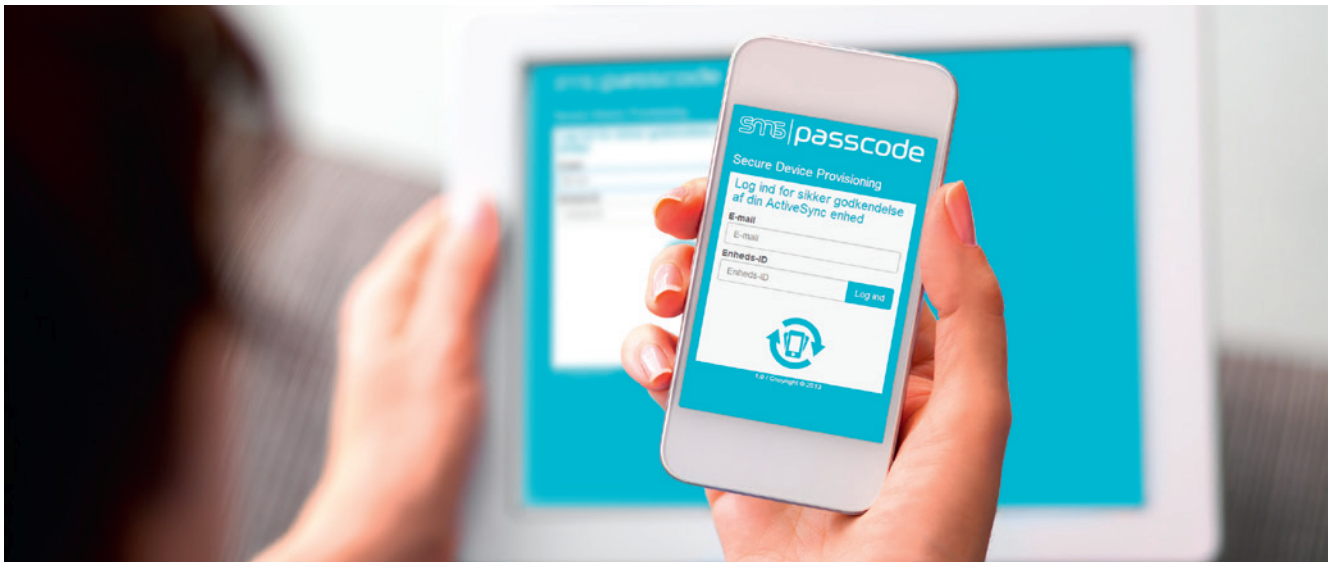
Whitepaper

sms|passcode

MULTI-FACTOR AUTHENTICATION AND BYOE:

3 BEST PRACTICES YOU NEED TO KNOW



When today's hacker and identity theft threats combine with the new challenges presented by the trend of 'bring your own device' (BYOD), companies must take decisive action to deliver secure, flexible and convenient authentication to employees and their devices alike.

Many security and IT administrators have spent sleepless nights trying to address well-known and widespread security issues surrounding data synchronization on unsecured devices accessing the corporate network. The 'holy grail' is an authentication solution that a) effectively blocks hacker threats, b) are easy for everyone to use and c) can be scaled to accommodate a large number of users. The perfect blend of these factors results in a strategy that is secure, flexible and convenient.

BYOD OR BYOE?

BYOD has always posed a headache to system administrators, since these mobile devices are accessing corporate data. In recent years, the trend has blossomed into BYOE, or "bring your own everything", as employees blur boundaries by bringing not only their own smart phones, tablets and laptops to the office, but also their own applications and networks. This infusion of personal devices, apps and networks into the corporate environment presents a significant security challenge, as controlling access to corporate data and network assets is complicated by the presence of devices, networks and applications not fully under the IT department's control.

Compounding the BYOE problem, mobile devices today often use ActiveSync – the PIM-data synchronization application from Microsoft – to automatically synchronize email, calendars and other information. Although ActiveSync is clearly convenient it also represents a security vulnerability when ActiveSync devices are being enrolled in the organization.

BEST PRACTICES

Security and IT administrators must take the following steps to minimize the impact of BYOE and enroll and manage devices in a secure way.

