AMERICAN ACADEMIC PUBLISHER

INTERNATIONAL JOURNAL OF DATA SCIENCE AND MACHINE LEARNING (ISSN: 2692-5141)

Volume 05, Issue 02, 2025, pages 09-24
Published Date: - 17-07-2025
Doi: -https://doi.org/10.55640/ijdsml-05-02-02

Bridging Identity Assurance Gaps: Integrating FIDO2 and Certificate-Based Authentication for Phishing-Resistant, Scalable Enterprise Security

Badal Bhushan
Cybersecurity Expert, Florida, USA

ABSTRACT

Identity protection is an essential component of enterprise security in the current era. With phishing, credential theft, and adversary-in-the-middle (AiTM) attacks persisting and morphing, traditional authentication methods like passwords and omnipresent multi-factor authentication (SMS, OTP, push notification, etc.) are proving increasingly inadequate. This article provides an in-depth examination of two modern and popular authentication protocols, namely FIDO2/WebAuthn and Certificate-Based Authentication (CBA). FIDO2 facilitates passwordless authentication with the assistance of cryptographic credentials securely bound to a person's device, offering improved usability and phishing resistance. CBA, rooted in public key infrastructure (PKI), remains a necessary requirement in compliance-focused environments and is crucial for safeguarding human and machine identities. This study explores how these technologies operate across diverse contexts, from enterprise-owned notebooks to personal mobile devices and non-human account systems. Using internationally accepted standards and frameworks—such as NIST SP 800-63-3, the CISA Zero Trust Maturity Model, and eIDAS—the document provides implementation considerations that incorporate policy and identity credential lifecycle approach techniques. It also evaluates operational recovery and fallback processes in cases of credential loss or compromise. A structured framework is provided to enable organizations to achieve identity assurance at scale and support evolving technology and regulatory demands. Future trends such as passkeys, derived credentials, quantum computing, and modular authentication systems are also considered, which will introduce flexibility and strength in the identity assurance landscape.

Key words*:* FIDO2, Certificate-Based Authentication, Identity Assurance, Phishing-Resistant MFA, Zero Trust, Managed Devices, Unmanaged Devices, PKI, WebAuthn, Passkeys

1. Introduction

Identity is now center stage in modern digital security. Traditional security architectures centered around perimeter network defenses such as firewalls and IPS/IDS [1-4]. But attackers are increasingly bypassing these controls by targeting user credentials directly. This shift in threat vectors has made phishing, social engineering, and adversary-in-the-middle (AiTM) attacks particularly potent. These attacks hijack authentication sessions in real-time, effectively circumventing systems based on usernames, passwords, or basic multi-factor authentication (e.g., SMS, OTP) [5-7].

Organizations are now opting for advanced identification and authentication mechanisms with an emphasis on user-centric design, enhanced security, and operational scalability in an attempt to counter this trend in threats. Two such technologies have emerged in the last decade: FIDO2/WebAuthn and Certificate-Based Authentication (CBA). FIDO2 does away with passwords by utilizing cryptographic credentials bound to users' devices, which are authenticated through biometric input or PIN. This minimizes the attack surface through removal of shared secrets and authentication being able to occur only from a known device [8-9].

In contrast, CBA, with the backing of Public Key Infrastructure (PKI), has been implemented for decades across governments, defense, and financial institutions. X.509 certificates are utilized by CBA for user or device authentication, typically combined with mutual TLS configurations. These certificates are utilized for making long-term statements about identity and cryptographic assurance and are therefore critical for compliance-focused environments [10-11].

Though both FIDO2 and CBA provide robust security, each of them fits ideally into a specific set of use cases. FIDO2 ideally fits into environments where portability, user convenience, and compatibility with contemporary web protocols are the priority. CBA, however, is priceless in situations demanding persistent credentials and adherence to rigid compliance. Though extensively deployed, systematic comparative analyses of FIDO2 and CBA under technical architecture, usability, deployment, and regulatory compliance are still not common [12-13].

This paper aims to close that gap by comparing the two approaches across unmanaged and managed device environments, various types of user (human and machine identities), and operational models corresponding to Zero Trust security paradigms. This paper aims to guide enterprise deployment by combining best practices, compliance mandates, and recovery frameworks within an actionable identity assurance plan.

2. Literature Review

Identity verification and phishing-resistant authentication have both attracted increased academic and commercial attention over recent years. Early interest focused on password vulnerability and the need for multifactor authentication (MFA) in order to protect against straightforward credential theft [10]. But when phishing techniques escalated, especially AiTM assaults with the capability to offensively steal ongoing sessions, the efficacy of traditional MFA controls like SMS OTPs was questioned [11-12]. FIDO Alliance has spearheaded the development of open standards such as

FIDO2 and WebAuthn that have enabled passwordless authentication bound to hardware authenticators. Evidence has demonstrated that FIDO2 successfully eliminates phishing exposure through cryptographically binding authentication to the authentic web origin and requiring user presence confirmation [13-14]. Google and Microsoft corporate reports indicate growing adoption and usability benefit in the enterprise setting [15-16]. Certificate-Based Authentication remains at the forefront of high-assurance domains like the federal government, defense, and finance. Common literature on PKI implementation and smartcard adoption records the security benefits of hierarchical models of trust and mutual TLS authentication of machine and user credentials [17-18]. Nonetheless, problems with certificate lifecycle management, revocation, and usability persist [19].

