

AUTHENTICATION MARKET

EXECUTIVE REVIEW

Stephen Watts, Co-founder, SecurEnvoy Ltd

SecurEnvoy Ltd

1210 Parkview, Arlington Business Park,
Theale, Reading. RG7 4TY

Tel: 0845 2600010

Email: sales@SecurEnvoy.com

www.SecurEnvoy.com

Table of contents

Authentication Market	1
Executive Review	1
Table of contents	2
1. Foreword	3
2.0 About SecurEnvoy	4
3.0 Executive summary	5
4.0 Key facts	6
5.0 Authentication analysis	7
6.0 This is the year	8
7.0 New solutions for a new age	9
8.0 The need for passwords	10
9.0 The growing requirement for RAS	11
10.0 Authentication is evolving	12
11.0 Contact us	12



1. Foreword

Welcome to the SecurEnvoy authentication market issues overview. As the pioneer in tokenless authentication we have seen massive growth in the market, and the need for an update is apparent.

The increase in mobile working and the requirement for users to have remote access to corporate systems has resulted in significant demand for two-factor authentication, and the market is rewarding innovation with orders.

This report is derived from the research we do at SecurEnvoy to make our solutions market-ready. We are seeing demand from both existing and new customers for our SecurAccess product, which gives them a simple, easy to use solution for two-factor authentication that is cost effective and manageable within their existing infrastructure.

The most recent version of our software includes leading edge functionality, patented for its innovation and rivalled by none, which in turn is enabling us to offer a range of exciting new solutions to the market. At SecurEnvoy we incorporate this innovation into products that are both usable and fit for purpose.

In the two-factor authentication market, most of the choices available still rely on users carrying a device such as a token, usb stick or smartcard. At SecurEnvoy our slogan is 'Next Generation' and we believe that the market has moved on from these little plastic tools of the twentieth century to focus on mobility.

Mobile phone technology is progressing in leaps and bounds with access to mobile broadband, super 3G and applications on the move. Our expectations of what we can do and from where also has no limits: people want to have access to everything they need to do their work, wherever they are. Technically this is definitely possible, but one fundamental issue still remains; how do companies know who is accessing their corporate systems without adding so many layers of security that the complexity of access makes mobility much less attractive?

The solution is simple. Everyone has a mobile phone. It's something that you always have to hand. We use them for storing messages, photos, even music. Moreover, it's the one thing that people take great care of and nearly everyone will report when stolen. For this reason it makes sense if phones are used as a mobile authentication device.

2.0 About SecurEnvoy

SecurEnvoy Ltd is a leading security technology company developing pioneering software for authentication solutions. Its current products include mobile two-factor authentication mechanisms for remote access, access in an emergency, securing email and Microsoft Windows password management.

Established in 2002, SecurEnvoy have offices in Theale (Reading) and serves UK and European customers from our Theale head office.

SecurEnvoy Ltd
1210 Parkview
Arlington Business Park
Theale, Reading
Berkshire.
UK RG7 4TY



SecurEnvoy offers cutting-edge technology and leads the market with its product portfolio. The company has four patents pending, and four applications within our tokenless two-factor authentication suite.

SecurEnvoy's aim is to be the dominant supplier of two-factor authentication solutions by designing and supporting innovative systems that are ahead of the competition in terms of cost, usability and support.

3.0 Executive summary

This report reviews the threats that our clients are faced with and approaches the authentication market with a viable alternative.

SecurEnvoy has designed an innovative solution that fulfils the needs for secure remote access and mobile working. As a result, the growth in the company's market presence and customer adoption is outstripping anything seen before. The technology reduces enrolment to zero footprint, provides a mechanism that is simple and easy to use, and is procured on a recurring fee basis with support and subscriptions all included in a one fee per year model. The market expects to pay highly for the 'plastic' in the first year and then periodically thereafter; it also expects to pay for platforms and databases, licenses and user counts. The SecurEnvoy solution is different - we have a one fee per year model based upon actual user numbers, and nothing more.

In comparison to the market as it was, our cost model is half that of the "plastic" alternatives. The costs that remain are spread across a recurring fee basis that enables our clients to budget and afford this security that is so needed in today's online world. Gone are the days of three-month deployments: we are now running at one thousand users per minute. Gone are complex replication issues and redundancy: we scale in line with the existing infrastructure. And gone are the integration issues: our solution has been tested and works with all of the respected vendors of appliances and remote solutions in today's market.

Why has it taken so long for two-factor authentication to gain the traction needed when security risks are so high? Simply cost and deployment. The DTI technical survey reports that 29 per cent of companies needing authentication couldn't justify the cost of the traditional offerings. Nineteen per cent didn't purchase because of the inconvenience to users and a further 13 per cent encountered deployment issues. A massive 61 per cent therefore (up from 45 per cent the previous year) had problems that restricted them from deploying authentication solutions.

SecurEnvoy is able to address the issues of cost, inconvenience and deployment. This review will discuss these three areas and assist companies to achieve two factor authentication within their own organisations.

