FDO Security Requirements

Final Document, September 13, 2022

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

Editor:
Security and Privacy Working Group (FIDO Alliance)

Copyright © 2023 FIDO Alliance. All Rights Reserved.

Abstract

This document outlines the security requirements for FIDO Device Onboard.

Table of Contents

1. Introduction§

2. FIDO Onboard Device:§

2.1. Introduction§

This document assesses the FIDO Device Onboard (FDO) protocol and specifies the security requirements that must be fulfilled in order to attain the stated security goals of this protocol.

2.1.1. Definition§

An automatic onboarding protocol for IoT devices permits late binding of device credentials, so that one manufactured device may onboard, without modification, to many different IOT platforms.

2.2. Device (The device being manufactured; later, the device being provisioned)§

This device has hardware and software configured on it, including a device ROE and a Management Agent. FDO Devices may be either natively IP-based or non-IP-based. In the case of FDO Devices natively connected to an IP network, the FDO Device is capable of connecting directly to the FDO owner or FDO Rendezvous Server.

FDO Devices not capable of IP protocols can still use FDO by tunneling the FDO message layer across a reliable non-IP connection.

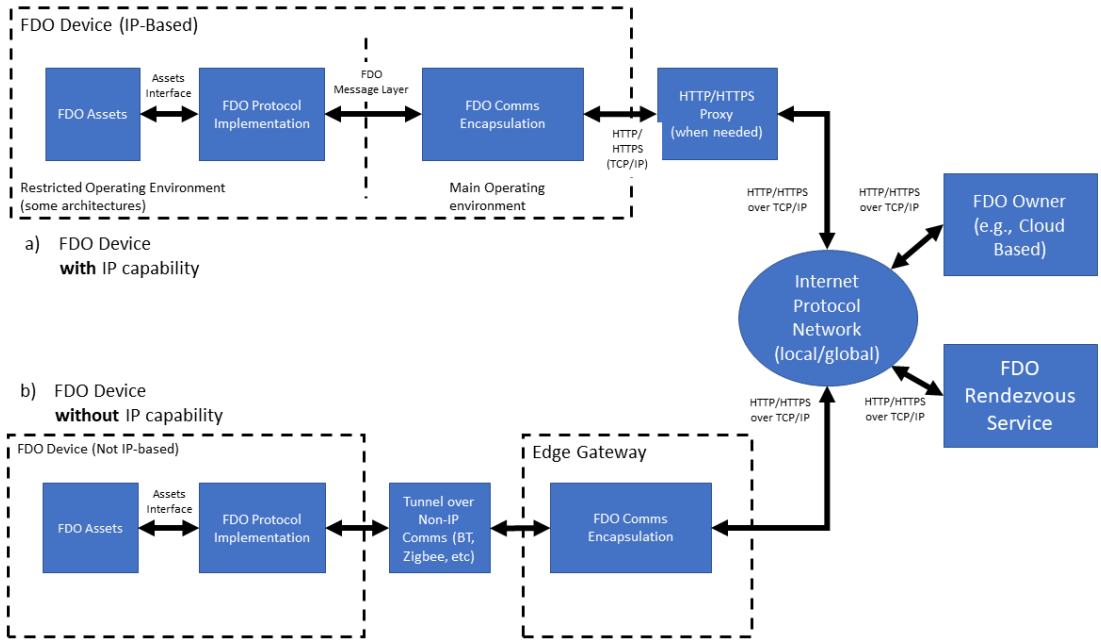


Figure 1 *Transport Interfaces*

2.3. Attack Classification§

1. Automated attacks focused on stealing FDO credentials during the manufacturing process.
2. Automated attacks focused on impersonating the Rendezvous Server.
3. Automated attacks focused on impersonating new device owner during ownership transfer.
4. Automated attacks to authenticated device sessions.
5. Non-automated attacks to steal device credentials for cloning

3. Security Goals§

3.1. Security Goals for Device§

Security Goal ID	Security Goal	Description
[SG-1]	`Secure communication`	Authenticate (i.e. recognize) a device to a Rendezvous Server with high (cryptographic) strength.
[SG-2]	`Secure storage of Confidential credentials`	Provide robust protection against eavesdroppers (e.g., be resilient to physical observation, resilient to targeted impersonation, resilient to throttled and unthrottled guessing).
[SG-3]	`Isolation of data`	Be resilient to phishing attacks and real-time phishing attacks, including resilience to online attacks by adversaries able to actively manipulate network traffic.
[SG-4]	`Secure data interfaces`	Minimize attack surfaces, validate input data.
[SG-5]	`Secure handling of personal data`	Be able to verify the device attestation credentials with confidence.

Security Goal ID	Security Goal	Description
[SG-6]	`Strong default security`	Device should have security functions enabled by default. Services not required for essential functions must be disabled by default.
[SG-7]	`Good security policies`	Develop and implement policies that support security of the device.
[SG-8]	`Secure handling of personal data`	Be able to comply with GDPR.
[SG-9]	`Secure supply chain`	Be able to verify the authenticity of device HW/SW components.
[SG-10]	`Resilience to outages`	Device should behave in a way that guarantees safety of its users.
[SG-11]	`Software integrity`	The integrity of software components (esp Operating System) of the device should be cryptographically verifiable.
[SG-12]	`Strong device authentication`	The device should be Uniquely identifiable and securely authenticated.
[SG-13]	`Security lifecycle`	The device development lifecycle should be Secure.
[SG-14]	`Secure update`	Guarantees that the device is always up to date with the latest security patches.
[SG-15]	`Standard cryptography`	Ensure the device uses secure crypto algorithms, cryptographic libraries and key length.
[SG-16]	`Secure installation, maintenance & decommissioning`	Ensures that the device is installed and configured and decommissioned securely.
[SG-17]	`Secure event monitoring and anomaly detection`	Ensures that unusual activity is detected and flagged.
[SG-18]	`Secure restricted operating environment`	Ensures that high security applications are executed in a secure environment.

3.2. Security Goals for FDO Application§

Security Goal ID	Security Goal	Description
[SG-19]	`Strong application authentication`	Authenticate (i.e. recognize) a device to a Rendezvous Server with high (cryptographic) strength.
[SG-20]	`Credential guessing resilience`	Provide robust protection against eavesdroppers, e.g. be resilient to physical observation, resilient to targeted impersonation, resilient to throttled and unthrottled guessing.
[SG-21]	`Credential disclosure resilience`	Be resilient to phishing attacks and real-time phishing attack, including resilience to online attacks by adversaries able to actively manipulate network traffic.
[SG-22]	`Unlinkablity`	Protect the protocol conversation such that any two relying parties cannot link the conversation to one user (i.e., be unlinkable).

Security Goal ID	Security Goal	Description
[SG-22]	`Attestability`	Be able to verify the application attestation credentials with confidence.

4. Security Assumptions

Security Assumption ID	Security Assumption
SA-1	The Authenticator and its cryptographic algorithms and parameters (key size, mode, output length, etc.) in use are not subject to unknown weaknesses that make them unfit for their purpose in encrypting, digitally signing, and authenticating messages.
SA-2	Applications on the user device are able to establish secure channels that provide trustworthy server authentication, and confidentiality and integrity for messages (e.g., through TLS).
SA-3	The computing environment on the FDO Device involved in an FDO operation acts as a trustworthy agent of the user
SA-4	The inherent value of a cryptographic key resides in the confidence it imparts, and this commodity decays with the passage of time, irrespective of any compromise event. As a result, the effective assurance level of authenticators will be reduced over time.
SA-5	The computing resources at the Rendezvous Server involved in processing an FDO operation act as trustworthy agents.

5. Asset to be Protected

For each primary asset to be protected, the threat(s) it faces in process, in motion, and in storage will be considered.

5.1. Primary Assets:

5.1.1. Device Attestation Key:

FDO uses cryptographic device attestation based on a signed Entity Attestation Token ([EAT]). The protocol can support many cryptographic mechanisms for device attestation, but this spec supports two basic capabilities: Intel® EPID and ECDSA. For each of the methods, there is a private key that is provisioned into the device, such as when the CPU or board is manufactured, for establishing the trust for a Restricted Operating Environment (ROE) that runs on the device. When signed by the device attestation key, this provides evidence of the code being executed in the ROE.

5.1.2. Ownership Credential:

This is a key pair that serves temporarily to identify the current owner of the device. When the device is manufactured, the manufacturer uses a key pair to put in an initial ownership credential. Later, the protocols conspire specifically to replace this credential with a new ownership credential, effecting ownership transfer.

5.1.3. Device Credential:

The Device credential does not identify the owner in general; it identifies the owner for the purposes of ownership transfer. The device credential from the manufacturer, stored in the device, must match the credential at one side of the Ownership Voucher. That is all. It is not intended that this key pair permanently identify the manufacturer or any of the parties in the Ownership Voucher. On the contrary, it is expected that the manufacturer may use different keys over time, and the owners will also use different keys over time, specifically

to obscure their identity in the FDO protocols and increase of the robustness of FDO.

5.2. Secondary Assets:

Secondary assets are all data supporting assets

5.2.1. IoT Platform:

The Rich OS where FDO application is installed

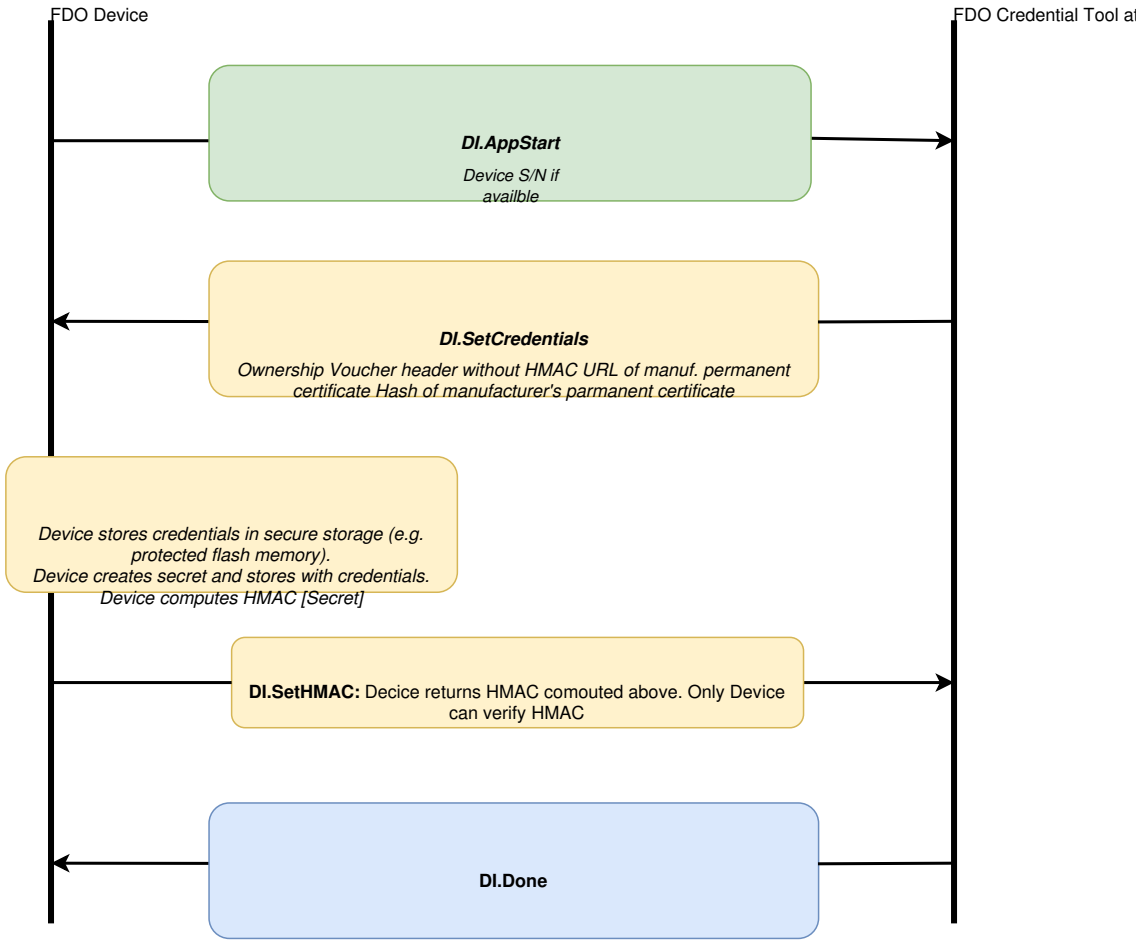
5.2.1.1. FDO Applications:

The application that executes the FDO process.

