FIDO Vendor Self-Assertion Checklist

This self-assertion checklist provides information about the security implementation of the authenticator. 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 FIDO specifications. They are called out again here in order to emphasize the critical nature of the requirement for meeting FIDO security and privacy principles.

All Vendors

The FIDO product adheres to all guidelines described in the FIDO Privacy Principles*. *Vendors are not required to provide the documentation. This item merely acknowledges that the vendor is familiar with industry best practices for cryptographic key generation and management and adheres to those practices throughout a key's lifecycle.	☐
Since passing the conformance tests, no changes have been made to the FIDO product that would alter its adherence to the FIDO specifications.	☐
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 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 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 is 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.			

Acknowledgement

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

Company Name	
Representative Name	
Representative Email	

Signature of FIDO Vendor Representative

Date