Tipos de (HSM) Hardware Security Module

Dependiendo de los requerimientos, los dispositivos HSM pueden clasificarse en dos tipos:

HSM de Propósito General

Dispositivos HSM que incluyen una variedad de algoritmos de cifrado estándar (simétricos, asimétricos y funciones de hash) con soporte para la interconectividad de la API utilizando el estándar de criptografía de clave pública (PKCS) #11, la interfaz de programación de aplicaciones criptográficas de Microsoft (CAPI), la API de criptografía de próxima generación (CNG), la arquitectura de criptografía de Java (JCA), la extensión de criptografía de Java (JCE) y otros. Estos dispositivos se suelen utilizar en entornos PKI, canales HTTPS, DNSSEC, protección genérica de datos sensibles y criptocarteras, entre otros.

HSM Financiero para Medios de Pago

Dispositivos HSM específicos para la protección de las transacciones de pago que incluyen el uso del PIN (generación, gestión, validación y traducción del Bloque PIN en las transacciones realizadas en TPV y cajeros automáticos), la protección de las transferencias electrónicas de fondos (EFT), la generación de datos para bandas magnéticas y chips EMV en los procesos de producción y personalización de tarjetas, el procesamiento de las transacciones de pago con tarjetas de débito y crédito y la validación de tarjetas, usuarios y criptogramas. Estos dispositivos suelen proporcionar soporte criptográfico para las aplicaciones de pago de la mayoría de las marcas de tarjetas, y sus interfaces de interconexión suelen ser más limitadas que las de los HSM de uso genérico.