5.2.1.2. Device Initialize Protocol (DI):

The protocol's function is to embed the ownership and manufacturing credentials into the newly created device's ROE. This prepares the device and establishes the first in a chain for creating an Ownership Voucher with which to transfer ownership of the device.

*ODM : Original Desi

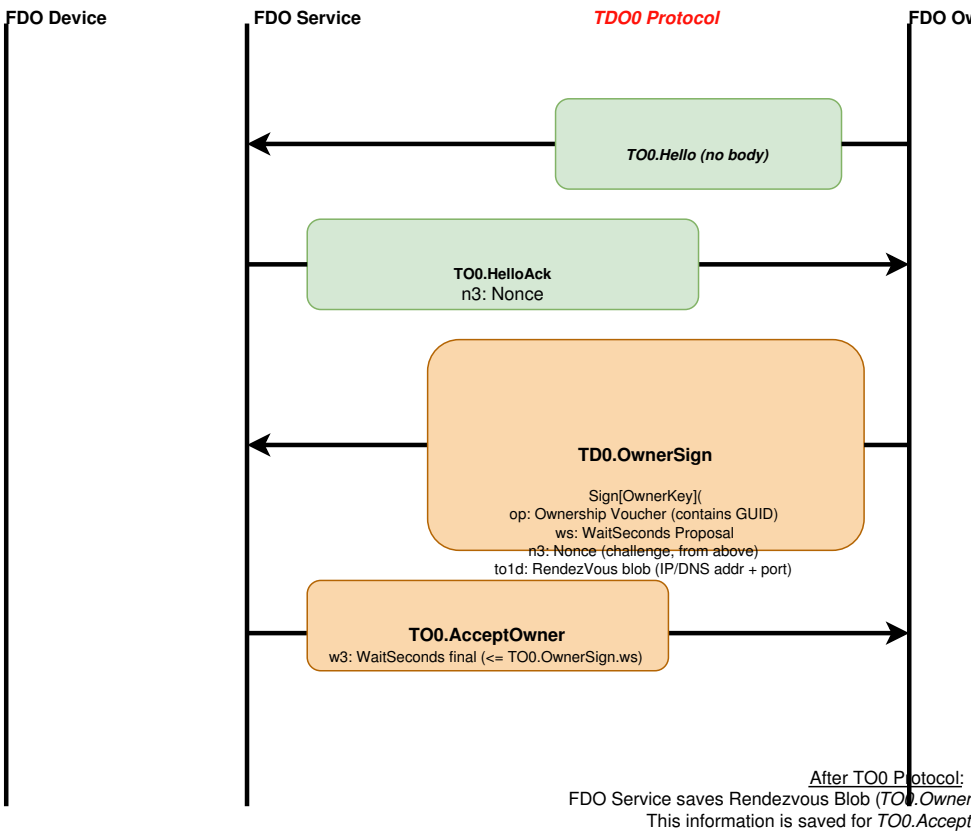


DI Protocol Diagram

Figure 2 *DI Protocol*

5.2.1.3. Transfer Ownership Protocol 0 (TO0):

Transfer Ownership Protocol 0 (TO0) serves to connect the Owner Onboarding Service with the Rendezvous Server. In this protocol, the Owner Onboarding Service indicates its intention and proves it is capable of taking control of a specific Device, based on the Device's current GUID.



TO0 Protocol Diagram

Figure 3 *TO0 Protocol*

5.2.1.4. Transfer Ownership Protocol 1 (TO1):

Transfer Ownership Protocol 1 (TO1) is an interaction between the Device ROE and the Rendezvous Server that points the Device ROE at its intended Owner Onboarding Service, which has recently completed Transfer Ownership Protocol 0. The TO1 Protocol is the mirror image of the TO0 Protocol, on the Device side.

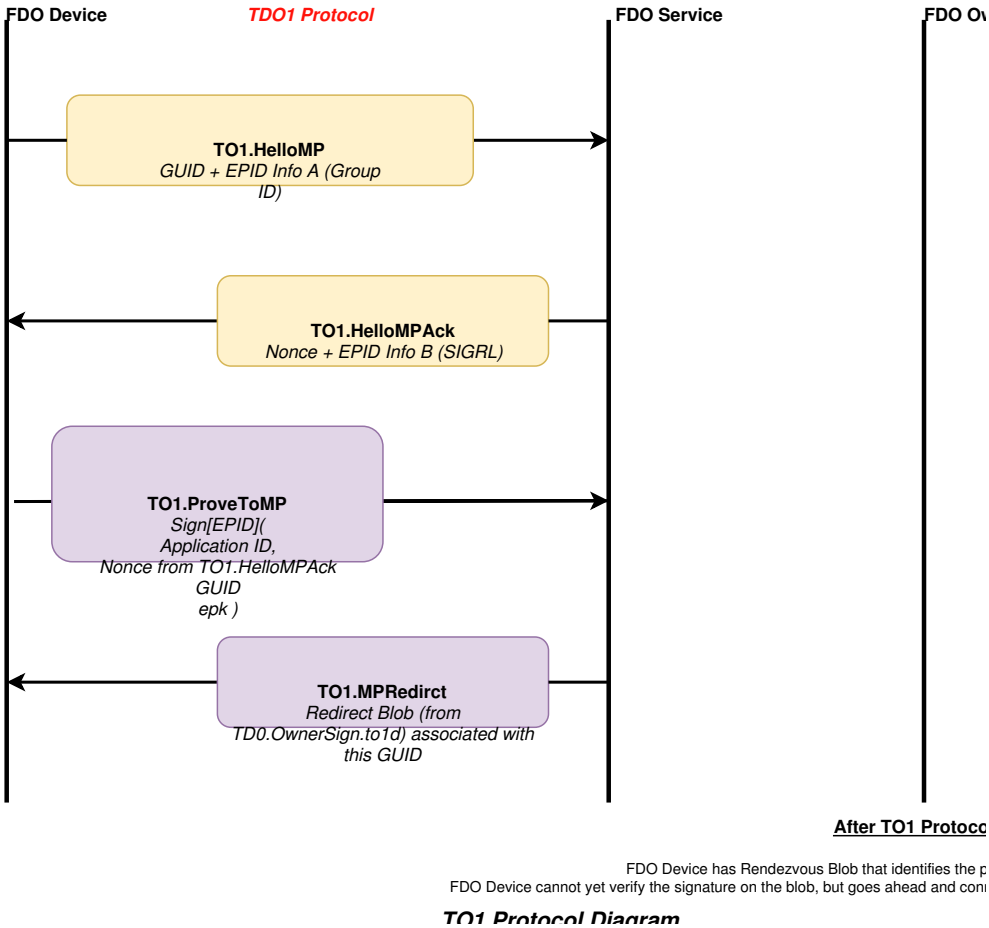


Figure 4 *TO1 Protocol*

5.2.1.5. Transfer Ownership Protocol 2 (TO2):

Transfer Ownership Protocol 2 (TO2) is an interaction between the Device ROE and the Owner Onboarding Service where the transfer of ownership to the new Owner occurs.

