**FIDO Testing Procedures**

**UAF Interoperability Testing Procedures**

Following the policies above, UAF testing will iterate through the prescribed combination of Authenticators / ASMs, Clients and Servers. This will require the following configuration for each set of tests:

按照上述策略，UAF 測試將反覆運算身份驗證器/ASM、用戶端和伺服器的規定組合。這將需要對每組測試進行以下配置：

* The Client+Authr combo, or Client and ASM+Authr combo will be loaded on to a single implementation
* The Server will install the metadata for the Authenticator with corresponding policies and permissions
* 用戶端+Authr組合，或用戶端和ASM+Authr組合將被載入到單個實現中
* 伺服器將使用相應的策略和許可權安裝身份驗證器的元數據

For each prescribed combination, the following tests will be performed in front of a facilitator:

對於每個規定的組合，將在主持人面前進行以下測試：

1. **Register:** perform valid registration with the server.
2. **Authenticate:**perform valid authentication with the server.
3. **Transaction:** perform a transaction with the server. The test must show a text or image indicator of the transaction that is being performed and confirmation that the transaction was successful.
4. **De-Register**: remove the registration from the device. Confirm that de-registration was successful by attempting an authentication with the server and confirming that it fails.
5. **註冊：**向伺服器執行有效註冊。
6. **身份驗證：**對伺服器執行有效的身份驗證。
7. **事務：**與伺服器執行事務。測試必須顯示正在執行的交易的文本或圖像指示器，並確認交易成功。
8. **取消註冊**：從設備中刪除註冊。通過嘗試向伺服器進行身份驗證並確認失敗，確認取消註冊成功。

Note that due to the time required for configuration of each test and the potential number of combinations for UAF interoperability testing, each test event will span three days. Implementers are expected to attend each day, even if their implementations have already passed all of their designated tests, to facilitate any necessary re-testing. If it is determined that fewer days of testing are required for the interoperability test, participants will be notified at minimum 7 days prior to the event or as soon as reasonably possible.

請注意，由於配置每個測試所需的時間以及UAF互操作性測試的潛在組合數量，每個測試事件將持續三天。即使他們的實施已經通過了所有指定的測試，也應每天參加，以促進任何必要的重新測試。如果確定互操作性測試所需的測試天數較少，則將在活動開始前至少 7 天或儘快通知參與者。

**U2F Interoperability Testing Procedures**

Following the policies above, U2F testing will iterate through the prescribed combination of Authenticators and Server. Interoperability testing is performed with the Chrome browser as the U2F Client. Testing is performed with the native U2F functionality of the browser and the U2F Chrome Extension will not be allowed in testing. This policy may be changed when other U2F Clients become available. Each combination of Authenticator and Server will be required to perform the following tests for a facilitator:

按照上述策略，U2F 測試將反覆運算身份驗證器和伺服器的規定組合。互操作性測試使用 Chrome 瀏覽器作為 U2F 用戶端執行。測試是使用瀏覽器的本機 U2F 功能執行的，並且不允許在測試中使用 U2F Chrome 擴展程式。當其他U2F用戶端可用時，此政策可能會更改。身份驗證器和伺服器的每個組合都需要為促進者執行以下測試：

1. **Register**: The U2F Authenticator will be required to register itself with the U2F Server.
2. **Authenticate**: The U2F Authenticator, after being registered with the server, will be required to demonstrate that it can authenticate with the server.
3. **註冊**：U2F 身份驗證器將需要向 U2F 伺服器註冊自身。
4. **身份驗證**：U2F 身份驗證器在向伺服器註冊后，將需要證明它可以向伺服器進行身份驗證。

Per the specifications, human interaction is required for each of these steps, such as the touch of a button; the insertion or removal of a device; etc. If the insertion of a device is being used as the form of human interaction, it should require being re-inserted each time a test step is performed.

根據規範，每個步驟都需要人工交互，例如觸摸按鈕;插入或移除設備;等。如果設備的插入被用作人機交互的形式，則應要求在每次執行測試步驟時重新插入。

Implementations may also perform the following test steps:

實現還可以執行以下測試步驟：

1. **Negative Register**: Register with an invalid certificate in a way that should be rejected by the server.
2. **Negative Authentication**: After valid registration, authenticate with invalid credentials in a way that may be rejected by the server.
3. **負寄存器**：以伺服器應拒絕的方式使用無效證書進行註冊。
4. **否定身份驗證**：有效註冊后，以伺服器可能拒絕的方式使用無效憑據進行身份驗證。

These optional steps are optional for a client to implement, since some implementations may have difficulty implementing invalid certificates or the other mechanisms required for performing these test steps. However, for clients that do perform these optional steps, servers are required to pass the interoperability testing.

這些可選步驟對於客戶端來說是可選的，因為某些實現可能難以實現無效證書或執行這些測試步驟所需的其他機制。但是，對於執行這些可選步驟的客戶端，伺服器需要通過互操作性測試。

**FIDO2 Interoperability Testing Procedures**

FIDO2 testing will iterate through the prescribed combination of Authenticators, Browsers, and Servers.FIDO2 測試將遍歷身份驗證器、瀏覽器和伺服器的規定組合。

This will require the following configuration for each set of tests:這將需要對每組測試進行以下配置：

