Seguridad SSL/TLS

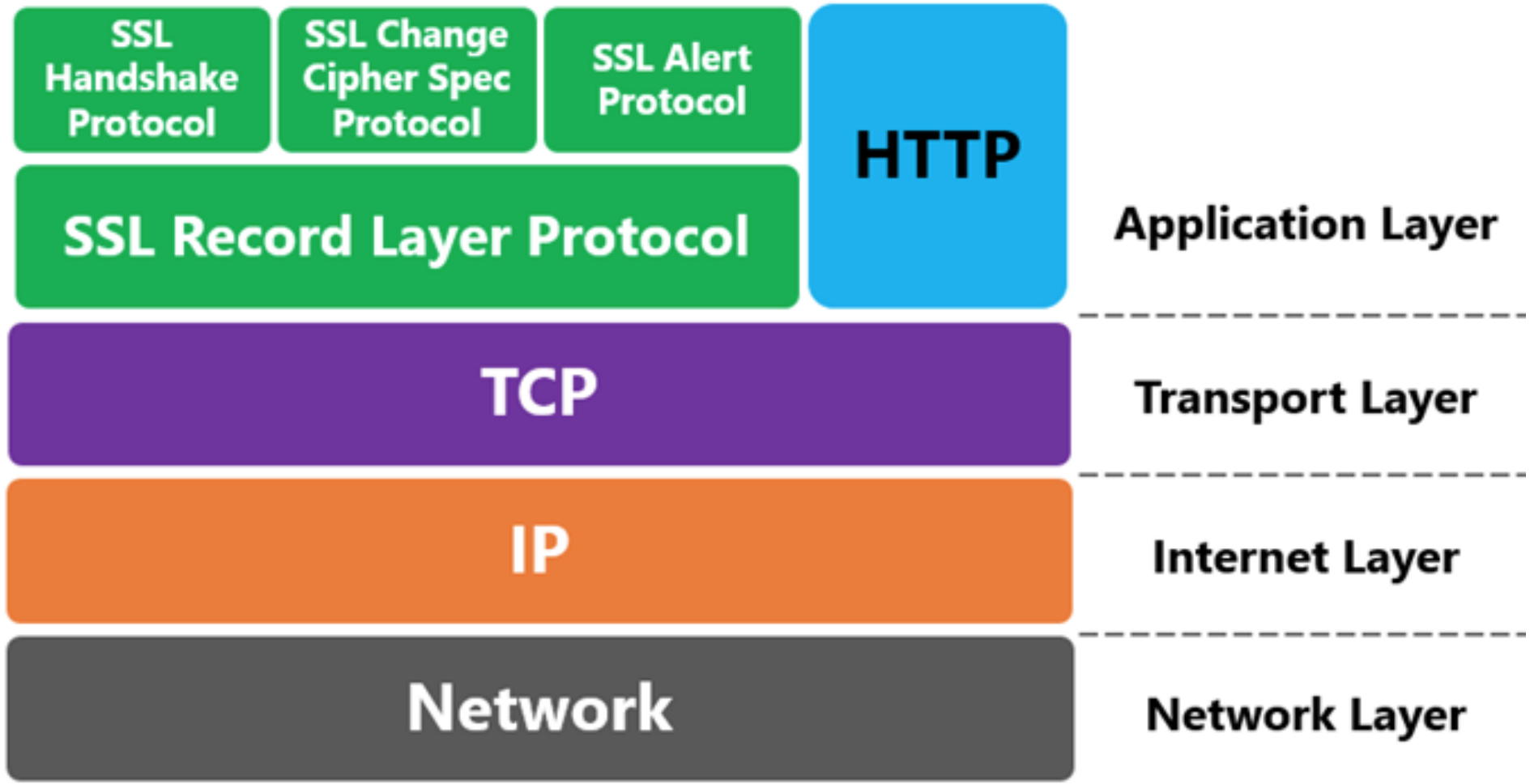
Agenda

- SSL/TLS
- Java Secure Socket Extension (*JSSE*)
- Truststore y Keystore
- Mutua autenticación

SSL/TLS

- Desarrollado originalmente por Netscape, la versión 2.0 se presentó en febrero de 1995
- Es independiente de la aplicación
- Última versión SSL v3 presentada en 1996
- Sucesor: TLS (Transport Layer Security)
  - Muy similar a SSL v3 (1999)
- Provee autenticación, integridad y privacidad
- Actualmente TLS 1.2 (RFC 5246, Agosto 2008)