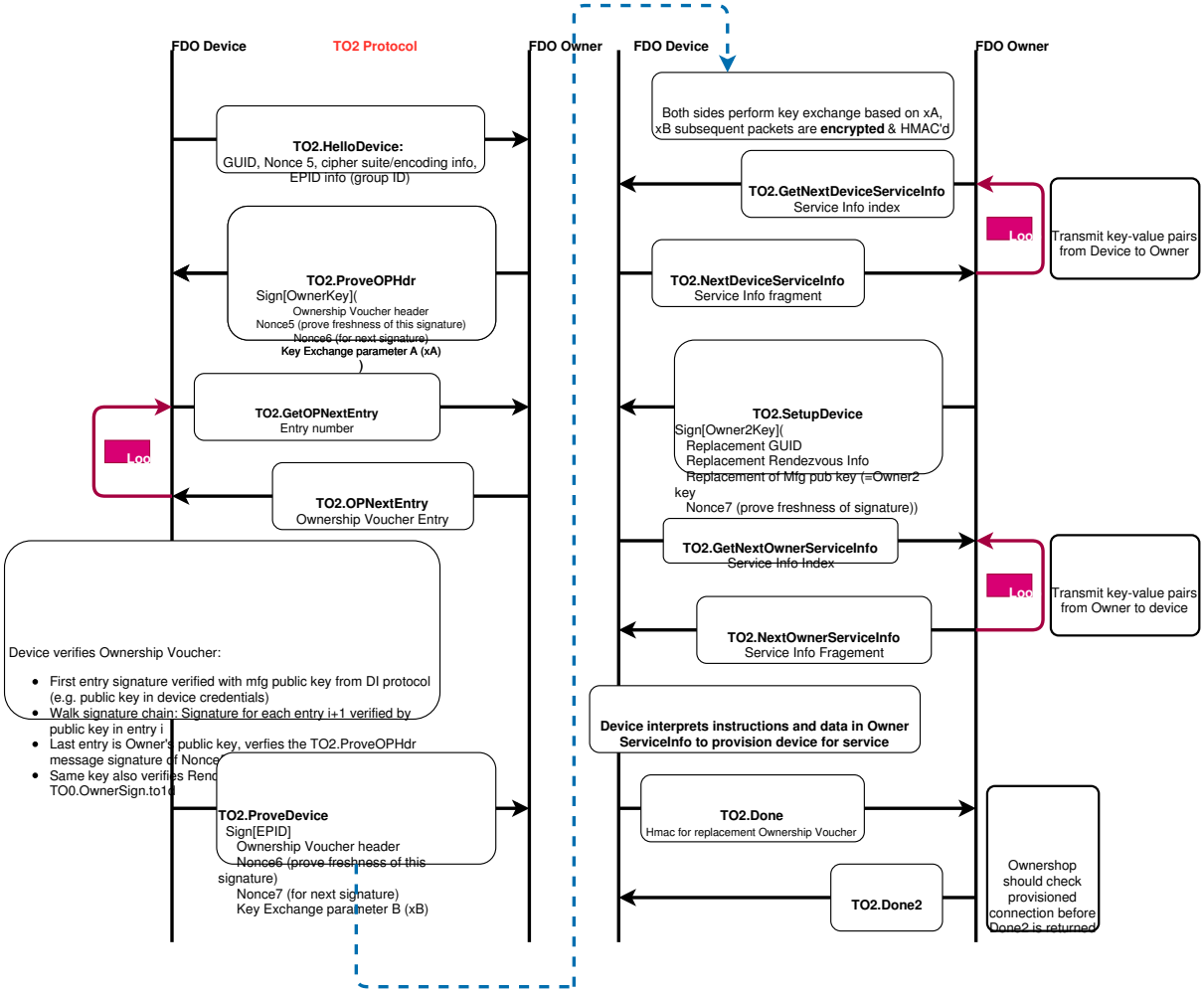


Figure 5 *TO2 Protocol*

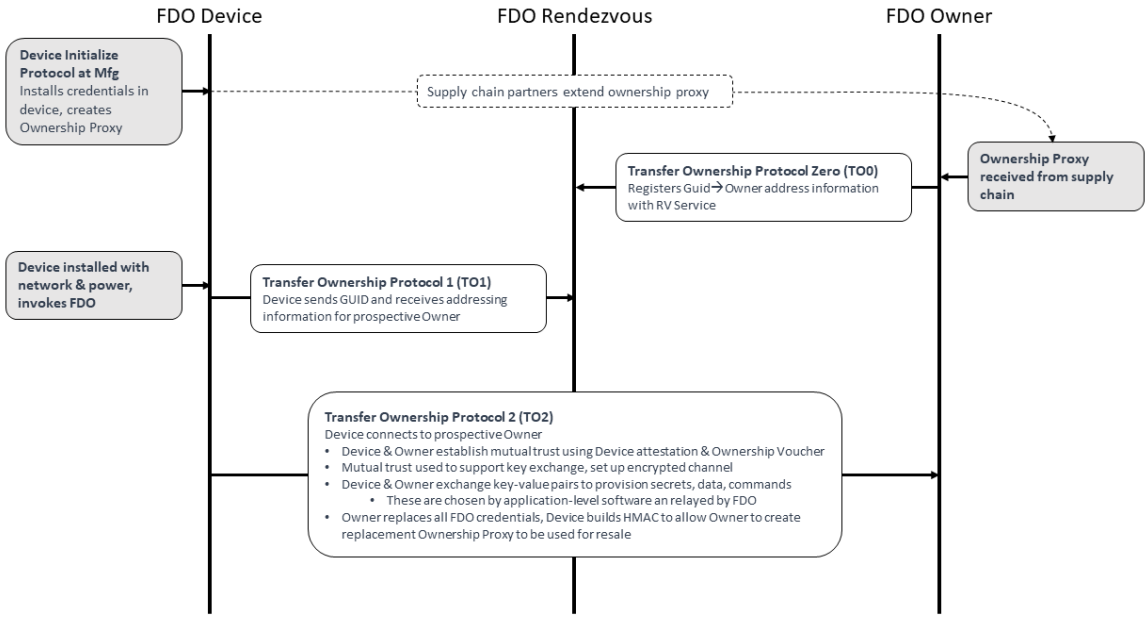


Figure 6 *FDO Protocol Bounce*

5.2.1.6. Image Showing the Interaction Between the Protocols

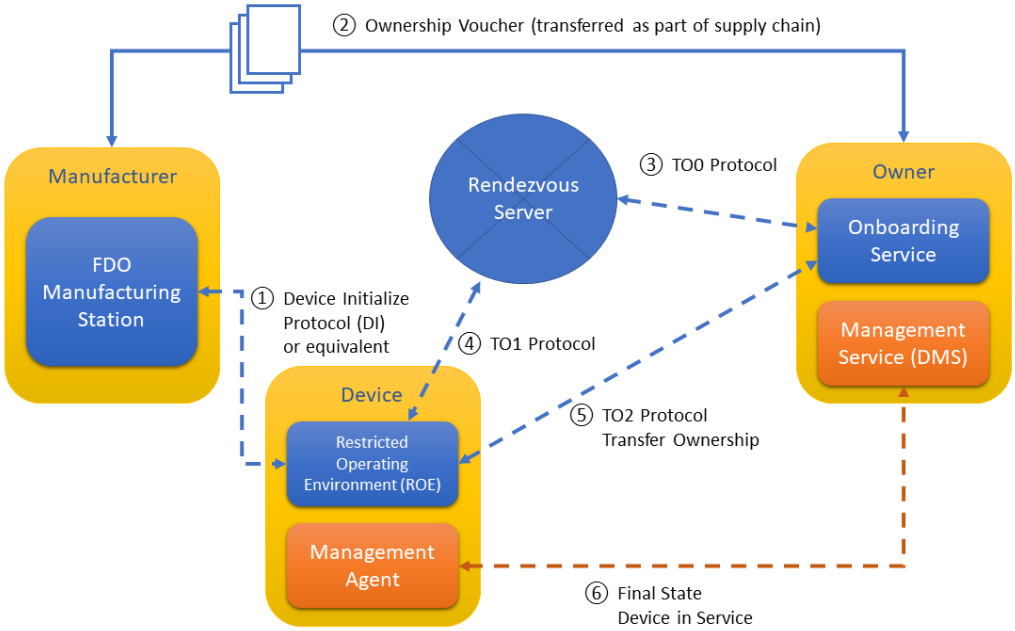


Figure 7 *Interaction between the protocols*

6. Threat Analysis§

6.1. General Threat List§

Threat-ID Number	Threat	Description
[TH-1]	`Replay of data`	In a "replay attack" (replay of data) attackers record valid messages and play this information later.
[TH-2]	`Leakage of data`	The threat of valuable data about a device or system being inadvertently revealed.
[TH-3]	`Injection of data (processed)`	The threat of unwanted and unauthorized data modification.
[TH-4]	`Deletion of data`	The threat of losing all or part of the data in its storage.
[TH-5]	`Man-in-the-middle`	The threat of an attacker sitting in the middle of the communication between the device and a server.
[TH-6]	`Disclosure of credentials`	The threat compromising sensitive credentials processed on the device, transported to/from the device, or stored on device.
[TH-7]	`Unauthorized access to the FDO application`	The threat of unauthorized access to the FDO application via any interface.
[TH-8]	`Physical attacks`	Threat that an attacker gains physical access to the device's internal components.
[TH-9]	`Organizational policies & Procedures`	Threats linked to bad or non-existent organizational policies.
[TH-10]	`Failure of the FDO application`	The threat of failure, malfunction or crash of the device software/ applications.
[TH-11]	`Malicious/ Vulnerable	The threat of device relying on vulnerable HW/SW components

Threat-ID Number	Threat	Description
[TH-12]	device components` `Exchanging data with a rogue server`	or components that contain backdoors. The threat of divulging confidential credentials to a rogue server.
[TH-13]	`Downgrade attacks & Exploiting an insecure software`	Linked to installation of vulnerable updates files, thus granting the attacker access.
[TH-14]	`Exploiting a device due to insecure configuration `	Threat of exploitation due to the device being unhardened. It is caused by a lack of documentation from the manufacturer.
[TH-15]	`Advanced persistent threats`	The threat of an attacker having longterm access to the device.

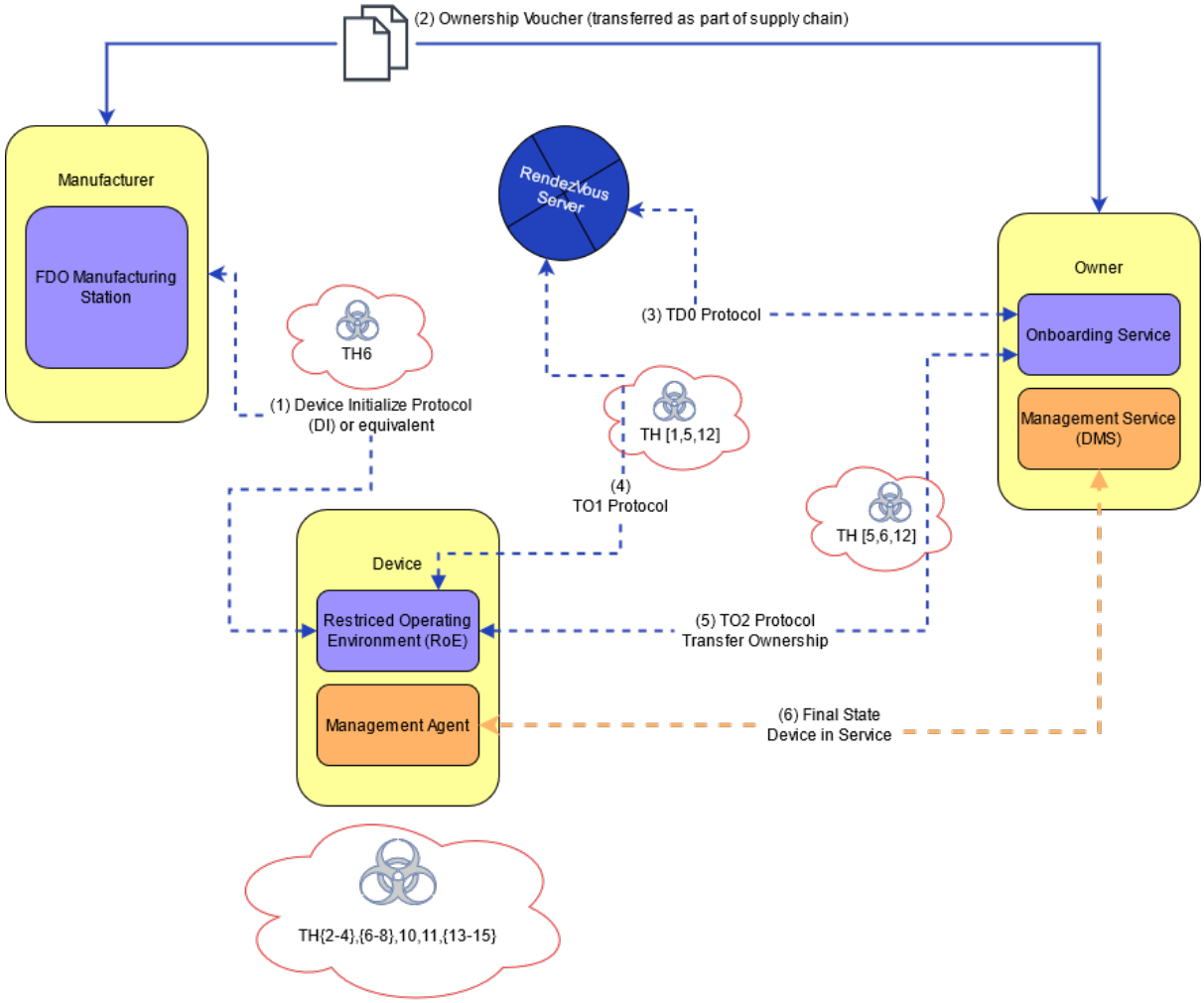


Figure 8 *FDO Flow Threats*

Image showing areas of the interaction that are impacted by specific threats.

6.2. Attack Scenarios

6.2.1. At Manufacturing

Threat-ID Number	Threat	Scenario
[TH-6]	`Disclosure of credentials`	An attacker obtains control of an ownership and manufacturing key or a key-issuing key during Device Initialize (DI).

Threat-ID Number	Threat	Scenario
[TH-11]	`Malicious/ Vulnerable device components`	Manufacturer's component suppliers provide compromised SW or HW components. Manufacturer uses vulnerable open-source codes/ libraries.

6.2.2. Device Platforms

Threat-ID Number	Threat	Scenario
[TH-2.1]	`Leakage of data`	An attacker extracts confidential credentials by observing timing, power etc.
[TH-3.1]	`Injection of data on the device during processing`	An attacker injects previously authenticated data.
[TH-4.1]	`Deletion of data`	An attacker deletes stored credentials and configuration files needed by FDO application.
[TH-5.1]	`Man-in-the-middle`	The threat of an attacker intercepting and extracting confidential credentials during communication between the device and a server.
[TH-6.1]	`Disclosure of credentials`	Attacker succeeds in extracting sensitive credentials on the device.
[TH-7.1]	`Unauthorized access to the FDO application`	A malicious application gains unauthorized access to the FDO application.
[TH-7.2]	`Unauthorized access to the FDO application`	An unauthorized user gains access to the device settings to alter security configurations.
[TH-8.1]	`Physical attacks`	An attacker gets physical access to the device and is able to conduct physical attacks on the device.
[TH-8.2]	`Physical attacks`	An attacker gets physical access to the device and removes the storage media (e.g., SD card).
[TH-9.1]	`Lack of organizational policies & Procedures`	A lack of vulnerability disclosure policies, default security policies, etc. causes an avoidable device vulnerability/ wrong configuration to go unnoticed
[TH-10.1]	`Failure of the FDO application`	An attacker sends maliciously crafted messages which cause the FDO application to crash or become unstable.
[TH-11.1]	`Malicious/ Vulnerable device components`	An attacker compromises internal PRNG state and entropy source before seeding.
[TH-11.2]	`Malicious/ Vulnerable device components`	An attacker compromises entropy source after seeding.
[TH-11.3]	`Malicious/ Vulnerable device components`	An attacker compromises internal PRNG state.

Threat-ID Number	Threat	Scenario
[TH-11.4]	`Malicious/ Vulnerable device components`	Cryptographically flawed key generation process.
[TH-11.5]	`Malicious/ Vulnerable device components`	A malicious application on the device conducts side channel attacks.
[TH-11.6]	`Malicious/ Vulnerable device components`	An attacker uses a backdoor to leak confidential credentials using covert channels on the device.
[TH-11.7]	`Malicious/ Vulnerable device components`	An attacker exploits the device using an unprotected SW/HW debug interface
[TH-13.1]	`Downgrade attacks`	The device is installed with an older, insecure version to render it exploitable using known exploits.
[TH-13.2]	`Exploiting an insecure software`	The device is "updated" with a new but maliciously altered version to render it exploitable according to the attacker’s wishes.
[TH-14.1]	`Exploiting a device due to insecure configuration `	Due to lack of documentation, the device is incorrectly configured.
[TH-15.1]	`Advanced persistent threats`	Log and event monitoring.

6.2.3. Communication

Threat-ID Number	Threat	Scenario
[TH-1.1]	`Replay of data`	An attacker edits and replays previously authenticated data between device and Rendezvous Server. (TO1)
[TH-1.2]	`Replay of data`	An attacker edits and replays previously authenticated data between Device and Onboarding Service. (TO2)
[TH-1.3]	`Replay of data`	An attacker edits and replays communication between device and Management Service. (Device in Service)
[TH-5]	`Man-in-the-middle`	The threat of an attacker intercepting and extracting confidential credentials during communication between the device and a server.

6.2.4. FDO Application

Threat-ID Number	Threat	Scenario
[TH-4.1]	`Deletion of data`	An attacker deletes stored credentials and configuration files needed by FDO application.
[TH-6.1]	`Disclosure of credentials`	Attacker succeeds in extracting sensitive credentials during processing, on the device.