Required for all Servers and Authenticators

所有伺服器和身份驗證器都需要

1. **Register**: The FIDO2 Authenticator will be required to register itself with the FIDO2 Server.
2. **Authenticate**: The FIDO2 Authenticator, after being registered with the server, will be required to demonstrate that it can authenticate with the server.
3. **Reset:**erase and revert back to factory settings and reauthenticate
4. **註冊**：FIDO2 身份驗證器將需要向 FIDO2 伺服器註冊自身。
5. **身份驗證**：FIDO2 身份驗證器在向伺服器註冊后，將需要證明它可以向伺服器進行身份驗證。
6. **重置：**抹掉並恢復為出廠設置並重新進行身份驗證

Optional Authenticator Functionality可選身份驗證器功能

1. **Client PIN:**demonstrate PIN-based user verification (if applicable)
   1. Set PIN
   2. Register with PIN
   3. Authenticate with PIN
   4. Change PIN
   5. Authenticate with new PIN
2. **Resident Key:**demonstrate that authenticator can create a resident key (if applicable)
3. **Multi-Account:**demonstrate that the authenticator can support multiple users at the same service (if applicable)
4. HMAC extension
5. **用戶端 PIN：**演示基於 PIN 的使用者驗證（如果適用）
   1. 設置密碼
   2. 使用密碼註冊
   3. 使用 PIN 進行身份驗證
   4. 更改密碼
   5. 使用新 PIN 進行身份驗證
6. **駐留金鑰：**演示身份驗證器可以創建駐留金鑰（如果適用）
7. **多帳戶：**證明身份驗證器可以支援同一服務的多個使用者（如果適用）
8. HMAC 擴展

Required Browser Interoperability所需的瀏覽器互操作性

1. **Servers**
   1. Firefox 61 or later with a reference U2F token
   2. Edge Edge Edge 44.17723.1000.0 with all eligible participating authenticators
   3. Chrome 69 or later with all eligible participating authenticators
2. **Authenticators**:
   1. **USB CTAP2 Authenticators**
      1. Edge Edge Edge 44.17723.1000.0 with all participating servers
      2. Chrome 69 or later with all participating servers
   2. **NFC CTAP2 Authenticators**
      1. Edge Edge Edge 44.17723.1000.0 with all participating servers
   3. **BLE CTAP2 Authenticators**
      1. Chrome 69 or later with all participating servers

Level 1 Authenticator Certification is a required component for FIDO Certification. All implementations must complete and pass the testing procedures for Level 1 Authenticator Certification (Section 5.4.4) in order to achieve FIDO Certification.

1 級身份驗證器認證是 FIDO 認證的必需元件。所有實施必須完成並通過 1 級身份驗證器認證（第 5.4.4 節）的測試程式才能獲得 FIDO 認證。

Per the specifications, human interaction is required for each of these steps, such as the user verification gesture; the insertion or removal of a device; etc. If the insertion of a device is being used as the form of human interaction, it should require being re-inserted each time a test step is performed.

根據規範，每個步驟都需要人工交互，例如使用者驗證手勢;插入或移除設備;等。如果設備的插入被用作人機交互的形式，則應要求在每次執行測試步驟時重新插入。

Level 1 Authenticator Certification Testing Procedures

For Authenticators seeking Level 1 Authenticator Certification, Authenticator Security Requirements below in Table 3 must be verified during Conformance Self-Validation or Interoperability Testing. For more information visit the [Authenticator Certification Level](https://fidoalliance.org/certification/authenticator-certification-levels/) page.

對於尋求 1 級身份驗證器認證的身份驗證器，必須在一致性自我驗證或互操作性測試期間驗證表 3 中的身份驗證器安全要求。有關更多資訊，請訪問[身份驗證器認證級別](https://fidoalliance.org/certification/authenticator-certification-levels/)頁面。

Requirements and the Vendor Questionnaire are defined in the Authenticator Security Requirements.

要求和供應商調查問卷在身份驗證器安全要求中定義。

**Note:**Authenticators completing L2 and higher are not required to demonstrate the Requirements during Conformance Self-Validation or Interoperability Testing, the Authenticator Security Requirements are evaluated by an Accredited Security Laboratory during the Security Evaluation step of Authenticator Certification.

**注意：**完成 L2 及更高級別的身份驗證器不需要在一致性自我驗證或互操作性測試期間證明要求，身份驗證器安全要求由認可的安全實驗室在身份驗證器認證的安全評估步驟中進行評估。

Evaluation Methods include Conformance Self-Validation and Interoperability Testing:

評估方法包括一致性自我驗證和互操作性測試：

* For **Conformance Self-Validation**, the Requirement is verified automatically during registration or testing.
* For **Interoperability Testing**, the Vendor shall demonstrate to the Test Proctor how the Authenticator meets the Requirement during Interoperability Testing.

1. 對於**一致性自我**驗證，要求在註冊或測試期間自動驗證。
2. 對於互操作性測試，供應商應在互操作性測試期間向測試監考人員證明身份驗證器如何滿足要求。

**L1 Interoperability Requirements Mapping**

**L1 互操作性需求映射**

| **Specification(s)** | **Authenticator Certification Requirement** | **Evaluation Method** |
| --- | --- | --- |
| UAF & FIDO2 | **1.4** | Interoperability Testing |
| UAF & FIDO2 | **1.9** | Interoperability Testing |
| UAF, U2F, & FIDO2 | **3.1** | Interoperability Testing |
| UAF & FIDO2 | **3.4** | Interoperability Testing |
| UAF & FIDO2 | **3.5** | Interoperability Testing |
| UAF, U2F, & FIDO2 | **3.9** | Interoperability Testing |
| UAF & FIDO2 | **4.4** | Interoperability Testing |
| UAF, U2F, & FIDO2 | **6.2** | Interoperability Testing |
| UAF, U2F, & FIDO2 | **6.3** | Interoperability Testing |