Managing security within the Database Engine is one of the most important tasks for a database administrator. Controlling access to SQL Server and the roles and rights that each user has within SQL Server, as well as the security of the data, are the main security concerns. Throughout this chapter, our goal is to discuss security in the manner in which we believe security measures are encountered: Windows security, SQL Server security, database security, and then protecting the physical data itself.

**Note** Security starts with the physical security of the equipment, network security, and detailed information about Windows security. But detailed information outside of Windows authentication and discussing the available options in the SQL Server Configuration Manager is beyond the scope of this book.

### Security Language

In SQL Server 2005, Microsoft introduced several new security features and changed the verbiage used when discussing security. Granted, terms like users, roles, and permissions still exist, but new words like principals, schemas, and securables emerged into discussions. SQL Server 2012 utilizes the same verbiage, so we want to make sure you are clear on the new terms and what they mean. Figure 7-1 provides a good visual representation of the security features and how they relate to each other. You may find it helpful to refer back to Figure 7-1 throughout the chapter as we discuss these features.
Principals

Principals are entities or objects that can request and access objects within SQL Server. There are three basic types: Windows’s principals, SQL Server principals, and database principals. The following list briefly defines the three types:

- Windows-level principals are generally domain and local server user accounts that authenticate to SQL Server using Windows authentication.
- SQL Server-level principals are SQL Server logins that authenticate to SQL Server using SQL Server authentication.
- Database-level principals are database users, database roles, or application roles.

Keep in mind that you have to map Windows and SQL Server principals to database principals in order to access the objects within a database.