

## Real-World Scenario 15-1: Understanding PKI

**Scenario:** Your boss wants you to set up a new website for customers that will allow for a secure login directly on the home page. Your task is to locate two vendors of SSL certificates that have up to 256-bit AES encryption and offer RSA encryption for key exchange.

Identify two SSL certificate vendors and describe their services.

Define what an SLA is.

Explain what happens if more than a certain number of users connect simultaneously.

## Real-World Scenario 15-1 Solution

There are plenty of Secure Sockets Layer (SSL) certificate providers. Examples include VeriSign, Comodo, and GoDaddy. The more trusted providers (such as VeriSign) use that trust to increase the price of their products.

A typical SSL certificate from VeriSign will offer RSA 2048-bit asymmetric key exchange with some type of SHA hashing, as well as variable symmetric session encryption. As of the writing of this book, it is common to have 256-bit AES for a certain number of users, and any users who connect beyond that get 128-bit AES or RC4 connections.

**NOTE** Remember that as of 1/1/2017, SHA-1 should be replaced with a more secure cryptographic hash.

An SLA is a service-level agreement, which is effectively a contract defining the terms of service. It is discussed more later in the book.

It's important to note that this technology changes quickly. Encryption methods are often considered uncrackable—that is, until they are cracked, and then there is a complete paradigm shift in the technology once again. It's unavoidable. For example, in 2009, a lot of websites used Triple DES (168-bit) for the session data. AES was still gaining traction, but now (as of the writing of this book) AES is the standard and Triple DES is all but extinct. Chances are, the algorithm of choice will be completely different every five years or so. Make sure you don't sign SLAs that have a span of more than two years. Keep the contracts short, review your technology (and the PKI used) often, and reconsider your options as time goes on.

**Video Solution:** Watch the video solution “15-1: Understanding PKI.”