Engineering and Technology Journal e-ISSN: 2456-3358

Volume 11 Issue 05 May-2026, Page No.-9669-9679

DOI: 10.47191/etj/v11i05.03, I.F. – 8.595

Implementation of FIDO2/Webauthn-Based Multi-Factor Authentication Module for E-Commerce Security on Prestashop

Muh. Zaki Erbai Syas[1], Rahmad Abdillah[2*], Novriyanto[3], Suwanto Sanjaya[4]

[1,2,3,4]Department of Informatics Engineering, Faculty of Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim Riau, Indonesia

ABSTRACT: This study presents the design, implementation, and empirical validation of a FIDO2/WebAuthn-based Multi-Factor Authentication (MFA) module for the PrestaShop e-commerce platform. As e-commerce transactions continue to grow, conventional password-based authentication remains a critical vulnerability exploited by phishing and credential theft attacks. The proposed module integrates passwordless authentication and second-factor verification using the W3C WebAuthn Level 2 standard, implemented as a non-invasive PrestaShop module utilizing the platform's native hook system. The module supports hardware security keys, platform authenticators (Windows Hello, Touch ID, Android Biometrics), and cross-device passkeys. Functional testing validates complete registration, authentication, and credential management flows across Chrome, Firefox, and Safari browsers. WebAuthn API testing confirms compliance with cryptographic security properties including origin binding, challenge entropy (256-bit), replay prevention, and signature verification. Results demonstrate that FIDO2-based authentication can be seamlessly integrated into existing e-commerce platforms without core system modifications, providing phishing-resistant authentication while maintaining backward compatibility with conventional password-based login.

KEYWORDS: FIDO2, WebAuthn, Multi-Factor Authentication, E-Commerce Security, PrestaShop, Passwordless Authentication

I. INTRODUCTION

Indonesia's e-commerce market continues to experience rapid growth, with transaction volumes reaching USD 75 billion in 2024 and projected to reach USD 125 billion by 2027 (PCMI, 2024). This rapid growth has made e-commerce platforms prime targets for cyberattacks, particularly credential-based attacks such as phishing, credential stuffing, and brute force attacks. The OWASP Top 10:2025 identifies authentication failures as a persistent critical vulnerability in web applications (OWASP, 2025), while NIST SP 800-63-4 now explicitly recommends phishing-resistant authenticators for digital identity verification (NIST, 2025). This recommendation is reinforced by CISA's implementation guidance, which identifies FIDO2 as the gold standard for phishing-resistant MFA (CISA, 2022).

Conventional password-based authentication, despite its widespread use, presents fundamental security limitations. Passwords are susceptible to phishing attacks, database breaches, and social engineering. Microsoft Threat Intelligence (2023) documented sophisticated Adversary-in-the-Middle (AiTM) phishing campaigns capable of bypassing conventional multi-factor authentication methods including SMS-based OTP and push notifications. Meyer et al. (2023) demonstrated through empirical analysis that while MFA reduces account compromise by over 99%, the effectiveness varies significantly depending on the MFA method employed, with FIDO2-based methods providing the strongest protection.

The FIDO2 standard, developed jointly by the W3C and FIDO Alliance, addresses these vulnerabilities through public-key cryptography. Unlike shared secrets (passwords, OTPs), FIDO2 credentials are asymmetric key pairs bound to specific origins (domains), making them inherently phishing-resistant (Barbosa et al., 2021; W3C, 2021). The FIDO2 framework consists of two complementary specifications: WebAuthn (the browser API) and CTAP2 (the authenticator protocol), together enabling both passwordless login and second-factor authentication.

PrestaShop, an open-source e-commerce platform powering over 160,000 active stores globally (Store Leads, 2026), currently lacks native support for FIDO2/WebAuthn authentication. While the platform provides a robust hook-based module system that enables non-invasive functionality extensions (PrestaShop, 2025), no open-source FIDO2 module exists in the PrestaShop ecosystem. This gap is significant given that security is a top concern for e-commerce merchants and consumers alike (Islam, 2024).

This research addresses the identified gap by designing, implementing, and validating a FIDO2/WebAuthn MFA module for PrestaShop. The specific objectives are: (1) to develop a modular, non-invasive FIDO2/WebAuthn authentication module that integrates through PrestaShop's native hook system; (2) to implement both passwordless and

second-factor authentication flows compliant with W3C WebAuthn Level 2; and (3) to validate the implementation through comprehensive functional and WebAuthn API testing.

II. LITERATURE REVIEW

A. *FIDO2/WebAuthn Standard*

The FIDO2 standard is a joint effort between the W3C and FIDO Alliance that provides a framework for strong, phishing-resistant authentication on the web. It consists of two specifications: (1) Web Authentication (WebAuthn), a W3C standard defining a browser API for creating and using public-key credentials (W3C, 2021); and (2) Client-to-Authenticator Protocol 2 (CTAP2), a FIDO Alliance specification enabling communication between clients and external authenticators (FIDO Alliance, 2018).

