密碼故事

了解 FIDO：註冊和認證

AEP韓國網
2019.4.10.18:20

FIDO（Fast IDentity Online）是應用"公鑰密碼學"的代表技術，根據應用加密技術的地方總結了運算的概念。

FIDO使用的"Public-Key Cryptography"僅使用屬於橢圓曲線密碼學（ECC）的ECDSA密碼算法。

作為參考，PKI 代表公鑰基礎設施，是一種除了公鑰加密方法之外還需要 CA 機構（外部公共機構）的方法。

在線快速身份識別 (FIDO)

FIDO使用人的生物識別信息（指紋、臉型、虹膜等）或外部認證設備（Yubikey、Titan Security key等）（Public Key Cryptography）"標準的認證協議，提供更方便和安全的認證功能. 也就是說，FIDO支持所有的認證技術，不僅包括生物識別技術，還包括現有的基於硬件的保護設備，如USB Security Token和Smart Card。另外，在註冊用戶認證器的過程中利用了現有的PKI技術。

FIDO 聯盟是由行業相關公司創建的組織，制定並公佈了 FIDO 標準。

由於FIDO是一種可以同時使用生物識別技術的認證標準，它順應時代潮流從用戶中誕生（智能手機支持生物識別信息掃描功能），作為實現沒有ID和密碼的世界的技術而備受關注。有。

在韓國，在檢查金融交易時，公共證書和 OTP（或安全卡）被用作基於所有權的認證方法，但隨著使用公共證書的義務被廢除，"基於生物特徵信息的認證技術"將取代公共證書作為下一代身份驗證的一種手段，它已被用戶強調。換句話說，"基於生物識別信息的認證技術"提供了安全性和便利性。作為參考，使用公共證書需要密碼。

綜上所述，FIDO是一次性取代ID、密碼、公共證書等現有認證技術的下一代認證技術，是一種僅存儲Public即可解決因服務器黑客攻擊導致的個人信息洩露問題的技術- 輸入服務器。

根據實施情況，有以下三個標準。
1）UAF（Universal Authentication Framework）：在認證過程中使用個人獨有的生物特徵信息代替ID和密碼認證方式。由於智能手機支持生物識別信息掃描功能，適用於智能手機等移動環境。

2）U2F（Universal 2nd Factor）：除了現有的ID和密碼認證方式外，"生物識別信息或單獨的二次認證設備"用於額外的認證目的。一款"FIDO U2F Certified Device"，即具有U2F認證的"hardware 2nd factor device"已經上市。適合現有的PC環境，因為它可以使用外部認證設備。

3）FIDO 2.0：對UAF和U2F進行了集成和擴展，使其可以在使用web瀏覽器的web環境中使用，為此，提出了WebAuthn標準，WebAuthn於2019年3月4日成為W3C Recommendation。（這意味著 W3C 已將 WebAuthn 作為標準發布）。

作為參考，UAF 和 U2F 屬於 FIDO 1.0。目前UAF最新版本為1.1，U2F最新版本為1.2。因此，FIDO版本也升級到了FIDO 1.1。

為了使用 FIDO 認證技術，需要稱為 Authenticator 的 H/W 功能，因此它不是用作一般服務的認證方法，而是僅用作使用智能手機在線支付時的認證方法它正在成為。FIDO 2.0已經被提出作為通用服務的認證方式，但要普及還需要時間。FIDO 2.0 還允許將智能手機用作外部驗證器。

