Communications of the CCISA
Vol. 30 No. 4 Nov. 2024

整合 FIDO 之線上信用卡交易驗證機制

楊舒蓁[1*]、羅嘉寧[2] 、楊明豪[3]
[1]國立政治大學、[2]國防大學理工學院、[3]中原大學
[1]113753503@nccu.edu.tw、[2]deer@ccit.ndu.edu.tw、[3]mhyang@cycu.edu.tw

摘要

3D 認證 (3-Domain Secure, 3DS) 為制定信用卡組織 (EMVco.) 針對線上無卡交易訂定的標準。其中，3DS 2.2 版本為確保身分準確性導入了快速身分驗證機制 (Fast Online Identity, FIDO)，並由商家擔任 FIDO 身分驗證角色。然而這樣的做法導致發卡銀行可能收到不真實的驗證結果，反而增加了身分冒用的風險。

因此，本研究提出 3DS-FIDO 架構來提升整體的註冊及交易流程。在此架構中，使用者的 FIDO 驗證器須先透過 EMV 卡片認證協定，完成實體卡綁定。並且，後續的每筆交易由發卡銀行驗證使用者的 FIDO 身分。這樣確保銀行進行 3DS 及 FIDO 雙重驗證，對使用者來說也免除需分別向各商家綁定 FIDO 的麻煩手續，更可降低身分冒用的風險。最後，我們針對 3DS-FIDO 進行安全分析，並證明我們所提之架構可全面抵抗各式攻擊。

本研究能有效提升 3DS 中身分驗證的安全性，並透過實體卡與驗證器綁定步驟，使得驗證器可作為合法實體卡的存在。相比原 3DS 流程更具安全性，更能有效防範線上無卡交易盜刷的發生。

關鍵詞：信用卡協議、3D 認證、快速身分驗證機制

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 30 No. 4 Nov. 2024

The Integration of FIDO in Online Credit Card Transaction Authentication Mechanism

Shu-Zhen Yang [1*], Chia-Ning Luo [2], Ming-Hao Yang[3]
[1]National Chengchi University, [2]College of Science and Engineering, National Defense University, [3]Chung Yuan Christian University
[1] 1113753503@nccu.edu.tw , [2] deer@ccit.ndu.edu.tw , [3] mhyang@cycu.edu.tw

Abstract

3D Secure (3DS), a standard developed by EMVCo. for online card-not-present transactions, aims to enhance security in such scenarios. In its 3DS 2.2 version, the Fast Online Identity (FIDO) authentication mechanism was introduced to ensure identity accuracy, with merchants acting as FIDO authentication entities. However, this approach may lead to issuing banks receiving potentially inaccurate authentication results, thereby increasing the risk of identity fraud.

This study proposes the 3DS-FIDO framework to enhance the overall registration and transaction processes. In this framework, the user's FIDO authenticator must first complete physical card binding through the EMV card authentication protocol. Subsequently, for each transaction, the issuing bank verifies the user's FIDO identity. This ensures dual verification via 3DS and FIDO by the bank, eliminating the inconvenience for users of binding FIDO credentials with individual merchants. It also reduces the risk of identity fraud. Finally, we conduct a security analysis of 3DS-FIDO and demonstrate that the proposed framework effectively resists various attacks.

This study significantly enhances identity verification security within 3DS. Through the binding of physical cards with authenticators, the authenticator is effectively validated as a representation of the legitimate physical card. Compared to the original 3DS process, this framework offers superior security and effectively mitigates the occurrence of online card-not-present fraud.

Keywords: Credit Card Protocol, 3DS and FIDO

壹、前言

隨著電子支付的普及,支付安全性已成為一個關鍵問題。為了保障電子支付的安全,信用卡維護組織 EMV 機構 (EMVco.) 制定了 3D 認證 (3-Domain Secure, 3DS) 協議 [2],可保護使用者於網路上進行無卡交易的安全性。儘管 3DS 一定程度的保護線上交易安全,盜刷的情形仍層出不窮,因此,如何提升安全性及更確實實施身分驗證為現今重要課題。

1.1 研究背景

最初的 3DS 1.0,要求顧客消費時至發卡銀行輸入綁定密碼進行驗證,此機制具容易忘記密碼或遭盜用等風險。因此,2.0 版本由 3DS 伺服器從持卡人的交易設備蒐集各項個人資訊,例如設備硬體規格、瀏覽器版本、進行交易地理位置等等,再結合交易資訊,與用戶的發卡銀行共享,使發卡銀行能夠評估該交易的風險等級以批准交易。

