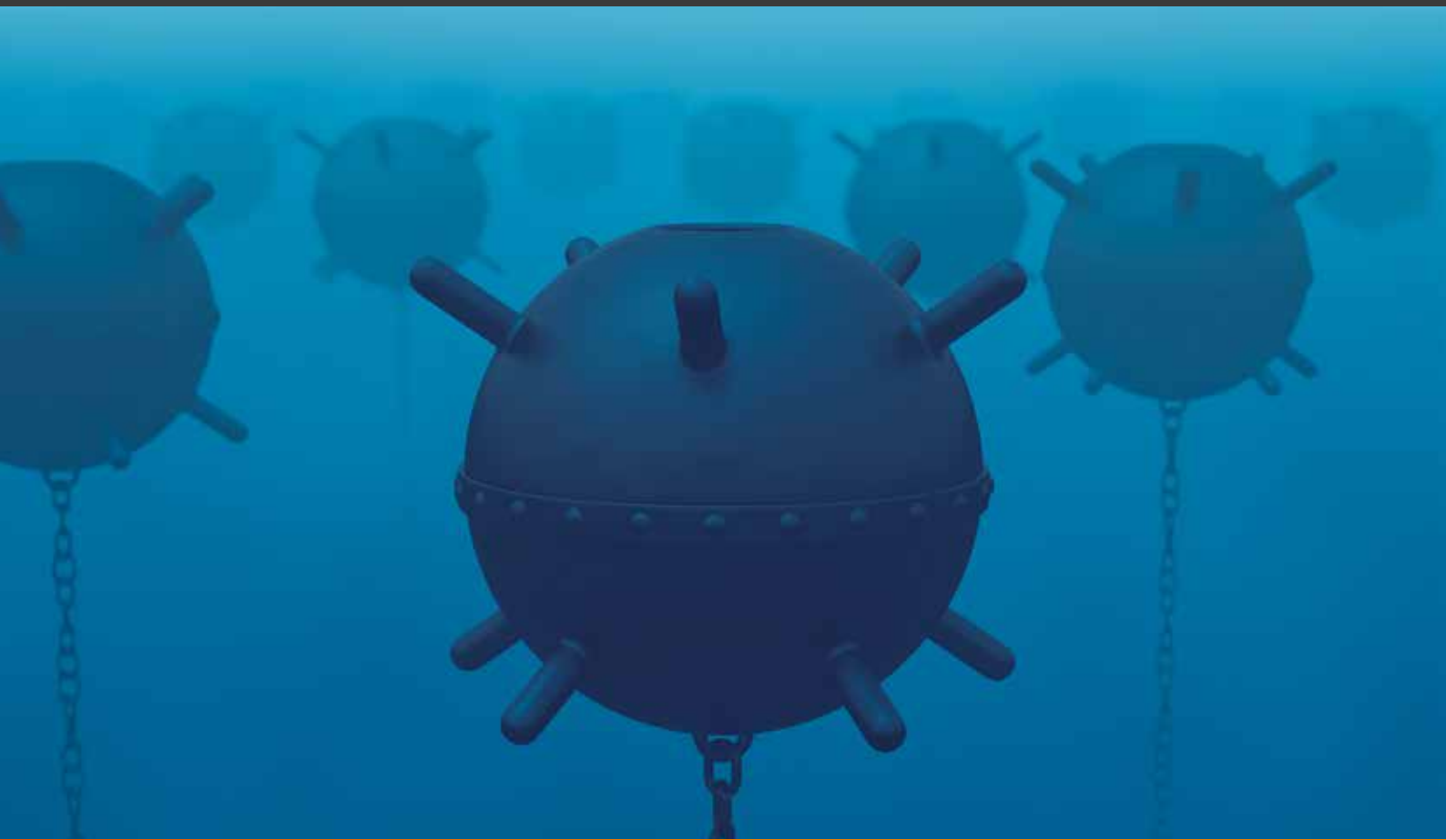
Whitepaper

sms passcode
adaptive user authentication

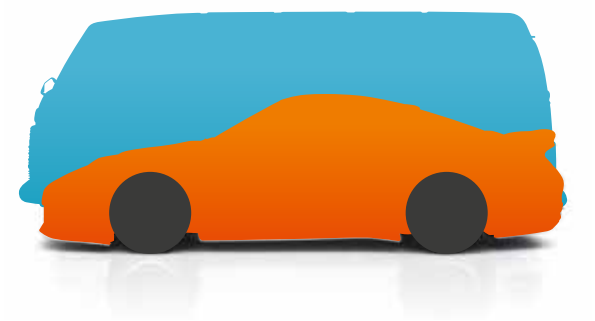
THE HIDDEN DANGERS OF 'GOOD ENOUGH' AUTHENTICATION SOLUTIONS



A STEP-BY-STEP GUIDE TO UNDERSTAND THE COMMON PITFALLS WHEN SELECTING AN AUTHENTICATION SOLUTION

The user authentication market is filled with hidden dangers. Use this step-by-step guide to understand the common pitfalls when selecting an authentication solution