Threat-ID Number	Threat	Scenario
[TH-7.1]	`Unauthorized access to the FDO application`	A malicious application gains unauthorized access to the FDO application configuration.
[TH-10.1]	`Failure of the FDO application`	An attacker sends maliciously crafted messages which cause the FDO application to crash or become unstable.
[TH-11.4]	`Malicious/ Vulnerable device components`	Cryptographically flawed key generation process.
[TH-12.1]	`Exchanging data with a rogue server`	The application accepts a rogue server as new owner and exchanges confidential credentials with it.

7. Impact and Likelihood for Consumer Environment

7.1. Define

- Defining Risk Impact:
- `Low Risk` : _Means that a threat event could be expected to have a **limited** adverse effect._
- `Medium Risk` : _Means that a threat event could be expected to have a **serious** adverse effect._
- `High Risk` : _Means that a threat event could be expected to have a **severe or catastrophic** adverse effect._
- Defining Likelihood:
- `Unlikely` : _**Could** occur at **some time**_
- `Likely` : _**Will probably** occur in **most circumstances**_
- `Almost certain` : _**Can be expected** to occur in **most circumstances**_

Impact x Likelihood	Unlikely	Likely	Almost Certain
Low Impact	`Low Risk`	`Medium Risk`	`Medium Risk`
Medium Impact	`Low Risk`	`Medium Risk`	`High Risk`
High Impact	`Medium Risk`	`High Risk`	`High Risk`

Impact is determined by variables that are context dependent, meaning the context of where the device is installed.

7.2. Impact

Scalability of Impact - Level of compromise

Impact	Low/Non-sensitive data	Limited Sensitive data	Complete Compromise/Physical Harm
Single device	`Low`	`Medium`	`Medium`
Local network	`Low`	`Medium`	`High`
Entire fleet	`Medium`	`High`	`High`

7.3. Likelihood

Proximity Required to carry out the attack **Technical Difficulty of the attack**

-

Likelihood	Difficult	Moderate	Easy
Physical	`Unlikely`	`Likely`	`Likely`
Proximity	`Unlikely`	`Likely`	`Almost Certain`
Remote	`Likely`	`Almost Certain`	`Almost Certain`

7.4. Manufacturing§

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk
[TH-6]	`Disclosure of credentials`	An attacker obtains control of an ownership and thread, manufacturing key, or a key-issuing key during Device Initialize (DI).	High Impact	Likely	High Risk
[TH-11]	`Malicious/ Vulnerable device components`	Manufacturer's component suppliers provide compromised SW or HW components. Manufacturer uses vulnerable opensource codes/ libraries.	High Impact	Likely	High Risk

7.5. Device Platforms§

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk
[TH-2.1]	`Leakage of data`	An attacker extracts confidential credentials by observing timing, power etc.	Medium Impact	Likely	Medium Risk
[TH-3.1]	`Injection of data on the device during processing`	An attacker injects previously authenticated data.	Medium Impact	Unlikely	Low Risk
[TH-4.1]	`Deletion of data`	An attacker deletes stored credentials and configuration files.	Medium Impact	Almost Certain	High Risk
[TH-6.1]	`Disclosure of credentials`	Attacker succeeds in extracting sensitive credentials on the device.	Medium Impact	Almost Certain	High Risk
[TH-7.1]	`Unauthorized access to the FDO application`	A malicious application gains unauthorized access to the FDO application.	Medium Impact	Likely	Medium Risk
[TH-7.2]	`Unauthorized access to the	An unauthorized user gains access to the device settings to	Medium	Almost	High Risk

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk
	FDO application`	alter security configurations.	Impact	certain	
[TH-8.1]	`Physical attacks`	An attacker gets physical access to the device and is able to conduct physical attacks on the device.	Medium Impact	Likely	Medium Risk
[TH-8.2]	`Physical attacks`	An attacker gets physical access to the device and removes the storage media (e.g., SD card).	Medium Impact	Almost Certain	High Risk
[TH-9.1]	`Lack of organizational policies & procedures`	A lack of Vulnerability disclosure policies, default security policies, etc. causes an avoidable device vulnerability/ wrong configuration to go unnoticed	High Impact	Likely	High Risk
[TH-10.1]	`Failure of the device OS/Firmware`	An attacker sends maliciously crafted messages which cause the OS/Firmware to crash or become unstable.	Medium Impact	Almost Certain	High Risk
[TH-11.1]	`Malicious/ Vulnerable device components`	An attacker compromises Internal PRNG state and entropy source before seeding.	High Impact	Unlikely	Medium Risk
[TH-11.2]	`Malicious/ Vulnerable device components`	An attacker compromises entropy source after seeding.	High Impact	Unlikely	Medium Risk
[TH-11.3]	`Malicious/ Vulnerable device components`	An attacker compromises internal PRNG state.	High Impact	Unlikely	Medium Risk
[TH-11.4]	`Malicious/ Vulnerable device components`	Cryptographically flawed key generation process.	High Impact	Unlikely	Medium Risk
[TH-11.5]	`Malicious/ Vulnerable device components`	A malicious application on the device conducts side channel attacks.	High Impact	Unlikely	Medium Risk
[TH-11.6]	`Malicious/ Vulnerable device components`	An attacker uses a backdoor to leak confidential credentials using covert channels on the device	High Impact	Unlikely	Medium Risk
[TH-11.7]	`Malicious/ Vulnerable device components`	An attacker exploits the device using an unprotected SW/HW debug interface	High Impact	Likely	High Risk
[TH-13.1]	`Downgrade attacks`	The device is installed with an older, insecure version to render it exploitable using known exploits.	High Impact	Almost certain	High Risk

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk
[TH-13.2]	`Exploiting an insecure software`	The device is "updated" with a new but maliciously altered version, to render it exploitable according to the attacker's wishes.	High Impact	Almost certain	High Risk
[TH-14.1]	`Exploiting a device due to insecure configuration `	Due to lack of documentation, the device is incorrectly configured.	High Impact	Almost certain	High Risk
[TH-15.1]	`Advanced persistent threats`	Log and Event monitoring.	High Impact	Likely	High Risk

7.6. Communications

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk
[TH-1.1]	`Replay of data`	An attacker edits and replays previously authenticated data between device and Rendezvous Server. (TO1)	High Impact	Almost Certain	High Risk
[TH-1.2]	`Replay of data`	An attacker edits and replays previously authenticated data between device and Onboarding service. (TO2)	High Impact	Almost Certain	High Risk
[TH-1.3]	`Replay of data`	An attacker edits and replays communication between device and Management Service. (Device in Service)	High Impact	Almost Certain	High Risk
[TH-5.1]	`Man-in-the-middle`	The threat of an attacker intercepting and extracting confidential credentials during communication between the device and a server.	Medium Impact	Almost Certain	High Risk

7.7. FDO Applications

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk
[TH-4.2]	`Deletion of data`	An attacker deletes stored credentials and configuration files needed by FDO application.	Medium Impact	Almost Certain	High Risk
[TH-6.1]	`Disclosure of credentials`	Attacker succeeds in extracting FDO sensitive credentials on the device.	Medium Impact	Almost Certain	High Risk
[TH-7.1]	`Unauthorized access to the FDO application`	A malicious application gains unauthorized access to the FDO application.	Medium Impact	Likely	Medium Risk
	`Unauthorized				High

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk
[TH-7.2]	access to the FDO application`	An unauthorized user gains access to the FDO app settings to alter security configurations.	Medium Impact	Almost certain	Risk
[TH-10.2]	`Failure of the FDO application`	An attacker sends maliciously crafted messages which cause the FDO application to crash or become unstable.	Medium Impact	Almost Certain	High Risk
[TH-11.4]	`Malicious/ Vulnerable device components`	Cryptographically flawed key generation process.	High Impact	Likely	High Risk
[TH-12.1]	`Exchanging data with a rogue server`	The application accepts a rogue server as new owner and exchanges confidential credentials with it.	Medium Impact	Likely	High Risk

8. Risk Mitigation and Security Requirements§

This section focuses on Level 1 (L1) security assurance by mitigating the "High Risk" consumer threats. Higher levels of security assurance will cover the "Medium and Low Risk" consumer threats.

8.1. Manufacturing Mitigations§

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk	Mitigation
[TH-6]	`Disclosure of credentials`	An attacker obtains control of an ownership and manufacturing key or a key-issuing key during Device Initialize (DI).	High Impact	Likely	High Risk	The manufacturer shall ensure a secure environment for production
[TH-11]	`Malicious/ Vulnerable device components`	Manufacturer's component suppliers provide compromised SW or HW components. Manufacturer uses vulnerable opensource codes/ libraries.	High Impact	Likely	High Risk	Manufacturer shall buy secure components from trusted suppliers, or test and validate against predefined requirements the security of each component provided by untrusted suppliers or each open-source component

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk	Mitigation
[TH-4.1]	`Deletion of data`	An attacker deletes stored credentials and configuration files.	Medium Impact	Almost Certain	High Risk	Security credentials in persistent storage shall be protected using data signature or hashing algorithms
[TH-6.1]	`Disclosure of credentials`	Attacker succeeds in extracting sensitive credentials on the device.	Medium Impact	Almost Certain	High Risk	Security credentials in persistent storage shall be protected using data encryption algorithms or tamper resistant storage
[TH-7.2]	`Unauthorized access to the FDO application`	An unauthorized user gains access to the device settings to alter security configurations.	Medium Impact	Almost certain	High Risk	Access control to minimize the risk of authorized access
[TH-8.2]	`Physical attacks`	An attacker gets physical access to the device and removes the storage media (e.g., SD card).	Medium Impact	Almost Certain	High Risk	Manufacturer may hide the removable media storage inside the FDO Device in order to increase the security of authorized physical storage
		A lack of vulnerability disclosure policies, default security policies, etc., causes an avoidable device vulnerability/ wrong configuration to				Manufacturer shall ensure a well-documented Vulnerability disclosure policies and default security policies in order to avoid any non-documented vulnerability.

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk	Mitigation
		go unnoticed.				
[TH-9.1]	`Lack of organizational policies and procedures`		High Impact	Likely	High Risk	
[TH-10.1]	`Failure of the device OS/Firmware`	An attacker sends maliciously crafted messages which cause the OS/Firmware to crash or become unstable.	Medium Impact	Almost Certain	High Risk	FDO Device shall handle all inputs and outputs in a secure manner such that an invalid input/output does not lead to a device malfunction/crash
[TH-11.7]	`Malicious/ Vulnerable device components`	An attacker exploits the device using an unprotected SW/HW debug interface	High Impact	Likely	High Risk	Debugging ports should be disabled for devices on production (e.g., JTAG)
[TH-13.1]	`Downgrade attacks`	The device is installed with an older, insecure version to render it exploitable using known exploits.	High Impact	Almost certain	High Risk	FDO Device should block any software downgrade attempts by implementing an anti-rollback functionality
	`Exploiting an	The device is "updated" with a new but maliciously				Device shall verify the authenticity and integrity of all software updates before they are installed. Where this is not practicable, a

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk	Mitigation
[TH-13.2]	insecure software`	altered version to render it exploitable according to the attacker's wishes.	High Impact	Almost certain	High Risk	trusted repository shall verify these updates before the device installs them. FDO Device shall also conduct updates via a secure network communication
[TH-14.1]	`Exploiting a device due to insecure configuration `	Due to lack of documentation, the device is incorrectly configured.	High Impact	Almost certain	High Risk	Manufacturer shall document all possible threats and vulnerabilities. Based on the documented risks and vulnerabilities, implement appropriate security measures specifically targeted to mitigate the vulnerabilities to an appropriate level
[TH-15.1]	`Advanced persistent threats`	Log and Event monitoring.	High Impact	Likely	High Risk	The device should be able to monitor log and activities on the device, enforce an access control of the monitored events to only authorized users.

8.3. Communication Mitigations§

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk	Mitigation
[TH-1.1]	`Replay of data`	An attacker edits and replays previously authenticated data between device and Rendezvous Server. (TO1)	High Impact	Almost Certain	High Risk	FDO Devices should use nonces to ensure that signatures are created on demand and not replayed (e.g., to ensure the "freshness" of signatures).