所有 FIDO 協議都有一個稱為註冊和身份驗證的過程。

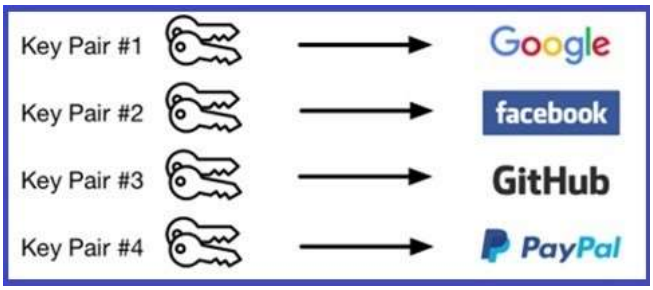
註冊和認證

要在在線環境中使用新服務，您必須首先註冊為用戶。

註冊用戶時，“FIDO authenticator（FIDO支持設備中嵌入的模塊或外部認證設備）”為服務生成新的“Key Pair（Private-key and Public-key）”，並將Public-key發送給FIDO 支持設備的 FIDO 服務器。私鑰安全地存儲在 Authenticator 內部的安全密鑰庫中，不得洩露到外部。作為參考，某些智能手機型號提供 TEE（可信執行環境）或 SE（安全元素）功能以支持更安全的安全密鑰存儲區（沒有 TEE 或 SE 功能的智能手機必須以 S/W 方式實現）。

在U2F方法中，所使用的“FIDO U2F Certified Device”，即通過U2F認證的“hardware 2nd factor device”，可視為一種“FIDO authenticator”。

由於為每個服務生成一個新的密鑰對，因此一個密鑰對只能用於一個服務。為了安全起見，認證器（認證設備）必須具有生成唯一密鑰對的功能。在 FIDO 中，這些密鑰對也稱為“憑證密鑰對”。



（來源：FIDO 聯盟）

公鑰被發送並存儲在服務提供商的 FIDO Server 中。這個FIDO Server是一個執行認證功能的服務器，Public-key用於對用戶進行認證。
的
在註冊過程開始時，FIDO Server向請求註冊的設備發送一個challenge（隨機數），這是一個防止重放攻擊的功能。

在“FIDO Support Device”中，在生成新的密鑰對之前，設備會接收並存儲用戶信息。用戶信息用於驗證用戶身份。如果生物識別信息用於驗證用戶身份，則用戶的生物識別信息由設備的Capture功能捕獲並僅存儲在設備內部，該生物識別信息不會發送給FIDO Server。

FIDO 標準中沒有定義用戶信息（包括生物識別信息）的註冊程序和存儲位置。因此，提供 FIDO 設備的公司必須自行做出決定。對於存儲，大多數使用 Authenticator 內的安全區域。

如果您使用“硬件第二因素設備”來驗證您的身份，例如，只需按下設備上的按鈕（這種方法稱為“用戶存在”。供參考，基於生物特徵信息，驗證身份是稱為“用戶驗證”）。

僅供參考，FIDO 也可能使用 PIN 碼來驗證您的身份。但是，這種方式與現有的密碼方式類似，安全性較低。

Attestation是在FIDO Server中註冊的過程中使用的一個過程，具體的---即用證明證書進行認證---在FIDO Authenticator（認證設備）中，用戶收到“認證信息（credential key） pair))”是一個用於證明它已被創建的過程。

認證時使用“認證密鑰對”，“認證密鑰對”是廠商生產“內置認證器的設備”時植入認證器中的密鑰對。準確的說是Private-key和Certificate（Public-key包含在Certificate中）。設備製造商為他們生產的每個型號植入相同的“私鑰和證書”。即使製造商相同，如果型號不同，“私鑰和證書”也不同。

“證明密鑰對”不同於前面提到的“憑證密鑰對”。只有一個“認證密鑰對”，為每個服務創建“憑證密鑰對”。

鑑權是證明用戶在註冊時使用特定的設備型號，使用密碼技術創建了認證信息。將生成的密鑰對的公鑰發送給服務公司的服務器時，將用認證私鑰簽名的簽名（電子簽名）和認證證書一起發送。換言之，服務器通過一起驗證接收到的證明簽名（驗證包括在證明證書中的證明公鑰）來驗證接收到的公鑰是從特定設備發送的。為此，服務器必須首先驗證證明證書是可信的。因此，設備製造商必須從授權的 CA 機構獲得設備證書。換句話說，證明過程利用了現有的 PKI 方法。