然而,攻擊者仍可以透過網路攻擊或社交工程攻擊取得信用卡資訊及消費習慣,冒用使用者身分進行盜刷。若進行風險評估的分析演算法不夠精確,詐騙者可以透過模仿合法用戶的行為模式欺騙系統。儘管銀行會針對高風險交易進行驗證,但最常被使用的 OPT 驗證碼已被證實無法有效防範詐騙的發生 [5],詐騙者可利用釣魚攻擊等手段,誘使用戶提供 OTP 驗證碼。

A. Ali 等人針對 3DS 2.0 進行逆向工程研究 [1]。研究團隊在持卡人與商家應用程式之間設置了反向代理程式,攔截並蒐集包括信用卡號、安全碼等敏感信息。他們利用了 3DS 2.0 對低風險交易較寬鬆的安全規範,成功執行了多次非本人授權交易。

為了應對這些挑戰,3DS 2.2 加入了快速身分驗證機制 (Fast Online Identity, FIDO) [4]。FIDO 透過公開金鑰加密進行多重因素驗證,使用者的機密資訊不會儲存在伺服器中。3DS 結合 FIDO 驗證提升線上交易的安全性。

1.2 研究動機與目的

3DS 2.2 標準建議由商家擔任 FIDO 信賴伺服器,進行 FIDO 驗證。3DS 伺服器將使用者是否通過商家的 FIDO 身分驗證作為鑑別因子之一,與其他 3DS 資料交由發卡銀行進行風險評估。然而這種做法存在潛在風險。

首先,由商家負責驗證 FIDO 的正確性,銀行無法直接參與身分驗證過程,只能接受商家的第二手驗證結果。其次,商家可能會遭受攻擊或存在惡意行為,而提交虛假的 FIDO 驗證結果。攻擊者可以使用自己的帳號完成 FIDO 驗證,登入商家網站,卻使用他人的信用卡進行交易,商家無法判斷登入者及信用卡非同一人,銀行也無從得知並非本人進行交易。此外,FIDO 標準因隱私考量,驗證器設計之初並無獨一無二的設備碼,FIDO 驗證器僅能證明可登入商家網站的資格,無法向銀行展示與信用卡之間的一對一

關係。且 3DS 2.2 未強制要求商家配備 FIDO 驗證機制，使用者無法確保每個商家的帳戶登入安全，只能被動接受商家設定的保護機制。
因此，由商家擔任驗證使用者身分的方式，無法驗證交易信用卡是否屬於正確的持卡人。一旦攻擊者竊取信用卡資料並綁定攻擊者的 FIDO 設置，會使發卡銀行的風險評估機制造成誤判。

為提升 3DS 協議的安全性，我們引入利用身分驗證、設備驗證與決策引擎來強化流程安全性。我們建議每筆交易均通過 FIDO 驗證，並由發卡銀行擔任 FIDO 認證伺服器，確保持卡人真實身分。驗證器註冊時，透過 EMV 協定中的卡片認證機制綁定實體卡 [3]，確保驗證器可信度。

我們提出的 3DS-FIDO 架構將 FIDO2 與 EMV 卡片認證技術融入 3DS 架構，在維持良好使用者體驗的同時，提升支付安全性。

1.3 攻擊者模型

為了確保設計的交易安全流程能抵抗潛在威脅，我們模擬了攻擊者在 3DS 2.2 協議下完成盜刷所需的條件和能力，並將威脅分為三類：

(1) 獲得實體物件

攻擊者需要取得或控制交易相關的實體物件，如實體信用卡。看到卡片上的帳號、到期日和安全碼後，攻擊者可以在線上商家進行盜刷。若銀行判斷為低風險，可直接通過交易。若是高風險交易，攻擊者可以偷查看受害者手機訊息或攔截簡訊，完成交易。

(2) 透過網路攻擊

攻擊者具備技術能力來操控數據傳輸和處理系統，包括攔截、修改或注入數據。攻擊者作為中間人秘密攔截通信信息，可能獲取受害者個人資訊來模擬其消費習慣，繞過 3DS 的挑戰流程。例如，模仿受害者的裝置硬體資訊和 IP 位置，使發卡銀行將交易判定為低風險而免去身份驗證。此外，攻擊者也可能在受害者進行帳號密碼登入或 FIDO 驗證時，竊聽從用戶端至伺服器端的數據傳輸，以攔截或影響驗證結果。

(3) 社交工程攻擊

攻擊者採用社交工程攻擊手段，騙取受害者的卡片及個人機敏資訊。例如，架設假的購物網站以騙取信用卡資訊，或透過釣魚攻擊獲得 OTP 驗證碼，進而通過銀行的身份驗證。

貳、3DS2、EMV 及 FIDO2 概述

3DS2 分為無摩擦式認證 (Frictionless Flow) 及挑戰式認證 (Challenge Flow) 兩種。當消費者於商家網頁發起交易挑戰時，商家配備的 3DS 伺服器會將消費者的 3DS 資訊