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk	Mitigation
[TH-1.2]	`Replay of data`	An attacker edits and replays previously authenticated data between device and Onboarding service. (TO2)	High Impact	Almost Certain	High Risk	FDO Devices should use nonces to ensure that signatures are created on demand and not replayed (e.g., to ensure the "freshness" of signatures).
[TH-1.3]	`Replay of data`	An attacker edits and replays communication between device and Management Service. (Device in Service)	High Impact	Almost Certain	High Risk	FDO Devices shall implement functionalities that detect replay and integrity violations of data-in-motion.
[TH-5.1]	`Man in the middle`	The threat of an attacker intercepting and extracting confidential credentials during communication between the device and a server.	Medium Impact	Almost Certain	High Risk	FDO Devices shall ensure data encryption in order to transmit and receive data protecting data from unauthorized disclosure. FDO Devices shall also implement a secure communication channel between trusted entities using the latest version of secure communication protocols.

8.4. FDO Application Mitigations§

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk	Mitigation
[TH-4.2]	`Deletion of data`	An attacker deletes stored credentials and configuration files needed by FDO application.	Medium Impact	Almost Certain	High Risk	Security credentials in persistent storage shall be protected using data signature or hashing algorithms.
		Attacker succeeds in				FDO Devices should include a hardware-level access control mechanism for memory, while

Threat ID Number	Threat	Scenario	Impact	Likelihood	Risk	Mitigation
[TH-6.1]	`Disclosure of credentials`	extracting FDO sensitive credentials on the device.	Medium Impact	Almost Certain	High Risk	security credentials in persistent storage shall be protected using data encryption algorithms or tamper-resistant storage.
[TH-7.2]	`Unauthorized access to the FDO application`	An unauthorized user gains access to the FDO app settings to alter security configurations.	Medium Impact	Almost certain	High Risk	FDO Device settings shall require authentication before any configuration item can be altered.
[TH-10.2]	`Failure of the FDO application`	An attacker sends maliciously crafted messages which cause the FDO application to crash or become unstable.	Medium Impact	Almost Certain	High Risk	FDO Devices shall handle all inputs and outputs in a secure manner such that an invalid input/output does not lead to a device malfunction/crash (e.g., checking for acceptable responses or output for both valid and invalid input).
[TH-11.4]	`Malicious/ Vulnerable device components`	Cryptographically flawed key generation process.	High Impact	Likely	High Risk	Third-party SW and HW components shall be reviewed and validated before being used on the device. The build environment and the toolchain used to create SW shall be under configuration management and version control while validating its integrity regularly.
		The application				FDO application shall enforce

Threat-ID Number	Threat	Scenario	Impact	Likelihood	Risk	Mitigation
[TH-12.1]	`Exchanging data with a rogue server`	accepts a rogue server as new owner and exchanges confidential credentials with it.	Medium Impact	Likely	High Risk	mutual authentication with remote entities (servers) before establishing a connection with them.

8.5. Security Profiles§

Device		Description	
Name	FIDO IoT Device Onboard	Basic Information	Details
Category	Application	Assets	Cryptographic Credentials
Usage	Device Onboarding & Authentication		FDO Application
Area of Use	Any Environment		Communication Protocols
• SFR: Security Functional Requirement • SAR: Security Assurance Requirement		Assumptions	security assumption(s)
		Security Features	security feature(s)

Threat ID	Threat	Asset	Vulnerability	Security Goal	SFR Ref	Security Function Requirement (SFF
[TH-5.1]	Man-in-the-middle	FDO Application Ownership Credential Device Credential	Insecure Data Transfer and Storage	Secure Communication	1.1	The device SHALL enforce data encryption to be able to transmit & receive user data ir a manner protected from unauthorized disclosure.
[TH-5.1]	Man-in-the-middle	IP Communication channel Non-IP Communication channel	Insecure Data Transfer and Storage	Secure Communication	1.2	The device SHALL provide a secure communication channel between itself and other trusted entities usin the latest stable version of secure communication protocols. Deprecated/Insecu older versioned protocols shall be disabled to prevent downgrade attacks.

Threat ID	Threat	Asset	Vulnerability	Security Goal	SFR Ref	Security Function Requirement (SFR
		Device Initialize Protocol (DI);				The device SHALL initiate communication via
[TH-5.1]	Man-in-the-middle	Transfer Ownership Protocol 0 (TO0); Transfer Ownership Protocol 1 (TO1); Transfer Ownership Protocol 2 (TO2);	Insecure Data Transfer and Storage	Secure Communication	1.3	secure channel for exchange of sensitive data such as authentication credentials, cryptographic keys, etc., to provide assured protection of the channel data from modification o disclosure.
[TH-1.1]	Replay of data	IoT Device Platform	Insecure Network Services	Secure Communication	1.4	The device SHALL prevent unauthorized connections on all service ports.
[TH-1.1]	Replay of data	IP Communication channel Non-IP Communication channel	Insecure Data Transfer and Storage	Secure Communication	1.5	The device SHALL implement functionalities that detect replay and integrity violations o data-in-motion OR shall use protocols that achieve the same goal.
[TH-12.1]	Exchanging data with a rouge server	IoT Device Platform	Insecure Network Services	Secure Communication	1.6	Access to device functionality via a network interface in the initialized state SHOULD only be possible after authentication on that interface.
[TH-12.1]	Exchanging data with a rouge server	IoT Device Platform	Insecure Network Services	Secure Communication	1.7	Device functionality that allows security-relevant changes in configuration via a network interface SHALL only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee

Threat ID	Threat	Asset	Vulnerability	Security Goal	SFR Ref	Security Function Requirement (SFR
						what configuration will be required for the device to operate.
[TH-4.1] [TH-4.2]	Deletion of data	FDO Application	Insecure Data Transfer and Storage	Secure Storage of Confidential Credentials	2.1	Integrity of Sensitiv security credentials in persistent storag SHALL be protecte using data signatur or hashing algorithms.
[TH-6.1]	Disclosure of credentials	IoT Device Platform FDO Application	Insecure Data Transfer and Storage	Secure Storage of Confidential Credentials	2.2	Confidentiality of Sensitive security credentials in persistent storage SHALL be protecte using data encryption algorithms or tampe resistant storage, to achieve data confidentiality.
[TH-6.1]	Disclosure of credentials	IoT Device Platform	Insecure Data Processing	Isolation of Data and Secure Restricted Operating Environment	3.1	The device SHALL ensure isolation in the execution of trustworthy service from less trusted or untrusted services.
[TH-6.1]	Disclosure of credentials	IoT Device Platform	Insecure Data Processing	Isolation of Data and Secure Restricted Operating Environment	3.2	The device SHOULD include a hardware-level access control mechanism for memory.
[TH-6.1]	Disclosure of credentials	IoT Device Platform	Insecure Data Processing	Isolation of Data and Secure Restricted Operating Environment	3.3	Devices that suppo suspension or hibernation states SHALL ensure integrity by signing the required resum state before going into low power mod and verifying this signed state upon resumption.
[TH-10.1]	Failure of the device OS/Firmware	IoT Device Platform FDO Application	Insecure Ecosystem Interfaces	Secure Data Interfaces	4.1	The device SHALL handle all inputs an outputs in a secure manner such that a invalid input/output does not lead to a device malfunction/crash.

Threat ID	Threat	Asset	Vulnerability	Security Goal	SFR Ref	Security Functional Requirement (SFR
[TH-10.1]	Failure of the device OS/Firmware	IoT Device Platform FDO Application	Insecure Ecosystem Interfaces	Secure Data Interfaces	4.2	The device SHALL validate all inputs and outputs before they are processed (e.g., checking for acceptable responses or outpu for both valid and invalid input).
[TH-11.7]	Malicious/ Vulnerable device components	IoT Device Platform	Lack of Physical Hardening	Secure Data Interfaces	4.3	There SHOULD be no access via debu interfaces, including JTAG and any form of scan chain
[TH-11.7]	Malicious/ Vulnerable device components	IoT Device Platform	Lack of Physical Hardening	Secure Data Interfaces	4.4	Where a debug interface is physically accessible, it SHAL be disabled in software. Where there is a business need to maintain ar interface on production devices, (for example, JTAG the device shall onl communicate with authorized and authenticated entities on the production devices.
[TH-12.1]	Exchanging data with a rouge server	IoT Device Platform FDO Application	Insecure Ecosystem Interfaces	Secure Data Interfaces	4.5	In the initialized state, the network interfaces of the device SHALL minimize the unauthenticated disclosure of security-relevant information.
[TH-8.2]	Physical attacks	IoT Device Platform	Lack of Physical Hardening	Secure Data Interfaces	4.6	Device hardware SHOULD not unnecessarily expose physical interfaces to attack.
[TH-14.1]	Exploiting a device due to insecure configuration	IoT Device Platform FDO Application	Insecure Default Settings	Secure Data Interfaces	4.7	All physical, networ and logical interfaces not required for the device's initial setup SHALL be disabled/inactive by default.

Threat ID	Threat	Asset	Vulnerability	Security Goal	SFR Ref	Security Function Requirement (SFR
[TH-14.1]	Exploiting a device due to insecure configuration	IoT Device Platform	Insecure Default Settings	Strong default security	5.1	Only software services that are used or required for the intended use or operation of the device SHALL be enabled.
[TH-14.1]	Exploiting a device due to insecure configuration	IoT Device Platform FDO Application	Insecure Default Settings	Strong default security	5.2	The device SHALL display adequate failure and error messages/ generic error codes to prevent leaking device information.
[TH-11]	Malicious/ Vulnerable device components	IoT Device Platform FDO Application	Use of Insecure or Outdated Components	Secure Supply Chain	6.1	Secure SW development processes SHALL be implemented for software components preser in the device.
[TH-11]	Malicious/ Vulnerable device components	IoT Device Platform	Use of Insecure or Outdated Components	Secure Supply Chain	6.2	Third-party SW and HW components SHALL be reviewed and validated befor being used on the device.
[TH-6]	Disclosure of credentials	IoT Device Platform FDO Application	Use of Insecure or Outdated Components	Secure Supply Chain	6.3	The device's development environment SHALL be separate from th business/ productio environment.
[TH-11]	Malicious/ Vulnerable device components	IoT Device Platform FDO Application	Use of Insecure or Outdated Components	Secure Supply Chain	6.4	The build environment and th toolchain used to create software SHALL be under configuration management and version control, and its integrity SHALL be validated regularly.
[TH-6]	Disclosure of credentials	IoT Device Platform	Insecure Manufacturing Process	Secure Supply Chain	6.5	The key insertion SHALL take place securely such that i protects the keys against copying.
[TH-	Exploiting an	IoT Device	Insecure			The device SHALL support a secure boot flow to ensure

Threat ID	Threat	Asset	Vulnerability	Security Goal	SFR Ref	Security Function Requirement (SFR
13.2]	insecure software	Platform	Default Settings	Software Integrity	7.1	only authorized software can be executed on the device
[TH-13.2]	Exploiting an insecure software	IoT Device Platform	Insecure Default Settings	Software Integrity	7.2	Software Images SHALL be cryptographically verified before each use.
[TH-13.2]	Exploiting an insecure software	IoT Device Platform	Insecure Default Settings	Software Integrity	7.3	If a component comprises multiple sub-images, each image SHOULD be verified separately
[TH-13.2]	Exploiting an insecure software	IoT Device Platform	Lack of Device Management	Software Integrity	7.4	The device SHALL provide a means of notification to alert the administrator whenever a SW or HW component fails verification.
[TH-13.1]	Downgrade attacks	IoT Device Platform	Lack of Secure Update Mechanism	Secure Update	8.1	The device SHALL implement anti-rollback functionality for all version-updateable components.
[TH-13.2]	Exploiting an insecure software	IoT Device Platform	Lack of Secure Update Mechanism	Secure Update	8.2	The device SHALL verify the authenticity and integrity of all software updates before they are installed. Where this is not practicable, a trusted repository shall verify these updates before the device installs them
[TH-13.2]	Exploiting an insecure software	IoT Device Platform Operational Environment	Lack of Secure Update Mechanism	Secure Update	8.3	The device SHALL conduct updates via a secure network connection from an authorized repository.
[TH-13.2]	Exploiting an insecure software	IoT Device Platform	Lack of Secure Update Mechanism	Secure Update	8.4	Device updates SHALL not modify user-configured preferences, security, and/or privacy settings without user notification.