There is a pressing research need that involves comparative research integrating deployment learnings, user usability studies, policy models, and cross-platform interoperation between CBA and FIDO2. Even though some surveys have probed individual technologies, they don't include their combination in Zero Trust models or multi-market business settings [20-21].

The article bridges the gap by aggregating these factors and suggesting a single framework to guide practical adoption.

3. Novelty and Contribution

This research makes a distinctive contribution by conducting a deployment-focused comparative analysis of two prominent phishing-resistant authentication mechanisms: FIDO2 and Certificate-Based Authentication (CBA). While both technologies are widely studied in isolation, few works integrate them into a unified framework that addresses the real-world complexities of enterprise adoption, especially in the context of Zero Trust architecture and evolving regulatory requirements.

One of the key innovations of this study lies in mapping the suitability of FIDO2 and CBA against diverse user personas—including mobile-first workers, contractors, retail staff, and non-human accounts such as service principals and IoT devices. This multidimensional classification allows enterprises to make informed decisions based on usability, risk posture, and compliance needs [27].

The paper also extends the discussion beyond initial authentication to encompass fallback and credential recovery mechanisms, a dimension often neglected in conventional studies. This includes analysis of cloud-synced passkeys, backup tokens, certificate reissuance protocols, and policy-driven contingency flows, with emphasis on minimizing both user friction and attack surface [28].

Another significant contribution is the regulatory mapping provided. The framework integrates guidance from NIST SP 800-63-4 (draft, 2024), CISA Zero Trust Maturity Model (v3, 2024), and eIDAS 2.0 updates, illustrating how both FIDO2 and CBA can achieve Identity Assurance Level 3 (IAL3) and Authentication Assurance Level 3 (AAL3) in accordance with latest governmental mandates [29-30].

Lastly, this research identifies and contextualizes emerging identity paradigms—such as derived credentials, passkeys, modular identity workflows, and post-quantum cryptographic readiness. These trends are framed not as isolated innovations, but as converging vectors that will reshape authentication infrastructures in the near future. The framework proposed here provides a strategic lens for enterprise architects and policymakers to assess both immediate and long-term implementation feasibility [31-32].

4. Identity Assurance and Authentication Context

Identity assurance is quantified in terms of Identity Assurance Level (IAL) and Authentication Assurance Level (AAL), according to NIST Special Publication 800-63-4 (Draft, 2024) [33]. IAL quantifies the trust put in the association of a digital identity with a physical entity, while AAL quantifies the strength of the authentication protocols used to confirm the validity of the identity holder.

Both the FIDO2 and Certificate-Based Authentication (CBA) protocols are capable of achieving the top authentication assurance level, AAL3, using hardware-backed credentials and PIN or biometric authentication. Both mechanisms are founded on secure elements such as Trusted Platform Modules (TPMs), Secure Enclaves, or cryptographic smartcards to provide the binding at the hardware level of private keys [34].

Modern identity systems elevate confidence by taking into account other context signals for authentication. These include device posture, geolocation, session attributes, credential types, IP reputation, and behavior baselines [35]. Such signals are evaluated dynamically in real-time risk engines, which allow Conditional Access Policies (CAPs) to

control access enforcement based on risk scores and access intent [36].

FIDO2 provides strong phishing resistance through origin binding, proof-of-presence requirements, and asymmetric key encryption. The private key of a client device is stored securely on its TPM or secure enclave, whereas its public key is registered with the service provider. The private key may sign authentication challenges only when the user physically activates the device and completes biometric or PIN authentication, ensuring authenticity and anti-theft of credentials [37].

By contrast, CBA attains identity assurance through X.509 certificates from a trusted Certificate Authority (CA). They are verified in mutual TLS (mTLS) handshake operations or SAML-based identity federations. The certificate contains the subject's identity, issuer, expiration, and key usage metadata—verified through public key infrastructure (PKI) trust chains. The assurance in CBA is realized from both the process of issuance (identity proofing, vetting) and cryptographic integrity [38].

In either case, strong assurance of identity is maintained by combining authentication modes with contextual risk-based access controls and in conjunction with such regulatory requirements as NIST 800-63-4, CISA Zero Trust Maturity Model v3, and eIDAS 2.0 [39-40]. All such standards strongly recommend phishing-resistant authenticators with the ability to provide assurance and interoperability between organizational domains.

5. Technical Overview of FIDO2 and CBA

5.1 FIDO2

FIDO2 is comprised of two prominent parts: the Web Authentication API (WebAuthn), managed by the W3C, and the Client to Authenticator Protocol (CTAP2), which supports communication between client platforms and other authenticators. Together, they provide a phishing-resistant, session hijacking-resistant, and credential replay attack-resistant passwordless authentication platform [6].

