# Thoughts on "Authenticating the Person"

A Sevan White Paper

Sevan has received feedback that claims that certificate-based authentication is authenticating the computer, not the person. This note compares certificate-based authentication to other forms of authentication. We conclude that all forms of authentication are based on assumptions, which may or may not result in "person authentication".

The OSI security model broadly categorizes all authentication schemes into three classes or combinations thereof:

- Something you know (typically passwords)
- Something you have (e.g. SecurID card or certificate)
- Some physical trait (e.g. Fingerprints or face recognition)

## Do password systems authenticate a person?

Rather than authenticating the owner of the password, password systems only verify knowledge of the password. When passwords are stolen or shared, the binding between the password and its owner is broken – the password no longer authenticates the owner.

The conventional wisdom is that the owner memorizes and protects the password so no one else knows the password. Real-life experience with password systems proves otherwise. Passwords are written down, shared, guessed, cracked, obtained through "social engineering", and are usually available to the administrators. From a practical perspective the binding between the owner and his password is just an approximation, and not a very good one at that.

We conclude that passwords do not authenticate a person.

## Do tokens or certificates authenticate a person?

Again, these schemes only verify possession of the "something you have". In the event that a thief gains access to the "something", the thief steals the owner's identity. For this reasons token cards are always backed up with passwords, providing a second-factor of authentication.

Similarly, if a thief gains access to your certificate, he can easily become you. More accurately, the thief must access your private key rather than your certificate. Unfortunately, the market has blurred the distinction between the private key and the certificate.

As with tokens, all trustworthy certificate systems have protections against a thief accessing your certificate. Examples include:

- Maintaining the certificate (actually the private key) on a tamper-resistant smart card or USB token, this can be kept with the owner (in a pocket or purse).
- Protecting the certificate with a PIN. PIN protection is supported by all main-stream smart cards, and tokens.
- If the certificate is stored on a computer, protecting the computer with a password. All modern operating systems have password protection.

### Do physical traits authenticate a person?

Only biometrics comes close to actually authenticating the person. However, even distinctive personal traits (e.g. voice or finger prints) can be manipulated so the biometric becomes a "something you have" authentication. When the attacker uses a voice recording or a mold of a finger, biometric authentication does not authenticate the person.

### Summary

We hope that this discussion clarifies the "authenticate the person" question. The short answer is that under the correct circumstances all methods authenticate the person. Conversely, any authentication scheme can be fooled so it does not authenticate the person.

We would like to finish this note with some thoughts on the value of certificate-based authentication. Sevan Networks chose certificates for the following reasons:

- Certificate-based authentication is supported by all browsers – no need for special software on the browser.
- Certificate-based authentication is the only method that allows the user to authenticate to un-trusted (possible unscrupulous) web sites without exposing sensitive information.
- Authentication to a PC is no longer an issue since computing devices dedicated to a particular person have become common place, whether the desktop, laptop, or palm computer.
- Sensitive personal and enterprise information is being stored on these personal computers, which demands protection of these computers. The certificate merely becomes yet another piece of sensitive information that is protected by the operating system.