While it's human nature to make comparisons, not all comparisons are helpful or accurate. When comparing a Porsche and a Volkswagen van, for example, the most you can say is that they are both vehicles, they both have wheels and doors and engines and will get you from Point A to Point B. But that is where the comparison ends. These two vehicles vary significantly: in terms of handling, smoothness of ride and value, they are worlds apart.



In a similar vein, not all mobile-based multi-factor authentication solutions are the same, so it is incorrect to compare them by this label alone. Many differentiators exist within the multi-factor authentication market, and they are not inconsequential. These differentiators can mean the difference between true security and susceptibility to phishing, between timeliness and late arrival of authentication codes and between user-friendly and hard-to-use solutions.

BEWARE OF PRE-ISSUED PASSCODES

The level of security is a significant differentiator among mobile-based multi-factor authentication solutions. SMS PASSCODE is a real-time solution that is challenge- and session-based. In other words, the code that users need to authenticate a session is not generated until some kind of challenge is fulfilled, and the code doesn't exist until then. Most authentication solutions, however, operate like token-based technologies with pre-issued one-time-passcodes that are based on a seed file somewhere. If codes are pre-issued based on a seed file, then they are vulnerable to hacking, i.e. through unauthorized usage or theft of seed files. This is not just a theoretical risk but has actually happened before, requiring the replacement of millions of hardware tokens. If the authentication code is pre-defined before the login, then it can be stolen and used for another login. That means that the system's security can be significantly compromised and the code can be exploited by phishing.

THE IMPORTANCE OF CHALLENGE- AND SESSION-BASED SECURITY

Being challenge-based enables organizations to set up systems that make employee remote logins even more secure. When the SMS PASSCODE solution generates a code, it's only after the user session has been confirmed. When the username and password are validated, the solution generates the code. By waiting to generate the code instead of relying on a pre-set bank of existing codes, SMS PASSCODE can see which computer workstation the login request is coming from. The solution then creates the code and links it to the computer so the code received via mobile phone can only be used from the machine the request was originally initiated. That's a huge security differentiator: if for any reason the code is intercepted, it cannot be used on any other computer. This helps protect against sophisticated attacks such as real-time phishing and man-in-the-middle attacks.

It's important to note that just because a solution is challenge-based, it doesn't necessarily mean that it is session-based as well. However, a solution cannot be session-based unless it is challenge-based. If these two elements are combined in a multi-factor authentication solution, then it eliminates the consequences of phishing. If a static SMS code merely takes the place of a token, it can still be phished just as easily as a token. True security, therefore, requires a different approach.

LOOK PAST THE SHINY SURFACE OF THE AUTHENTICATION APPS

Certainly mobile apps are cool, and most users are familiar with using them on their smartphones. But as an authentication mechanism, the 'coolness' of the mobile app will quickly fade once an organization starts deploying in the real world. Making sure an app is successfully deployed to everyone in an organization will not be hassle-free, and maintaining compliance so that everyone is using the most up-to-date version won't be hassle-free, either. At SMS PASSCODE, our philosophy is to reduce any dependencies that can impact the day-to-day operations and make people's job more difficult. If an organization opts for an authentication solution that requires user-deployed software, then it drastically increases dependency since the success of the security solution relies on all users having the software deployed and up to date. In addition, the solution relies on all users having a smart phone, which is not always the case. The mobile app (unless used as a basic soft token) also requires a data connection to work, and this can be impractical and expensive to use for employees while travelling.

