Contacto: info@appluslaboratories.com

Evaluaciones de seguridad FIDO

El objetivo de la FIDO Alliance (Fast Identity Online) es reducir la dependencia en las contraseñas de las aplicaciones móviles y en línea, ofreciendo en su lugar un ecosistema de autenticación interoperable basado en la criptografía de llave pública. La FIDO ha desarrollado un esquema de certificación para respaldar el desarrollo y la adopción de nuevas soluciones de autenticación, permitiendo a los usuarios identificar fácilmente las soluciones que ofrecen los mayores niveles de calidad y confianza.

La certificación FIDO permite evaluar la seguridad e interoperabilidad de una solución de autenticación. Los niveles de certificación se refuerzan entre sí, mediante la acumulación de requisitos. En la actualidad, los productos pueden ser evaluados en los dos primeros niveles y se están desarrollando nuevos niveles que incluirán requisitos de seguridad más estrictos.
Applus+ Laboratories es uno de los pocos laboratorios acreditados por la FIDO Alliance para realizar evaluaciones de la seguridad de los sistemas de autenticación.

Aplicaciones de pago móvil

Los servicios móviles compensan constantemente un acceso rápido y fácil con una autenticación de seguridad robusta. El objetivo de la FIDO es dar la vuelta a la situación, conseguir una seguridad en línea más sencilla y una mejor experiencia de usuario, todo ello con mayor seguridad y reduciendo riesgos.
Los proveedores de servicios bancarios y de pago siguen evolucionando sus servicios hacia los servicios móviles y en línea, pero compensan constantemente un acceso rápido y fácil con una autenticación de seguridad robusta. El objetivo de la FIDO es dar la vuelta a la situación, conseguir una seguridad en línea sea más sencilla y una mejor experiencia de usuario, todo ello con mayor seguridad y reduciendo riesgos.
Las certificaciones FIDO de nivel L2 y superiores requieren que usted evalúe la protección de autenticación FIOD contra ataques básicos y escalables. Esta evaluación debe ser realizada por un Laboratorio de Seguridad Acreditado por FIDO.

Trusted Execution Environment

En los niveles superiores al L3, los autenticadores requieren el uso de algún tipo de elemento seguro para proteger los activos.
El TEE ofrece un nivel de protección contra ataques de software generados en el sistema operativo y ayuda en el control de derechos de acceso. Lo consigue alojando aplicaciones sensibles 'de confianza', que necesitan estar aisladas y protegidas del sistema operativo y de cualquier software malicioso que pueda estar presente. El TEE también es adecuado para los métodos de identificación biométrica (reconocimiento facial, sensores de huellas dactilares y autorización por voz), que pueden resultar más fáciles de utilizar y más difíciles de robar que las contraseñas y los códigos PIN.
Estas características hacen del TEE una solución adecuada para añadir seguridad adicional a los autenticadores FIDO. Las certificaciones FIDO de nivel L2 y superiores requieren que usted evalúe la protección de autenticación FIOD contra ataques básicos y escalables. Esta evaluación debe ser realizada por un Laboratorio de Seguridad Acreditado por FIDO.

Biometría

La FIDO suele confiar en los mecanismos de autenticación biométrica para confirmar la identidad de los usuarios. También suele utilizarla como mecanismo de autenticación para acceder o utilizar datos desde un elemento seguro, como por ejemplo el TEE.
Estos mecanismos de autenticación biométrica forman parte de los autenticadores y como tales están incluidos en la evaluación. Las certificaciones FIDO de nivel L2 y superiores requieren que usted evalúe la protección de autenticación FIOD contra ataques básicos y escalables. Esta evaluación debe ser realizada por un Laboratorio de Seguridad Acreditado por FIDO.

Nota: Dado que Applus+ Laboratories está acreditado como laboratorio independiente por varios esquemas de certificación, los ingenieros de Applus+ nunca participan en el desarrollo de producto o la implementación de soluciones, garantizando así su imparcialidad.