- Communications Level
- Framework Providers
- Web Services Providers
- Security Products
- Supporting Levels

K. Apshankar et al., *Web Services Business Strategies and Architectures*
© Apress 2002
Web Services Security

At the InfoWorld Next Gen Web Services conference in January 2002, 51% of the attendants considered security the single largest obstacle to general acceptance of Web Services. Are these fears warranted, or are these people just scared of something they don't fully understand? Is the security of Web Services so precarious? Can we overcome these problems so that businesses and the general public will trust these services? We'll take a look at these issues trying to evaluate the situation. We don't pretend to be comprehensive but instead touch on the most important issues.

First we should take a look at the participants in this game. We can distinguish four basic roles related to Web Services (some institutions could support combinations of them):

- **Provider** – This is a person or business that creates a Web Service and places it in a public repository. They only want authorized customers to access their services.

- **Keeper of repositories of Web Services** – These are the institutions that provide public catalogs of services. They must assure authorized access to these catalogs.

- **Keeper of Web Services** – These store the Web Services code and data. They may be the same as the keepers of repositories or the Web Services providers, but could also be specialized institutions.

- **Consumer of Web Services** – They expect high quality services without malicious software. If they send their data to a Web Service, this data should be used in the proper way and protected from leakage or corruption.

The expectations of these roles imply in turn the following security requirements:

- Secure authentication between principals. This is a precondition for applying authorization to access Web Services.