

Why strong authentication is essential to secure SSL VPN's

Who are you?

The popularity for SSL VPN systems is due to the increased demand from our users to provide *Anywhere Access* to our most sensitive business systems.

We need to allow our trusted users to connect to our core business applications from any convenient computing device across any public Internet or wireless link, and SSL VPN technology is making this much easier to deliver.

However, this new *Anywhere Access* approach puts the Identity of our users at the centre of our security model, with the critical question being: '*Is each remote user really who they claim to be?*'



SSL VPN delivers easy, *Anywhere Access* but is each remote user really who they claim to be?

From Fortress to Airport Security

To meet the demand for *Anywhere Access*, we can no longer build 'fortress' style IT security where we simply trust everything on the inside and regard everything outside as hostile.



With SSL-encrypted web connections from teleworkers, Extranet sessions from clients, wireless Lans in the boardroom and the boss wanting to read his e-mail from an Internet café on holiday, the security model we have to build is much closer to that of an airport.

You have to accept all-comers into your outermost, low security areas, but as individuals request access to more sensitive resources, you filter and control them according to their identity and their access privileges.

Identity is the foundation of trust

As in an airport, trust is entirely based upon the individual's identity and authorisation level which must be proved at each checkpoint they pass. Instead of showing their passport and visa to an Immigration Officer, the on-line user is challenged by their organisation's SSL VPN server or other access control device to present their 'digital identity' which comprises their *Username* plus their *Authentication Credentials*.

Given that the user may be connecting from any web-connected computer anywhere, we are now *entirely reliant* on this digital identity to differentiate our trusted users from the rest of humanity on the Internet.



The threat of Identity Theft

Your users' digital identities are their keys to your critical business systems. If a user's password or other authentication credentials are stolen, shared or borrowed, then that user's entire digital identity is compromised.

In the wrong hands the stolen identity can be used to impersonate the victim and gain access to your most sensitive resources. This is Corporate Identity Theft.

It is difficult to protect your systems once you have suffered Identity Theft. An imposter can present another person's stolen identity to your SSL VPN or other perimeter defence systems, and will be allowed to enter without further challenge. Given that their session will be logged as being that of the registered user, it is unlikely that their activities will ever be reviewed or detected.

Authentication is key

Given that Identity Theft is now the world's fastest growing crime (U.S. Federal Trade Commission 2005), we must take a long hard look at:

- How we authenticate the identity of each remote user,
- The forms of authentication credential that can be used securely from an unknown location on an untrusted PC,
- How we issue these identity credentials to our users,
- How we manage and support our users over their working life to keep their identities secure and private at all times.

The Problem with Passwords

For many organisations rolling out SSL VPNs, the classic 'username and password' combination is all that stands between their most sensitive business information and hostile prying eyes. Static passwords can provide only 'weak authentication' of a user's identity. They must be re-used every time the user logs in and can be easily snooped, phished, cracked or guessed by an attacker.

If the password can be acquired by snooping the user's network connection or installing a simple keyboard logging device or Trojan software on the user's machine, then the password can be reused by the attacker time and time again.

Once someone's username and password has been hijacked, that person's entire digital identity is vulnerable and the attacker instantly acquires all the privileges of his/her victim. All this can happen without the victim being aware that their password has been compromised and, if the attacker is careful, no-one may ever know that the attack has happened.

With the weak authentication provided by standard passwords you can never be really sure that a user is who they claim to be.



Hardware keystroke logger

What form of Strong authentication credentials are best?

Stronger forms of authentication credentials that a user can present to rigorously validate their identity can take many forms: a one-time passcode, a token, smartcard, biometric or any combination of these factors.

Typically a user must present two different forms of credential:

- **Something the user knows:** a secret PIN or password
- plus
- **Something the user has:** a unique token, smartcard, mobile phone, PDA or other uncloneable device

Despite the claims of the various manufacturers – there's no one form of strong authentication credential that is ideal for all users and applications.

One-time Passcodes: the user presents a different passcode every time they login, which means that even if a user's session is snooped, the copied passcode cannot be reused. OTP's can be sent on request to a user's mobile phone or PDA by SMS or e-mail. They are ideal for *Anywhere Access* because the user is not tied to logging in from any specific PC.

Tokens: typically tokens (eg RSA SecurID) are used, in combination with a secret PIN, as the most secure and convenient to generate One-time Passcodes. They are ideal for any form of corporate remote access: whether VPN, Web or RAS based.

Smartcards & USB Smartkeys: used to securely store a user's PKI digital certificate, these devices can be used to 'digitally sign' documents and most appropriate for corporate 'Single Sign-On' and hotdesking projects where the users will always be logging in from a corporate-controlled PC or laptop. Modern 'Combo' tokens can now support both OTP and USB smartkey authentication methods.

Biometrics: despite generating many column inches in the press, fingerprint, iris and other forms of biometric authentication are mostly used for physical access security rather than as a digital ID for network access. The user is tied to a using a computer with an appropriate reader or scanner attached, so most biometrics are not suitable for SSL VPN based *Anywhere Access*.

No one system fits all needs

The reality is that each of these forms of authentication is appropriate for different users and in different applications. There's no one perfect system that fits all needs and budgets. Larger organisations often find that they need to implement several different authentication systems to support travelling staff, teleworkers, supply chain and consumer access.

This can end up in an Identity Management nightmare where people find they have to carry different digital ID's and authentication credentials to access different systems and applications.

Identity Management takes more than just technology

Whatever form of authentication that you choose to implement, you will find that secure identity management cannot be delivered by technology alone. To handle the roll out of devices, PIN's and passwords to a widespread user base you need well integrated policies, procedures and logistics, and then you need to provide your users with lifetime management and 24x7 support to ensure your that their digital ID's are secure and can be trusted at all times.



How Signify delivers Secure Identity Management

Signify is unique in delivering strong user authentication as a fully managed service, making it straightforward, quick and cost effective for organisations of all sizes to roll out and enforce secure digital ID's across their user community; whether they have 5 users or 50,000.

Signify's Service Portfolio includes:

- **RSA SecurID from Signify** - based on the market-leading RSA SecurID token
- **Signify Passcode OnDemand** - delivers secure one-time passcodes to your mobile phone or PDA by SMS or e-mail
- **Signify SmartID** - USB Smartkey based authentication and digital signing (PKI)

Consistent management via the Signify IMC

All these services are managed via Signify's innovative web-based **Identity Management Centre** (IMC). This allows clients to mix and match the appropriate forms of authentication to fit the requirements and budget of different projects and user groups, without having to run multiple back-end authentication systems.

Signify's service takes care of not only of the authentication technology, but also the softer, human aspects of Identity Management such as security policy definition, device provisioning and replacement, end user support and emergency access.

Signify provides a complete framework for **Secure Identity Management** which you can quickly adopt, integrate into your e-Business applications and roll out to your users without having to go through the pain of building the entire technical, procedural, logistics and support framework from scratch.



Signify delivers secure, simple sign-on to your desktop, network, applications and on-line services.