鑑證起到防止Public-Key在交付給服務公司的過程中被篡改的作用。但是，由於設備和服務公司之間的通信已經通過使用 TLS 協議的加密通信進行，因此公鑰不可能在傳輸過程中被外部攻擊者篡改。 - 即使您使用證書，服務公司可以接受，這個功能叫做Self Attestation（或Surrogate Attestation）。

UAF 和 U2F 都有自己的證明格式，用於在內部存儲證明相關信息或將其發送給服務公司。

作為參考，為每個模型創建認證密鑰和證書，因此無法通過認證密鑰或認證證書跟踪用戶。如果違反FIDO規定為每台設備頒發認證證書，用戶的隱私將得不到保護。

唯一型號和元數據服務 (MDS)

由於服務公司需要了解請求服務的認證器設備，因此在註冊時需要 FIDO 定義的唯一型號。也就是說，支持FIDO的設備必須有一個唯一的型號，並且在註冊時連同其他信息（Public-Key、鑑證簽名、鑑證證書）一起發送給服務公司。

根據使用的 FIDO 方法，唯一型號稱為如下。

UAF：AAID（驗證者證明 ID）
U2F：認證證書密鑰標識符
FIDO 2.0：AAGUID（Authenticator Attestation Globally Unique ID）

在FIDO MDS（元數據服務）的記錄中，記錄了"唯一型號"、"認證根證書"和"設備的元數據"。"認證根證書"是簽發"認證證書"的CA機構的證書，元數據是指與設備"安全和生物特徵"相關的信息。

MDS的記錄是通過接收設備供應商發布的元數據聲明來配置的，FIDO Server（服務公司的服務器）會定期創建一個簽名的"元數據目錄"文件，其中包含可以驗證元數據聲明的URL地址. 下載後，用於檢查設備的完整性。為了驗證簽名，必須獲得FIDO聯盟的根證書。

當服務公司從設備收到"唯一型號"時，它會在 MDS 中搜索記錄，如果匹配，則使用記錄中包含的"認證根證書"來驗證認證證書。通過驗證簽名密鑰，用戶的公鑰被驗證。

使用 MDS 功能的目的是只對已註冊的設備進行註冊和認證。

MDS在功能上類似於PKI的Certification Revocation List功能，據說如果能通過其他方式管理欺詐認證者，就沒有必要使用它了。

身份驗證和斷言

鑑權有兩種情況：登錄鑑權和交易確認鑑權。

FIDO設備使用與註冊時相同的用戶識別方法（生物識別信息、PIN、外部認證設備等）（例如，通過將手指放在指紋讀取器上或按下USB令牌按鈕）來確認用戶身份。 . 如果與設備中存儲的用戶信息不匹配，則不會繼續進行。首先，用戶驗證的目的是使用存儲在設備驗證器中的私鑰。

如果通過以上步驟，FIDO Device向FIDO Server請求認證使用自己的賬號，FIDO Server向Device發送challenge（隨機數）（實際實現中，收到challenge後，為了執行用戶身份驗證過程)..