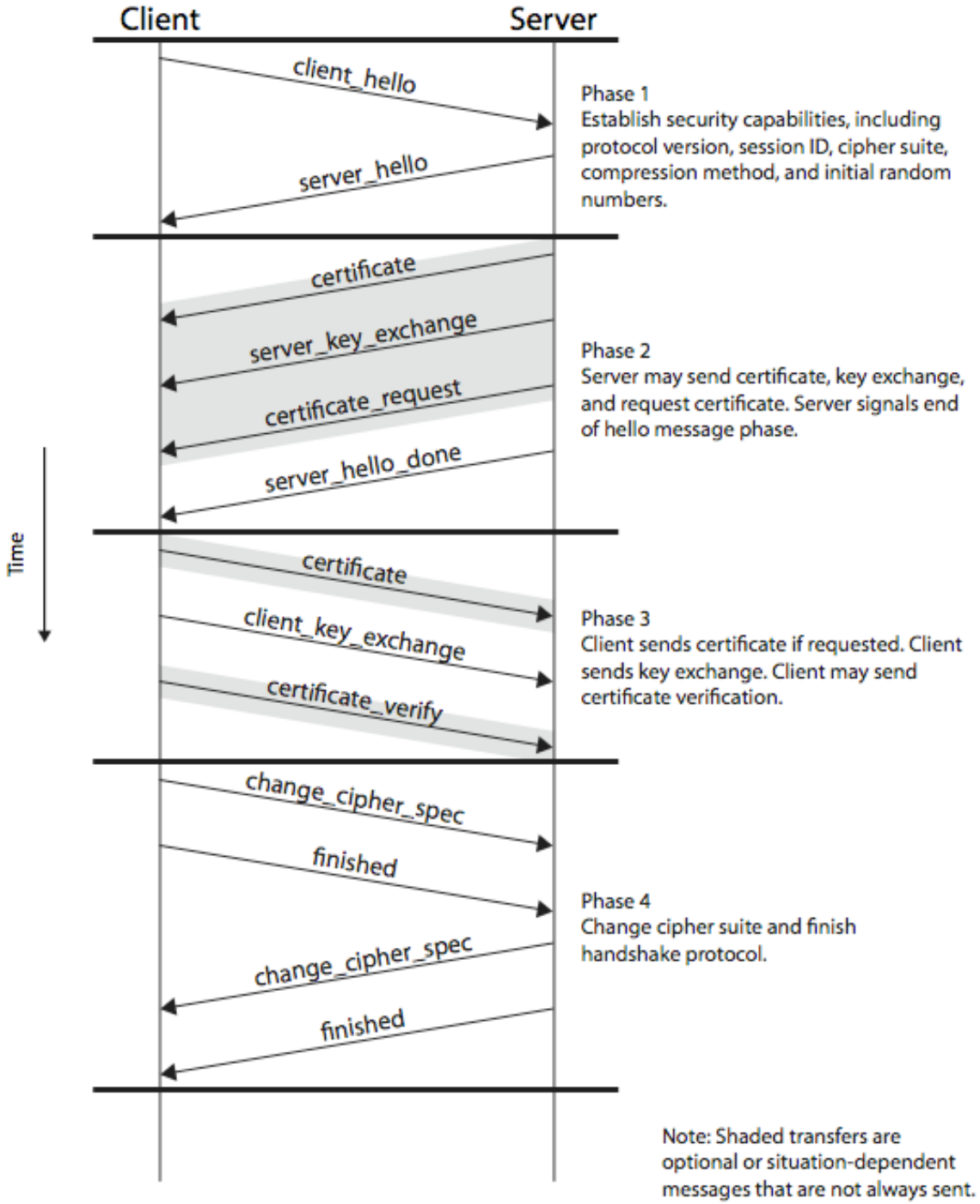
Arquitectura SSL



Arquitectura SSL

- SSL Record layer Protocol
  - Confidencialidad, autenticación, y protección
  - Define el formato para intercambiar los datos
- SSL Alert Protocol
  - Gestiona la sesión SSL y los mensajes de error
- Change Cipher Spec Protocol
  - Registros CCS se utilizan con el fin de indicar un cambio en los códigos de cifrado.
  - Se utiliza normalmente como parte del Handshake.
- SSL Handshake Protocol
  - Intercambio de claves

