

**Article:** The changing face of tokens  
**Author:** Steve Watts, SecurEnvoy  
**Submitted to:** InfoSec  
**Date:** 27<sup>th</sup> November 2007  
**Word count:** 1061  
**PR contact:** Amy Redhead, SPARX  
[amy@sparxgroup.co.uk](mailto:amy@sparxgroup.co.uk) / 0207 487 8443

---

Many organisations have long recognised that relying solely on usernames and passwords to control access to confidential systems and information is outdated and misguided. But the search for stronger, more proven methods of authentication has, to date, brought with it as many problems as it has solved.

Being the most basic, usernames and passwords remain the default level of user authentication – the ‘something you know.’ Adding ‘something you have’ such as a token or smart card has been the traditional second layer in two-factor authentication, while ‘something you are,’ the fundamental principal behind biometric technologies, provides an additional, third level.

However, each extra layer of security adds new levels of complexity, set-up time, administration and management to the process. And, since the token or smartcard is currently more accurate than the most affordable biometrics systems, it remains the most popular choice for backing up usernames, PINs and passwords.

The use of token-based second factor authentication has also increased thanks to the increase in remote working and the availability of common services over the internet. Both of these have the potential to open up swathes of sensitive data to unauthorised but determined prying eyes, and make secure network access a priority. But traditional tokens or smartcards aren’t a universal solution, and in many cases they simply aren’t practical.

Let’s look at the growing number of employees who need to log on to corporate systems while out of the office: the ‘Martini’ workers who need any time, any place, anywhere computing – with ‘any device’ as an added extra. These users don’t want to be restricted to accessing their organisation’s networks from their company-issued PC or laptop alone. They want to log in securely wherever they need to - whether it is from their home PC, a laptop in a hotel or airport, or even from their smart phone.

Smartcards that require dedicated readers, or USB tokens that need the correct software certainly provide security – but they don’t provide the flexibility needed by these hyper-mobile workers. They face a choice: either productivity or protection is compromised. And it’s a choice that most organisations are no longer prepared to make.

The other popular alternative is to use hardware-based tokens that generate a constantly-changing PIN. They do allow authentication from any machine, but the user has to carry the token with them at all times to be able to access the data they need securely. Any users who forgets or loses their token are effectively blocked from doing any work, until it is retrieved. The tokens are also expensive to purchase and, since they require PIN administration, have costly overheads – particularly when the replacement of easily lost and broken units is factored in.

There is also a problem that is common to all these traditional two-factor authentication methods: they lack spontaneity. To use them, employees must be set up in advance and provided with the necessary hardware. But what happens when a user needs to access the network remotely when they haven't needed to previously? If an unexpected event - like traffic problems, storm damage or even a sick child – prevents them getting to their usual workplace and they haven't got the right equipment then they too cannot access the data and applications they need.

It isn't practical to issue tokens to all office-based employees simply as an insurance policy. But equally an emergency situation is no excuse for a security lapse – and users who need to access the corporate network over an SSL VPN, for example, cannot solely rely on Microsoft usernames and passwords.

The solution that many companies keep coming back to when attempting to solve this dilemma is to use mobile phones as the second authentication device. According to Ofcom, there are approximately 70 million mobile phones in the UK – more than one for every member of the population. If users are already carrying a mobile phone – and the figures suggest that they are - then it makes sense to use the phone itself as part of the security process.

But the phone-as-token solution has to be adopted in the right way.

Some companies have tried installing software on the phone to support the authentication process. But since there are so many different types of phones and operating systems this method leads to real challenges for the IT team – both during installation and in ongoing support. This system is only really workable if organisations limit the type of phone to be used to just one or two devices. This method also creates additional problems if phones are lost or stolen, as they all too frequently are. Replacement devices need reinstalled software – and so the headaches continue.

A more practical and increasingly popular approach is to use SMS to send users a one-time passcode. SMS doesn't require any software to be pre-installed on the device, and messages can be sent to any make and model of phone. It is also a technology that users are familiar with, which keeps training time and support queries to a minimum.

The main problem that can arise through the use of SMS for two-factor authentication is the potential for delays between the passcode being sent and its arrival on the user's device. This becomes an issue with systems that send users a passcode in real time as they are in the process of logging on to the network. If the user happens to be in an area with little or no mobile phone reception, then they cannot log in. However, if users are sent their initial passcode as soon as they are enrolled, and the code is immediately replaced with the next number as soon as it is used, this problem of SMS delay is resolved.

Furthermore, in an emergency situation, using mobile phones for two-factor authentication means that businesses can easily enable secure remote access for all users with just a flick of a switch. Employees can simply be pre-registered for remote access, and added to a database of phone numbers. They will then have their first passcode sitting on their phone, just waiting until it is needed.

At a time when security threats are growing and mobile working is increasing in popularity, two-factor authentication to ensure secure remote access is more important than ever. But it needs to be low-cost, convenient and support flexibility. Fortunately with the new technology available, these demands can now be met.