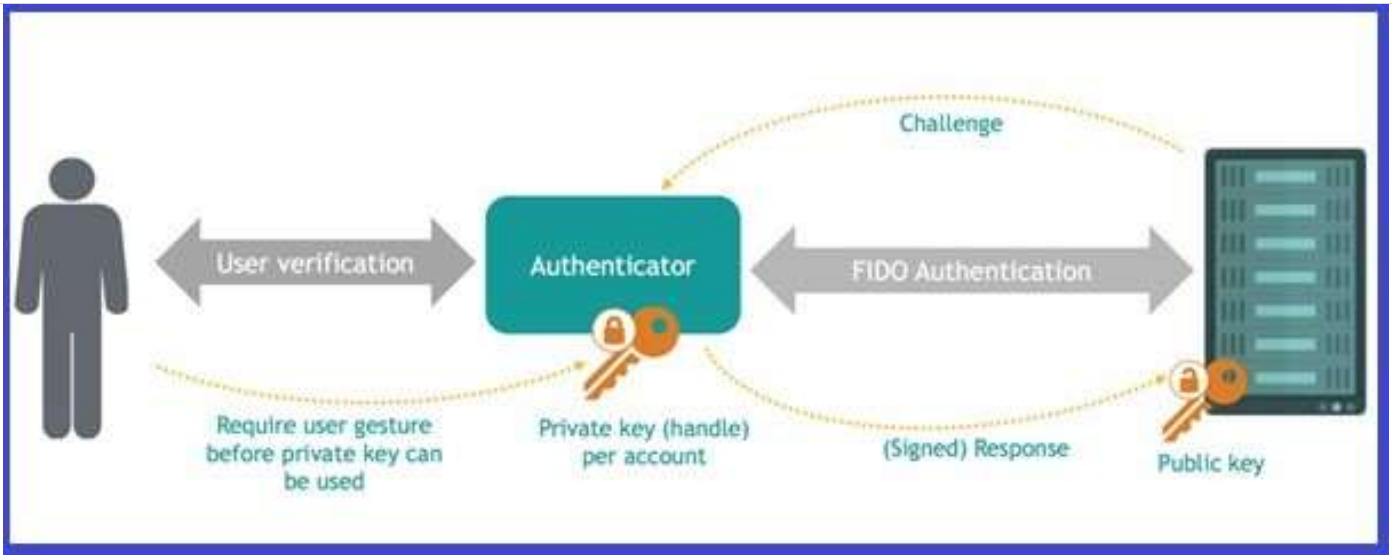
設備使用其私鑰簽署（電子簽名）質詢並將其發送到 FIDO 服務器。在設備上用私鑰進行簽名的功能稱為斷言（批准），用於斷言的私鑰是屬於上述"憑證密鑰對"的密鑰。即設備向FIDO Server發送斷言請求。

FIDO 服務器驗證用內部持有的用戶賬戶對應的公鑰簽名的質詢，並在驗證通過後通知設備驗證已完成。

換句話說，斷言是認證時執行的過程之一。

在身份驗證過程中，服務器向客戶端發送一個挑戰（隨機數），客戶端用自己的私鑰簽署（電子簽名）挑戰並將其發送回服務器。它應該被驗證 -鑰匙。這種方法稱為"基於公鑰密碼學的質詢-響應協議"。UAF是"基於公鑰密碼學的挑戰-響應協議"和智能手機生物信息識別功能的結合。
的
簡單描述FIDO認證方式時，稱為"在用戶終端認證後，將數字簽名值發送給FIDO認證服務器進行最終認證的方式"。第一個"認證"是指"本地認證"，第二個"認證"是指"在服務器端進行遠程認證"。描述的話應該描述為"這是一種先在用戶端對用戶進行驗證，然後將數字簽名值發送到 FIDO 認證服務器，在服務器上進行最終認證。"