WebAuthn operates on asymmetric cryptography. During registration (attestation), the authenticator generates a unique public-private key pair. The private key never leaves the authenticator, while the public key is sent to the Relying Party (server) for storage. During authentication (assertion), the server sends a random challenge; the authenticator signs it with the private key, and the server verifies the signature using the stored public key. Credentials are cryptographically bound to the Relying Party's origin (domain), preventing phishing attacks where credentials are presented to malicious sites.

Barbosa et al. (2021) provided the first formal provable security analysis of the FIDO2 protocol suite, demonstrating that the combination of WebAuthn and CTAP2 achieves strong authentication guarantees under standard cryptographic assumptions. Their analysis confirmed that FIDO2 provides protection against man-in-the-middle attacks, credential theft, and replay attacks.

B. *FIDO2 Implementations Across Platforms*

Rivera-Dourado et al. (2021) analyzed existing WebAuthn and FIDO implementations, identifying key challenges including cross-platform compatibility, user experience design, and recovery mechanisms. Their subsequent work introduced FIDO2CAP, a novel protocol using captive portals for FIDO2 network authentication (Rivera-Dourado et al., 2024), and EAP-FIDO, extending FIDO2 to IEEE 802.1X network authentication (Rivera-Dourado et al., 2025). These studies demonstrate the versatility of FIDO2 beyond web applications.

Ou et al. (2024) integrated FIDO2 with blockchain technology for decentralized identity authentication, demonstrating that FIDO2 can adapt to modern security infrastructures. Krishnapatnam (2025) implemented a passkey-based approach in healthcare systems, validating FIDO2's applicability in high-security domains. These implementations collectively demonstrate that FIDO2 is suitable for diverse contexts, yet e-commerce platform integration, particularly for open-source PHP-based platforms, remains underexplored.

C. *E-Commerce Security and Authentication*

Affia et al. (2020) established that authentication is a critical security component in e-commerce systems through systematic threat-driven analysis. Kishnani & Das (2024) conducted a comprehensive privacy and security analysis of 90 e-commerce websites, identifying significant vulnerabilities in authentication implementations and recommending adoption of stronger mechanisms including FIDO2. Aburbeian & Fernández-Veiga (2024) developed a framework integrating MFA with machine learning for secure financial transactions, emphasizing the importance of robust MFA in financial contexts.

Islam (2024) demonstrated that secure payment systems with strong encryption and MFA are critical components in protecting customer sensitive information. These studies collectively confirm that authentication security is fundamental in modern e-commerce platforms.

D. *Security and Usability Analysis*

Yadav & Seamons (2024) conducted a comprehensive security and usability analysis of FIDO2, demonstrating strong protection against remote threats while identifying limited risks in local attack scenarios. Their usability study showed positive user perception, with a majority reporting faster and easier authentication compared to conventional MFA. Kunke et al. (2021) evaluated account recovery strategies for FIDO2-based passwordless authentication, proposing mechanisms that balance security and usability.

E. *Research Gap*

Based on the comprehensive literature review, this research addresses three significant gaps: (1) the absence of an open-source FIDO2/WebAuthn module fully integrated with PrestaShop's hook system; (2) the lack of technical documentation for implementing FIDO2 on PHP-based e-commerce platforms with modular hook architectures; and (3) the limited empirical studies of non-invasive FIDO2 implementation on e-commerce platforms with validation against W3C WebAuthn Level 2 specifications.

III.METHODOLOGY

A. *Research Design*

This is an applied research study using a Research and Development (R&D) approach implemented through an Iterative Development SDLC model. The research was conducted in six phases: (1) Literature Study, (2) Requirements Analysis, (3) Architecture Design, (4) Implementation, (5) Testing, and (6) Documentation.

B. *Requirements Analysis*

Functional requirements include: credential registration and management, WebAuthn-based authentication with signature verification, backward compatibility with password

authentication, and integration with PrestaShop hooks. Non-functional requirements include: compliance with W3C WebAuthn Level 2, compatibility with modern browsers, and a user-friendly interface with comprehensive documentation.

C. Architecture Design

The module employs a Layered Architecture with five distinct layers:

1. ***Presentation Layer***: PrestaShop Front Office for registration, authentication, and credential management interfaces.
2. ***Application Layer***: Three front controllers handling FIDO2 authentication, registration, and credential management flows.
3. ***Service Layer***: Business logic components including Challenge Manager, Attestation Validator, Assertion Verifier, and Credential Manager.
4. ***Data Access Layer***: Repository classes (Credential Repository, Challenge Repository) for database operations.
5. ***Database Layer***: MySQL tables for credential and challenge storage.

