Why "Identity" Is Central To IT Security
by John Stewart - CEO and Co-Founder of Signify - Monday, 29 November 2004.

The increasing demand from our users to provide ‘Anywhere Access’ to our most sensitive business systems; allowing them to connect from any computing device across any public Internet or wireless link, is forcing us to take an entirely new approach to securing our networks and data.

This new 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?’ Also, it makes us take a long hard look at how we define the policies and procedures of Identity Management: how we issue the digital identities to our users and support them over their working life to keep their identities secure and private at all times.

From fortress to airport security

To meet this 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 VPN connections from teleworkers, Extranet web 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 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 Web Portal, VPN or RAS server to present their ‘Digital ID’ which comprises their Username plus their Authentication Credentials.

This Digital ID is then verified against an Authentication Server to ensure that the credentials match the identity, and that the individual has the appropriate level of authority to be allowed access.

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.

What form of Authentiation Credentials are best?

The authentication credentials that a user presents to validate their identity can take many forms: a standard password, a one-time passcode, a token, smartcard, biometric or any combination of these factors. Despite the claims of the various manufacturers – there’s no one form of authentication credential that is ideal for all users and applications.

Passwords: while suitable to protect low grade resources it widely accepted that passwords are too weak to protect the digital ID’s of corporate users. They can be so easily be guessed, snooped, copied or cloned that IdentityTheft becomes easy for an attacker who can walk through your firewalls and other defences using the stolen ID. With passwords you can never be really sure that a user is who they claim to be.
One-time Passcodes: the user presents a different passcode everytime 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.
Biometrics: despite generating many column inches, fingerprint, iris and other forms of biometric authentication are mostly used for physical access security rather than as a digital ID for network access. Again, the user is tied to a using a computer with an appropriate scanner, so most biometrics are not suitable for 'Anywhere Access'. The exception is voice authentication which has significant promise in this area.

No-one system fits all

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 Managment 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 24x7 support to ensure your that their digital ID's are secure and can be trusted at all times.