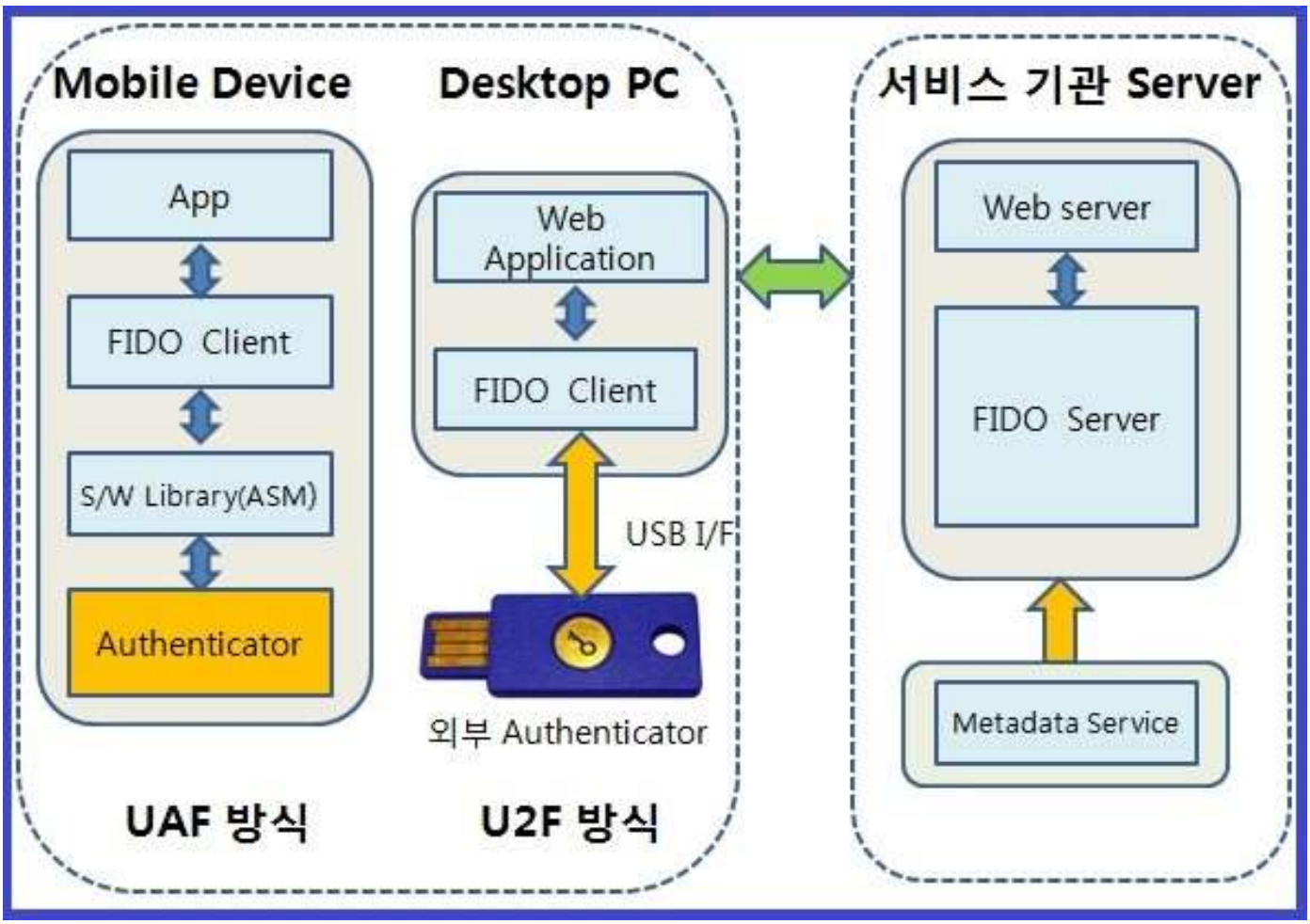
下圖顯示了身份驗證過程的概念。



（來源：FIDO 聯盟）

FIDO 1.0 Device & Server 內部運行結構

下圖是"UAF-supporting FIDO mobile device"和"U2F-supporting device"的內部運行結構和服務器的運行結構。



※ Authenticator：執行ECDSA密鑰對生成和簽名功能的H/W模塊

※ ASM (Authenticator Specific Module)：移動設備供應商提供的軟件庫

※ 在U2F方式中，外部驗證器和I/F方式支持藍牙和NFC以及USB。

※ App和Web Application稱為RP（Relying Party）Client，Web Server稱為RP Server。

FIDO 2.0

FIDO 2.0 是將FIDO 1.0 的組件FIDO Client、ASM 和Authenticator 集成到一個由OS 和Web Browser 組成的平台上來實現的。為了支持外部認證器，還開發了一種稱為 CTAP（客戶端到認證器協議）的新標準協議。CTAP支持USB、藍牙、NFC I/F（供參考，據說CTAP是基於U2F 1.2開發的）。