4.0 Key facts

History shows less than five per cent of remote users have access to an authentication system using anything other than a username and password. What is also interesting is that users of tokens or other hardware-based authentication systems have not increased in numbers from the last decade to this. This reinforces the facts that:

- Authentication has to be easy to use
- Administrators must find it easy to deploy
- Users must be capable of using it wherever they are
- The company must be able to afford the solution

In businesses that we visit, via our distributors and reseller channel, we receive feedback that problems with one of the four issues above has stopped clients from deploying two-factor authentication.

Previous two-factor authentication solutions, both tokenless and hardware-based, have been difficult to use, with multiple logons and mixed passwords and pass-phrases. Users dislike enrolment and deployment issues, which can be laborious and delay their access. Administrators encounter the complexities of deployment and endless helpdesk requests. Finally the greatest of all the stumbling blocks is cost.

End users understand the need for authentication. They are told endlessly that they need chip and PIN or two forms of identity in their private lives, so using two factors at work makes sense. With the SecurEnvoy solution it is easy, as they only need to carry their phone with them.

The true cost to the business of deploying alternatives are so great that, in many cases, no solution at all is purchased; it's too expensive to justify. That has changed with our solution. Customers no longer have to delay implementing authentication solutions because of other pressing purchases or security holes to fix.

When prospective customers trial the SecurEnvoy solutions, over 90 per cent decide to purchase the product. It is so successful, easy to deploy and manage that a permanent license is sought and the solution remains. Cost is no longer a hurdle to overcome, and acceptance and ease of use are established in the trial stage.

5.0 Authentication analysis

Companies know that they have got to be online, and that they have got to allow remote access. But many assume that if they have SSL in place they will be secure. Unfortunately, this isn't the case.

Once a secure tunnel is achieved using the SSL protocol, the data flowing across it is protected with encryption. However, the real issue is who is actually on the other end reading this data. You can't hear them, you can't see them, so how do you know it is the correct user accessing enterprise data? In essence you don't. Other systems have come and gone – confirming mac addresses, checking the serial number of the memory and a whole host of other bizarre alternatives - all proving it may be the right device accessing the network, but is it the right user?

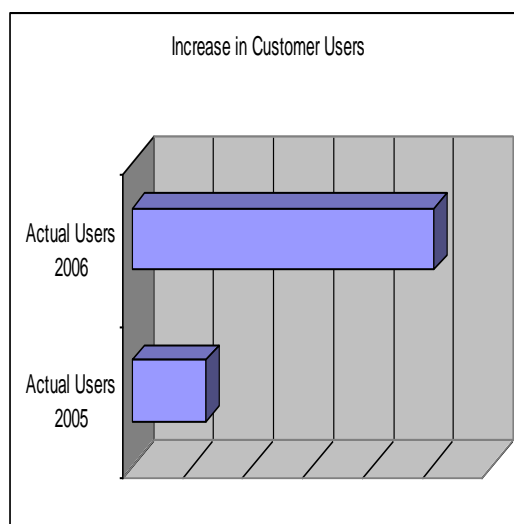
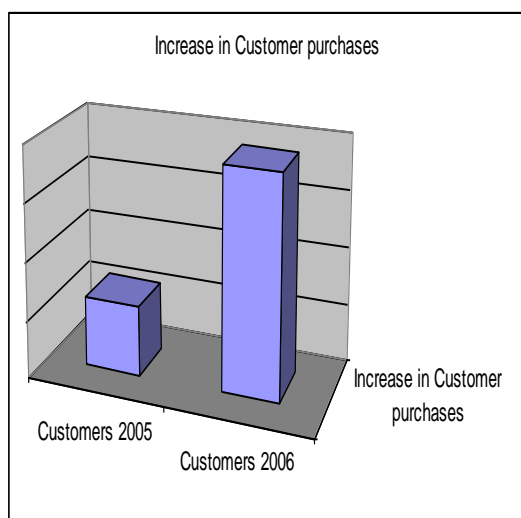
Passwords are accepted as an appropriate method of checking local users, so why is it different for remote users? Simply we know if our colleague is at the right machine as we work with them everyday, we know their face, mannerisms and voice, we have door entry systems and sometimes security access to get in to the office. Combined with a password this seems acceptable access when you work from the office. But remote access is different. No one can see the user, no one has checked their badge, or recognises them. How then would the administrator know that the user trying to get online is who they claim to be, and not one of the other 2 billion people that are also on the internet?

6.0 This is the year

Over the last ten years we have heard the same ring sounding "this is the year of the smartcard." And every year it is not.

However, the most recent data released from the annual DTi survey shows that authentication is growing at last. The market has invested and has increased remote access users authenticating with two-factor authentication from five per cent to nine per cent.

The market has accepted that authentication is critical for the remote user and has grasped the nettle. These increases in adoption correlate with our own statistics. From 2005 to 2006 our customer base has increased by 283 per cent and the amount of customers using the service has risen by 396 per cent. (Statistics based on actual users in 2005 directly proportional to actual users in 2006).



