STRONGKEY™

FIDO2 SERVER
A TRUE FIDO2 CERTIFIED® SERVER

HIGHLIGHTS

STANDARD

- FIDO2—latest version of FIDO
- Works w/any FIDO Authenticator
- FIPS-certified Level 2 Trusted Platform Module (TPM)
- Open source development
- Key management
- Apple- and Android-compatible
- No per-user fees
- Single-tenant philosophy
- On-prem/hosted/private cloud deployment options
- Customer-focused architecture

OPTIONAL

- Hardware Security Modue (HSM)
- Encryption and Tokenization

EXPERIENCE

- Early member and frequent contributor to the FIDO standard through working groups and white papers
- Proven on 6 continents in a variety of implementations
- Compatible with any FIDO Certified® FIDO2 Authenticator
- Easy adoption; global support

STRONGKEY
DURHAM, NC
&
CUPERTINO, CA
GetSecure@StrongKey.com
STRONGKEY.COM
+1 408-331-2000

StrongKey joined the FIDO Alliance in 2014, built a U2F server in 2015, and our FIDO2 Server was **among the earliest certified**—and being FIDO Certified® matters—this isn't just "supporting" or "complying" with FIDO protocols.

FIDO FOR EVERYONE

FIDO2 authentication will soon be an industry norm. We believe in the standard so much that we've made our server available freely and openly on GitHub.
For those who want more support, security, and integration help, we're there for you.

FIDO FOR ANDROID AND IPHONE

Tellaro open source software solution enables Android devices to serve as FIDO authenticators use FIDO security keys for authentication without the need to register a Google Play Services account. StrongKey now also now supports Apple Attestation, enabling current iPhones to use platform FIDO keys with a native iOS app.

- Support for FIDO on Android (version 9 or later) apps to use FIDO without needing a Google Play Services account
- An Android client library that uses the Android KeyStore, leveraging a Trusted Execution Environment (TEE) or a secure element
- FIDO registration, authentication, and transaction authorization leveraging Android biometric prompts
- Turns current iPhones into authenticators with a native iOS app that calls WebView to perform the registration/authentication

FIDO SINGLE SIGN-ON

StrongKey's open source FIDO Certified® passwordless authentication solution enables single sign-on across DNS domains without the need for an external SSO platform, significantly reducing cost and improving manageability. The StrongKey SSO solution is designed for businesses of all sizes that want to migrate away from less secure SSO implementations that use multi-factor authentication (MFA) and one -time passwords (OTPs) that are vulnerable to phishing attacks and credential theft.

- Built-iln Single Sign-on (SSO) across multiple DNS domains
- Java library for web application verification of a JSON web token (JWT) using a JSON (JWS) signed with X.509 certificate-based keys
- Security Policy Module that permits a relying party (RP) to define and update FIDO security policies without re-coding

STRONGKEY™

FIDO2 SERVER

SECURITY FIRST

We have a single-tenant philosophy, and your cryptographic keys stay in your control. Our appliances make use of a standard Trusted Platform Module (TPM, FIPS Level 2-certified), or a Hardware Security Module (HSM, FIPS Level 3-certified). We have identified vulnerabilities in traditional FIDO deployments and have structured our product to protect against them.

UNCOMPROMISINGLY OPEN SOURCE

Traditional authentication companies charge per-user, per-month fees, which stack up quickly. StrongKey is an open source company, with the world's first FIDO2 Certified® open source FIDO2 server. This means no license fees and straightforward, flat pricing.

Scale your FIDO deployment without scaling your costs.

FLEXIBLE IMPLEMENTATION

StrongKey's FIDO2 Certified® Server is available **as an on-prem appliance,** as a **hosted solution** at our secure data centers, or set up in **your own private cloud environment**.

POWERFUL ADDITIONAL FEATURES

We're a data security company—not a FIDO company. We provide:

- Key management
- Encryption/tokenization (**Pseudonymization**)
- Risk management
- Regulatory compliance: **GDPR CCPA PSD2 PCI DSS**
- Payments and **card capture services** (CCS)
- Digital signatures on every send

These features are often on the same appliance as our FIDO2 Server.

We help you findyour best solution—not just what we sell.

ABOUT STRONGKEY

StrongKey (StrongAuth, Inc.) makes data breaches irrelevant by redefining how businesses and government agencies secure their information against the inevitability of a breach. While other security companies focus on protecting the perimeter, StrongKey secures the core through strong authentication, encryption, digital signatures and hardware backed keymanagement—keeping the core safe even with an attacker on the network. Based in Silicon Valley, CA and Durham, NC, StrongKey has provided cryptographic security solutions to companies such as AT&T, Pfizer, Xerox, Allergan, StubHub, and SurveyMonkey, among others.