FDO Mismatched Crypto Options Analysis

Final Document, October 10, 2023

This version:
https://fidoalliance.org/specs/fidoiot/fdo-appnote-6-mismatch-crypto-v1.0-fd-20231010.html

Issue Tracking:
GitHub

Editor:
Geoffrey Cooper (Intel)

Version:
1.0

Copyright © 2023 FIDO Alliance. All Rights Reserved.

Abstract

In the FDO specification, section 3.6.5, a table indicates certain combinations of Device- and Owner-level crypto that are "not recommended" because the crypto on one side of the connection is stronger than the crypto on the other side. However, these options are actually legal options in FDO. This note discusses situations that can give rise to mismatched crypto, and how to best deal with this situation.

Table of Contents

1. Introduction§

In the FDO 1.1 specification, section 3.6.5, a table lists the cryptographic choice for key exchange, based on the cryptography used in the Device (client) and the Owner (server). The intent of the table is to clarify the choice of key exchange algorithm, which is not at issue here. However, certain combinations are marked with the warning: "Not a recommended configuration", which has resulted in some Q&A at the IoT Technical Working Group. This note attempts to clarify the meaning of this warning and give advice about what to do if these options are indeed needed.

In addition, some of the notations of "not recommended" are on the wrong table entry.

The following table lists entries that have mismatched crypto. We omit the 3rd column of the table here, and we also include the correct set of mismatched crypto entries. RSA2048RESTR has the same crypto strength as RSA2048, so it is omitted from the table.

Also, the EPID entries in the table are not marked (or included here), although Intel® EPID v1 and Intel® EPID v1.1 do have different cryptographic strength relative to the other entries. The assumption is that EPID is chosen because of its cryptographic privacy properties, so the discussion here is of less interest.

Device Attestation	Owner Attestation	Corrected from Spec
ECDSA NIST P-256	RSA2048	✔
ECDSA NIST P-384	RSA2048	✔
ECDSA NIST P-384	RSA3072	✔
ECDSA NIST P-256	ECDSA NIST P-384	
ECDSA NIST P-384	ECDSA NIST P-256	

NOTE: RFC6605 (section 1) references the equivalence of strength for ECDSA P-256 and RSA 3072.

In each of these options, the strength of the cryptography differs greatly between the choice for the Device and the choice for the Owner. Usually, in cryptography, the client and server are approximately matched in cryptographic strength. The reason for this is that an attacker is assumed to favor the weakest cryptographic link, so the overall strength of the cryptography is judged by the weakest part. In this case, if attestation is 384-bit in one direction and 256-bit in the other, the overall strength of the cryptography is 256-bit, and the added work for the 384-bit crypto is essentially wasted.

In the FDO 1.1 specification, these listed combinations are marked as not "recommended" because they may lead to a false sense of security if a naive implementer were to see the stronger crypto and think it adds some benefit. However, these combinations are indeed legal FDO options and FDO operations between entities so configured are completely compliant with the FDO 1.1 specification.

As an aside, we assume here that NIST P-256 and RSA2048 have about the same level of security, as do NIST P-384 and RSA3072. Since the sophistication of attacks on each mechanism changes over time, this is not reliably true at any moment in time. We take it as a common approximation.

In the rest of this document, we focus on the 3rd table entry, where the Owner attestation uses ECDSA NIST P-384, and the Device uses ECDSA NIST P-256.

2. Mismatched Crypto can Occur Naturally§

How could mismatched crypto in FDO occur in a real-world scenario? Consider a vendor who decides to simplify the supply chain by using a single crypto option for the Ownership Vouchers of any device. In this way:

- The manufacturing and supply-chain stations that extend the Ownership Voucher need only one cryptographic option
- The parties that provide public keys to place in these ownership vouchers (the next party in the supply chain) need to provide only one key on file, or one key per order

A good security decision is to choose stronger security when a single option is chosen, so ECDSA P-384 is chosen for all Ownership Vouchers.

But not all Devices are equal in power and cryptographic operations. What if a Device is poor at running ECDSA P-384 operations or its hardware key store can only store P-256? In this case, the device may choose the smaller key size. Since the vendor has standardized the Ownership Vouchers, a mismatched configuration appears.

3. Choosing the Best Options for Mismatched Crypto§

In the previous section, we outlined how a mismatched ECDSA configuration could reasonably occur. In this section, we analyze different strategies for dealing with that situation.

Here are three ways to implement FDO using an Owner / Ownership Voucher at ECDSA P-384 and a client with capability for ECDSA P-256:

A) We adjust the Owner's crypto level, so the Ownership Voucher implements P-256 to match the device. This requires changing crypto through the supply chain, so it might not be possible in all situations.

B) The device implements P-256 and the Ownership Voucher implements P-384

C) The device implements a P-384 key, but wraps it using a P-256 key from the hardware keystore. Protocols run at P-384, but crypto is performed in software to achieve P-384.

How to select the best option? Machine efficiency might be an important factor. In a given Device architecture, Option (A) may run faster than either (B) or (C), because the Device key store has hardware cryptography for P-256. For this reason alone, (A) might be a rational choice. After all, if the entire solution's security is pegged at 256 bits, why pay more to run any operation at 384-bit?

Alternately, if we look at different phases of FDO operation, there are parts that involve the Device and other parts that do not. After the DI protocol, which has no security posture of its own, all manufacturing and supply-chain operations in FDO are impacted only by the crypto in the Ownership Voucher. An attacker who attempts to subvert the crypto measures in the Ownership Voucher must break P-384, regardless of the crypto level of the Device. Thus, an Ownership Voucher using P-384 is indeed safer from cryptographic attacks for all attackers in the supply chain (options (B) and (C)). If attacks on the supply chain are more likely, or if the onboarding network has local defenses, such as physical security or link encryption, then assuring stronger crypto in the supply chain might be a good choice.

Despite the increased use of P-384 crypto, option (C) appears at first to give little additional strength over option (B), since overall security is judged by the smaller wrapping key. However, for protection against a strictly network-based attack, (C) is far stronger than (B). Option (C) is a good choice if all network operations must run over the Internet or other non-secured network, but the device itself is in a secured location and is not subject to on-device attack. This might be true for a zero-user IoT device, housed in a secured facility.

Conversely, from the point of view of the Device-based attacker, the cryptographic strengths of (A), (B) and (C) are the same, since all see cryptographic operations at the 256-bit level. However, if (A) and (B) perform cryptographic operations in a (256-bit limited) TPM, and (C) requires that the P-384 key be exposed to OS-based attackers, the attack against (C) is probably easier.

Further, between (A) and (B), the pure P-256 solution (A) enables all crypto to be implemented in the 256-bit TPM, but (B) includes some P-384 operations that must be performed in software (at OS level). So (A) is preferable to (B) overall.

The following table summarizes these results:

Single Attacker	**Best Approach**	**Why**
Supply chain attack only	(B) & (C)	Attacker must break Ownership Voucher crypto
Network-based attack only	(C)	Attacker sees stronger P-384 operations on network
Device-based attack only	(A)	All key storage and crypto performed in a TPM with special defenses. The Device key in (C) is particularly exposed to Device-based attacker

4. Conclusion§

Whenever possible, choose the strongest crypto, and use the same crypto-level on both Device and Owner. When the Device- and Owner-levels of crypto cannot match, an increase in security posture is still possible if some modes of attack are more likely than others.