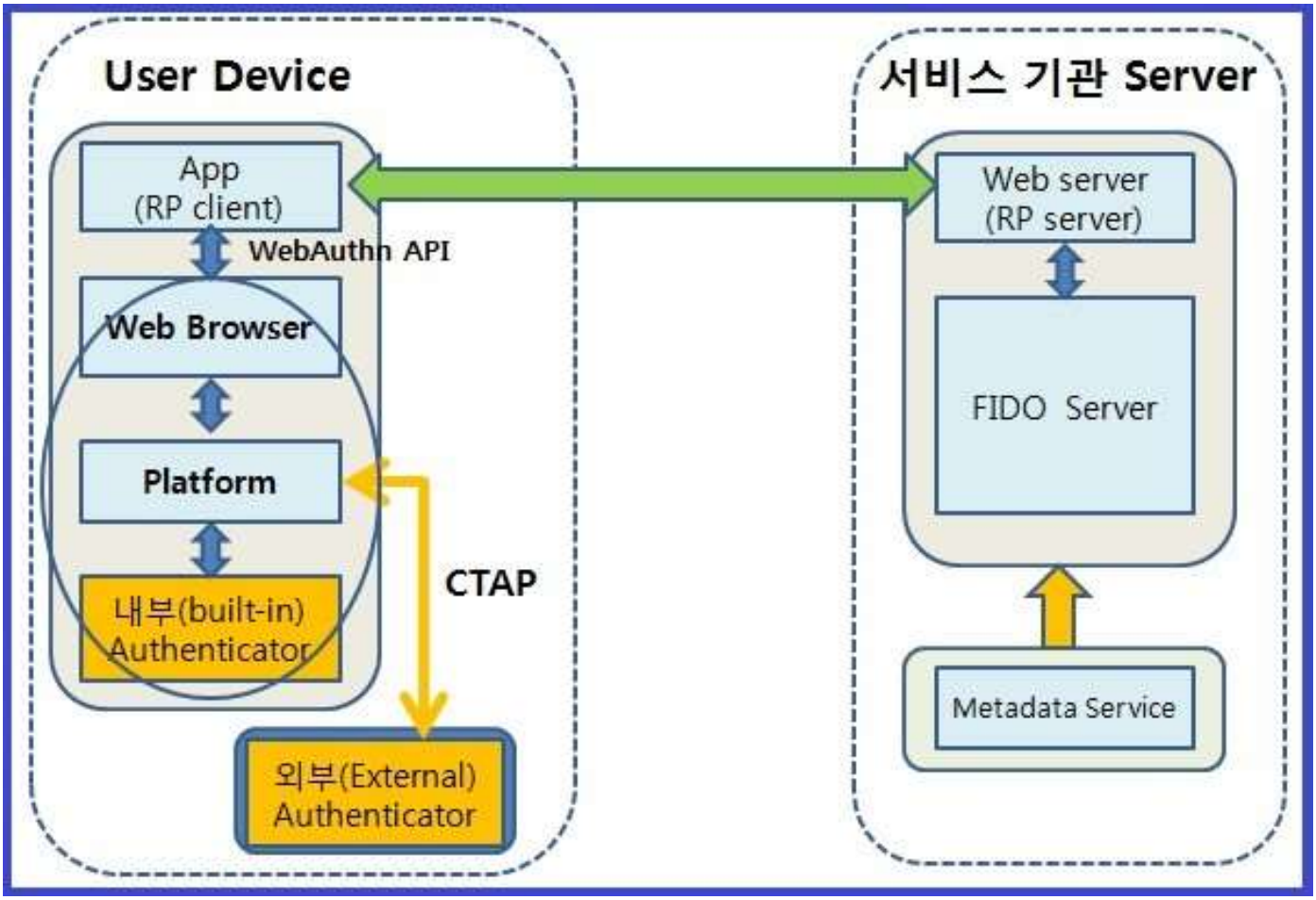
此外，我們還開發了一個名為 Web 身份驗證 (WebAuthn) 的標準 API，以便它可以在用戶應用程序中使用。“WebAuthn API”是一種 JavaScript API，可在 Web 瀏覽器中啟用 FIDO 身份驗證。

