Appnote - FIDO Device Onboard: Error Codes and Security Considerations

Final Document, July 10, 2023

This version:
https://fidoalliance.org/specs/FDO/fdo-appnote-2.eror-codes.html

Issue Tracking:
GitHub

Editor:
Giridhar Mandyam (Qualcomm)

Version:
1.0

Abstract

A template for creating an Errata for a published PS

Table of Contents

1. Introduction§

The FIDO Device Onboard (FDO) specification provides a method for secure onboarding of IoT devices with minimal user involvement. During protocol operation, errors [FDO-Specification] may be sent by the associated endpoints due to various issues that may or may not be security-related (i.e. lossiness in the transmission medium, processing errors at the endpoints, etc.). Although an error has occurred, the actual cause of the error may not always be accurately reflected in the error code. This note provides some potential reasons why the error code may not necessarily correspond to the actual error. As a result, endpoints should not rely on the semantics associated with a particular error code in commercial offerings.

2. Use of 3rd-party Libraries§

Certain 3rd-party libraries may be used for processing FDO messaging at a given endpoint. If that is the case, the reason for failure provided by the library may not correspond to the precise reason that the message was not

received correctly. For instance, the error code 001 (INVALID_JWT_TOKEN) may have occurred, but the library may only be capable of returning an INVALID_MESSAGE_ERROR (code 101). Both error conditions may be valid, but the level of specificity is different.

3. Message Corruption in Transit§

A message may be successfully received by an endpoint, but bit corruption could occur to the message within the endpoint (e.g. buffer conditions resulting in bit error instances). Such errors may be manifested as an INVALID_MESSAGE_ERROR in the most general sense, but could also result in more specific errors if they are detectable (e.g. INVALID_GUID, in the case of the TO0.OwnerSign message).

4. Error Messages as an Attack Vector§

Status codes may also be used to hide malicious activity at a compromised endpoint. Although such attacks have not been reported for FDO specifically, similar exploits have been observed with HTTP status codes (see [MALWARE]). A compromised endpoint could use error codes to probe or manipulate any actor in the FDO protocol (device owner, rendezvous server, or IoT device). If the endpoints do not tailor responses to specific error codes then it becomes more difficult for attackers to exploit them.

5. Additional Considerations§

Future versions of the specification can clarify that returning an error MUST occur when a non-compliant message is received, but the actual error code SHOULD correspond to the actual error condition. Moreover, for scenarios where precise error reporting is required, FDO endpoints that support secure debug interfaces could make detailed error information available to authorized entities as opposed to using the error codes themselves. Finally, implementors can make use of the generic HTTP 500 error code for situations where a message was received in error, but the precise reason cannot be identified.

References§

Informative References§

[FDO-Specification]
Geoffrey Cooper; et al. *FIDO Device Onboard Specification*. 19 April 2022. Proposed Standard. URL: https://fidoalliance.org/specs/FDO/FIDO-Device-Onboard-PS-v1.1-20220419/FIDO-Device-Onboard-PS-v1.1-20220419.html

[MALWARE]
Tab Atkins; Bat Snikta. *HTTP Status Codes Command This Malware How to Control Hacked Systems* URL: https://thehackernews.com/2020/05/malware-http-codes.html