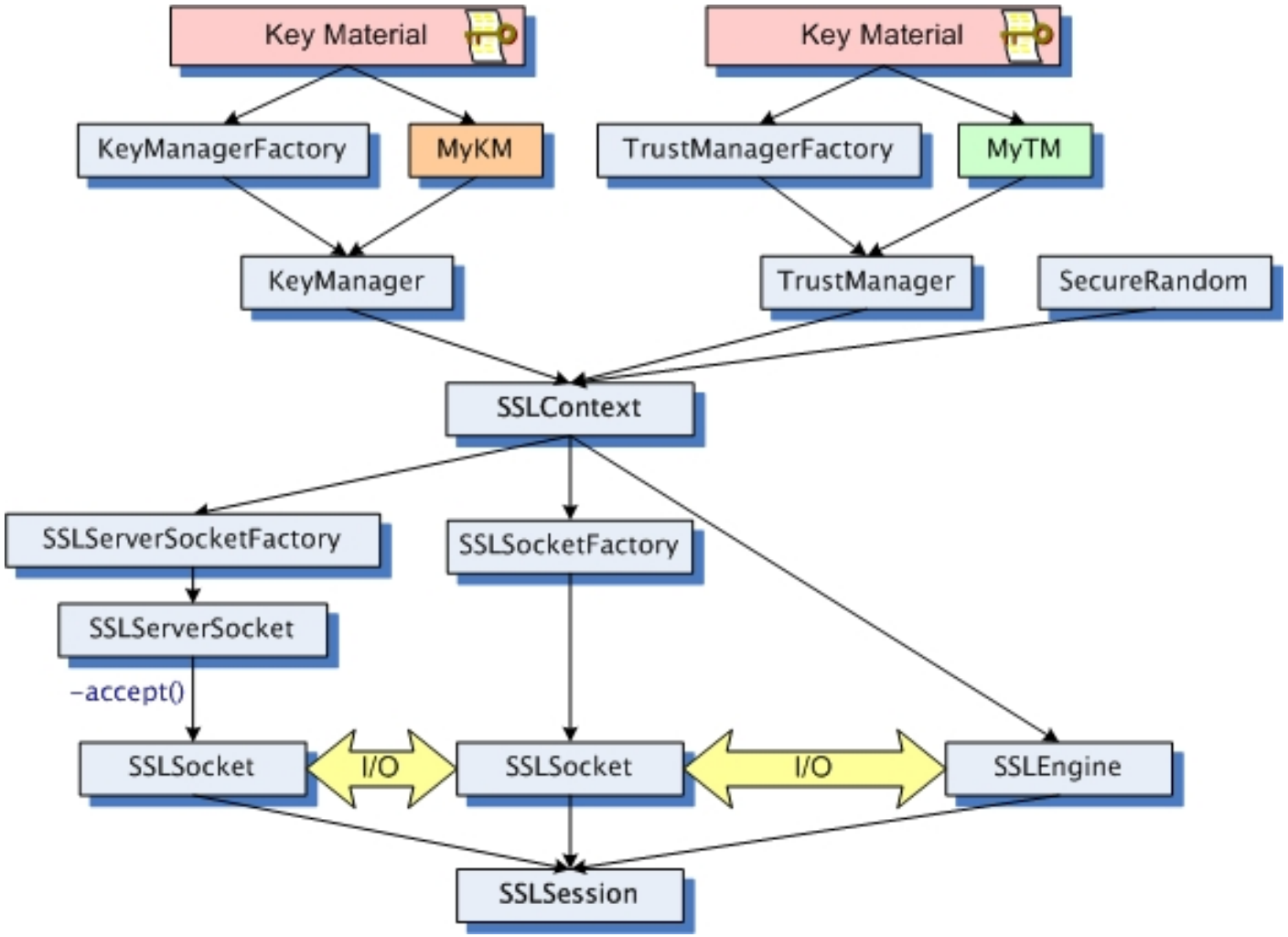
SSL Handshake



Java Secure Socket Extension (*JSSE*)

- Implementa SSL y TLS
  - SSLSocket (usado por los clientes)
  - SSLServerSocket (usado por los servidores).
- Representacion de socket context (SSLContext).
  - SSLEngine
  - SSLSocketFactory para SSLSocket
  - SSLServerSocketFactory para SSLServerSocket
- Interfaces Key y trust manager (X.509 especifica)

Java Secure Socket Extension (*JSSE*)



Truststore y Keystore

- Keystore
  - Repositorio de claves privadas
  - Claves publicas (Ej configuracion ssl)
  - PKCS12 y JKS
- Truststore
  - Igual que la keystore en formato
  - Solo para certificates de confianza
  - CA certificates
- Keytool herramienta para manejo de Keystore/Truststore

Mutua autenticación

- 2WAY authentication
- Autenticación y no repudio
- Requiere certificado del cliente

Mutua autenticación (Ejemplos)

- Tomcat
  - `clientAuth="true"`, (want | true | false)
- Jboss/Wildfly
  - Wildfly verify-client="REQUIRED" (REQUESTED | REQUIRED | NOT_REQUESTED)
  - `Jboss verify-client="true"`, (want | true | false)
- Apache httpd
  - `SSLVerifyClient require`, (optional_no_ca | optional | none | require)
- Nginx
  - `ssl_verify_client on`, (on | off | optional | optional_no_ca)

Ejemplos y referencias

- Ejemplo webapp ssl https://github.com/wildfly/quickstart/tree/10.x/helloworld-war-ssl
- Ref keytool http://docs.oracle.com/javase/8/docs/technotes/tools/windows/keytool.html
- Comandos mas usados https://github.com/fedesierr/cap/wiki/The-Most-Common-Java-Keytool-Keystore-Commands
- Authentication Modules Wildfly https://docs.jboss.org/author/display/WFLY10/Authentication+Modules