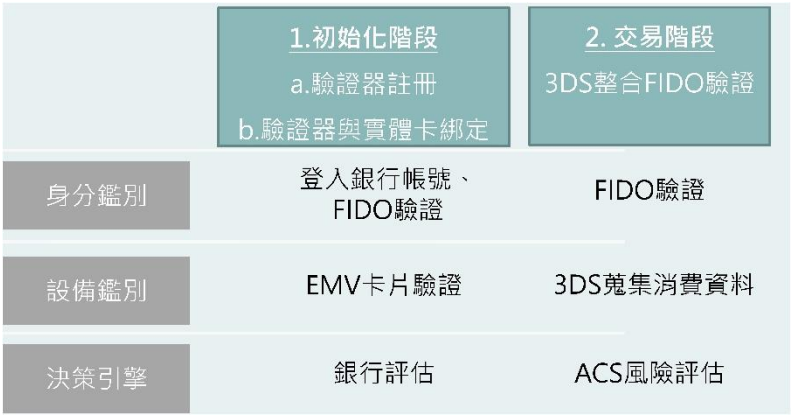
經由數據交換伺服器傳送給發卡銀行，由發卡銀行進行風險評估。銀行若判斷為低風險交易，會進入無摩擦式認證流程。此流程中，銀行不會再對消費者進行身分認證，轉由收單銀行進行支付流程。而高風險交易，則進入挑戰式認證流程。發卡銀行會對消費者進行身分驗證，例如簡訊 OTP 或輸入密碼等，完成身分驗證後再繼續支付流程。

EMV 刷卡協定中，信用卡與發卡銀行之間使用了非對稱金鑰、計數器及數位簽章等機制來確保交易的安全性。EMV 交易流程包括初始化、卡片認證、持卡人認證及交易授權。我們的研究僅需要確認卡片合法性，不須進入交易流程，所以只採前兩個步驟。為防止卡片偽造，在卡片驗證步驟使用了靜態數據驗證 (Static Data Authentication, SDA) 及動態數據驗證 (Dynamic Data Authentication, DDA) 兩種方法。SDA 是卡片使用私鑰靜態資料進行簽章。DDA 則是對終端機發出的隨機數進行簽章，來確保卡片是否被竄改。

FIDO (Fast Identity Online) 是一種基於公開金鑰加密和生物特徵識別的開放標準。在註冊階段，使用者的設備生成一對公私鑰，其中公鑰儲存在 FIDO 伺服器，而私鑰留在使用者的設備中安全保管。當使用者登入時，網站會生成一個隨機挑戰值，驗證器使用私鑰對其進行加密簽名。網站接收到簽名後，通過事先儲存的公鑰來驗證簽名的有效性，這樣就可以確認使用者的身份而無需傳送密碼或其他憑證。

參、研究方法

研究設計了 3DS 整合 FIDO 身分驗證的線上交易系統，在 FIDO 驗證器的部分做進一步的改良，讓使用者在持合法 EMV 實體卡的前提下，與驗證器進行綁定。我們提出 3DS-FIDO 架構，此架構分為兩個階段—FIDO 驗證器初始化及 3DS 交易階段。如圖一。



圖一：3DS-FIDO 架構圖

在初始化階段分為兩個部分，驗證器註冊及實體卡綁定。在驗證器註冊中，使用者必須在發卡銀行的伺服器上註冊驗證器。接下來的綁定步驟，為了加強安全，使用者必須通過 FIDO 驗證，與此同時完成 EMV 卡片驗證，以進行安全的綁定。在使用者持正

確卡片的前提下，能更有效的證明使用者的身分正確性。一旦初始化完成，發卡銀行將記錄相關卡片，未來的每一筆交易都將附加 FIDO 身分驗證作為安全保障。

在線上無卡交易的交易階段，當持卡人在線上商家進行交易時，發卡銀行將在原有的 3DS 安全架構下進行 FIDO 身分驗證。銀行收到 3DS 驗證請求後，ACS 除原有的風險評估外，會審核該卡的紀錄，然後發起 FIDO 驗證流程。除原有 3DS 機制可完成的設備驗證，還加入了 FIDO 身分驗證，對使用者也不會造成額外的操作負擔，顯著提升了整體的交易安全性。