Threat ID	Threat	Asset	Vulnerability	Security Goal	SFR Ref	Security Function Requirement (SFR
[TH-14.1]	Exploiting a device due to insecure configuration & management	IoT Device Platform	Lack of Device Management	Strong Device Identification	9.1	The device SHALL contain a unique an tamper-resistant device identifier.
[TH-14.1]	Exploiting a device due to insecure configuration	IoT Device Platform	Lack of Device Management	Secure Installation, Maintenance and Decommissioning	11.1	The manufacturer SHOULD provide users with guidance on how to securely set up their device.
[TH-14.1]	Exploiting a device due to insecure configuration	IoT Device Platform Operational Environment	Lack of Device Management	Secure Installation, Maintenance and Decommissioning	11.2	Guidance SHALL include all possible security measures related to the operational environment where the device is being used.
[TH-14.1]	Exploiting a device due to insecure configuration	IoT Device Platform	Lack of Device Management	Secure Installation, Maintenance and Decommissioning	11.3	Guidance SHALL describe the basic requirements needed for the successful installation of the device
[TH-14.1]	Exploiting a device due to insecure configuration	IoT Device Platform Confidential Credentials	Lack of Device Management	Secure Installation, Maintenance and Decommissioning	11.4	The supplier or manufacturer of any devices and/or services SHALL provide information about how the device removal and/or disposal is to be carried out to maintain the end user's privacy and security.
[TH-14.1]	Exploiting a device due to insecure configuration	IoT Device Platform	Lack of Device Management	Secure Installation, Maintenance and Decommissioning	11.5	Policy for secure decommissioning and recommissioning of devices SHALL be documented and followed by all concerned parties.
[TH-14.1]	Exploiting a device due to insecure configuration	IoT Device Platform Confidential Credentials	Lack of Device Management	Secure Installation, Maintenance and Decommissioning	11.6	A decommissioned device SHALL mak secrets and identities permanently inaccessible, denying attestation

Threat ID	Threat	Asset	Vulnerability	Security Goal	SFR Ref	Security Function Requirement (SFR
						and access to any bound data.
[TH-14.1]	Exploiting a device due to insecure configuration	IoT Device Platform Confidential Credentials FDO Application	Lack of Device Management	Secure Installation, Maintenance and Decommissioning	11.7	A device that is returned from decommissioned state SHALL become indistinguishable from a new device.
[TH-15.1]	Advanced persistent threats	IoT Device Platform FDO Application	Lack of Device Management	Secure Event Monitoring and Anomaly Detection	12.1	The device SHALL be able to generate a log of at least the following auditable events: user authentication, and security configuration changes.
[TH-15.1]	Advanced persistent threats	IoT Device Platform	Lack of Device Management	Secure Event Monitoring and Anomaly Detection	12.2	The device SHALL enforce an access control of the log files to only authenticated and authorized users.
[TH-15.1]	Advanced persistent threats	Operational Environment	Lack of Device Management	Secure Event Monitoring and Anomaly Detection	12.3	Device usage and measurement data, SHALL be examine for security anomalies.
[TH-11.12]	Malicious/ Vulnerable device components	IoT Device Platform	Weak Guessable, or Hardcoded Passwords	Credential Guessing Resilience	13.1	When a defined number of unsuccessful authentication attempts has been met or surpassed, the application SHALL implement a timeout throttle for the authentication functionality.
[TH-11.12]	Malicious/ Vulnerable device components	IoT Device Platform	Weak Guessable, or Hardcoded Passwords	Credential Guessing Resilience	13.2	The application SHALL exponentially increase retry attempt delays in th event of multiple unsuccessful authentication timeouts.
						Password entry SHALL follow the

Threat ID	Threat	Asset	Vulnerability	Security Goal	SFR Ref	Security Function Requirement (SFR
[TH-11.12]	Malicious/ Vulnerable device components	IoT Device Platform	Weak Guessable, or Hardcoded Passwords	Credential Guessing Resilience	13.3	standard recommendations. See FDO Allowed Cryptography List o the secure passwor policy.
[TH-11.12]	Malicious/ Vulnerable device components	IoT Device Platform	Weak Guessable, or Hardcoded Passwords	Credential Guessing Resilience	13.4	Where the device interface uses a PIN or password login f access control, the initial password or factory reset password SHALL b unique to each device in the produ family.
[TH-16.1]	Regulatory Sanctions	FDO Application	Insufficient Privacy Protection	Secure Handling of Personal Data	14.1	The confidentiality personal data transiting between a device and a service, especially associated services SHOULD be protected, with best practice cryptography. Refe to FDO Allowed Cryptography List
[TH-12.1]	Exchanging data with a rouge server	FDO Application Operational Environment	Lack of Device Management	Strong Application Authentication	15.1	The application SHALL enforce mutual authentication with remote entities (servers) before establishing a connection with them.
[TH-7.1]	Unauthorized access to the FDO application	FDO Application	Lack of Device Management	Strong Application Authentication	15.2	The application SHALL require authentication before any configuration item can be altered.
[TH-7.2]	Unauthorized access to the FDO application	Device Configuration	Lack of Device Management	Strong Application Authentication	15.2	The device settings SHALL require authentication before any configuration item can be altered.
[TH-7.2]	Unauthorized access to the FDO application	FDO Application	Lack of Device Management	Strong Application Authentication	15.3	The application SHALL require authentication before any configuration item

Threat ID	Threat	Asset	Vulnerability	Security Goal	SFR Ref	Security Function Requirement (SFR
						can be altered.

9. Security and Privacy Requirements Catalog§

Ref	Security Requirement Catalog	Security Goal	Assets
0.1	The vendor SHALL document an explicit device boundary. The device boundary SHALL include any component that performs or software that implements functionality used to fulfill the FDO Device Onboarding Requirement. NOTE: The Vendor SHOULD provide a clear description of the HW, supported OS versions that the evaluation is covering. (Name of the Device, Hardware Type and Version, Underlying Software Platform/OS). In addition, the vendor MUST provide a high-level physical and logical representation of the device security boundary. The documentation provided by the vendor SHOULD cover software attack protection and, if required, hardware attack protection.	Device Onboarding Definition and Key Management	n/a
0.2	The vendor SHALL document all FDO relevant security and cryptographic functions implemented within the onboarding device, both those on the § 11 FDO Allowed Cryptography List {#FDO_Allowed_Cryptography_List} and those not on the list.	Device Onboarding Definition and Key Management	n/a
0.3	The vendor SHALL document where device onboarding user private keys are stored and explain how these private keys are related to those used by the Device. Memory isolation is therefore important to prevent leakage of keys across applications, containers, or virtual machines. Private keys SHALL never be stored in plaintext. Private keys SHALL only be stored on encrypted disks or databases, or in hardware security-based storages such as TEE, SE, HSM, or TPM. If the private key is stored in a file or database, its encryption SHOULD be anchored in a hardware-based root of trust, such as a trusted platform module (TPM) or crypto tokens, to prevent theft of keys not in use. Applications performing the signing operations SHOULD only run on dedicated systems that are not being used for general computing to reduce the risk of side-channel attacks to obtain the keys. The system on which the private key is stored SHOULD be physically protected from theft.	Device Onboarding Definition and Key Management	n/a
0.4	The vendor SHALL document all Device Security Parameters (DSPs). Data parameters used by or stored within the onboarding device which are FDO Relevant are called “Device Security Parameter." These SHALL, at minimum, include all FDO user verification reference data, GUID, Intel EPID Signing Key, Intel EPID Group ID, Ownership Voucher extension (OVE) key pair, private key, ownership credential (containing GUID,	Device Onboarding Definition and Key Management	n/a

Ref	Security Requirement Catalog	Security Goal	Assets
	HMAC secret and other credentials), Manufacturing Credentials, Ownership Voucher, signature or registration operation counters, and FDO Relevant cryptographic keys.		
0.5	For each Device Security Parameter, the vendor SHALL document the protections that are implemented for this parameter in order to support the FDO Device Onboarding Security Goals or FDO Device Onboard Security Requirements, the location where this parameter is stored, how the parameter is protected in each storage location, how and when the parameter is input or output from the Device, in what form the parameter is input or output, and when (if ever) the parameter is destroyed. Those Device Security Parameters whose confidentiality MUST be protected in order to support the FDO Device Onboard Security Goals or FDO Device Onboard Security Requirements SHALL be documented as “Secret Device Onboard Security Parameters”;	Device Onboarding Definition and Key Management	n/a
1.1	The device SHALL enforce data encryption to be able to transmit and receive user data in a manner protected from unauthorized disclosure.	Secure Communication	Transfer Ownership Protocol 2 (TO2);
1.2	The device SHALL provide a secure communication channel between itself and other trusted entities using the latest stable version of secure communication protocols. Deprecated/Insecure older versioned protocols shall be disabled to prevent downgrade attacks.	Secure Communication	Transfer Ownership Protocol 2 (TO2);
1.3	The device SHALL initiate communication via a secure channel, for exchange of sensitive data like authentication credentials, cryptographic keys, etc., to provide assured protection of the channel data from modification or disclosure.	Secure Communication	Transfer Ownership Protocol 2 (TO2);
1.3.1	The device SHOULD use a transport protocol providing secure communication, where resources allow. If this requirement is not met, this MUST be reported in the user guidance.	Secure Communication	Device Initialize Protocol (DI) Transfer Ownership Protocol 0 (TO0) Transfer Ownership Protocol 1 (TO1) Transfer Ownership Protocol 2 (TO2);
1.4	The device SHALL prevent unauthorized connections on all service ports.	Secure Communication	IoT Device Platform

Ref	Security Requirement Catalog	Security Goal	Assets
1.5	The device SHALL implement functionalities that detect replay and integrity violations of data-in-motion OR shall use protocols that achieve the same goal.	Secure Communication	IP Communication channel Non-IP Communication channel
1.6	Access to device functionality via a network interface in the initialized state SHOULD only be possible after authentication on that interface.	Secure Communication	IoT Device Platform
1.7	Device functionality that allows security-relevant changes in configuration via a network interface SHALL only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate.	Secure Communication	IoT Device Platform
2.1	Integrity of Sensitive security credentials in persistent storage SHALL be protected using data signature or hashing algorithms.	Secure storage of Confidential credentials	FDO Application
2.2	Confidentiality of Sensitive security credentials in persistent storage SHALL be protected using algorithms from the § 11 FDO Allowed Cryptography List {#FDO_Allowed_Cryptography_List} or tamper resistant storage, to achieve data confidentiality	Secure storage of Confidential credentials	IoT Device Platform FDO Application
3.1	The device SHOULD ensure isolation in the execution of trust worthy service from less trusted or untrusted services, where applicable.	Isolation of Data and Secure Restricted Operating Environment	IoT Device Platform
3.2	The device SHOULD include a hardware-level access control mechanism for memory, where applicable.	Isolation of Data and Secure Restricted Operating Environment	IoT Device Platform
3.3	Devices that support suspension or hibernation states SHALL ensure integrity by signing the required resume state before going into low power mode and verifying this signed state upon resumption.	Isolation of Data and Secure Restricted Operating Environment	IoT Device Platform
4.1	The device SHALL handle all inputs and outputs in a secure manner such that an invalid input/output does not lead to a device malfunction, crash or violation of the security goals.	Secure Data Interfaces	IoT Device Platform FDO Application
4.2	The device SHALL validate all inputs and outputs before they are processed (e.g., checking for acceptable responses or output for both valid and invalid input).	Secure Data Interfaces	IoT Device Platform FDO Application

Ref	Security Requirement	Security Goal	Assets
4.3	There SHOULD be no access via debug interfaces, including JTAG and any form of scan chain.	Secure Data Interfaces	IoT Device Platform
4.4	Where a debug interface is physically accessible, it SHALL be disabled in software. Where there is a business need to maintain an interface on production devices, (for example, JTAG) the device shall only communicate with authorized and authenticated entities on the production devices.	Secure Data Interfaces	IoT Device Platform
4.5	In the initialized state, the network interfaces of the device SHALL minimize the unauthenticated disclosure of security-relevant information.	Secure Data Interfaces	IoT Device Platform FDO Application
4.6	Device hardware SHOULD not unnecessarily expose physical interfaces to attack.	Secure Data Interfaces	IoT Device Platform
4.7	All physical, network, and logical interfaces not required for the device's initial setup SHALL be disabled/inactive by default.	Secure Data Interfaces	IoT Device Platform FDO Application
5.1	Only software services that are used or required for the intended use or operation of the device SHALL be enabled. More specifically, services only needed for onboarding are disabled after onboarding completes.	Strong default security	IoT Device Platform
5.2	The device SHALL display adequate failure and error messages/ generic error codes to prevent leaking device information if a display is available.	Strong default security	IoT Device Platform FDO Application
6.1	Secure SW development processes SHALL be implemented for software components present in the device, following best security practices (e.g., Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities).	Secure Supply Chain	IoT Device Platform FDO Application
6.2	Third party SW and HW components SHALL be listed, reviewed, and validated before being used on the device.	Secure Supply Chain	IoT Device Platform
6.3	The device's development environment SHALL be separate from the business/ production environment.	Secure Supply Chain	IoT Device Platform FDO Application
6.4	The build environment and the toolchain used to create software SHALL be under configuration management and version control, and its integrity SHALL be validated regularly.	Secure Supply Chain	IoT Device Platform FDO Application