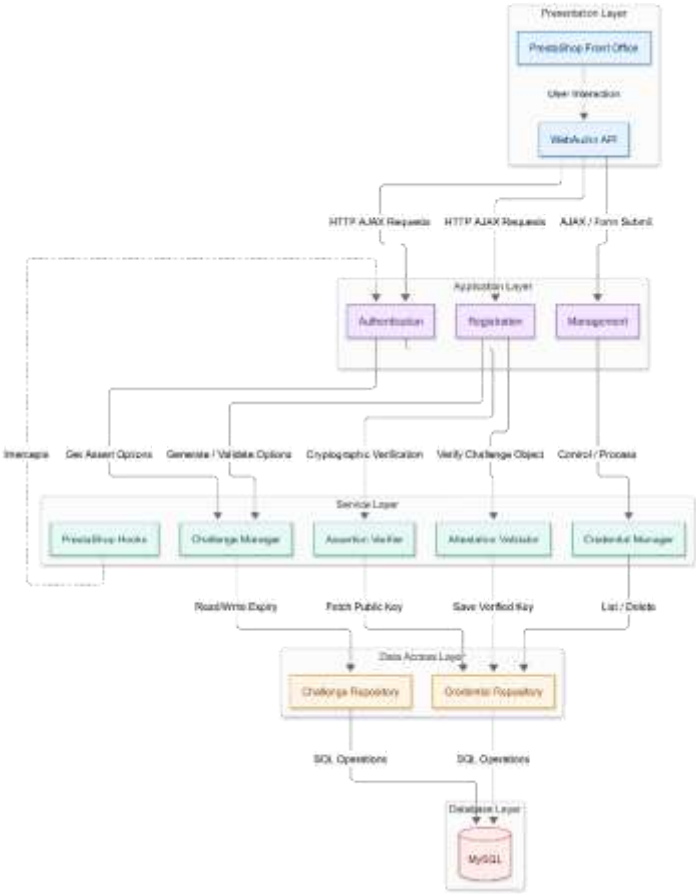

Figure 1. High-Level Architecture

This diagram illustrates the interaction between PrestaShop's core hook system, the module's layered components, and the WebAuthn API client.

D. Technology Stack

Table I. Technology Stack

Component	*Technology*	*Justification*
Language (Back-End)	PHP 8.1+	Type safety, modern features
Language (Front-End)	JavaScript ES6+	Native WebAuthn API support
WebAuthn Library	web-auth/webauthn-lib (Spomky, 2025)	Comprehensive PHP WebAuthn implementation
WebAuthn API	Level 2	Latest W3C standard
Database	MySQL 5.7+	PrestaShop native DBMS
COSE Algorithms	ES256, RS256, EdDSA + variants	Broad authenticator compatibility

E. Database Schema

Table II. Database Schema

Table	*Key Fields*	*Purpose*
fido2_credentials	id_fido2_credential, id_customer, credential_id, credential_public_key, attestation_type, sign_count, aaguid, transports, device_name, user_agent, created_at, last_used_at, is_active	Stores registered credential public keys and metadata
fido2_challenges	id_fido2_challenge, challenge, user_handle, id_customer, challenge_type, created_at, expires_at, used	Stores temporary cryptographic challenges with expiration

F. Testing Plan

Testing is organized into two categories:

1. ***Functional Testing***: Validates registration flow, authentication flow (passwordless and MFA), credential management, and cross-browser compatibility.
2. ***WebAuthn API Testing***: Validates compliance with W3C WebAuthn Level 2 including challenge generation, credential creation options, assertion verification, origin binding, and replay prevention.

IV. IMPLEMENTATION

A. *Module Structure*

The implemented module follows PrestaShop's module conventions with the following directory structure:

```
fido2auth/
├── fido2auth.php
├── controllers/
│   └── front/
│       ├── authentication.php
│       ├── registration.php
│       └── manage.php
├── src/
│   ├── Service/
│   │   ├── AssertionVerifier.php
│   │   ├── AttestationValidator.php
│   │   ├── ChallengeManager.php
│   │   └── CredentialManager.php
│   ├── Entity/
│   │   ├── Fido2Credential.php
│   │   └── Fido2Challenge.php
│   └── Repository/
│       ├── CredentialRepository.php
│       └── ChallengeRepository.php
├── views/
│   └── templates/
│       ├── front/
│       │   ├── authentication.tpl
│       │   └── manage.tpl
│       └── hook/
│           ├── costumer_account.tpl
│           └── login_form.tpl
└── sql/
    ├── install.php
    └── uninstall.php
```

B. *Registration Flow (Attestation)*

The registration flow implements the WebAuthn attestation ceremony:

