

About SecurEnvoy

SecurEnvoy are the inventors of tokenless authentication and provide two-factor authentication via mobilephones. Passcodes are sent to the user's mobile phone in order to access corporate internal networks, cloud based services or private emails.

SecurEnvoy's products - SecurAccess, SecurPassword, SecurICE and SecurMail - are adopted worldwide.

Customers benefit from reduced support time, no database management as existing LDAP servers are used and zero footprint as no token deployment is required, so ROI for organisations is relatively high.

SecurEnvoy distributes through the channel, providing customers the value added benefits of working with

local partners. It has built up a technical and sales

infrastructure that supports most languages and

cultures around the world. Partners include: Juniper, Citrix, Fortinet, Sonic Aventail, Cisco, Checkpoint, Celestix, Microsoft and F5. SecurEnvoy's customers include T-Mobile, Symantec, John Lewis, NHS and Save The Children.

Founded by Andrew Kemshall and Stephen Watts in 2003, SecurEnvoy is based in Theale, Berkshire.

For more information about SecurEnvoy and its products, visit www.securenvoy.com.



SecurEnvoy Ltd

1210 Parkview

Arlington Business Park

Theale

Reading, RG7 4TY

T: +44 (0) 845 260010

E: info@securenvoy.com

Quick Selling Guide



Quick Selling Guide



Who are SecurEnvoy?

SecurEnvoy are the inventors of SMS based tokenless two factor authentication and have been leading the way in the development of this next generation of authentication technology since 2000. SecurEnvoy are a UK based company, privately owned with products distributed across the globe.

What is SecurAccess?

SecurAccess from SecurEnvoy allows organisations to provide remote staff with industry standard two factor authentication without the pain and cost of deploying legacy hardware tokens.

SecurAccess turns any GSM mobile phone into a two factor authentication token. Software is not required on the users phone which eliminates complex testing, support and training issues.

SecurAccess fully integrates into Microsoft Active Directory, Novell E-Directory, Sun Directory Server and OpenLDAP. Integration is simple and requires no schema changes. No additional database's are required which reduces costs and simplifies on-going support.



Key Benefits:

- Strong, affordable, convenient two-factor authentication
- Enhanced security
- Reduced helpdesk costs
- No password reset or PIN management issues
- No token/smartcard deployment, renewal or replacement costs
- No need to carry additional devices
- No software required on the mobile phone
- No delays waiting for a passcode
- Passcode always available even if temporarily out of communication

Key Features

- Any GSM mobile phone can be transformed into an authentication token
- No additional hardware token required
- No end-user hardware deployment costs
- No end-user hardware failure problems
- Supports any system that includes a Radius client, such as all known VPN servers
- Direct integration to your existing user directory, no addition database is required.
- Protects applications that run on Microsoft IIS, no integration or code changes required
- Simple six-digit SMS authentication code
- Single-use passcodes prevent all known password attacks

Who are using it already?

Private Sector



Public Sector



Key Target Markets:

Retail/Manufacturing

Focus on cost savings with this sector as due to the economic climate, these organisations will be very keen to save money.

Local Government

Due to the latest version of the Government Connect Code of Connection all remote access users connecting to the GCSx network must use two factor authentication.

Contacts to target: • IT Manager • IT Director • IT Security Manager • Infrastructure Manager

Key Sales Questions

- I am trying to contact the person responsible for remote access strategy?
- How do you currently authenticate your remote access users, do you use any form of two factor authentication?
- If Yes, what type of two factor authentication technology do you use, tokens, smartcards, mobile phones?
- If tokens or smartcards, would you be interested in reviewing your current solution if I could offer you something that was easier to use, easier to manage, greener and save you up to 60%?
- If no two factor authentication in place, would you be interested in looking at the state of the art two factor authentication solution that utilises the users mobile phone as the token and is easy to use and manage, quick to deploy, green and cost effective?
- If you are interested, please can I book you an online demonstration with a SecurEnvoy representative to take you through the product in more detail?
- If yes, what dates and times can you make in the next 14 days?

Objection handling

1. What if the end user loses their mobile phone?	As with RSA SecurID, SecurEnvoy SecurAccess can allow the administrator to provide the end user with a static password while they are without their phone or token. The difference comes is that SecurEnvoy can automate the change back to one time mode after a number of days, where as an RSA administrator may have to chase the user to find out when they next had their token. End users tend to pay a lot more personal security to their mobile phone than they do a piece of plastic forced onto them by the company. End users are much more likely to know that their mobile is missing and a lot quicker than they would do that their token is missing. Hardware tokens may not be noticed missing until user next logs in which could be a number of days or weeks. The end user is much more likely to feel a moral obligation to report their mobile phone missing compared to token which they are most likely going to report missing when it is convenient for them.
2. Where I live has bad or no GSM coverage how do you manage this?	If you frequent a place that has intermittent coverage, it is possible to utilise the day code option within the software. This means that a passcode can be reused for between 1 and 99 days. Being that SecurEnvoy works on pre-loaded methodology the user will always have a working code on their phone. Alternatively the security server can be configured to send 3 one time codes with-in each SMS message. Finally it is possible for SecurAccess to send a passcode to a landline telephone or DDI number behind a PBX.
3. Some of my users do not have mobile phones how can I use this solution?	These users may not have a company supplied phones, but they almost certainly have their own mobile phones as statistics say that there are nearly twice as many live handsets as people in the UK. Even if they don't have a personal mobile phone, SecurAccess can still send a passcode to a landline telephone or even a DDI number behind a PBX.
4. What if end users do not want to use their personal mobile phone?	The question is why don't they want to use their own phones? You will not be putting any software on their phone. You will simply be sending them an SMS message which will not cost the end user anything. In some cases its simply that they don't want to receive phone calls from other employees. Personal mobile number are stored encrypted so that only the SecurEnvoy administrators can read it which prevents other staff trying to call it. What is more inconvenient to the user, using up pocket space for a token or using virtual space on their mobile phone?
5. How good is the GSM phone coverage?	GSM network consists of over 860 networks in 220 countries/areas of the world. Coverage Maps can be found at: http://www.gsmworld.com/roaming/gsminfo/index.shtml
6. How well can the SecurEnvoy server scale?	This answer is very well. SecurEnvoy scales directly with Active Directory as this is it's database, therefore the question should be "how well can your existing AD scale?". Microsoft have spent much time and money perfecting the replication between domain controller servers. SecurEnvoy benefit from this replication as it directly integrates with AD or other LDAP servers such as eDirectory.
7. What happens if the end user deletes their SMS message?	Simply enter your username and complete the logon process without the passcode, the system will see this as a bad logon and send a new passcode. This will work as long as you have not gone passed the set number of concurrent failed logons, otherwise the account will be disabled.

Other vendors you may come across: • RSA • CryptoCard • Swivel • Vasco • Signify • Aladdin • Entrust