FIDO Security Evaluation Service

What atsec offers

FIDO, short for “Fast IDentity Online”, is a series of authentication standards to help reduce the reliance on passwords. As the accredited security laboratory by the FIDO Alliance, atsec information security (short for “atsec”) offers the following security evaluation services for your authenticator products:

- FIDO2: FIDO2 is comprised of the W3C Web Authentication (WebAuthn) and corresponding Client-to-Authenticator Protocols (CTAP) from the FIDO Alliance.
    - WebAuthn: WebAuthn defines a standard web API that is being built into browsers and platforms to enable support for FIDO Authentication.
    - CTAP2: CTAP2 allows the use of external authenticators (FIDO Security Keys, mobile devices) for authentication on FIDO2-enabled browsers and operating systems over USB, NFC, or BLE for a passwordless, second-factor or multi-factor authentication experience.
    - CTAP1: Formerly known as “FIDO U2F”, CTAP1 allows the use of existing FIDO U2F devices (such as FIDO Security Keys) for authentication on FIDO2-enabled browsers and operating systems over USB, NFC, or BLE for a second-factor experience.
- FIDO UAF: FIDO UAF supports a passwordless experience for online service on users’ own devices with local authentication mechanisms such as swiping a finger, looking at the camera, speaking into the mic, entering a PIN, etc.

The FIDO2 and FIDO UAF protocols have identified within the common specification authenticator security goals. There are 16 Security Goals (SG) identified by FIDO, 29 Security Measures (SM) that can be implemented to cover the security goals for FIDO authenticators, and 10 Security Requirements are derived to support the Security Measures:

- Authenticator definition Derived Requirements
- Key Management and Authenticator Security Parameters
- Authenticator’s Test for User Presence and User Verification
- Privacy
- Physical Security, Side Channel Attack Resistance and Fault Injection Resistance
- Attestation
- Operating Environment
- Self-Tests and Firmware Updates
- Manufacturing and Development
- Operational Guidance

The accredited security laboratories performing FIDO Security Evaluations are listed on the official website of FIDO Alliance: https://fidoalliance.org/certification/authenticator-certification-levels/accredited-security-laboratories/
In addition, atsec is also one of the FIDO members (https://fidoalliance.org/members/) and makes our contribution to the industry.

Why our services are important to you

Passwords and other forms of legacy authentication such as SMS OTPs, are knowledge-based, a hassle to remember, and easy to phish, harvest, and replay. FIDO helps shift from this legacy, knowledge-based authentication scenario to a modern, possession-based and phishing-resistant authentication scenario.

The security testing of the authenticator products against FIDO standards, allows vendors to integrate their authenticators into modern and FIDO-enabled online services, and provide their users with a flawless authentication experience. This also reduces the risk of password forget or stolen.

atsec is ready to partner with you to help you understand the requirements of the standard, test your authenticator products, and achieve the FIDO certification.

The products being compliant with the FIDO2 and FIDO UAF specifications and evaluated by a security laboratory (e.g. atsec) can be certified and listed by FIDO alliance on the official website:

https://fidoalliance.org/certification/fido-certified-products/

For more information

More information about atsec FIDO services and our public resources can be found at http://www.atsec.com and at the FIDO Alliance website at https://fidoalliance.org/