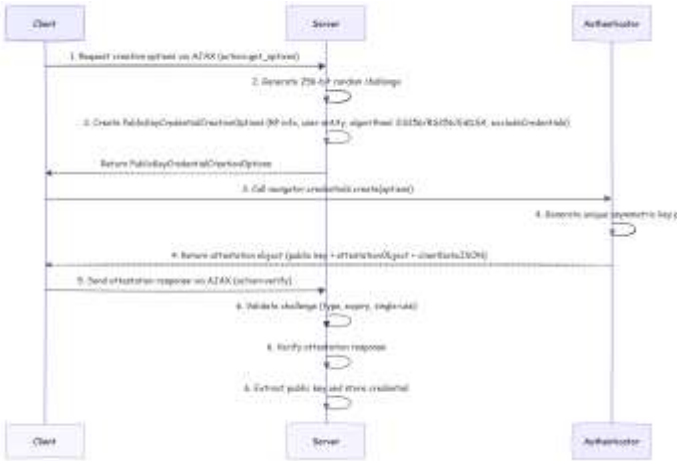

Figure 2. Registration Flow

1. ***Client*** requests creation options via AJAX (`action=get_options`).
2. ***Server*** generates a 256-bit random challenge, creates `PublicKeyCredentialCreationOptions` with RP info, user entity, supported algorithms (ES256, RS256, EdDSA), and existing credential exclusion list. The server-side Algorithm Manager additionally supports ES384, ES512, RS384, and RS512 for verification compatibility.
3. ***Client*** calls `navigator.credentials.create()` with the options, prompting the authenticator.
4. ***Authenticator*** generates a unique key pair, returns the attestation object.
5. ***Client*** sends the attestation response to the server (`action=verify`).
6. ***Server*** validates the challenge (type, expiry, single-use), verifies the attestation response, extracts the public key, and stores the credential.

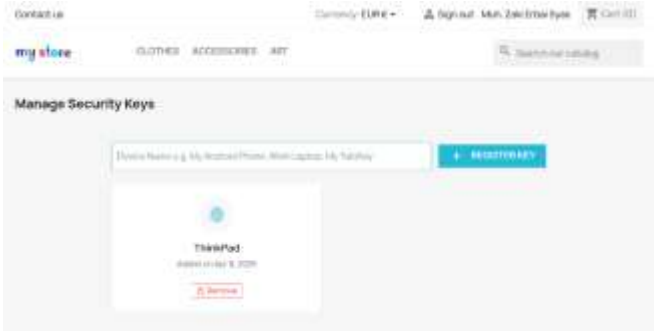

Figure 3. Security Keys Management Interface

This interface allows users to register new passkeys and manage existing credentials within their account dashboard. The device name, registration date, and last used date are displayed for each credential.

C. *Authentication Flow (Assertion)*

The module supports two authentication modes:

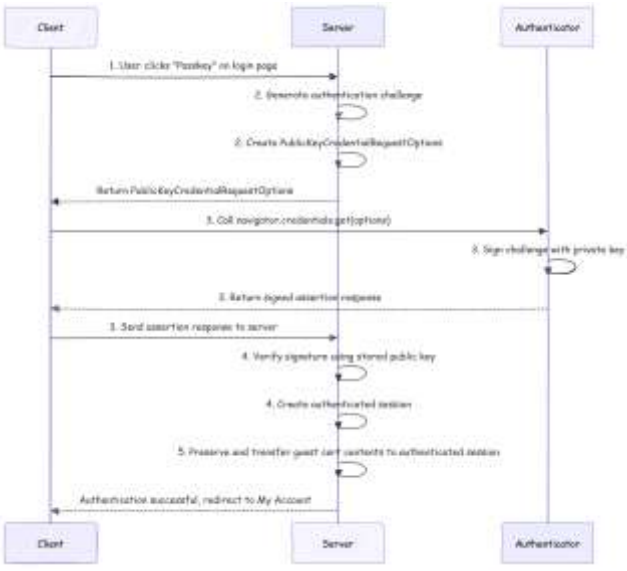

Figure 4. Authentication Flow (Passwordless)

Passwordless

1. User clicks "Passkey" on the login page.
2. Server generates authentication challenge and `PublicKeyCredentialRequestOptions`.
3. Client calls `navigator.credentials.get()`, authenticator signs the challenge.
4. Server verifies the signature using the stored public key, creates a session.
5. Guest cart contents are preserved and transferred to the authenticated session.

Figure 5. Passwordless Login Interface

The module non-invasively injects a "Passkey" button into the standard login form, allowing users to authenticate directly using their device's FIDO2 authenticator without entering a password.

MFA Verification

1. User logs in with password (conventional flow).
2. `actionAuthentication` hook checks if the customer has registered credentials.
3. If credentials exist, `fido2_mfa_pending` flag is set in the session cookie.
4. `actionFrontControllerSetMedia` hook intercepts access to protected pages (account, checkout, order history) and redirects to the FIDO2 verification page.
5. After successful verification, user is redirected back to the originally requested page.

Figure 6. MFA Verification Interface

When a user with registered credentials logs in using a password, they are redirected to this verification page before accessing protected account areas.

