SecurEnvoy

White Paper

Harness the power of seven billion phones to authenticate, what are your options?

Table of contents

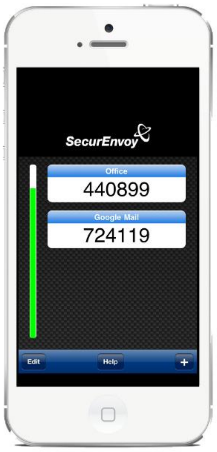
Introduction

There are as many mobile phones as there are people on Earth in 2014, according to an estimate by the International Telecommunication Union (ITU) - which means about seven billion devices and of these the use of smartphones has now surpassed that of conventional mobile phones. These multi-purpose devices have become constant companions for business and personal purposes. Thanks to the presence of mobile internet technology, the devices allow e-mail retrieval, Internet browsing and web-based telephony even when out and about. This white paper explains the most effective way to use smartphones in order to ensure secure access to corporate networks.

Proven tools rather than new investment

People who want to access data and information usually have to prove their identity in order to do so, often by means of a username and password. Even greater security is provided by two-factor authentication solutions, as they require two separate verifications of identity: in addition to personal login details, the user also enters a one-time passcode (OTP). In some cases, this passcode is generated using a dedicated hardware token, which means the user always has to have this token with him/her for this purpose. The drawback for companies with this approach is the cost relating to distribution, provisioning and maintenance of the tokens. Furthermore, lost tokens also mean "lost" system access. A less complicated approach is offered by tokenless two-factor authentication systems, as these use existing mobile devices such as phones and tablets to provide users with passcodes via e-mail, SMS or an app. So instead of having to think about an additional token, users simply make use of their existing mobile devices.

Example of hardware tokens



Passcodes in the SecurEnvoy solution

The user has full control

SecurEnvoy, the inventor of the SMS tokenless method, considers it to be important to give users full control and flexibility. As a result, conventional mobile phones, also known as feature phones, can be used for authentication purposes. Thanks to SMS they can receive passcodes via text messages. However it’s worth considering what would happen if the user has no signal or is experiencing delays in receiving SMS messages? These issues can be avoided from the outset with SecurEnvoy’s patented business grade preloaded SMS approach. This means that once a code has been entered it is immediately replaced by a new numeric sequence for use during the next authentication process. Moreover, thanks to a little known SMS trick it is also possible to update the existing SMS message with the new passcode digits rather than sending a new text message thus users don’t need to delete used text messages.

Alternatively owners of smartphones can opt to use a soft token app which includes One Swipe. The advantage of this is that the app can generate passcodes in real time without needing any connection; a new numeric passcode sequence is created every 30 seconds in the same way as a physical token. This application is available for smartphones, tablets and laptops and works on the operating systems iOS, BlackBerry, Android, Mac OSX, Windows XP, Vista, 7 and 8. With the One Swipe method, the user generates a one-time QR code in the app, with this code containing all the necessary authentication information including the user ID. This QR code is then scanned using a webcam on a laptop or tablet, enabling easy verification of the user's identity. Looking to the future, SecurEnvoy is also working on developing secure authentication processes that use fingerprints and NFC (Near Field Communication enables the contactless exchange of data over short distances using wireless technology). In the same way that Apple Air Pay will allow micro payments, One Swipe will use the same end user procedure to allow remote access to corporate resources.

ONE-SWIPE, EASIER THAN A PASSWORD WITH ALL THE STRENGTH OF 2FA
TAP
SCAN
DONE

Illustration of the One Swipe method

And even if users do not have a mobile device with them, they can still prove their identity in a virtual fashion. For this, SecurEnvoy has developed the Voice Call option. After entering the login information, the login screen displays a passcode. At the same time, the system makes a landline call, which the user picks up before simply entering the code using the telephone keypad. This allows him/her to be authenticated so that access can be granted.

