FIDO Device Onboard: Privacy Considerations

Final Document, September 13, 2022

This version:
https://fidoalliance.org/specs/fdo-security-requirements/fdo-privacy-policy-v1.0-fd-20220913.html

Editor:
Security and Privacy Working Group (FIDO Alliance)

Version:
1.0

Abstract

The FIDO Device Onboard (FDO) specification provides a method for secure onboarding of IoT devices with minimal user involvement. As with all FIDO technologies, user privacy is important and safeguards are provided within the specification to prevent potential abuses of information that could be used to track a device (and therefore potentially an end user). This document lays out the privacy guidelines for FDO-compliant implementations, and is intended to serve as a basis for FDO security and privacy certification requirements.

Table of Contents

1. Introduction§

The FIDO Privacy Principles document provides several underlying guidelines that are intended to prevent the inadvertent or intentional sharing of personally-identifying information (PII). This document specifically addressed the area of authentication, where sensitive information is collected from the end user (e.g. biometric templates) that would be required for user verification. If biometric template data ever leaves a user's personal device, then the consequences could be dire: a password can be replaced but it is not so easy to replace a fingerprint. Moreover, the typical FIDO authenticator supports multiple scoped credentials, i.e. authentication credentials that are unique for a given relying party. If the usage of the credential is not sufficiently isolated for each relying party then there is a possibility that relying parties can collude and track a given user across their services.

In contrast, FDO devices are often purpose-specific and will only contain a single device identifier and authentication credential at any given instant in time. This is ensured by a process known as Transfer of Ownership (TO). When a device is manufactured, it is initialized with manufacturer-provided credentials along

with an initial identifier. However, when the device is powered up for the first time at the end user premises, it will go through Transfer of Ownership through two protocol exchanges (TO1 and TO2) and emerge with an owner-provided identifier and credential. The only time when a device would change the identifier and credential is either through owner-directed replacement or a factory reset of the device. In this regards, and FDO device can be thought of as following a “single relying party” model, where the relying party is either the manufacturer or the owner.

In addition, it is sometimes the case where neither the device nor the single relying party corresponds to a human being. Such devices might still interact with human beings or their surrogates as part of their operation (e.g., a turnstile for entry to a stadium). However, if the device is known to have no human interaction, whether during or outside of FDO operation, then personal privacy concerns do not apply to this device.

In the FDO system architecture, there are other possibilities for privacy violation beyond the device. An example is the Rendezvous Service (RS). The RS is the first online service that a device contacts during transfer of ownership,and directs authenticated devices to the Device Owner. The RS could be handling requests from devices corresponding to multiple owners, and could also be tracking devices through ownership transition (e.g. factory reset followed by re-initialization of TO). However, privacy protections related to network elements such as the RS are beyond the scope of this document. Rather, this document lays out several underlying privacy principles that are specific to FDO devices and can be used as a baseline for privacy requirements in an overall security certification program. Note that these principles are meant to be complimentary to the existing FIDO privacy principles, and both can be applicable when an FDO device integrates a FIDO-compliant authenticator.

2. All Keys Required for FDO Must only Be Used for FDO Operations§

The credentials and identifiers required for device ownership transfer in the TO1 and TO2 protocol stages must only be used in that context. They must not be used for any operations after ownership transfer completes. DAA keys that cannot be used to trace device ownership (such as EPID keys) may be used for other operations, if care is taken that no other FDO parameter permits tracing of the device after it is onboarded.

3. Ownership Transfer Must Occur Once during a Device Lifecycle§

A device must not undergo ownership transfer again after initial completion unless an action such as a factory reset takes place (where all user data is assumed to be erased). This ensures that user data on the device is not inadvertently shared between device owners.

This is not meant to exclude a device from using FDO multiple times in order to accomplish onboarding multiple hardware or software components within a single device with multiple components. For example, onboarding multiple virtual machines running within the device or a device with multiple hardware-based sub-devices.

4. FDO Attestation Must Contain the Minimum Amount of information Necessary to Complete Ownership Transfer

Permissible FDO attestation formats such as the Entity Attestation Token (EAT) are extensible and can be used to convey information that could effectively fingerprint a device. While this may be desirable in certain contexts such as IoT endpoint protection systems, such “rich” attestation formats must only be supported at the discretion of the owner after ownership transfer has completed. If a “rich” attestation is desired, it may be performed during ServiceInfo, where the TO2 protocol protects the privacy of the attestation.

5. Ownership Vouchers Should Contain the Minimum Amount of information Necessary to Validate the Supply Chain

TO is a mutually-authenticated process. Similar to the goal of only allowing a Device Owner to manage a genuine

device, similarly an FDO device uses the presented Ownership Voucher to determine the legitimacy of the owner. The Ownership Voucher is an extensible chain of signatures, similar in trust function to a certificate chain, and any information in each link must be the minimum necessary for the device to verify. The OVEExtra field SHOULD NOT be used to extend the information in the Ownership Voucher, any information required for the onboarding application MUST be justified. Similarly, the Ownership Voucher entries SHOULD NOT use X5CHAIN encoding and include additional certificates in each OVEntry. If this is needed for the onboarding application, any information there MUST be justified.

> NOTE: although this spec says you SHOULD NOT use OVEExtra and X5CHAIN, we have added these features so they can be used with justification. Any use of this will be evaluated for privacy by the FIDO Certification Secretariat.

Note that the Device can be reset to a factory state as part of a re-conditioning process, invalidating all outstanding Ownership Vouchers for the Device, but support of such a reset is not mandatory and may not be most useful (e.g. in the case of owner-to-owner re-sale using FDO).