3.1 FIDO 驗證器初始化

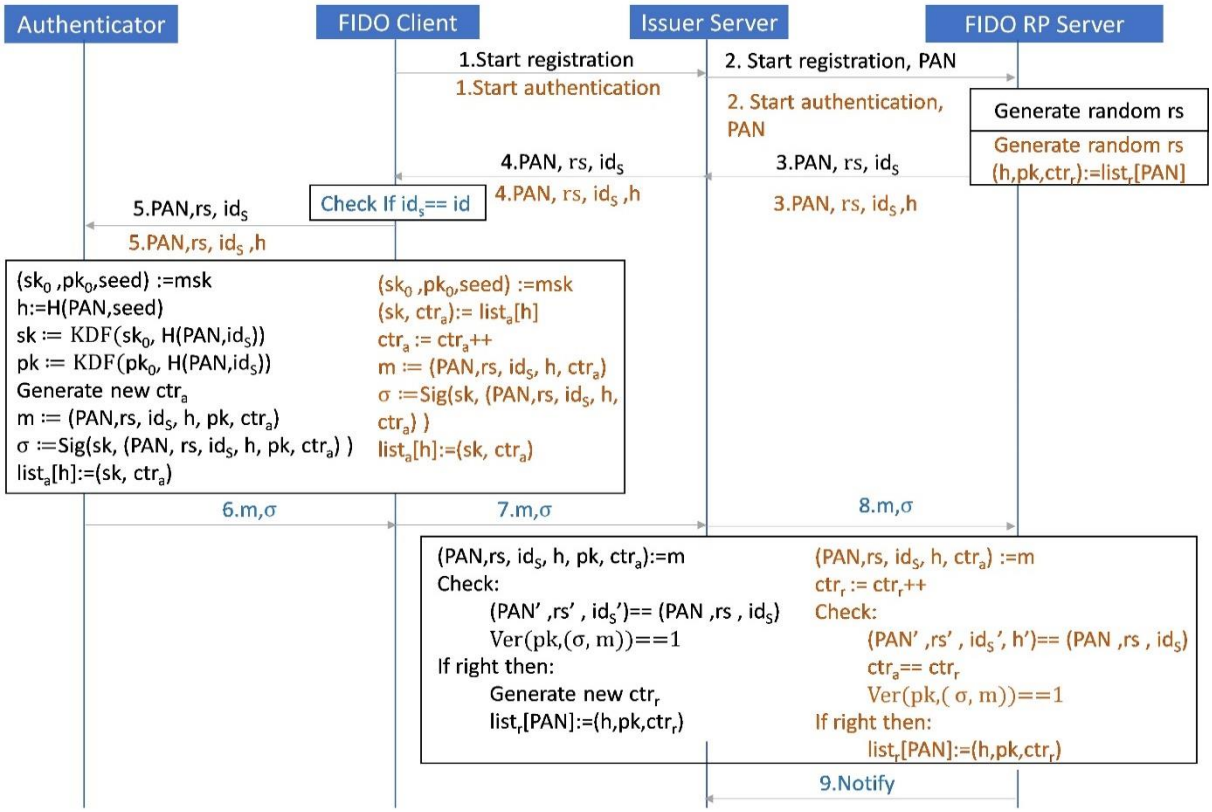
在開始初始化階段前，我們假設使用者已經持有發卡銀行核發的 EMV 卡，具登入銀行網站的能力，並且持有 FIDO 驗證器。可以使用手機模擬 EMV 刷卡協定的終端機，使用者僅須透過考卡感應完成實體卡驗證。

為確保安全性，在驗證器註冊時，使用者需要使用帳號密碼或相關機敏資訊登入銀行，作為身分鑑別的依據，才可以完成 FIDO 驗證器的註冊。然而，這樣還不足夠有效證明使用者的正確性。因此，我們在綁定階段，要求使用者需要先通過 FIDO 的身分驗證，接著出示合法的 EMV 實體卡片，完成 EMV 卡片認證。在這個過程中，驗證器可做為身分鑑別的因子，而實體卡則是設備鑑別的因子，最後再交由銀行內部進行評估，並決策是否通過驗證器初始化請求。

(1) 驗證器註冊

假設每個銀行 RP Server 裡面有一個清單 list 在儲存用戶的帳戶資料，在清單中輸入帳號 (Primary Account Number, PAN) 即可查找該用戶的公鑰及其他相關資料。在每個驗證器中也會有一個清單 list 作為儲存私鑰等資料使用，可以透過 key handle(h) 作為索引，來進行查找動作。驗證器的部分會初始有一組主秘鑰 msk，其中包含使用 ECDSA 生成主金鑰對 sk_0 及 pk_0，以及一個隨機值 seed 作為隨機化 key handle 使用，(sk_0 ,pk_0,seed) 共同組成驗證器的主金鑰 msk。

