Correlating FDO with the Installer

Final Document, July 10, 2023

This version:
https://fidoalliance.org/specs/fidoiot/fdo-appnote-4-correlationid-v1.0-fd-20230710.html

Issue Tracking:
GitHub

Editor:
Geoffrey Cooper (Intel)

Version:
1.0

Abstract

Introduces a correlation ID into the OVEExtra facility. Discusses the responsibilities and level of trust in the FDO installer. Even though FDO follows an "untrusted installer" model, there is still some trust required. Moreover, the work of the installer must be coordinated and correlated with the work of the Owner Server (the "NOC") to be useful.

Table of Contents

1 Introduction

2 Correlation Early in the Supply Chain

3 Supplying Correlation ID's

4 Overriding the Correlation ID

5 Example of how OVEExtraTypeCorID value is used

1. Introduction§

FDO self-describes as following an "untrusted installer" model, where the installer person does not participate in the communications protocol. However, the installer *is* trusted for other things. In particular, the installer is trusted to install the physical hardware and to report accurately what hardware is installed where. This trust is critical to achieving the correct operation of remotely controlled hardware that is installed with FDO.

Consider an installer with a pallet of network-controllable lighting fixtures to install using FDO. We expect the installer to install one lighting fixture in each room. One way to do this is to register each device with a room number in the controlling operations center, then label the room number on each fixture. However, this would require the installer to waste time searching for the right fixture as he moves from room to room. A likely workflow is for the installer to take one fixture, at random, from a pallet of new equipment as he moves from room to room in the most convenient order. Then the installer fills in a form or spreadsheet to show which fixture ended up where. The installer needs an identifier to put on the form, presumably a value read or scanned from the outside of the fixture or the box it came in.

Now we assume that each fixture is turned on. FDO onboards the fixture to the Owner Server, which logs the transaction using fields it has from the Ownership Voucher, the network connection and from FDO.

Now the Owner Server must correlate the information from the FDO connection with the information from the installer, to determine which lighting fixture ended up in each room. The obvious conclusion is that the correlation value must be somewhere in the Ownership Voucher.

There are various ways to correlate the ownership voucher with a device that has been installed. In this App Note, we propose adding a value to the OVEExtra field to perform this function.

2. Correlation Early in the Supply Chain§

We have described how an installer at the end of the supply chain needs to correlate his actions with the Ownership Voucher. A similar correlation can happen earlier in the supply chain.

It is possible for a module that performs FDO to be included in a larger deliverable. For example, a smart lighting module might be included in a lighting fixture; a motor control unit might be included in a window frame with blinds to raise and lower.

In this case, the correlation problem happens in reverse; any correlation ID on the device is obscured, as the device is enclosed within another. One simple solution would be to copy the correlation ID on the module to the external device. However, the external device may already have its own ID or bar code, placed prominently on the case or box, so it might be better to adopt this correlation ID than to try to add another one.

3. Supplying Correlation ID's§

We propose adding an explicit "correlation ID" to the Ownership Voucher, stored as a field in the OVEExtra facility:

```
OVEExtraType = int

# Definitions for CorID as (Type,Value)
# The OVEExtraInfoType is already a bstr, we pack the correlation ID
# directly into it.
OVEExtraTypeCorID     = 2
OVEExtraInfoTypeCorID = bstr
```

where:

- OVEExtraTypeMaxLength indicates the maximum length that an Ownership Voucher segment may have (this is the topic of another App Note).
- OVEExtraTypeCorID indicates the correlation ID.
- OVEExtraInfoTypeCorID is identical to OVEExtraInfoType, which is a bstr.
- The `bstr` value for OVEExtraTypeCorID is the correlation value, encoded into a byte string (e.g., 6 bytes for 48 bits, and so on).

If the value of OVEExtraTypeCorID is chosen as a cryptographic random number, a 48-bit value is likely sufficient even for very large FDO deployments. If the value is chosen from a product-specific numeric space, another size may be appropriate.

A 48-bit cryptographic random number for OVEExtraTypeCorID is recommended.

4. Overriding the Correlation ID§

Since the correlation ID (identified with OVEExtraTypeCorID) appears in the Ownership Voucher entry

`OVEntryPayload.OVEExtra`

it is possible for multiple a correlation ID to appear in more than one Ownership Voucher entry. This is interpreted as the later correlation ID *overriding* the previous ID.

Thus, to obtain the correct correlation ID to use, the Ownership Voucher entries must be scanned, from first to last entry, for the presence of OVEExtraInfoType, and the last value used. This operation may be implemented as a stand-alone scan or as an addition to existing FDO code that scans the Ownership Voucher, such as the code that verifies the integrity of the Ownership Voucher when a new voucher is received.

5. Example of how OVEExtraTypeCorID value is used§

- A chip manufacturer which embeds FDO credentials in a chip (e.g., a TPM) is placed in OVEExtraInfoType in the first entry of the Ownership Voucher. Later the chip is embedded in a module, which inherits the OVEExtraInfoType entry.
- The module is included in a larger device with a bar code on the box, and a new OVEExtraInfoType added to match the ID on the box.
- The larger device is consumed by an installer organization that assigns it a new ID for installation. This is added to the box as a sticker, and the Ownership Voucher extension contains a new OVEExtraInfoType entry.
- The installer scans the sticker and provides information about where the device with this sticker was installed, which is correlated with the Ownership Voucher at the device manager.

↑

→