Ref	Security Requirement Catalog	Security Goal	Assets
6.5	The key insertion, if applicable, SHALL take place securely such that it protects the keys against copying.	Secure Supply Chain	IoT Device Platform
7.1	The device SHOULD support a secure boot flow to ensure only authorized software can be executed on the device. If this requirement is not met, this MUST be reported in the user guidance.	Software Integrity	IoT Device Platform
7.2	Software Images SHOULD be cryptographically verified before each use. If this requirement is not met, this MUST be reported in the user guidance.	Software Integrity	IoT Device Platform
7.3	If a component comprises multiple sub-images, each image SHOULD be verified separately	Software Integrity	IoT Device Platform
7.4	The device SHALL provide a means of notification to alert the administrator, during or after onboarding, whenever a SW or HW component fails verification.	Software Integrity	IoT Device Platform
8.1	The device SHALL implement anti-rollback functionality for all version-updateable components. NOTE: Anti-rollback is designed to prevent attacks such as reflashing a device with an older, more vulnerable image, in order to exploit its known vulnerabilities or to roll back some device settings to factory settings. This can be done by making sure earlier versions of the firmware cannot be loaded by malicious users. Similarly, it can be used to protect FDO Security Parameters from being reverted. Rollback is possible for recovery purposes but only if authorized.	Secure Update	IoT Device Platform
8.2	The device SHALL verify the authenticity and integrity of all software updates before they are installed. Where this is not practicable, a device-authenticated, trusted repository shall verify these updates before the device installs them. In case of inline updates via service info, the FDO Owner must verify the updates before the device installs them.	Secure Update	IoT Device Platform
8.3	If the device cannot verify the authenticity and integrity of any software updates before they are installed, the device SHALL conduct updates via a secure network connection from an authorized repository.	Secure Update	IoT Device Platform Operational Environment
8.4	Device updates SHALL NOT modify preferences, security, and/or privacy settings that are user-configured without user notification.	Secure Update	IoT Device Platform
9.1	The device SHALL contain a unique device identifier (FDO GUID). This device identifier SHOULD be tamper-resistant.	Strong Device Identification	IoT Device Platform
10.1	The device SHALL be capable of continuous minimal operation in adverse situations (e.g., loss of network access) and recover cleanly when the network signal is regained.	Resilience to Outages	IoT Device Platform

Ref	Security Requirement Catalog	Security Goal	Assets
11.1	The manufacturer SHALL provide users with guidance on how to set up their device securely, according to the threat model of this certification.	Secure Installation, Maintenance and Decommissioning	IoT Device Platform
11.2	Guidance SHALL include all applicable security measures related to the operational environment where the device is being used.	Secure Installation, Maintenance and Decommissioning	IoT Device Platform Operational Environment
11.3	Guidance SHALL describe the basic requirements needed for the successful installation of the device.	Secure Installation, Maintenance and Decommissioning	IoT Device Platform
11.4	The supplier or manufacturer of any devices and/or services SHALL provide information about how the device removal and/or disposal is to be carried out to maintain the end user's privacy and security.	Secure Installation, Maintenance and Decommissioning	IoT Device Platform Confidential Credentials
11.5	Policy for secure decommissioning and factory reset of devices SHALL be documented and delivered to all concerned parties. NOTE: For the definition of decommissioning, refer to section 3.2.6 in Security Evaluation Standard for IoT Platforms (SESIP) v1.1 | GP_FST_070	Secure Installation, Maintenance and Decommissioning	IoT Device Platform
11.6	A decommissioned device SHOULD make secrets and identities permanently inaccessible, denying attestation and access to any bound data. If this requirement is not met, this MUST be reported in the user guidance. FDO credentials are excluded from this requirement.	Secure Installation, Maintenance and Decommissioning	IoT Device Platform Confidential Credentials
11.7	A device that is factory reset SHALL become indistinguishable from the original device with exception of the firmware version and the FDO Credentials.	Secure Installation, Maintenance and Decommissioning	IoT Device Platform Confidential Credentials FDO Application
12.1	The device SHALL be able to generate a log of at least the following auditable events: user authentication and security configuration changes.	Secure Event Monitoring and Anomaly Detection	IoT Device Platform FDO Application
12.2	The device SHALL enforce an access control of the log files to only authenticated and authorized users.	Secure Event Monitoring and Anomaly Detection	IoT Device Platform

Ref	Security Requirement Catalog	Security Goal	Assets
12.3	The Vendor SHALL provide documentation on how Device usage and measurement data can be examined for security anomalies.	Secure Event Monitoring and Anomaly Detection	Operational Environment
13.1	If the device authenticates users, when a defined number of unsuccessful user authentication attempts has been met or surpassed, the application SHALL implement a timeout throttle for the authentication functionality.	Credential Guessing Resilience	IoT Device Platform
13.2	If the device authenticates users, the application SHALL exponentially increase retry attempt delays in the event of multiple unsuccessful user authentication timeouts.	Credential Guessing Resilience	IoT Device Platform
13.3	Password entry SHALL follow best security practices (e.g., ANSSI recommendations in section 4 of https://www.ssi.gouv.fr/uploads/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf).	Credential Guessing Resilience	IoT Device Platform
13.4	Where the device interface uses a PIN or password login for access control, the initial password or factory reset password SHALL be unique to each device in the product family.	Credential Guessing Resilience	IoT Device Platform
14.1	The confidentiality of personal data transiting between a device and a service, especially associated services, SHALL be protected, with best practice cryptography. Refer to § 11 FDO Allowed Cryptography List {#FDO_Allowed_Cryptography_List}	Secure Handling of Personal Data	FDO Application
15.1	The application SHALL enforce mutual authentication with remote entities (servers) before establishing a connection with them.	Strong Application Authentication	FDO Application Operational Environment
15.2	The device settings SHALL require authentication before any configuration item can be altered.	Strong Application Authentication	IoT Device Platform
15.3	The application SHALL require authentication before any configuration item can be altered.	Strong Application Authentication	FDO Application
16.1	All FDO keys (base and derived cryptographic key material) SHALL only be used for FDO operations. In other words, these keys SHALL NOT be used for any purpose but what is required to execute the TO1 and TO2 protocol exchanges.	Privacy	IoT Device Platform
16.2	Ownership transfer SHALL occur only once during the device lifecycle. If the device is re-commissioned (factory reset) then ownership transfer can occur again. 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 (e.g., onboarding multiple virtual machines running within the	Privacy	IoT Device Platform

Ref	Security Requirement Catalog	Security Goal	Assets
	device or a device with multiple hardware-based sub-devices).		
16.3	FDO Attestation SHOULD contain only the information specified in the specification for the payload. Each COSE header SHOULD contain the minimum number of fields needed to perform a signing operation, with other fields MUST be justified for privacy for a given application. Each COSE body SHOULD NOT contain OVEExtraInfo fields. Extra fields MUST be justified for privacy for a given application Each COSE body PublicKey SHOULD NOT use X5CHAIN and SHOULD NOT contain additional certificates. Any deviations MUST be justified for privacy for a given application. NOTE: Although this spec states OVEExtra and X5CHAIN SHOULD NOT be used, these features have been added so they can be used with justification. Any use of these options will be evaluated for privacy by the FIDO Certification Secretariat.	Privacy	IoT Device Platform
16.4	The Ownership Voucher SHALL contain the minimum amount of information necessary to validate each entity in the supply chain.	Privacy	IoT Device Platform

10. Security Parameters Stored on FDO Device§

The following is a classification of security parameters that are stored in the FDO Device.

- Externally provisioned credentials
- FDO Protocol parameters
- TLS parameters and TLS connection parameters, if TLS is in use

The following table describes parameters in each category:

Category	Name	Item	Preserve	Description
Externally Provisioned Credentials	Device Key	Private Key From Device Keypair	CAI*	Keypair may be ECDSA or EPID. Public key and/or Device certificate may be stored on the device but is not used for FDO. Certificate is stored in Ownership Voucher.
FDO Protocol Parameters	DCActive (bool)	Switch to Enable FDO on Boot	AI	Boolean examined on device boot to determine if FDO should be run or if the device should be booted normally.
FDO Protocol Parameters	DCProtVert (uint16)	Protocol Version	AI	Version of the FDO protocol to which FDO parameters pertain.
		HMAC secret for		HMAC secret for the HMAC in the

Category	Name	Item	Preserve	Description
FDO Protocol Parameters	DCHmacSecret (bstr)	HMAC in Ownership Voucher		Ownership Voucher header is protected by HMAC (See spec: OVHeaderHMac). The device stores the key to this HMAC.
FDO Protocol Parameters	DCDeviceInfo (tstr)	Device Info String	AI	String that describes the kind of device, often used to determine which capsule of initialization data is appropriate. Format is up to the device manufacturer.
FDO Protocol Parameters	DCGuid (bstr .size 16)	Device GUID	AI	Device identifier for onboarding, allocated at random by device manufacturer. Reset by Owner during TO2.
FDO Protocol Parameters	DCRVInfo (formatted CBOR array)	RendezvousInfo	AI	Structured instructions for finding a rendezvous server.
FDO Protocol Parameters	DCPubKeyHash (cbor: [int,bstr])	Hash of Mfg Public Key	AI	Hash of the manufacturer's public key, OVPubKey in the Ownership Voucher. This value anchors the base of the Ownership Voucher in the device, allowing the Ownership Voucher to be verified.
FDO Protocol Parameters	Nonce (bstr .size 16)	Nonces	AI	Nonces used during the FDO protocol, stored during protocol execution. 5 different nonces are used across the FDO protocols. See spec, section 3.3.7.
FDO Protocol Parameters	Selected Key Exchange suite	kexSuiteName	AI	Key exchange method selected by Device during TO2 protocol.
FDO Protocol Parameters	Selected Cipher Suite	cipherSuiteName	AI	Cipher suite mechanism selected by Device during TO2 protocol.
FDO Protocol Parameters	Rendezvous information derived from TO1 protocol	Rendezvous Blob	A	Identification of the TO2 server for purposes of FDO or TLS+FDO, derived from a Rendezvous Server as result of TO1 protocol. Used as the target for FDO or TLS+FDO connection in the TO2 protocol.
TLS parameters	TLS trust anchor	TLS Trusted Certificate Database	AI	List of server certificates trusted for TLS, usually CA certificates. Used to determine trust in the remote TLS server
TLS parameters	TLS Client Key	TLS Client Private Key	CAI	Client private key, if used with TLS. FDO is silent on whether a client certificate authentication is used with TLS.
TLS	TLS Client	TLS Client		Client certificate, which matches client private key, if used with TLS.

Category	Name	Item	Preserve	Description
Parameters	Certificate	Certificate	AI	FDO is silent on whether a client certificate authentication is used with TLS.
TLS Connection Parameters	TLS Ciphersuite	TLS Ciphersuite Code	AI	Selected ciphersuite during TLS connection.
TLS Connection Parameters	Key Exchange Mechanism	Selected Key Exchange Mechanisms	AI	Selected key exchange mechanism during TLS connection.

(*) CAI - Requirement for: C - Confidentiality; A - Availability; I - Integrity.

10.1. The following sources were consulted in the course of this work§

- FIDO Device Onboard Specification: https://fidoalliance.org/specs/FDO/fido-device-onboard-v1.0-ps-20210323/fido-device-onboard-v1.0-ps-20210323.html#OV
- FIDO Security Reference: https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-security-ref-v2.0-id-20180227.html#dfn-sa-1
- ARM PSA Platform Security Architecture Model: https://armkeil.blob.core.windows.net/developer/Files/pdf/PlatformSecurityArchitecture/Architect/DEN0079_PSA_SM_ALPHA-03_RC01.pdf
- ETSI EN 303 645: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- EUROSMART IoT SCS: https://www.eurosmart.com/eurosmart-iot-certification-scheme/
- OWASP IoT Vulnerabilities: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf
- GlobalPlatform Security Evaluation Standard for IoT Platforms (SESIP): https://globalplatform.org/specs-library/security-evaluation-standard-for-iot-platforms-sesip-v1-0-gp_fst_070/

11. FDO Allowed Cryptography List {#FDO_Allowed_Cryptography_List}§

11.1. Requirements for Additional Candidates§

If a vendor wants to add a cryptographic security function to the Allowed Cryptography list, then the vendor / lab shall provide a written argument that:

- Additional candidates for algorithms shall at least support a security strength of 112 bits,
- It iIs not a proprietary solution,
- It fulfills the required security attributes (e.g., if the use requires confidentiality and data authentication, the primitive provides this),
- It as a security strength that can be readily characterized,
- It is accepted or recommended by at least one major international standardization group (e.g.,ISO, IETF), or one national or European organizations (e.g., NIST [SP800-131Ar2], ANSI, SOGIS [SOGISCrypto]) and
- It has undergone extensive public review.