註冊的詳細的註冊步驟如圖二中的黑體字。首先，FIDO Client 發起註冊請求給 Issuer Server，Issuer 接收後將請求與 PAN 轉送 FIDO RP Server。RP 收到後生成亂數 rs，並將參數傳送給 Issuer 發起註冊挑戰。Issuer 將請求傳至 FIDO Client，檢查 id_S 與來源 id 是否匹配，並將請求轉成 CTAP 命令發至 Authenticator。使用者完成手勢後，使用 PAN 和 seed 生成 h，並通過 KDF 生成新密鑰對 sk、pk。隨後，初始新計數器 ctra，將產出及參數寫入 m 後使用私鑰 sk 簽名 σ，並將結果傳至 RP。取出 m 中的數值，確認 PAN、rs 及 id_S 是否與發送時相同，並使用 pk 驗證簽名 σ。驗證通過後，RP 初始新計數器 ctrs，並將數據儲存於 list 中，最後通知 Issuer 註冊完成。



圖二：FIDO驗證器註冊及驗證流程(黑體字為註冊流程，橘體字為驗證流程)

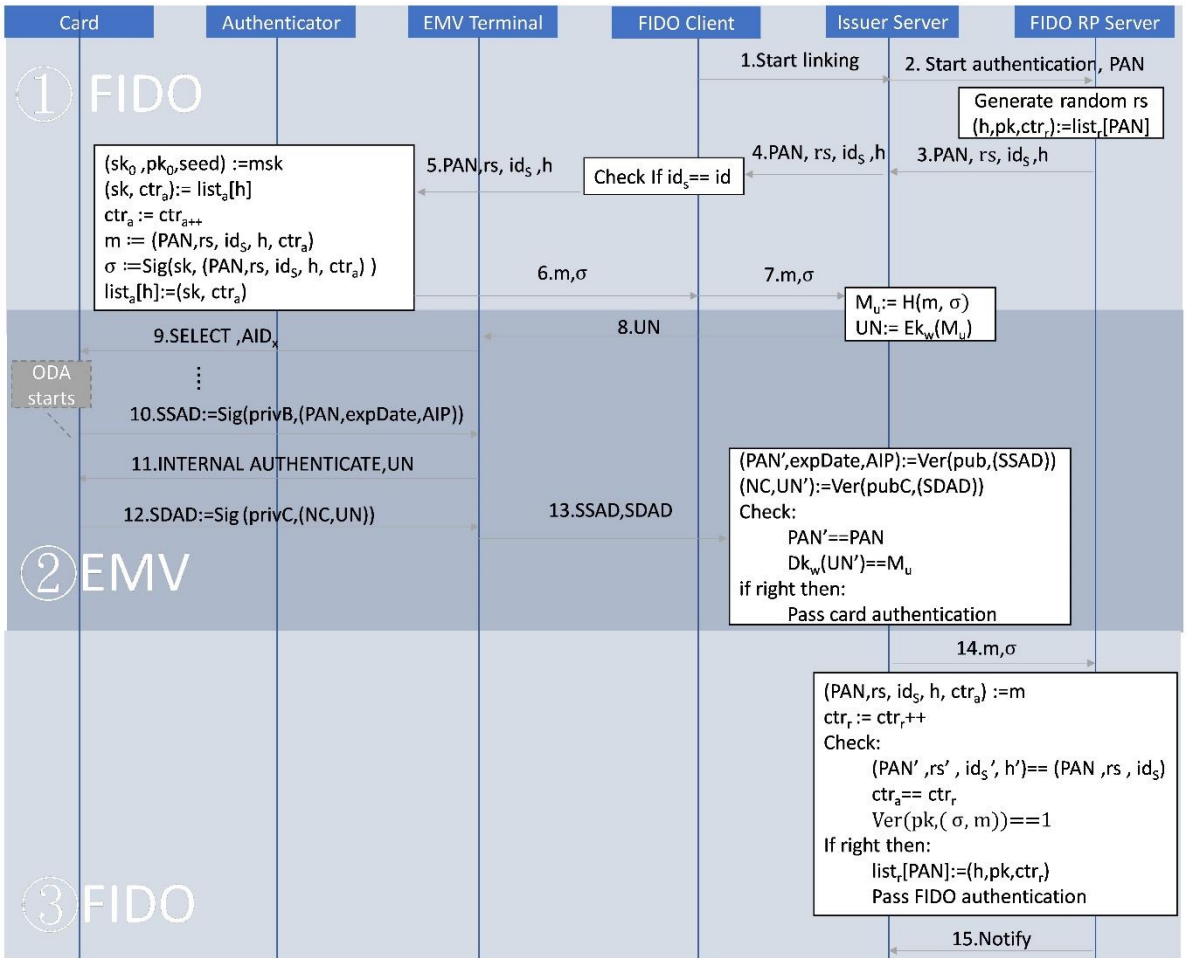
表一：符號表

符號	全名	代表意義
PAN	Primary Account Number	信用卡、借記卡等支付卡上的賬號
idS	Server identify	伺服器的識別碼
h	Key handle	資料索引
sk	Secrete key	私鑰
pk	Public key	公鑰
seed	seed	用於生成隨機化的數值
msk	Master Secret Key	主密鑰
ctr	Counter	計數器
Sig	signature	簽名演算法
Ver	Verify	驗證演算法
UN	Unpredictable Number	EMV 中終端的不可預測數
