FIDO Security Evaluations

The aim of the FIDO Alliance is to reduce reliance on passwords in mobile and online applications by offering a secure, standardized and interoperable authentication ecosystem based on public encryption keys. FIDO has developed a certification scheme to support the development and adoption of new authentication solutions, allowing users to easily identify the solutions which offer the highest levels of quality and trust.
FIDO Certification allows for the security and interoperability of an authentication solution to be evaluated. The different levels of certification build on each other, accumulating the requirements. Currently, products can be evaluated under the first two levels, with more levels currently under development which will include stricter security requirements.
Applus+ Laboratories is one of very few laboratories accredited by the FIDO Alliance to carry out security evaluations on authentication systems.

Mobile Payment Apps

Mobile services are constantly trading off fast and easy access with robust authentication security. FIDO aims to turn that around and make online security a simpler and better user experience while providing stronger security and reducing risks.
Banks and payments services providers continue to evolve service delivery to online and mobile services, but are constantly trading off fast and easy access with robust authentication security. FIDO aims to turn that around and make online security a simpler and better user experience while providing stronger security and reducing risks.
FIDO Certification at L2 and higher require you to evaluate the FIDO authenticator protection against basic and scalable attacks. This evaluation must be carried out by a FIDO Accredited Security Laboratory.

TEE

Beyond L3, authenticators require the use of some sort of secure element to protect the assets.
TEE offers a level of protection against software attacks generated in the mobile OS and assists in the control of access rights. It achieves this by housing sensitive, 'trusted'

applications that need to be isolated and protected from the mobile OS and any malicious malware that may be present. TEE is also well-suited for supporting biometric ID methods (facial recognition, fingerprint sensor and voice authorization), which may be easier to use and harder to steal than PINs and passwords.
These characteristics make TEE a well suited solution for adding additional security to the FIDO authenticators. FIDO Certification at L2 and higher require you to evaluate the FIDO authenticator protection against basic and scalable attacks. This evaluation must be carried out by a FIDO Accredited Security Laboratory.

Biometrics

FIDO typically relies on biometric authentication mechanisms to verify the identity of the users. Biometrics also tends to be used in FIDO as an authentication mechanism to access or use data from a secure element such as the TEE.
These biometric authentication mechanisms form part of the authenticators and as such also are included as part of the evaluation. FIDO Certification at L2 and higher require you to evaluate the FIDO authenticator protection against basic and scalable attacks. This evaluation must be carried out by a FIDO Accredited Security Laboratory.

Note: Because Applus+ Laboratories is accredited as a third party laboratory by several evaluation and certification schemes, and in order to guarantee its impartiality, Applus+ engineers are never involved in actual product development or solutions implementation.