D. Security Measures

1. ***Challenge Security***: 256-bit random challenges generated with `random_bytes(32)`, stored with expiration timestamps, consumed after single use.
2. ***Origin Binding***: RP ID dynamically derived from the HTTP host, ensuring credentials are domain-bound.
3. ***Replay Prevention***: Challenges are marked as used after validation, sign count is tracked and updated.
4. ***CSRF Protection***: All AJAX endpoints validate PrestaShop's static security token.
5. ***Credential Safety***: Soft-delete mechanism, ownership verification on all operations.
6. ***User Handle***: Customer ID hashed with SHA-256 to prevent information leakage.

E. PrestaShop Integration

The module integrates non-invasively through five PrestaShop hooks, requiring zero modifications to the platform's core codebase:

Table III. Hook Integration

Hook	*Purpose*
displayCustomerAccount	Adds "Manage Security Keys" link to My Account page
displayHeader	Loads module CSS on FIDO2 and login pages
displayCustomerLoginFormAfter	Injects "Passkey" button into the login form
actionAuthentication	Sets fido2_mfa_pending flag if customer has registered credentials
actionFrontControllerSetMedia	Saves intended URL and redirects protected pages to MFA verification

V. RESULTS AND DISCUSSION

A. Functional Testing Results

Functional testing was conducted manually across three major browsers to validate all module features. Testing covered the complete registration, authentication, credential management, and cross-browser compatibility flows.

Table IV. Registration Flow Test Results

Description	*Expected*	*Actual*	*Status*
Register security key with valid device name	Credential stored with device name, success	Credential successfully stored in database with the specified device	PASS

Description	*Expected*	*Actual*	*Status*
	message displayed	name. Success notification "Success! Key Registered." displayed.	
Register second key (first key excluded)	Second credential stored, first key listed in exclude Credentials	Second credential registered successfully. First key's credential ID present in excludeCredentials array of the options response, preventing re-registration.	PASS
Register with empty device name	Warning message displayed	Warning message "Please enter a name for this security key." displayed.	PASS
Register duplicate authenticator	Error indicating credential already registered	Browser blocked the operation via excludeCredentials mechanism. The authenticator was not re-registered.	PASS
Cancel registration prompt	Error message displayed	Error message "The operation cancelled or timed out." displayed. No credential stored.	PASS

Table V. Authentication Flow Test Results

Description	*Expected*	*Actual*	*Status*
Passwordless login with registered passkey	Login successful redirect to my-account	User authenticated and session created without password. Page redirected to My Account. Customer name displayed in header.	PASS
MFA verification after password login	MFA completed redirect to intended page	After password login, user redirected to FIDO2 verification. After passkey verification, fido2_mfa_pending cleared and user redirected to the originally requested page.	PASS
Access protected page with MFA pending	Redirect to FIDO2 verification page	Accessing My Account with MFA pending triggered redirect to the FIDO2 authentication page with intended URL saved.	PASS
Browse catalog pages with MFA pending	Access allowed (not protected) without redirect	Product catalog, category pages, and product detail pages accessible normally despite MFA pending flag.	PASS
Cart retention after passkey login	Cart products preserved after authentication	Products added to cart as guest preserved after passwordless login. Cart quantity and items remained identical.	PASS
Cancel authentication prompt	Error message displayed	Error message "The operation cancelled." displayed. User remained on authentication page without session changes.	PASS

Table VI. Credential Management Test Results

Description	*Expected*	*Actual*	*Status*
List registered credentials	All active credentials displayed with metadata	All registered security keys displayed with device name, registration date, and last used date.	PASS

Description	*Expected*	*Actual*	*Status*
Delete a registered credential	Credential soft-deleted, removed from list	Credential marked as inactive (is_active=0). Removed from the displayed list. Confirmation message shown.	PASS

Table VII. Compatibility Results

Browser	*Version*	*Status*
Chrome	145.0.7632.160	PASS
Firefox	148.0.2	PASS
Safari	26.3	PASS

All 13 functional test cases passed successfully across all three browsers, achieving a 100% pass rate. The results confirm that the module's registration, authentication, credential management, and MFA enforcement flows operate correctly and consistently.

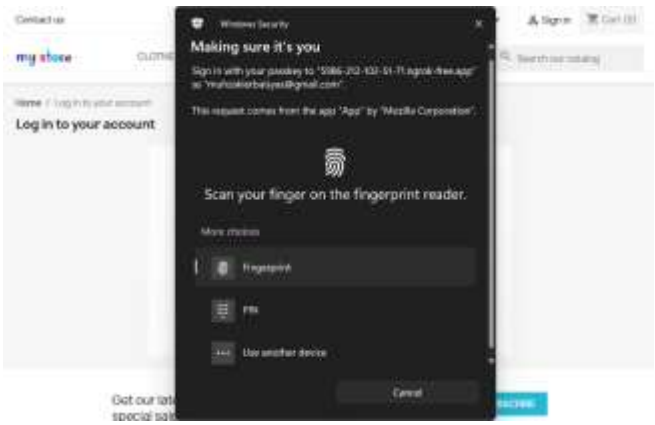

Figure 7. Windows Hello WebAuthn Prompt

The implementation correctly triggers the native Windows Security Key and Biometric dialogue interface.

