



USB Keys – 2 factor authentication with evolve™

Alongside many significant enhancements, evolve™ version 3.1 also saw a fundamental change to the way users log in to the system.

Up to then, users have been required to login using a conventional username and password – typically a combination of 1st name and then an alphanumeric password, both of which are encrypted and then passed to the system to authenticate.

This approach has many disadvantages however, not least of which is the inevitable conflict between users who would ideally like easy to remember, simple passwords and the ‘complex’ passwords that are really necessary from a security point of view.

Put simply ‘charlie’ is a much easier password to remember than ‘nL991&s4Ssa4’ is (although the latter is much less susceptible to being cracked by brute force).

The problem is not limited simply to password choice though; there are many other disadvantages with this approach.

Consider for instance that most people at some point will write their username and password down. If someone catches sight of it is very likely that you will never know! Understandably, in this day and age, people have so many passwords to remember that very often it is easier to use the same one for everything...

And although all evolve™ traffic is encrypted (so a username and password can’t be intercepted - or ‘sniffed’ to use the jargon), there is always the possibility that that ‘universal’ password will be intercepted somewhere else and used.

The essential problem is that username and password systems provide no real way of knowing that the person who has logged in using a particular username and password is actually the person who they were issued to, with sensitive commercial and personal data, integrity, accountability and security are paramount.

The Solution – 2 Factor Authentication ‘Something you have and Something you know’

Fortunately in the real world these occurrences are rare and the most troublesome thing most of us have to contend with is forgetting which username and password we use for what...

Happily, by using a hardware key we can not only overcome all of these problems but also use them in an number of other ways to make our online lives more secure.

How they work

The keys themselves are USB (Universal Serial Bus) devices, compatible even with the oldest version of USB dating back to Windows 95, some 7 years ago. They come in a few shapes and sizes, but the ones evolve™ uses look like this:



The Aladdin R2 USB token

Shown approximately actual size of 16mm x 47mm



In fact, a similar kind of device – the USB drive will be familiar to many people as they are frequently used as a useful means of carrying small amounts of data around from machine to machine.

Although the hardware key looks similar to a storage device however, that is where the similarity ends.

Rather than having a chip that is capable of carrying your data (as the USB drive does), it instead carries a chip that contains a unique electronic signature (a very long string of numbers and characters) – one that cannot be changed, exported or copied from the chip by any means.

This 'Private' signature is created at the point at which the key is generated and is the other half of a pair (the other being your 'Public' signature which is made freely available).

The important point is that it is impossible to determine the 'Private' signature from the 'Public' one. No amount of mathematical trickery will do it; similarly the 'Public' cannot be derived from the 'Private' (even if you were able to read it from the chip...).

Crucially though, the two Signatures are uniquely related. Something 'Signed' (electronically tagged) with your 'Private' key can only have been 'Signed' by this key – something that is verified because only the 'Public' key will match as the other half.

Similarly, if someone wants to make sure you are who you say you are (as we do with evolve™), they can check your 'Public' signature against you 'Private' signature (this all works without you 'Private' signature being exposed). Only the 'Private' key will return the correct answer to the electronic question.

Protecting the Key

Access to the hardware key itself (actually they are normally called 'Tokens') is then restricted by a simple password. When the key is inserted in to the computer, you are asked to enter your password once. Removing the key automatically logs you out.

This 'Two Factor' authentication (something you have – the physical key) and something you know (your password) is a very secure way of making sure someone is who they claim to be which is why it is used to protect everything from your bank account (ATM card and PIN) to weapons systems.

The great thing is that the password doesn't actually need to be terribly complex ('charlie' would be fine for this) as all it is designed to do is prevent casual use.

If you get the password wrong 3 times in a row and the key is electronically locked its no use to anyone – only reformatting and generating a new 'Signature' will work at that point.

If the key is lost, we can instantaneously revoke the 'Public' signature (make it invalid) and issue a new key to the user.

Other Uses

Although we use the keys for authenticating users, there are many other things they can be used for, all of which can take advantage of both the Public / Private system and single password access. These include:

- Windows Network Login – replacing the username / password to load your profile.
- Laptop protection – boot authentication and encryption.
- Email Signing – Electronically signing and / or encrypting email communication.
- Encryption – Encrypting files, folders or even complete drives allowing access to only a select set of key holders.
- VPN network access – Secure encrypted access to internal network systems.

Although most of these will require additional software and configuration, they all benefit from the same robust simplicity that a hardware key system offers. **Do ask for further information if you would like to know more about any of these or any other uses.**



Other Facts about the Keys and their use with evolve™.

Use with evolve™

- If for some reason your PC or Laptop doesn't have USB (or doesn't have enough slots / they are inaccessible) it is easy and cheap to fit a 3rd party USB expansion.
- Lost keys can be replaced via overnight courier service. A spare key login will be made available to the user until they have their new key. A charge will be made for lost keys of £75 – this covers the replacement of the key and the courier service.

Removing the key automatically logs the individual out. A record is kept of every login and out time (it could be used instead of timesheets or punch card systems).

Other facts

- The keys themselves don't require external power or batteries – they draw power (a miniscule amount) directly from the PC's USB bus.
- They are water resistant and manufactured with a tamper evident high impact resistant casing.
- They will fit happily on your keyring – they weight only 5 grams (about 2 paperclips)
- The digital Signature is comprised of a 120 bit number – that is 2^{120} or

1,329,227,995,784,915,872,903,807,060,280,344,576 possible combinations.

The encryption layer is 128 bit – that is 2^{128} or

340,282,366,920,938,463,463,374,607,431,768,211,456 possible combinations

With current technology, it would take more time than there are years left in the universe to try every combination (*source : Thawte Security*).