RELIABILITY OF SERVICE – THE CRUCIAL ELEMENT TO A SUCCESSFUL IMPLEMENTATION

When using a solution that leverages SMS as a delivery mechanism for the OTP (One-Time-Passcode), the reliability of the SMS arriving on time becomes mission-critical. Users are waiting to log in to critical business applications remotely and cannot proceed until the code arrives. There is a huge difference between the SMS arriving within 10 seconds or two minutes (or even 10 minutes). If the solution is not designed and programmed to effectively deliver the SMS on time, it might create a situation in which a high percentage of the codes will arrive late. Some authentication providers will claim that SMS delivery is not reliable enough and, as a result, they encourage the use of pre-issued codes. However, this lowers the level of security significantly because the OTP cannot be generated in real-time and can be a dangerous trade-off to make.

RELIABILITY OF SERVICE: FLEXIBLE AND INTELLIGENT PASSCODE DELIVERY

SMS PASSCODE's mobile-centered platform offers maximum flexibility and reliability through a number of real-time OTP delivery methods and a sophisticated automatic fail-over mechanism. SMS PASSOCDE

supports a broader range of OTP options, including SMS, voice-call, e-mail, cloud keys, soft tokens from Microsoft or Google Authenticator and even traditional hard tokens.

Should an OTP for some reason not be delivered via the primary delivery method, then SMS PASSCODE's failover mechanism will automatically kick in and deliver the OTP via one of the secondary methods. This adds extra certainty that OTPs will be delivered on time and that users will be able to log in. The solution can also be configured to automatically detect where the user is logging in from and dynamically choose the most appropriate OTP delivery method based on the user's location.

USER CONVENIENCE: THE DEVIL IS IN THE DETAILS

SMS PASSCODE has done research into how the human brain perceives different kinds of patterns, and some patterns are easier to remember than others. As a result SMS PASSCODE uses trademarked passcodes called memoPasscodes™ that are easy to remember at a glance. Even though they are easy to remember, these patterns are also very secure: a FIPS 140-2 approved evaluation algorithm is used to generate the code. This FIPS 140-2 code refers to the level of difficulty of cracking a given random code, since 'randomness' is not the same as being hard to compromise from a security standpoint. While a code should be random, it also must be very hard to compromise. The algorithm SMS PASSCODE uses is still 140-2 evaluated, which means that hard-to-pronounce codes are eliminated and easy-to-pronounce ones are passed on to users in real time.

Another factor to keep in mind regarding the user experience is the way the SMS message is delivered on the user's phone. Instead of sending the code to a user's inbox, requiring the user to navigate to it, SMS PASSCODE sends a flash SMS that pops up on the user's screen. When the user clicks on the message after the code has been entered, it vanishes from the device for added protection.

USE CONTEXTUAL INFORMATION TO YOUR ADVANTAGE

Another consideration when choosing a mobile-based multi-factor authentication solution is its level of adaptive support. SMS PASSCODE takes full advantage of contextual information such as login behavior patterns, geo-location and the type of login system being accessed. This provides some powerful benefits for an organization in terms of added user convenience. The solution can be configured to dynamically adjust the level of security based on 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 comfort of their home – where he or she has logged in from before, then he or she will not be prompted for an OTP in order to authenticate. On the other hand, if the user is attempting to log in while traveling (i.e. from an airport lounge or hotel with public Wi-Fi), then an OTP is mandatory to gain access.

'GOOD ENOUGH' OR BEST POSSIBLE: THE CHOICE IS YOURS

If all you need is a rig to load your garage sale finds into, a Volkswagen van is just fine. But if you need a vehicle that delivers high performance at high speeds, a Porsche is a much better choice. Just as all cars are not created equal, neither are all authentication solutions. Security, reliability and ease of use are just some of the many vital components to consider when choosing among providers.

To move beyond 'good enough', visit **www.smspasscode.com** to learn more about how adaptive, multi-factor authentication can meet your requirements and keep your data safe.

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 log-on 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

ABOUT THE AUTHOR

David Hald is a founding member of SMS PASSCODE A/S, where he acts as a liaison and a promoter of the award-winning SMS PASSCODE multi-factor authentication solutions. Prior to founding SMS PASSCODE A/S, he was a co-founder and CEO of Conecto A/S, a leading consulting company within the area of mobile- and security solutions with special emphasis on Citrix, Blackberry and other advanced mobile solutions. In Conecto A/S David has worked with strategic and tactic implementation in many large IT-projects. David has also been CTO in companies funded by Teknologisk Innovation and Vækstfonden. Prior to founding Conecto, he has worked as a software developer and project manager, and has headed up his own software consulting company. David has a technical background from the Computer Science Institute of Copenhagen University (DIKU).

www.smspasscode.com

sms | passcode
adaptive user authentication