Figure 8. macOS Touch ID WebAuthn Prompt

Demonstration of native integration with Apple's Touch ID biometric sensor for secure FIDO2 authentication.

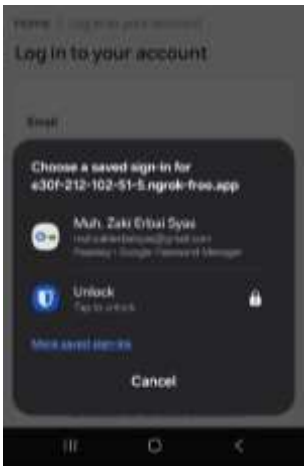

Figure 9. Android Biometric WebAuthn Prompt

The cross-platform nature of the module is validated by triggering the Android native biometric authentication lock.

B. WebAuthn API Testing Results

WebAuthn API testing was conducted by inspecting the AJAX request and response payloads through browser Developer Tools (Network tab with Persist Logs enabled). This validates compliance with the W3C WebAuthn Level 2 specification at the protocol level.

1. ***Registration API (PublicKeyCredentialCreationOptions)***

The following JSON response was captured from the registration `get_options` endpoint:


```
{
 "success": true,
 "options": {
  "rp": {
   "name": "PrestaShop",
   "id": "28e7-193-148-16-6.ngrok-free.app"
  },
  "user": {
   "id": "TgdAhWK-24tgzgXB3s_jrRa3IjCWfeAfZAt-
   Rym0n84",
   "name": "muhzakierbaisyas@gmail.com",
   "displayName": "Muh. Zaki Erbai Syas"
  },
  "challenge": "Bl2p3sKonteoWMSSQJjiXMb6a81Tw5
  URVgphgWzi5Hc",
  "pubKeyCredParams": [
   {
     "type": "public-key",
     "alg": -7
   },
   {
     "type": "public-key",
```

```
      "alg": -257
    },
    {
      "type": "public-key",
      "alg": -8
    }
  ],
  "timeout": "60000",
  "excludeCredentials": [],
  "authenticatorSelection": {
    "authenticatorAttachment": null,
    "requireResidentKey": false,
    "residentKey": "preferred",
    "userVerification": "preferred"
  },
  "attestation": "none"
 }
}
```


Table VIII. Registration API Validation

Property	*Expected*	*Actual*	*Compliant*
rp.id	Current domain	28e7-193-148-16-6.ngrok-free.app	Yes
rp.name	Configured RP name	PrestaShop	Yes
challenge length	≥ 16 bytes (128-bit)	32 bytes (256-bit)	Yes
pubKeyCred Params	Includes ES256 (-7)	ES256(-7), RS256(-257), EdDSA(-8)	Yes
authenticator Selection. userVerifica-tion	"preferred"	"preferred"	Yes
authenticator Selection. residentKey	"preferred"	"preferred"	Yes
attestation	"none"	"none"	Yes
timeout	Matches configured value	60000	Yes

2. ***Authentication API (PublicKeyCredentialRequestOptions)***

The following JSON response was captured from the authentication `get_options` endpoint:


```
{
 "success": true,
 "options": {
  "challenge": "kGbXwCp0HJSg-TJixSVOi3nfuhnoR
  jUv8RBzI6JjaUo",
  "timeout": "60000",
  "rpId": "28e7-193-148-16-6.ngrok-free.app",
  "userVerification": "preferred",
 }
}
```


Table IX. Authentication API Validation

Property	*Expected*	*Actual*	*Compliant*
rpId	Current domain	28e7-193-148-16-6.ngrok-free.app	Yes
challenge length	≥ 16 bytes, unique per request	32 bytes, unique on each request	Yes
userVerification	"preferred"	"preferred"	Yes
timeout	Matches configured value	60000	Yes

3. ***Security Properties Validation***

Beyond API structure compliance, the following security properties were validated through targeted testing:

Table X. Security Properties Validation

Property	*Method*	*Expected*	*Result*
Origin Binding	Verify rpId matches current domain	rpId = HTTP host	rpId matched the ngrok tunnel domain exactly
Challenge Entropy	Decode and measure challenge bytes	≥ 32 bytes (256-bit)	Decoded challenge = 32 bytes (256 bit)
Challenge Uniqueness	Compare two consecutive challenges	Different challenge values	Two consecutive challenges produced entirely different base64url strings
Challenge Expiration	Wait for challenge to expire (> 5 minutes), then attempt verification	Server rejects expired challenge	Server returned error "Timed out" after expiration period
Replay Prevention	Capture a valid challenge, complete authentication,	Server rejects reused challenge	Server returned error "Challenge

Property	*Method*	*Expected*	*Result*
	then resubmit the same challenge		has already been used" on second attempt
Sign Count	Authenticate twice and verify sign_count in database	sign_ count increme-nts	sign_count incremented from 0→1→2 after two successful authenticati-on

All 6 security property tests passed, confirming that the implementation enforces the critical security guarantees specified by the WebAuthn standard.