NC	Nonce	EMV 中卡片提供的隨機數
SSAD	Signed Static Authentication Data	簽章的靜態驗證資料
SDAD	Signed Dynamic Authentication Data	簽章的動態驗證資料
σ	Signed message	使用私鑰簽章的訊息

(2) 驗證器與實體卡綁定

在綁定階段，FIDO 的認證流程會與 EMV 實體卡的卡片認證進行整合，此階段分為三部分，FIDO 簽名、實體卡認證、FIDO 驗證。FIDO 驗證器完成第一部分簽名後，回傳訊息到發卡銀行會暫時擱置。進行第二本分卡片驗證，此時，用戶需要將卡片靠近手機，卡片與終端機完成 SSAD 及 SDAD 資料後，銀行進行驗證。完成 EMV 卡片認證後，再接續第三部分的 FIDO 驗證。一旦驗證成功，綁定過程即告完成。

詳細步驟如圖三。首先，用戶啟動綁定程序，Issuer Server 隨即通知 RP 開始 FIDO 登入驗證。這一過程與平常的驗證流程相似，挑戰碼會被送入驗證器進行簽名，然後送回。但回應訊息傳送到 Issuer Server 時，Issuer 會暫時擱置。進行第二本分卡片驗證。Issuer 會利用收到的數據和簽名，進行雜湊處理後，使用對稱密鑰 w 加密，產生 UN。當終端機收到 UN 後，啟動 EMV 實體卡交易流程，此時，用戶需要將卡片靠近手機，直到卡片的驗證資料被讀取，包括 SSAD 和 SDAD。終端機會驗證 SSAD 和 SDAD 的正確性，然後將 SDAD 發送給 Issuer Server。Server 用公鑰進行驗證，並與原始的 UN 進行比對，再用 w 解密比對。完成 EMV 卡片認證。隨後，Issuer Server 將 FIDO 挑戰的回應傳回給 RP 進行驗證，一旦驗證成功，綁定過程即告完成。

