Large OVEExtra Message Guidance

Final Document, July 10, 2023

This version:
https://fidoalliance.org/specs/fidoiot/fdo-appnote-3-oveextra-guidance-v1.0-fd-20230710.html

Issue Tracking:
GitHub

Editor:
Geoffrey Cooper (Intel)

Version:
1.0

Abstract

OVEExtra message guidance

Table of Contents

1. Introduction§

FDO version 1.1, section 3.4.2 defines a mechanism called OVEExtra. This mechanism permits information from the supply chain to be added to an Ownership Voucher (OV). The information is signed as part of the OV and is sent to the Device during the TO2 protocol. The device verifies the signature as part of FDO authentication.

The addition of OVEExtra has caused some issues for clarification:

- What types to use for OVEExtra data items
- Maximum size of OVEExtra data
- Limits on the use of OVEExtra data
- How to allocate buffering for OVEExtra data
- What protocol actions to take if a Device cannot buffer OVEExtra data

2. OVEExtra data type numbers§

Each OVEExtra datum is stored with a type OVEExtraInfoType, which is an**int**; the data itself is a byte string (**bstr**). No OVEExtraInfoType’s are defined in the FDO 1.1 specification, and the space of OVEExtraInfoType is from -65536 to the minimum negative integer in CBOR type 1, being -(2^64). Numbers in the range from -65536 to 65535 are reserved to be assigned by FIDO in the future.

3. Maximum size of OVEExtra data§

The limit on the OVEExtra data in FDO 1.1 is based on the message size limit, expressed in section 3.2 as **msglen**, which is a uint16. A given Device might have a smaller limit, based on memory constraints.

Supply chain entities must verify that their OVEExtra message fits into a legal TO2.OVNextEntry message.

To understand how much data can be added to OVEExtra, the implementation must take into account other overheads that appear within the message:

The FDO message format, **StreamMsg** (section 3.3.1) has fields:

- msglen
- msgtype
- protver
- TO2.OVNextEntry array overhead
- OVEntryNum
- CoseSignature overhead
- OVEntryPayload (OVEExtra is one of the entries in here)

If a fixed size data item is being defined for OVEExtra, future evolution of cryptography is also a consideration. The crypto used for the hashes and signature in the Ownership Voucher may evolve over time and might be larger than now. For example, some post-quantum signature mechanisms have large signatures.

4. Limits on the use of OVEExtra data§

Since OVEExtra is a customization extension for FDO, there is no specific intended usage. As a practical matter (within the FDO framework), we can anticipate how OVEExtra data is capable of being embedded and used:

- There is no intrinsic mechanism to encrypt OVEExtra data, so it is easiest to see this as data that does not have a privacy requirement, or token data that is interpreted over some future protocol connection with its own privacy mechanism (e.g., TLS).

  There is no prohibition on encrypted data. Data may be encrypted if the decryption key is stored in a supply chain entity or in the Device. This is conceivable in a given supply chain, but FDO does not have internal support for this.

- Supply-chain entities may embed data in the OV for the Device to use during or after onboarding.

  Since a supply chain entity has access to the Ownership Voucher when the information is added, it can maintain a copy of the Device Certificate so that it can authenticate the device during a later information request. After this authentication, suitable privacy mechanisms can be used to share additional data.

  Example: if a supply-chain entity normally would install some databases or software on the Device, it can make this data available by embedding a URL and/or token in the OV that the device can use to fetch the data during the eventual onboarding. This removes the need to unbox, power on, and rebox the device during the supply chain. The device can authenticate itself by signing the request with the Device key used in FDO; the supply-chain entity can verify this signature using a saved copy of the Device certificate.

- Supply-chain entities may embed data in the OV for later supply-chain entities to use.

  The supply-chain entity cannot use FDO techniques to verify the data in the Ownership Voucher, unless it has an independent way to verify the manufacturer’s public key (OVPubKey). However, the Owner may use the Device itself as an oracle to verify the Ownership Voucher, since a successful TO2 protocol implies that the OV was authenticated.

```
EXAMPLE 1
This data may have information about the manufacture or storage of a
device that is useful for quality and warranty purposes.
```

5. OVEExtraTypeMaxLength field

We recommend the following OVEExtra field be added to the first entry of each Ownership Voucher that gives the maximum length segment that can be received by this Device. In other words:

StreamMsg.msglen >= maximum length given

This field is encoded in OVEExtra as OVEExtraTypeMaxLength:

```
OVEExtraType = int
OVEExtraTypeMaxLength = 1
OVEExtraMaxLength = bstr .cbor uint
```

OVEExtra values are always a bstr. The value of OVEExtraMaxLength is a CBOR-encoded, unsigned integer, which gives the maximum StreamMsg.msglen value this device is capable of processing.

```
EXAMPLE 2
OVEExtraMaxLength = bstr .cbor 512 # each message must fit into 512 bytes
OVEExtraMaxLength = bstr .cbor 65535 # each message must fit in 0xffff bytes
```

No information about the message length may be gleaned from a device that does not have an OVEExtraMaxLength field. An empirical value must be determined via testing.

It is recommended that the Ownership Voucher entries be scanned to find the first OVEExtraMaxLength message. However, in some cases, the first ownership voucher entry is signed by a remote manufacturer (eg. ODM) that does not include this option. It is thus acceptable for a later ownership voucher entry to contain OVEExtraMaxLength.

It is assumed that the maximum message length is known when the device is shipped from the first Owner (e.g., the factory). Thus, the first value of OVEExtraMaxLength found in the Ownership Voucher may be used.