C. Discussion

The implementation demonstrates that FIDO2/WebAuthn-based MFA can be effectively integrated into an open-source e-commerce platform without modifying its core codebase. Several key findings emerge from this study:

1. ***Non-Invasive Integration***: The module's exclusive use of PrestaShop's hook system confirms that complex security features can be added modularly. Five hooks suffice to cover the complete authentication lifecycle: UI injection, login interception, page access control, and asset loading. This approach preserves upgrade compatibility and does not conflict with other modules.
2. ***Dual Authentication Modes***: The implementation of both passwordless and MFA modes provides flexibility for merchants. Passwordless mode offers the strongest security and simplest user experience, while MFA mode provides a graduated security upgrade path for platforms migrating from password-only authentication. The dynamic redirect mechanism ensures that MFA verification does not disrupt user navigation flow.
3. ***Cart Retention***: A significant engineering challenge in passwordless login is preserving the guest shopping cart through the authentication boundary. The implemented solution of capturing guest cart contents before `Context::updateCustomer()` and re-adding them post-authentication ensures uninterrupted user shopping experience, an important factor for e-commerce conversion rates.
4. ***WebAuthn Compliance***: The module implements the WebAuthn Level 2 specification faithfully. Challenge generation uses cryptographically secure random bytes (256-bit), challenges are single-use with server-side expiration (preventing replay attacks), and credentials are bound to the Relying Party origin (preventing phishing). The module advertises three primary COSE algorithms (ES256, RS256, EdDSA) in the credential creation options, while the server-side Algorithm Manager supports seven algorithms (ES256, ES384, ES512, RS256, RS384, RS512, EdDSA) for broad authenticator verification compatibility.
5. ***Comparison with Related Work***: Unlike the general-purpose FIDO2 implementations analyzed by Rivera-Dourado et al. (2021), this module specifically addresses e-commerce concerns: shopping cart persistence across authentication boundaries, protected page access control, and configuration through the platform's native admin interface. While Ou et al. (2024) focused on decentralized identity and Rivera-Dourado et al. (2025) on network-level authentication, this research fills the gap of FIDO2 integration in the e-commerce platform layer with an emphasis on practical deployment.

D. Limitations

This study has several limitations: (1) testing was conducted in a development environment using ngrok for HTTPS tunneling, which may introduce behavioral differences compared to production deployments with dedicated SSL certificates; (2) performance benchmarking (authentication latency, server load) was not within the scope of this study; and (3) usability testing with end-users was not conducted.

VI. CONCLUSIONS

This research successfully designed, implemented, and validated a FIDO2/WebAuthn-based MFA module for the PrestaShop e-commerce platform. The key conclusions are:

1. The module demonstrates that FIDO2/WebAuthn authentication can be integrated into PrestaShop through its native hook system without any core system modifications, validating the feasibility of non-invasive security enhancement for open-source e-commerce platforms.
2. Functional testing confirms that both passwordless login and MFA verification flows operate correctly across Chrome, Firefox, and Safari browsers, with proper cart retention, dynamic page redirection, and credential management functionality. All 13 test cases achieved a 100% pass rate.
3. WebAuthn API testing validates compliance with W3C WebAuthn Level 2, confirming that the implementation enforces security properties including origin binding, 256-bit challenge entropy, replay prevention through single-use challenges, and asymmetric signature verification. All 6 security property tests passed.
4. The open-source module and comprehensive documentation provide a replicable reference for

implementing FIDO2 on other PHP-based e-commerce platforms with modular hook architectures.

Future work may include: usability testing with e-commerce customers, performance benchmarking under production loads, integration with account recovery mechanisms, and extension to PrestaShop's back-office (admin) authentication, and implementation of a trusted device management system. The current implementation relies on platform-bound authenticators whose private keys are hardware-locked to a single device's TPM or Secure Enclave. Future research should explore the integration of FIDO2 with a trusted device management mechanism that bridges authentication security and authentication convenience. Such a mechanism would enable users to register, view, and manage credentials across multiple trusted devices from a unified dashboard, complementing FIDO2's cryptographic security guarantees with improved cross-device portability and user experience.

ACKNOWLEDGMENT

The authors would like to express sincere gratitude to Universitas Islam Negeri Sultan Syarif Kasim Riau, particularly the Department of Informatics Engineering, Faculty of Science and Technology, for providing the academic environment and resources that supported this research.

We also extend our deepest appreciation to the open-source community, specifically the contributors to the PrestaShop project and the WebAuthn PHP framework, for providing the foundational tools that enabled the development of this module.

Finally, the authors thank the W3C Web Authentication Working Group and the FIDO Alliance for developing and standardizing the WebAuthn and FIDO2 specifications that form the foundation of this work.