1. SECURE ACCESS TO DATA

Today users obtain access to their PIM data by simply entering their email address and their Windows password on their mobile device. Based on the settings of your Exchange Server the device will either be automatically approved and the data synchronization will begin. This however presents a security vulnerability because the users are only poorly authenticated by their username and password (single-factor authentication). Alternatively the device will be quarantined until manually approved by the administrator. The problem with this approach, especially in larger companies, is:

how does the system administrator know whether to approve a quarantined device or not? How does he distinguish between a valid user device and a hacker attempting to get access to a user's e-mail using the ActiveSync protocol?

To authenticate the identity of the user requesting remote access to company systems and data, take the following steps:

› Ensure authentication of the users accessing data

› If data is synchronized:

- Ensure that the device is *authenticated*
- Link the device to a named user
- Encrypt the transport of data

› If there is granted access to centralized systems:

- Authenticate the user
- Use virtualization to minimize the security risk

2. STRIVE FOR DEVICE INDEPENDENCY

At SMS PASSCODE, our end goal is ensuring that any user accessing any kind of data is who he or she claims to be. To do so, a device-independent philosophy is highly convenient. If the company's authentication policy is dependent on what specific device is being used to access company systems or data, then that strategy loses effectiveness.

Therefore, it is imperative to make an authentication strategy as independent as possible, including independence from devices. By removing dependence on anything device-related from the authentication discussion, the strategy is centered entirely on controllable factors. This approach allows companies to permit access to its services via server-side processes that authenticate the user regardless of the device he or she is using.

3. USE VIRTUALIZATION TO MINIMIZE THE SECURITY RISK

The safest way to access centralized systems and/or data which is not meant to be synchronized is to use a virtualization solution, such as Citrix. And the idea is that no data is transferred to the device and no application accessing data is executed on the device except the application granting access to the virtualized environment. Thereby you minimize the exposure of data and systems for threats coming from and being on the device. But regardless of the use of virtualization or synchronization of data or a combination of them both, you need to ensure the identity of the user.

CHECKLIST

To authenticate the identity of the user requesting remote access to company systems and data, take the following steps:

✓ **Ensure authentication of the users accessing data**

If data is synchronized:

- ✓ Ensure that the device is authenticated
- ✓ Link the device to a named user
- ✓ Encrypt the transport of data

If there is granted access to centralized systems:

- ✓ Authenticate the user
- ✓ Use virtualization to minimize the security risk

✓ **Strive for device independency**

- ✓ design your authentication policy to avoid dependency on certain devices being used

IF THESE BEST PRACTICES ARE ENFORCED, IT WILL BOOST ACCESS CONTROL SECURITY FOR DATA AND SYSTEMS AND MINIMIZE THE RISK OF SYSTEM COMPROMISE.

SMS PASSCODE DELIVERS SUPERIOR AUTHENTICATION

SMS PASSCODE has built its core business on superior remote access user authentication. Today, SMS PASSCODE protects cloud applications and remote access solutions, such as Citrix, Cisco, VMware, and Microsoft with its highly flexible solution. With the latest version of the SMS PASSCODE solution, users can easily enroll new ActiveSync devices by themselves without compromising security. SMS PASSCODE thereby secures BYOD access to centralized systems and data in a highly secure, flexible and convenient way.

ABOUT SMS PASSCODE

SMS PASSCODE is a technology leader in adaptive multi-factor authentication, improving enterprise security and productivity by delivering an easy to use and intelligent solution that helps ensure the safety of corporate networks and applications.

SMS PASSCODE authenticates users through their mobile devices, helping IT managers address evolving business needs with cloud applications and mobile security by dynamically authenticating users based on geo-location and login behavior patterns.

The solution secures remote access systems including Microsoft, Citrix, Cisco and Checkpoint.

Governments, telcos, enterprises and financial institutions in more than 40 countries appreciate its cost-effective, secure and easy-to-maintain offering, making SMS PASSCODE their trusted partner to securely authenticate access to services while preventing identity theft.

For more information, visit www.smspasscode.com

www.smspasscode.com

sms | passcode
adaptive user authentication