FIDO User Authentication
Vendor Self-Assertion Checklist

This self-assertion checklist provides information about an implementation’s security, privacy, and feature support for authenticators, clients, and servers. By filling out this checklist you acknowledge your implementation meets the requirements selected. Please complete the appropriate sections for your implementation.

Note: some checklist items represent specific requirements described in the normative sections of FIDO specifications. They are called out again here to emphasize the critical nature of the requirement for meeting FIDO Security Requirements and Privacy Principles.

All Vendors: Authenticators (FIDO2, U2F, and UAF) and Servers

The FIDO product adheres to all guidelines described in the FIDO Privacy Principles*. *Vendors are not required to provide documentation demonstrating adherence to the guidelines but acknowledge and self-attest that the design and implementation of their authenticator, client, and/or server adhere to all guidelines described in the FIDO Privacy Principles.	□
Since passing the conformance tests, no changes have been made to the FIDO product that would alter its adherence to the FIDO specifications.	□

All Authenticator Vendors (FIDO2, U2F, and UAF)

Metadata describing a FIDO authenticator that has been submitted to the FIDO Alliance is accurate and correctly describes the characteristics of the authenticator.	□

UAF Authenticator Vendors

The FIDO authenticator’s Authenticator Attestation ID (AAID) and the associated attestation key pair and certificate are shared only by devices of the same model and security characteristics. At least 100,000 authenticators of a specific model, that are sharing the same AAID, must exist before a new attestation key pair and certificate is obtained.	□
The FIDO UAF authenticator only generates a new key pair to be registered or performs a sign operation with an existing key ONLY after the user verification process defined in the FIDO specifications has succeeded. *This requirement does not apply to silent authenticators.	□

U2F Authenticator Vendors

The FIDO U2F authenticator uses an attestation private key and certificate that is shared among multiple devices in accordance with the FIDO Privacy Principles.	□
The FIDO U2F authenticator only generates a new key handle or performs sign operations with an existing key ONLY after a successful confirmation gesture by the user.	□

FIDO2 Authenticator Vendors

The FIDO2 authenticator uses an attestation private key and certificate that is shared among multiple devices in accordance with the FIDO Privacy Principles.	□
The FIDO authenticator's Authenticator Attestation GUID (AAGUID) and the associated attestation key pair and certificate are shared only by devices of the same model and security characteristics. At least 100,000 authenticators of a specific model, that are sharing the same AAGUID, must exist before a new attestation key pair and certificate are obtained.	□
The FIDO2 authenticator only generates a new key handle or performs sign operations with an existing key ONLY after a successful confirmation gesture by the user or non-gesture with a silent authenticator.	□

FIDO2 Authenticator Vendors: Security Profile and Feature Support

The FIDO2 Authenticator is a Consumer only authenticator.	□
The FIDO2 Authenticator is an Enterprise-only authenticator. Please see the next section for additional questions.	□
The FIDO2 Authenticator is a Consumer+Full Feature Support authenticator.	□
The FIDO2 Authenticator is an Enterprise+Full Feature Support authenticator. Please see the next section for additional questions.	□

FIDO2 Authenticator Vendors: Supporting Enterprise Attestation

The FIDO2 device is an enterprise authenticator, enabled with an enterprise profile, and will only be sold either directly to an enterprise entity or to an enterprise entity through an authorized reseller.	□
The enterprise entity purchasing your FIDO2 enterprise authenticator is going to use the authenticator for the purpose of enterprise authentication.	□

Acknowledgement

We certify that to the best of our knowledge and ability, all that we have asserted in this questionnaire is true.

Company Name	
Implementation Name	
Representative Name	
Representative Email	

____ ________________________

Signature of Vendor Representative Date