The complete source code of the FIDO2/WebAuthn module developed in this research is publicly available as an open-source at https://github.com/rel1vee/fido2auth.

REFERENCES

1. Aburbeian, A. M., & Fernández-Veiga, M. (2024). Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. *AI*, 5(1), 177-194. https://doi.org/10.3390/ai5010010
2. Affia, A. A. O., Matulevičius, R., & Nolte, A. (2020). Security Risk Management in E-Commerce Systems: A Threat-Driven Approach. *Baltic Journal of Modern Computing*, 8(2), 213-240. https://doi.org/10.22364/bjmc.2020.8.2.02
3. Barbosa, M., Boldyreva, A., Chen, S., & Warinschi, B. (2021). Provable Security Analysis of FIDO2. In *Advances in Cryptology - CRYPTO 2021* (pp. 125-156). Springer. https://doi.org/10.1007/978-3-030-84252-9_5
4. CISA. (2022). *Implementing Phishing-Resistant MFA*. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
5. FIDO Alliance. (2018). FIDO User Authentication Specifications. https://fidoalliance.org/specifications
6. Islam, S. (2024). Impact of Online Payment Systems on Customer Trust and Loyalty in E-Commerce. *Available at SSRN 5064838*. https://dx.doi.org/10.2139/ssrn.5064838
7. Kishnani, U., & Das, S. (2024). Dual-Technique Privacy & Security Analysis for E-Commerce Websites. *arXiv preprint arXiv:2410.14960*. https://doi.org/10.48550/arXiv.2410.14960
8. Krishnapatnam, M. (2025). Next-Generation Identity Security in Healthcare: A Passkey-Based Approach. *International Journal of Computing and Engineering*, 7(3), 23-33. https://doi.org/10.47941/ijce.2701
9. Kunke, J., Wiefling, S., Ullmann, M., & Iacono, L. L. (2021). Evaluation of Account Recovery Strategies with FIDO2-Based Passwordless Authentication. *arXiv preprint arXiv:2105.12477*. https://doi.org/10.48550/arXiv.2105.12477
10. Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., & Ferres, J. L. (2023). How Effective is Multifactor Authentication at Deterring Cyberattacks?. *arXiv preprint arXiv:2305.00945*. https://doi.org/10.48550/arXiv.2305.00945
11. Microsoft Threat Intelligence. (2023). Detecting and Mitigating a Multi-Stage AiTM Phishing and BEC Campaign. *Microsoft Security Blog*. https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign
12. NIST. (2025). *NIST SP 800-63 Digital Identity Guidelines*. https://pages.nist.gov/800-63-4
13. Ou, H. H., Pan, C. H., Tseng, Y. M., & Lin, I. C. (2024). Decentralized Identity Authentication Mechanism: Integrating FIDO and Blockchain for Enhanced Security. *Applied Sciences*, 14(9), 3551. https://doi.org/10.3390/app14093551
14. OWASP. (2025). Introduction - OWASP Top 10:2025 RC1. https://owasp.org/Top10/2025/0x00_2025-Introduction
15. PCMI. (2024). Indonesia's E-commerce Market: Trends & Growth 2024-2027.

https://paymentscmi.com/insights/indonesia-ecommerce-market-data

16. PrestaShop. (2025). Developer Documentation. https://devdocs.prestashop-project.org
17. Rivera-Dourado, M., Gestal, M., Pazos, A., & Vázquez-Naya, J. M. (2021). An Analysis of the Current Implementations Based on the WebAuthn and FIDO Authentication Standards. *Engineering Proceedings*, 7(1), 56. https://doi.org/10.3390/engproc2021007056
18. Rivera-Dourado, M., Gestal, M., Pazos, A., & Vázquez-Naya, J. (2024). A Novel Protocol Using Captive Portals for FIDO2 Network Authentication. *Applied Sciences*, 14(9), 3610. https://doi.org/10.3390/app14093610
19. Rivera-Dourado, M., Xenakis, C., Pazos, A., & Vázquez-Naya, J. (2025). EAP-FIDO: A Novel EAP Method for Using FIDO2 Credentials for Network Authentication. *Computer Networks*, 111348. https://doi.org/10.1016/j.comnet.2025.111348
20. Spomky. (2025). web-auth/webauthn-framework: FIDO-U2F / FIDO2 / WebAuthn Framework. GitHub. https://github.com/web-auth/webauthn-framework
21. Store Leads. (2026). The State of PrestaShop in 2026. https://storeleads.app/reports/prestashop
22. W3C. (2021). Web Authentication: An API for Accessing Public Key Credentials - Level 2. https://www.w3.org/TR/webauthn-2
23. Yadav, T. K., & Seamons, K. (2024). A Security and Usability Analysis of Local Attacks Against FIDO2. *Network and Distributed System Security (NDSS) Symposium*, 2024(327). https://doi.org/10.14722/ndss.2024.24327