Various options for optimal passcode transmission

In addition to the various transmission channels available, end users can also select the passcode update procedure that best suits the specific working environment of their company's needs. This makes it possible, for example, to circumvent temporary reception problems. The following possibilities are available:

- **SMS:**

Preload

Real-time,
code displayed
directly on the
screen

Three codes in a single SMS,
entered codes are
immediately replaced
by new codes

Periodic codes,
update every
every 1-90 days
(freely selectable)

- **Soft Token, with One Swipe option:**

for smartphones

for laptops and tablets

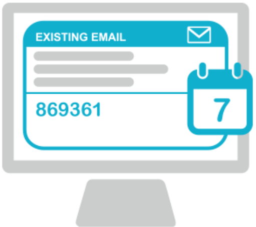
One Swipe QR code

- **E-Mail:**

Preload

Real-time

Three codes in a
single E-mail,
entered codes are
immediately replaced
by new codes



Periodic codes,
update every 1-90
days
(freely selectable)

- **Voice Call:**

Users can manage their own device changes

With regard to ease of use in the IT department, tokenless solutions score highly as a result of their optimised life cycle management. These days, individual mobile devices often have quite short lifespans in companies, and it is not unusual for a whole "fleet" of mobile devices to be replaced once a new model comes on the market. This is why SecurEnvoy allows users to have full control in this context - in other words, users can make the transition from old device to new device without the need for help from anyone else. And the transition is also very conveniently carried out using two-factor authentication. Here an example involving a change from the iPhone 5 to the latest iPhone 6: first, the user logs in, via the app or via SMS, from the old device to the “Manage My Token” portal using two-factor authentication. He/she then scans the QR code that is displayed using the new device, in order to provision it with a new seed record (a special algorithm that generates the passcodes). The security server then automatically deletes the old seed record, so the old device can be safely re-deployed or offered for resale. No usable codes remain on the old device and the user's identity is not distributed over older devices. In addition, the fact that users can carry out the entire procedure themselves relieves the workload on the IT department.

This method therefore compares favourably with those using dedicated hardware tokens, because at this stage the latter would require the cumbersome re-registration and distribution of tokens. If a company switches to new tokens, whether due to theft, loss or maintenance reasons, or for compliancy to the IEEE directive regulations, the IT staff have to collect all the old tokens. Each new token then has to be individually registered for a specific user and provided with the appropriate settings. It may also take a few days for a new device to be received if the employee is working in a different country. And, in the worst case scenario, the token may be damaged during shipping and require a re-issue - this can easily get out of hand and mean that the user is without a specially secured method of remote access for quite a long time.

Don’t spread your identity

With the advent of BYOD more and more end users like to spread their working environment across multiple devices including tablets, home PC, smartphones, business lounges, laptops etc. The key to maintaining control over all these devices is to nominate one of them - normally the phone as the software token - and use it when authenticating on all other devices. Clearly this has major advantages over solutions that try to authenticate each and every device with digital certificates or multiple soft tokens. Trying to manage the life cycle of all of these devices will inevitably lead to at least one of them being re-deployed or sold on by mistake. SecurEnvoy’s approach is to only allow the use of one token device per user but to make it very easy for the end user to switch his device should he feel the need to do so. This approach simply means it is impossible to splatter user’s identity across multiple devices.

Maximum security provided by split seed records

And while we are talking about specially secured methods, it should be noted that two-factor authentication does not equate to "this solution is secure" as such. Any 2FA manufacturer that creates cryptographic keys, also known as seed records and then distributes these keys to its customers have a fundamental security issue as you must trust that the copy of the keys held by the manufacturer is kept secure and can’t be accessed by hackers or government agencies. SecurEnvoy, however, adds an additional level of security. The seed records, are never generated or stored by the manufacturer. This is ensured by the automatic separation of the records: one part is created locally on the client server, while the second is generated using specific characteristics of the mobile device, e.g. information about the SIM card, the CPU or equivalent. Each time the app creates a passcode, the end device decrypts the first seed record part and derives the second part accordingly. This approach means it is impossible for malware on the smartphone to capture the seed record as part of it doesn’t ever exist on the device.

Summary

In terms of pure arithmetic, almost every person on the Earth now possesses a mobile phone, with some even having multiple devices as they also have a company phone. Laptops and tablets are also widely used by the ever increasing number of staff who work remotely. Businesses, government agencies and other organisations can therefore take advantage of this fact and use the devices as the authentication tool. Putting the user in control of which device to use as the authenticator and allowing them to change or upgrade their device is a better solution compared to token-based offering. This approach is cheaper, less labour-intensive and more secure, especially if seed records are separated, as is the case with SecurEnvoy solutions, in order to prevent the manipulation of devices.