## 互操作性測試活動

互操作性測試活動是實施者收集和驗證其實施是否相互兼容的論壇。這意味著每個實施者將與其他實施者一起測試他們的實施。例如，一個 FIDO UAF 客戶端將在 UAF 互操作性事件中使用所有 UAF 服務器和所有 UAF 驗證器進行測試；同樣，FIDO U2F 服務器需要在 U2F 互操作性事件中使用所有 U2F 驗證器進行測試。對於每個參與者組合，將執行下面列出的相應 UAF 和 U2F 測試程序。實施表明他們可以在活動中通過所有其他實施的測試程序，或者可以表明任何失敗的測試程序不是由於其實施不符合 FIDO 規範，認證。

互操作性活動至少每 90 天舉行一次，其時間表可在下方找到。在註冊互操作性事件之前，實現必須通過一致性自我驗證，並且在互操作性事件之前不得更改實現。參與者必須至少在活動開始前 14 天註冊。需要簽訂保密協議來保護所有測試參與者的機密信息。保密協議可在此處獲得。

如果沒有足夠的實施來舉辦互操作性測試活動，活動將被取消，潛在參與者將在活動開始前 12 天收到通知。

作為互操作性事件註冊期間的選項之一，將向實施者提供是否參與預測試的選擇。預測試的目的是讓將要參加互操作性活動的公司能夠在活動開始前相互交換軟件、元數據和進行測試。對於那些選擇加入預測試的實施者，他們的聯繫信息將在活動開始前與其他實施者共享，以便他們可以相互溝通以共享適當的信息並執行預測試。

鼓勵實施者親自參加互操作性活動，以幫助促進互動和解決問題。對於無法前往互操作性活動的參與者，將提供遠程訪問；然而，遠程參與不是首選，因為它使互操作性活動期間的交流和參與變得更加困難。遠程參與者應準備好設置網絡攝像頭和屏幕共享功能，以便可以在執行互操作性步驟時對其進行視覺驗證。

將為規範的活動版本舉行互操作性活動，這包括尚未達到日落日期的所有版本。請參考當前支持的認證版本表。

# 互操作性事件（FIDO2、U2F 和 UAF）

**FIDO 2022 互操作性活動日期：**

- 2022 年 12 月 13-16 日

Register Now

---

# 按需測試

引入按需測試作為參加互操作性活動的替代方法。全年提供按需測試。

按需測試使用 FIDO® 認證參考實施來完成測試。如果參考實現的數量等於測試的最低要求（每個實現類中來自三個唯一供應商的三個實現），則該實現有資格進行按需測試。供應商可以查看參考實施庫。

具有認證實施的 FIDO 成員可以通過填寫捐贈表格將其實施捐贈給 FIDO 參考實施庫。

目前有一個選項可用於按需測試：

**虛擬的**

虛擬按需認證要求提交按需測試的供應商向認證秘書處提供其實施操作的訪問權限和說明。認證秘書處將促進按需互操作性測試過程。必須提供供應商公司代表的聯繫信息，並且如果在測試期間出現任何問題或問題，該代表必須在他們的測試時段內可用。

獲得認證

功能認證

認證的身份驗證器級別

生物識別組件認證

認證維護和更新

互操作性測試

互操作事件

1. **註冊**：向服務器進行有效註冊。
2. **Authenticate**：與服務器進行有效的認證。
3. **事務**：執行與服務器的事務。測試必須顯示正在執行的交易的文本或圖像指示符以及交易成功的確認信息。
4. **取消註冊**：從設備中刪除註冊。通過嘗試與服務器進行身份驗證並確認它失敗來確認註銷成功。

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，每個測試活動將持續三天。即使他們的實施已經通過了所有指定的測試，實施者也應該每天參加，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，將至少在活動開始前 7 天或在合理可能的情況下盡快通知參與者。

