Autenticación multifactor basada en «tokens»

El empleo de tokens o dispositivos físicos (como llaves USB o smart cards) se utiliza para la autenticación por múltiples factores. Esta conlleva autenticar al usuario en varios niveles, en la conocida «Autenticación de doble Factor (2FA)»: primero se accede mediante usuario/contraseña y luego se introduce un «código de un solo uso» enviado ya sea por SMS, correo, o generado en un dispositivo físico (token) del usuario.

Generalmente se utiliza el móvil como dispositivo físico, donde se ha instalado la aplicación que genera el «código de un solo uso». Entre los protocolos usados en la generación de estos códigos están los basados en eventos: OATH – HOTP; y los basados en tiempo: OATH – TOTP. Ejemplo de estos últimos son Authy, Google Authenticator, Microsoft Authenticator, etc.

Los métodos más avanzados sustituyen la generación de los códigos, por claves criptográficas generadas por algoritmos de clave asimétrica, y se denominan Universal 2nd Factor (U2F). Aquí el usuario posee un token, que en el segundo paso de autenticación, debe ser conectado ya sea por un puerto USB, mediante NFC o por Bluetooth. Una vez conectado el usuario deberá pulsar un botón para finalizar la autenticación.

Su ventaja radica en que el código generado no se visualiza en ningún momento, considerándose más robusto que los métodos de generación de códigos a nivel de software. Un ejemplo de estos tokens es Yubikey.