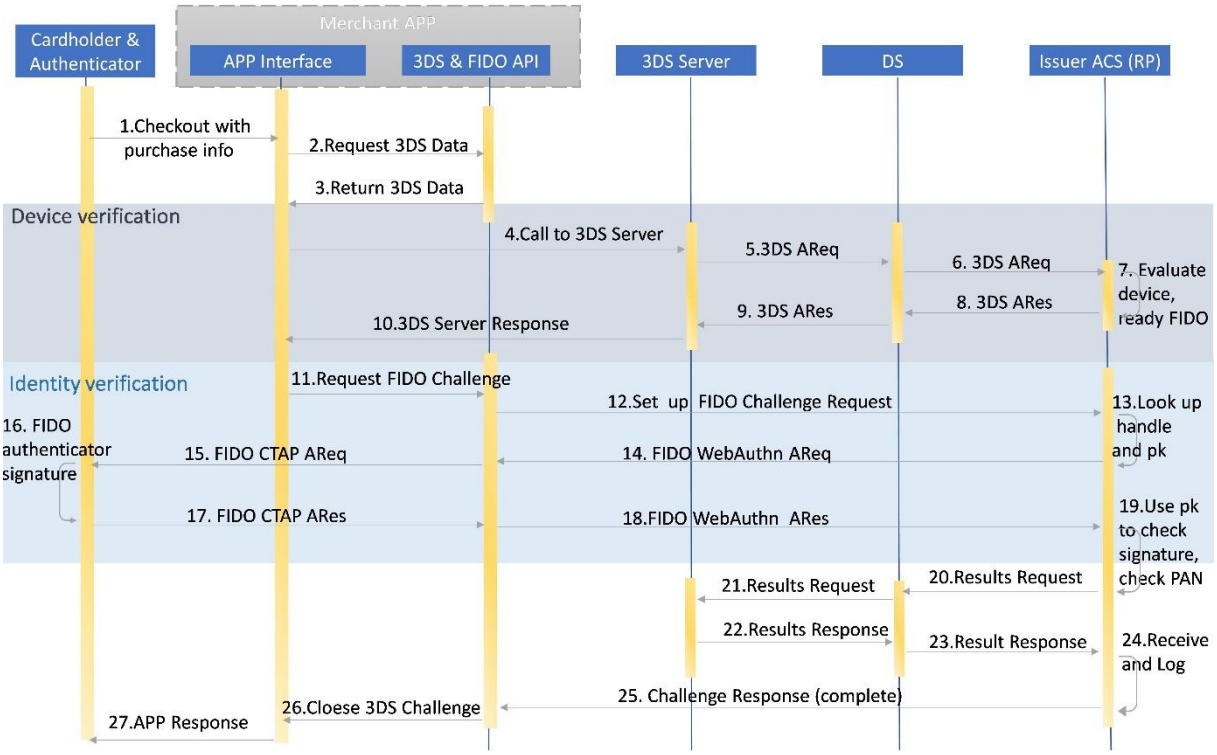


圖三：驗證器與實體卡綁定流程

3.2 交易階段

在交易階段，為了確保系統與 3DS 規範相容，我們在研究中選擇將原始的 3DS 挑戰流程架構與 FIDO 驗證流程進行整合。在我們改良的架構中，ACS 不僅進行常規的風險評估，還將對使用者的身份進行額外的 FIDO 驗證，增強安全性。

在這個交易的階段，原本的 3DS 機制會蒐集使用者的設備資訊作為設備鑑別的依據。流程接下來會進行 FIDO 驗證，此驗證結果可作為身分鑑別。最後將設備鑑別及身分鑑別結果交由銀行的風險評估伺服器，進行信任推斷及決策，以確認此交易的安全性。



圖四 ： 交易流程

詳細步驟如圖四。持卡人在商家的應用程式介面上輸入訊息後，應用程式向 3DS API 申請用戶資訊並接收回傳的資訊。接著，應用程式呼叫 3DS 伺服器，並將消費資訊及用戶資訊交給伺服器，伺服器隨後向 DS 傳送認證請求。DS 將請求傳送給相應的發卡銀行 ACS。ACS 根據消費習慣和交易裝置數據進行 3DS 驗證，儲存風險評估結果，並發起 FIDO 身分驗證挑戰，將結果回傳並要求開啟 FIDO 身分驗證。DS 轉送至 3DS 伺服器，3DS 伺服器再傳送要求 FIDO 身分驗證至應用程式畫面，通知持卡人。應用程式呼叫 FIDO 挑戰，FIDO API 向 ACS 請求 FIDO 身分驗證。ACS 生成挑戰值並查找 handle 及相應的公鑰後，傳送 FIDO WebAuthn 認證挑戰至 FIDO API。FIDO API 驗證來源後，轉為 CTAP 格式，傳至使用者的驗證器，驗證器生成私鑰並進行簽名。簽名結果回傳至 FIDO API，轉為 WebAuthn 格式並回傳至 ACS。ACS 使用公鑰驗證簽名後，根據 3DS 和 FIDO 驗證結果進行風險評估，決定是否授權交易。ACS 將認證結果傳送至 DS，DS 再轉送至 3DS 伺服器，伺服器收到後回應確認訊息，並轉送給 ACS。ACS 紀錄交易結果，傳送完成挑戰通知至應用程式的 3DS API，結束挑戰流程並通知持卡人交易結果。在這個流程中，12 至 19 步驟為 FIDO 驗證流程，詳細參數傳遞及運算如圖二橘體字所示。

肆、安全分析

在我們的攻擊模型中，我們分析了在線上交易中，攻擊者分別具三類能力來完成盜刷。接下來，我們將分別探討如何防範這些潛在的攻擊，並且與現有的 3DS 進行比較，以證明我們的方法更具安全性。

4.1 攻擊模型的防範

(1) 獲得實體物件:

在初始化流程中，如果攻擊者能仿冒受害者登入銀行並試圖註冊自己的 FIDO 設備，仍因無法通過 EMV 實體卡的認證而綁定失敗。同樣地，即使攻擊者取得受害者已註冊的 FIDO 驗證器，若無法出示合法的 EMV 實體卡，綁定同樣會失敗。此外，即便攻擊者偷到受害者的實體卡，若無法登入銀行網站或無法出示受害者的 FIDO 設備，綁定也無法完成。

因此，攻擊者若欲成功綁定，需同時掌握銀行登入資訊、FIDO 驗證器及合法的 EMV 實體卡，這對攻擊者是一大挑戰。配合 FIDO 驗證器的生物辨識功能，能夠進一步提升系統整體的安全性。

在交易階段，即便攻擊者獲得卡片資訊，因無法完成 FIDO 身份驗證，也無法完成交易。此外，3DS-FIDO 由發卡銀行擔任 FIDO 驗證伺服器及 3DS 風險評估伺服器，使用者必須持與消費卡號綁定之驗證器才能通過交易。這種嚴格的安全措施有效防止了盜刷行為。

