

Real-World Scenario 15-2: Certificate Creation Example

Scenario: Examine the figure below. What are we attempting to accomplish using the syntax that was typed?

A terminal window with a dark background. The title bar shows three window control icons and the text 'lamprocles@workstationB: ~'. The terminal content shows the command 'openssl req -new -sha256 -newkey rsa:2048 -nodes -keyout key.pem -out req.pem' being entered at the prompt 'lamprocles@workstationB:~\$'.

```
lamprocles@workstationB: ~  
lamprocles@workstationB:~$ openssl req -new -sha256 -newkey rsa:2048 -nodes -keyout key.pem -out req.pem
```

Real-World Scenario 15-2 Solution

We are looking at the terminal in Linux (specifically, Ubuntu 14.04). The syntax that was typed will start the SSL certificate request process to a certificate authority (CA); for example, VeriSign. OpenSSL is installed to this version of Ubuntu by default, but other versions of Linux might need OpenSSL installed before attempting this task. Client versions of Windows will definitely need OpenSSL installed first.

The certificate signing request (CSR) starts with the creation of a private 2048-bit RSA key. In this scenario we are hashing the process with SHA256 and are creating two files: the private key (called key.pem) and the certificate request file (called req.pem). These are both sent to the CA.

Video Solution: Watch the video solution “15-2: Certificate Creation Example.”