Why do we need to use these certificates? Why can't we just use login and password?

Why do we need to use these certificates? Why can't we just use login and password?

Answer

If MIT had only one web site or only one administrative application, then indeed a login name and password would suffice. However we have many websites at MIT that require "logging in" and we will have more in the future. Each site that requires a different login name and password is another opportunity for a security risk. Certificates provide a way to have "single sign on" where we authenticate once and then can access any site at MIT that accepts certificates for logging in.

There are other ways of obtaining single sign on, however they have their own set of problems/issues. After a certain amount of configuration and education, certificates provide a secure and convenient method of deploying institute wide authentication services.

Certificates are used at MIT today just to provide for web authentication. However the same certificate that you use today for web authentication may in the future be usable for other applications. An interesting potential future application is for secure electronic mail. The technology already exists, but is not yet easy enough to use for IS&T to formally support it.