NOTE: The vendor is responsible for any extension of the COSE and EAT protocols to support a new cryptographic security function.

11.2. Allowed Cryptographic Functions§

The stated security level identifies the expected number of computations that a storage-constrained attacker (who has access to more than 2^80 bytes of storage) shall expend in order to compromise the security of the

cryptographic security function, under the currently best-known attack that can be conducted under this storage constraint. This has been extracted from the currently best-known relevant attacks against each cryptographic primitive, and is expected to shift over time as attacks improve.

At the time of this document's is publication, there are not yet any standardized (NIST Project or ISO/IEC JTC 1/SC 27/WG 2 SD8 on Post-Quantum Cryptography) quantum-safe cryptographic algorithms for asymmetric algorithms (e.g., signature, key protection based on RSA, and anonymous attestation). It is also not yet clear if the key size SHOULD (or SHOULD NOT) be increased for symmetric algorithms.

If the security level stated is n (*where the security level is here defined with a classical computing power, and does not take into account quantum cryptanalysis*), then the `expected number of computations` is less than the expected number of computations required to guess an `(n+1)-bit random binary string`, and `not less than the number of computations required` to guess an `n` bit random binary string (*i.e., on average, the number of computations required is less than `2^n` computations and greater than or equal to `2^(n-1)` computations.*)

11.2.1. Post-Quantum Cryptography

Requirements or rules other than those specified in this list of cryptographic algorithms may apply. Please refer to FDO specifications [FDO-Specification] for additional information and requirements.

Quantum computers are expected to solve problems faster than conventional computing can do. To what extent quantum computers will shorten the time needed to solve some difficult mathematical problems is a matter of controversy. In theory, a large scale, stable, and fault-tolerant quantum computer leveraging Shor's algorithm could break asymmetric cryptography based on either RSA or Elliptic Curve technology. This means that the factorization of large composite numbers (on which RSA security is based) or the computation of discrete logarithms (on which DSA and ECDSA are based) would become feasible with the use of a quantum computer regardless of the sizes of the keys.

When such mature quantum computers will be available for cryptanalysis purposes is another unknown. Yet because of the serious consequences of this threat becoming a reality, the NIST has decided to start developing standards for asymmetric quantum safe cryptography (https://csrc.nist.gov/projects/post-quantum-cryptography). A call for contributions has started the process for the selection of quantum safe algorithms eligible for standardization back in 2016. Discussions on standardization of quantum safe cryptographic primitives are also ongoing at ETSI CYBER and ISO/IEC JTC 1/SC 27. Stateful hash-based signatures are the first family of quantum safe cryptographic mechanisms standardized (NIST SP 800-208 and ISO 14888-4).

NIST has recently published the list of selected post-quantum algorithms for asymmetric cryptography after the conclusion of the Round 3 of the screening process (https://csrc.nist.gov/projects/post-quantumcryptography/round-3-submissions). This list includes 3 finalist (Crystals-Dilithium, Falcon, Rainbow) and 3 alternate (GeMSS, Picnic, Sphincs+) candidates for a signature algorithm, and 4 finalist (Kyber, NTRU, SABER, Classic McEliece) and 5 alternate (Bike, FrodoKEM, HQC, NTRUprime, SIKE) candidates for a Key Encryption Mechanism/Encryption algorithm. NIST expects to select at most one candidate between Kyber, NTRU and Saber for KEM, and one between Dilithium and Falcon (all based on structured lattices). The final standard will be released as draft for public comment in 2022-2023, and finalized by 2024.

NIST has not planned to standardize key agreement mechanisms to replace DH/ECDH. NIST explained the rationale in its FAQ: "NIST believes that in its most widely used applications, such as those requiring forward secrecy, Diffie-Hellman can be replaced by any secure KEM with an efficient key generation algorithm." Another solution is to use a hybrid approach, mixing a "classical" algorithm with a quantum-safe one. In this case, keys derived by a hybrid key establishment scheme remain secure if at least one of the underlying schemes is secure. NIST plans to incorporate a hybrid key establishment construction in a future revision of NIST SP 800- 56C.

Dealing with symmetric cryptography, a conservative approach regarding post-quantum symmetric cryptography is to double the key size (i.e., migrating from AES-128 to AES-256) and increase the digest size (i.e., migrating from SHA-256 to SHA-384). But Grover's algorithm (which could theoretically be used to weaken the security of block ciphers and hash functions) will provide little or no advantage for attacking symmetric cryptography or hash functions. Consequently, AES-128, AES-192 and SHA-256 are still recommended in this version of the document.

11.2.2. Confidentiality Algorithms§

When using a symmetric algorithm with a particular mode of operation (e.g., counter mode) or in a combination (e.g., data authentication algorithm as the combination of a MAC and a hash), the resulting security strength is the lowest security strength of the underlying primitives.

NOTE: Provide confidentiality, up to the stated security level.

Algorithm	Specified in	Security Level (bits)
AES-128	[FIPS197], [ISOIEC-18033-3]	128
AES-192	[FIPS197], [ISOIEC-18033-3]	192
AES-256	[FIPS197], [ISOIEC-18033-3]	256

11.2.3. Hashing Algorithms§

NOTE: Provide pre-image resistance, second pre-image resistance, and collision resistance.

Algorithm	Specified in	Security Level (bits)
SHA-256	[FIPS180-4], [ISOIEC-10118-3]	128
SHA-384	[FIPS180-4], [ISOIEC-10118-3]	192
SHA-512	[FIPS180-4], [ISOIEC-10118-3]	256

11.2.4. Data Authentication Algorithms§

NOTE: Provide data authentication. It is not uncommon to truncate the result of a MAC, but to be resistant, the final length should be at least 96 bits (see SOGIS Note 14-MACTruncation96 in SOGISCrypto). The security level cannot exceed the final length.

Algorithm	Specified in	Security Level (bits)
HMAC using an allowed hashing algorithm	[FIPS198-1]	Minimum of the length of the output of the hash used[1], one-half of the number of bits in the hash state[2], or the number of bits in the HMAC key.
HMAC-SHA256	RFC4868	256
HMAC-SHA384	RFC4868	384
HMAC-SHA512	RFC4868	512

NOTE: [1]Both due to the obvious guessing attack, and covers the case where the supplied key is hashed for the HMAC. [2]Based on a birthday attack; a collision of the final state can lead to an existential forgery of longer messages with the same prefix.

11.2.5. Key Protection Algorithms§

NOTE: Provide confidentiality and data authentication.

Algorithm	Specified in	Security Level (bits)
RSAOAEP	[RFC3447]. Key generation must be according to [FIPS186-4](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf).	Depends on the parameter size: according to NIST, 112 bits for RSA 2048 and 128 bits for RSA 3072
CBC Mode	[SP800-38A]	

11.2.6. Agreement Algorithms

Allowing two or more parties to generate a shared secret. It is generally followed by a key derivation function (KDF), as described in the next section, to generate one or several keys from the shared secret.

Algorithm	Specified in	Security Level (bits)
Diffie-Hellmann (DH) with 2048-bit key	[SP800-56Ar3], [ISOIEC-11770-3]	>= 112
ECDH on P-256	[SP800-56Ar3], NIST P-256, ISO/IEC 13157-2	128
ECDH on P-384	[SP800-56Ar3], [FIPS186-4], ISO/IEC 13157-2	192

11.2.7. Key Derivation Functions (KDFs)

Algorithm	Specified in	Security Level (bits)
KDF in counter mode	[SP800-108]	min(Bit length of key derivation key Ki used as input, Security level of PRF)

11.2.8. Signature Algorithms

NOTE: Provide integrity, authentication, and non-repudiation.

Algorithm	Specified in	Security Level (bits)
ECDSA on NIST P-256	[ECDSA-ANSI], [FIPS186-4], [ISOIEC-14888-3]	128
ECDSA on NIST P-384	[ECDSA-ANSI], [FIPS186-4], [ISOIEC-14888-3]	192
RSA2048 PKCS v1.5	[FIPS186-4] [ISOIEC-9796-2]	112
RSA2048 PKCS v2.1 (PSS)	[FIPS186-4] [ISOIEC-9796-2]	112
RSA3072 PKCS v1.5	[FIPS186-4] [ISOIEC-9796-2]	128
RSA3072 PKCS v2.1 (PSS)	[FIPS186-4] [ISOIEC-9796-2]	128

11.2.9. AEAD Algorithms§

NOTE: Provide confidentiality and data authentication.

Algorithm	Specified in	Security Level (bits)
AES-GCM	[SP800-38D]	Equal to the security strength of the underlying cipher.
AES-CCM	[SP800-38C]	Equal to the security strength of the underlying cipher.
ChaCha20-Poly1305	RFC8439	256

NOTE: ChaCha20-Poly1305 is specified in the given IETF RFC, but it is on the informational track. It is recommended by French ANSSI.

Appendix A: Cryptography Table List§

For an overview of Cryptography used in FDO, see[FDO-Specification] Appendix C (https://fidoalliance.org/specs/FDO/FIDO-Device-Onboard-RD-v1.1-20211214/FIDO-device-onboard-spec-v1.1-rd-20211214.html)

NOTE: **FIDO Alliance** *is aware of a later use of* **Future Crypto (Enhanced Strength for Quantum Safe Cryptography)** *and will update the tables once* **standardized** (NIST, ISO/IEC).

References§

Normative 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

Informative References§

[EAT]
G. Mandyam; L. Lundblade; J. O'Donoghue. *The Entity Attestation Token (EAT) draft-ietf-rats-eat*. Standards Track. URL: https://datatracker.ietf.org/doc/draft-ietf-rats-eat

[ECDSA-ANSI]
Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography ANSI X9.63-2011 (R2017). 2017. URL: https://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.63-2011+(R2017)

[FIPS180-4]
FIPS PUB 180-4: Secure Hash Standard (SHS). August 2015. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[FIPS186-4]
FIPS PUB 186-4: Digital Signature Standard (DSS). July 2013. URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[FIPS197]
FIPS PUB 197: Specification for the Advanced Encryption Standard (AES). November 2001. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[FIPS198-1]
FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC). July 2008. URL: http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

[ISOIEC-10118-3]
SM3 Cryptographic Hash Algorithm. October 2018. URL: https://www.iso.org/standard/67116.html

[ISOIEC-11770-3]
ISO/IEC 11770-3: Information Technology – Security Techniques - Key Management - Part 3: Mechanisms using asymmetric techniques. 2015-08. URL: https://www.iso.org/standard/60237.html

[ISOIEC-14888-3]
SM2: Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves: Part 1: General November 2018. URL: https://www.iso.org/standard/76382.html

[ISOIEC-18033-3]
ISO/IEC 18033-3 Information Technology - Security Techniques - Encryption algorithms – Part 3: Block ciphers. 2010-12. URL: https://www.iso.org/standard/54531.html

[ISOIEC-9796-2]
ISO/IEC 9796-2: Information Technology – Security Techniques - Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms. 2010-12. URL: https://www.iso.org/standard/54788.html

[RFC3447]
J. Jonsson; B. Kaliski. *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*. February 2003. obsoleted by RFC 8017. URL: https://tools.ietf.org/html/rfc3447

[SOGISCrypto]
SOG-IS Crypto Working Group. *SOG-IS crypto evaluation scheme agreed cryptographic mechanisms*. January 2020. URL: https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

[SP800-108]
Lily Chen. *NIST Special Publication 800-107: Recommendation for Key Derivation Using Pseudorandom Functions*. October 2009. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf

[SP800-131Ar2]
E. Barker; A. Roginsky. *NIST Special Publication 800-131A: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. March 2019. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

[SP800-38A]
M. Dworkin. *NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. Dec 2001. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[SP800-38C]
M. Dworkin. *NIST Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*. July 2007. URL: http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf

[SP800-38D]
M. Dworkin. *NIST Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. November 2007. URL: https://csrc.nist.gov/publications/detail/sp/800-38d/final

[SP800-56Ar3]
Elaine Barker; et al. *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. April 2018. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf

↑

→