We expect this increase to continue in 2007, and it is this year and the next few that will show users adopting mobile tokenless solutions as standard.

Tokens, sticks and cards are expensive to distribute to end users, and the cost of deployment far outweighs the actual cost of the token. However much the price of the token is reduced, there is still a large spend needed to deploy, manage and administer remote token users. However, companies using the SecurEnvoy tokenless mobile solution have already seen that the cost of ownership, compared to alternatives, is reduced by at least 45 per cent. Taking into account deployment, broken and faulty tokens, helpdesk issues and administration overhead our customers are saving more than 60 per cent compared to hardware devices.

(Comparison available on line at

http://www.securenvoy.com/products/secuaccess/SecurEnvoy_Token_Cost_Comparison.xls)

7.0 New solutions for a new age

Now established as a viable and attractive contender to the ageing alternatives, the true power of the mobility case can be seen.

If users are unable to get into their workplaces in case of an emergency, such as extreme weather conditions, flu epidemics, natural or forced catastrophe, the heightened security that should be implemented traditionally could not.

Should such a disaster take place, how long will it take for enterprises to mobilise their workforces? Remote access needs to be rolled out quickly in such an event, but how do you distribute all those extra tokens, cards or sticks to the end users? How do you reach them to enrol them and set up their first PIN or secret? And how likely is it that by the time you order and receive the authentication devices the disaster has passed?

In a crisis situation it is perhaps more important than ever that security systems are available. With our new SecurICE solution, we can now provide for thousands of users in the event of an emergency. Users already have their Microsoft Windows password, they have remote access, and they own a phone – the combination allows the company's IT administrator to bring additional users online securely in just minutes. At the press of one button, all users already selected for this disaster recovery option will have their accounts activated. The second factor has already been deployed to the mobile phone, allowing instant access as soon as the user needs it.

Increases in business disruption are making every organisation think about their own business continuity plans. We have developed and patented this product as an emergency service. It is simple to deploy, easy to use and affordable: exactly what is needed for disaster recovery and business continuity planning.

8.0 The need for passwords

Businesses regularly quote the cost of a helpdesk call, how many they receive each month from the average user and the amount of downtime caused by password issues. Passwords need to be changed; and many users do indeed change them monthly. But it still requires a degree of complexity to avoid tables that can crack them.

To ensure their ongoing security, companies have got to find an answer to the problem. Passwords are an identifier, one element needed to securely enable access to corporate systems. But another aspect should be used to really confirm a user's identity, without increasing password management costs, especially as passwords get more complex. SecurPassword is SecurEnvoy's solution to the everlasting password reset problem.

Rather than depending on the helpdesk, SecurPassword relies on the user's mobile phone as their second factor, and a simple way of carrying their authentication token at all times. Likewise, SecurPassword enables password resets online, 24x7, alleviating the expense and regularity of helpdesk calls. By confirming their second factor, the system allows the user to reset their own passwords. It also links directly to the active directory, enabling the company to check immediately that the new password meets the necessary complexity rules.

SecurPassword is a simple solution for a simple problem. Everyone forgets their password from time to time, especially if it is complex. Now there is a simple and cost effective reset method.

For a trial please visit <http://www.securenvoy.com/trial.aspx>.

9.0 The growing requirement for RAS

Record numbers of people have access to home and business broadband. ISPs are now providing wireless broadband and allowing users access globally. Good news for communication, home working and flexibility, and good news for the vendors of wireless access points. A recent report produced by PWC confirms these vendors have reached a penetration of 84 per cent of the VPN market place.

With such great numbers accessing corporate resources remotely, the need for secure identification of end users is growing considerably. We believe, however, that the method needs to be simplified and deployment made quicker and easier. A major step in our latest release, Version 4, allows deployment to one thousand users every 60 seconds. That provides scale and speed for deployments of all sizes. As for end user experience, in our own research with existing customers that have upgraded from traditional tokens to our SecurAccess solution, 100 per cent of end users agreed that using the mobile was easier and quicker than their previous experience with tokens.

10.0 Authentication is evolving

SecurEnvoy has taken the traditional market of plastic authentication devices and made them a virtual solution that uses the existing infrastructure of mobile phones. Globally accepted as the mobility device of choice, every business user has a mobile phone. They all know that without the phone they cannot conduct business, so the device is guarded and protected.

If the company IT Manager were to describe the ideal solution, they would write the requirement as:

WANTED - Cost-effective method of two-factor authentication that is simple to setup, deploy and administer and one that my users can easily use.

Wish list; For users to self service their passwords, simply and securely, but adhere to company security standards.

Dream solution; Allow all of my users to gain access remotely in the event of a disaster and all I need do is press a button to activate.

All of the above is now achievable – SecurEnvoy is making the next generation of authentication solutions available now.

11.0 Contact us

SecurEnvoy Ltd
1210 Parkview
Arlington Business Park
Theale, Reading
Berkshire.
UK RG7 4TY

Telephone: +44 (0)845 2600010
Fax: +44 (0)845 2600014
Email: sales@SecurEnvoy.com
Web: www.SecurEnvoy.com