(2) 透過網路攻擊

在我們提出的交易流程中，即使攻擊者能竊取機敏資訊，模擬使用者的消費習慣，由於我們加入了 FIDO 身份驗證程序，攻擊者無法繞過 3DS 身份檢查，因此盜刷嘗試將失敗。

即使通信中的信息被攔截並成功解析，也不會對安全造成威脅。在所有的挑戰-簽名流程中，所使用的私鑰都安全地存儲在 FIDO 驗證器及 EMV 實體卡的硬體中，不會在任何階段被傳送出去。同時，我們加入了計數器機制，可有效防止攻擊。

(3) 透過社交工程攻擊

不論攻擊者透過何種管道成功盜取受害者的機敏資訊，在初始化階段及交易階段，都需出示 EMV 實體卡和 FIDO 驗證器，並完成動態簽章，才能完成綁定或交易。

4.2 結果分析與比較

我們將 3DS-FIDO 與其他版本 3DS 機制進行比較，比較結果如表 2 所示。3DS 1.0 僅使用傳統帳號密碼方式進行驗證，具有冒用風險，且沒有對消費設備進行驗證，無法有效防範假冒及社交工程攻擊。3DS 2.0 及 2.2 版本加入了設備驗證，但是在身分驗證的部分，若銀行判斷為低風險交易，就不會實施。除使之外，誠如前言所述，這兩個版本的身分驗證方式，仍有被冒用的風險。

然而，3DS-FIDO 確保每一筆交易都需要進行身分驗證及設備驗證，在決策評估時可以有更可信的依據。搭配卡片綁定 FIDO 驗證器技術，使得驗證更為精確，能夠更好的防範各式攻擊，有效提升數位支付環境的安全性。

表二：3DS機制比較表

	3DS 1.0	3DS 2.0	3DS 2.2	3DS-FIDO
身分驗證	弱	弱	弱	強
設備驗證	無	有	有	有
決策引擎	弱	弱	弱	強
卡片綁定FIDO驗證器	無	無	無	有
防止假冒攻擊	無	無	無	有
防止社交工程攻擊	無	無	無	有

伍、結論

現行的線上交易協議 3DS 標準仍存在許多安全漏洞，因為沒有確實進行身分驗證，使得盜刷事件頻繁。3DS 2.2 的版本中，我們認為由商家進行 FIDO 驗證的方式，惡意使用者在盜取持卡人的相關信息後，仍有機會通過商家端的 FIDO 驗證，導致身份冒用的風險增加。

因此，我們提出了 3DS-FIDO 架構，以提升線上交易安全。在此架構中，FIDO 驗證器需要先與實體卡綁定，在驗證 EMV 卡片真實性的基礎上，進而提升 FIDO 驗證器的可信度。同時，每筆交易均需由發卡銀行進行 FIDO 身分驗證，確保消費者身分，避免了商家端驗證可能帶來的安全風險，有效防止身份冒用。這樣的作法也不會為消費者帶來操作的不便利性，FIDO 驗證時僅需觸碰一下裝置，改善過去輸入密碼或 OTP 的繁雜手續。

本研究提出的架構，相比現行的 3DS 協議，可以提供更高的安全性，且不需要付出太高的額外成本，對使用者來說也不會帶來操作上的麻煩。並且在身份驗證的安全性進行了全面的分析和驗證，與各現有協定具高度相容性，在實務上也具有很高的可行性和應用價值。

[誌謝] 感謝國家科學及技術委員會（NSTC）對本研究的支持，經費編號為 NSTC 113-2221-E-606-012 與 NSTC 113-2634-F-004-001-MBK，讓本研究得以順利完成。

參考文獻

[1] Ali and A. van Moorsel, "Designed to be broken: A reverse engineering study of the 3D Secure 2.0 Payment Protocol," *in Financial Cryptography and Data Security: 23rd International Conference, FC 2019*, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers, 2019, pp. 201–221.

[2] EMVCo. (n.d.). 3-D Secure. EMVCo. https://www.emvco.com/emv-technologies/3-d-secure/

[3] EMVCo. (n.d.). EMV® Contactless Chip. EMVCo. https://www.emvco.com/emv-technologies/emv-contactless-chip/

[4] FIDO Alliance. (n.d.). FIDO Alliance. https://fidoalliance.org/

[5] Hyunki Kim, J. Lee, and H. Cho, "Analysis of vulnerabilities that can occur when generating one-time password," *Applied Sciences*, vol. 10, no. 8, pp. 2961, 2020.