9. Authentication

9.1 Reasons for authentication

Management would normally want an authentication system to be implemented. This should preferably be a single system, e.g. not different log-ons for e-mail, PC access or the Internet. Many network optimization strategies rely on authentication – for example, for the enforcement of usage policies (to identify users who break the rules described in the policy).

It is recommended that all users sign the policy document before they are given an account to log on to the network. It is not a good idea to let users use the Internet without logging on, because there is no way of knowing why large amounts of bandwidth are being used, why the connection is slow at certain times, and who is abusing the system.

Activities such as hacking into other systems are also less likely if everyone has to log on.

Authentication improves security, enables administrators to trace problems to specific users, and allows the option of charging for usage.

9.2 Authentication systems

Different authentication systems are discussed in Appendix A; there is a technical description of the various systems that enable a single log-on across all systems. This is necessary because most users can deal with only one password; password administration otherwise becomes too difficult. Modern operating systems such as Windows XP, Windows 2000, Windows NT and Linux can all be used to authenticate from a single user directory. While the log-on of older operating systems such as Windows 95, 98 and ME can easily be bypassed, it is possible to enforce a log-on for these systems before users access the Internet. When users open their Web browser and try to access the Internet, they are first presented with a log-on dialog box; they cannot access the Internet before entering their username and password.

On these systems, it might be preferable in a multi-user environment for the institution's Web-based e-mail service to be used rather than an e-mail client. This is because Windows 95, 98 and ME don't support multi-user profiles properly, and therefore cannot keep different users' e-mail separate. Additionally, using Web-based e-mail on these systems allows for authentication to take place in the Web browser instead of at operating-system level.

9.3 Password creep

Password creep is when users share passwords to get around difficulties caused by a strict but ill-conceived security policy. Where a desire for security introduces multiple barriers to users, such as separate passwords for different applications, or regular changes to them, users will start to freely exchange passwords just to get to the Internet or to get their work done. In this way, what was intended to be a highly secure system can become very insecure and the measures become counter-productive. When this occurs, management must recognize that the password policy has failed and needs to be revised. These principles should be followed:

- Password security should be easy for users.
- A single authentication scheme should be implemented. If an e-mail password is not the same as the password used to log on to the workstation or network, users will switch to commercial Web-based e-mail when they have a problem.
- User log-ons should be equivalent where possible – there should be no reason why users would want to find out what someone else's log-on is because that log-on enables them to do more. User log-ons should not give the user access to anything that needs to be protected by strong security.

If these principles are applied, there should not be an incentive for 'password creep'.