# U2F 互操作性測試程序

按照上述政策，U2F 測試將迭代驗證器和服務器的規定組合。使用 Chrome 瀏覽器作為 U2F 客戶端執行互操作性測試。測試是使用瀏覽器的本機 U2F 功能執行的，測試中不允許使用 U2F Chrome 擴展程序。當其他 U2F 客戶端可用時，此政策可能會更改。Authenticator 和 Server 的每個組合都需要為服務商執行以下測試：

1. **註冊**：U2F 驗證器需要向 U2F 服務器註冊。
2. **Authenticate**：U2F Authenticator 在向服務器註冊後，將被要求證明它可以向服務器進行身份驗證。

根據規範，每個步驟都需要人機交互，例如觸摸按鈕；插入或移除設備；等 如果插入設備被用作人機交互的形式，則每次執行測試步驟時都應要求重新插入。

實現還可以執行以下測試步驟：

1. **Negative Register**：以服務器應拒絕的方式註冊無效證書。
2. **Negative Authentication**：有效註冊後，以服務器可能拒絕的方式使用無效憑據進行身份驗證。

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，服務器需要通過互操作性測試。

# FIDO2 互操作性測試程序

FIDO2 測試將迭代驗證器、瀏覽器和服務器的規定組合。

這將需要為每組測試進行以下配置：

所有服務器和身份驗證器都需要

1. **註冊**：FIDO2 驗證器需要在 FIDO2 服務器上註冊。
2. **Authenticate**：FIDO2 Authenticator 在向服務器註冊後，將被要求證明它可以向服務器進行身份驗證。
3. **重置**：擦除並恢復為出廠設置並重新驗證

可選的驗證器功能

1. **客戶端 PIN**：演示基於 PIN 的用戶驗證（如果適用）
    1. 設置密碼
    2. 使用 PIN 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
2. **Resident Key**：證明 authenticator 可以創建一個 resident key（如果適用）
3. **多賬戶**：證明身份驗證器可以支持多個用戶使用同一服務（如果適用）
4. HMAC 擴展

Level 1 Authenticator Certification 是 FIDO Certification 的必需組件。所有實施都必須完成並通過 1 級驗證器認證（第 5.4.4 節）的測試程序，才能獲得 FIDO 認證。

根據規範，每個步驟都需要人工交互，例如用戶驗證手勢；插入或移除設備；等 如果插入設備被用作人機交互的形式，則每次執行測試步驟時都應要求重新插入。

# 一級認證器認證測試程序

對於尋求 1 級認證器認證的認證器，表 3 中的認證器安全要求必須在一致性自我驗證或互操作性測試期間得到驗證。有關詳細信息，請訪問身份驗證器認證級別頁面。

要求和供應商調查問卷在認證器安全要求中定義。

**注意：**完成 L2 及更高級別的認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，認證器安全要求由認可的安全實驗室在認證器認證的安全評估步驟中進行評估。

評估方法包括一致性自我驗證和互操作性測試：

- 對於**一致性自我驗證**，要求在註冊或測試期間自動驗證。
- 對於**互操作性測試**，供應商應向測試人員證明認證器在互操作性測試期間如何滿足要求。

### L1 互操作性需求映射

| 規格） | 認證器認證要求 | 評估方法 |
|---|---|---|
| UAF 和 FIDO2 | 1.4 | 互操作性測試 |
| UAF 和 FIDO2 | 1.9 | 互操作性測試 |
| UAF、U2F 和 FIDO2 | 3.1 | 互操作性測試 |
| UAF 和 FIDO2 | 3.4 | 互操作性測試 |
| UAF 和 FIDO2 | 3.5 | 互操作性測試 |
| UAF、U2F 和 FIDO2 | 3.9 | 互操作性測試 |
| UAF 和 FIDO2 | 4.4 | 互操作性測試 |
| UAF、U2F 和 FIDO2 | 6.2 | 互操作性測試 |
| UAF、U2F 和 FIDO2 | 6.3 | 互操作性測試 |

獲得認證

功能認證

認證的身份驗證器級別

生物識別組件認證

認證維護和更新

互操作性測試

互操作事件