支持“WebAuthn API”的網絡瀏覽器包括谷歌的 Chrome、微軟的 Edge 和 Mozilla 的 Firefox。

綜上所述，FIDO 2.0支持的兩個標準是WebAuthn和CTAP。

基於平台的FIDO 2.0據說是由微軟和谷歌等平台公司提供的。當然，據說會開發出很多支持FIDO 2.0，也就是支持CTAP的外部認證設備。如果智能手機支持CTAP，那麼智能手機也可以作為FIDO 2.0的外部認證設備。

作為參考，該平台也被稱為Web平台，Web平台是由萬維網聯盟（W3C）和IETF. 表示一組
的
下圖展示了FIDO 2.0的內部工作結構。



國際電聯標準

FIDO 聯盟於 2018 年 12 月 18 日宣布採用 UAF 1.1 和 CTAP 規範作為 ITU 標準（（ITU-T Recommendations）。

FIDO UAF 1.1：ITU-T X.1277 建議書
CTAP：ITU-T X.1278 建議書
的
的

FIDO的缺點

每個服務公司都必須經過註冊程序，也就是說，必須為每個服務創建一個“憑證密鑰對”。這實際上可以提高安全性

由於在支持FIDO的設備中創建和存儲的私鑰不能外傳，如果用戶更換設備，必須重新註冊才能使用所有服務。為了克服這個問題，他們正在研究一種安全複製 .Private-key 的功能。
的
如果支持 FIDO 的設備損壞或丟失（包括暫時丟失），並且沒有替代的身份驗證方法，則服務不可用。

雖然不是缺點，但如果存儲在 FIDO 服務器中的用戶公鑰被外部攻擊者篡改，用戶將無法再使用他/她的帳戶。當然，你可以重新註冊一個賬號使用，但是作為服務公司，你的形象會受到損害。因此，從服務公司的角度來看，用戶的公鑰必須安全保存，就像之前的密碼一樣。也就是說，如果FIDO Server被黑客入侵，個人信息不會洩露，但會受到拒絕服務攻擊。

最大的潛在問題不是技術方面，而是新的社會犯罪現像出現的問題。由於不法分子無法通過黑客手段達到目的，因此存在身體犯罪的可能，即竊取智能手機等FIDO Device，如果需要機主的生物識別信息，則很可能通過其他犯罪行為獲取生物識別信息信息。換句話說，網絡犯罪會減少，但物理犯罪可能會增加。不知道是不是我提前多慮了。

#FIDO #FIDO2 #UAF #U2F #WebAuthn #CTAP #認證器 #證明 # 斷言 # 密碼 #生物識別 #認證設備

8個 3個

AEP韓國網

IT·計算機

我們是向韓國供應英國 Ultra I&C (www.ultra.group/gb/our-business-units/intelligence-communications) 產品的分銷商。我們向韓國提供 X.25 網關設備、HSM 設備和密碼通信設備。(www.kn.co.kr)

添加鄰居

這個博客 密碼故事 類別帖子

同態加密庫：SEAL

2019年6月14日

6 0

用於密碼存儲的密碼算法

2019年4月19日

0 0

了解 FIDO：註冊和認證

2019年4月10日

8 3個

HSM 和白盒密碼學

2019年3月19日

3 一

TLS 프로토콜에서 사용하는 Cipher Suite

2019. 2. 27.

5 0

Galaxy Watch 4 Wi-Fi（無線網絡）功能

2021年9月13日

29 7

HTTP 嚴格傳輸安全 (HSTS) 功能

2019.7.2.

3 0

RSA 公鑰 DER 格式

2017. 9. 4.

3 0

比特幣中使用的橢圓曲線密碼術 (ECC)

2018.1.5.

21 0

謎語故事

2019. 10. 17.

6 4

Cobalt Strike

2020. 1. 20.

6 1

TLS 프로토콜

2019. 2. 27.

5 0

SNMP의 Con

2020. 9. 28.

2 0

스테가노그라

2018. 8. 20.

9 0

RSA 私鑰格式

2020年3月12日

1 0

回到頂部

電腦版查看