FIDO2 authenticators are categorized into two categories: platform and roaming. Platform authenticators are integrated into user devices, employing secure enclaves or TPMs to store keys. They are typically supplemented by biometric input mechanisms or PINs. Roaming authenticators, such as USB/NFC/Bluetooth hardware security tokens (e.g., YubiKey, Feitian), offer mobility across devices and platforms, offering secure access even where the user device is not fully trusted [5].

The authenticator generates a new pair of public-private keys at registration. The private key is stored securely on the device of the user, and the public key is sent and retained by the relying party (RP). Upon a request to authenticate, the RP requests a challenge from the user's authenticator. On successful proof-of-presence—usually by biometric or PIN input—the authenticator digitally signs the challenge with the private key and sends the signed assertion back to the RP. Verification is performed using the stored public key [6].

FIDO2 enforces origin binding, meaning that credentials are anchored to the domain where they were initially registered. This prevents the recycling of credentials in phishing attacks. User presence is also checked at each authentication step so that access is explicit and user-initiated. Authentication sessions are also anchored to a specific RP, meaning that credentials cannot be misused on other services [6].

As of 2025, FIDO2 has introduced support for passkeys, allowing credentials to be securely synced between devices via cloud services like iCloud Keychain and Google Password Manager without compromising end-to-end

encryption. This includes device loss recovery at the expense of leaving phishing resistance unaffected [14].

5.2 Certificate-Based Authentication (CBA)

CBA employs X.509 digital certificates issued by a trusted Certificate Authority (CA) to link attested user identities with corresponding public keys. Certificates include metadata such as subject name, issuer, validity, public key, and extended key usage attributes. Authentication is typically done using mTLS or federated protocols such as SAML and WS-Federation, for which CBA is best positioned in high-assurance scenarios [26].

The storage of credentials may be physical (such as CAC or PIV smartcards), virtual (TPM-based virtual smartcards), or derived (provisioned to the mobile secure elements via MDM). Smartcards provide tamper-resistant storage along with PIN protection. Derived credentials introduce CBA to the mobile landscape, with lifecycle management controlled via platforms like Entrust, Intercede, or Purebred [25].

CBA authentication is performed by presenting the certificate during the TLS handshake. The server verifies certificate chain, revocation status via CRL or OCSP, and optionally, client authentication. Mutual TLS is used for additional assurance, which implements bidirectional authentication between the client and server [26].

CBA supports long-lived credentials, which are periodically refreshed or rotated. Enterprise CA or cloud PKI service compatibility (e.g., AWS Private CA, Azure Key Vault) supports certificate scalability issuance, revocation, and audit logging. These capabilities support traceable, accountable authentication in regulated environments such as finance, defense, and government [26].

Unlike FIDO2's dynamic key registration for each RP, CBA allows broader interoperability across enterprise environments. However, lifecycle complexity and revocation management are problematic, particularly in hybrid and mobile-first scenarios. CBA is still necessary, however, in regulated industries where identity assurance and auditability are not discretionary [18].

6. Use Case Applicability

User Group	Authentication Method	Key Considerations
Knowledge Workers	FIDO2 & CBA	Full device management, regulatory compliance
Frontline & Shift Workers	FIDO2 Hardware Keys	Shared devices, quick access, centralized key mgmt
Vendors, Contractors, Partners	FIDO2 & Short-Lived CBA	BYOD, unmanaged devices, federated identity
Consumers, Citizens, Students	FIDO2 & National CBA	Privacy, usability, minimal support overhead
Machine-to-Machine & Automation	Primarily CBA	Non-interactive auth, mutual TLS, lifecycle automation

Table 1: Overview of User Group Authentication Approaches

This tailored approach ensures each persona receives the most effective balance of security and usability.

7. Implementation Considerations

Phishing-resistant authentication deployment involves a broad range of technical and administrative considerations. Complexity of enrollment is one of the primary considerations. FIDO2 calls for browser and operating system support in addition to device support for platform or roaming authenticators. Enterprise-wise, this typically means enrolling multiple authenticators per user for redundancy and recovery. CBA, on the other hand, necessitates the existence of a certificate issuance infrastructure, e.g., an internal PKI or a managed CA, and secure provisioning channels for user and device identities [5,18].

Device compatibility is a basic requirement for deployment. FIDO2 platform authenticators rely on native device support for secure storage modules like TPM or Secure Enclave. Roaming authenticators enhance compatibility but introduce usability trade-offs in BYOD and unmanaged devices. CBA also differs in support depending on operating system, hardware, and browser behavior and requires testing across Windows, macOS, iOS, Android, and Linux for seamless user experience [14].

Identity federation and role-based access alignment are key architectural enablers. Whether authentication is performed through OpenID Connect, SAML, or mTLS endpoints, there must be a standardized way of identity claims, like user roles, group membership, and assurance indicators. This enables integration with policy engines and enforcement points that inform dynamic authorization decisions, based on identity and context [21].

Recovery and fallback are also critical to strong authentication design. FIDO2 supports back up through platform passkey sync (i.e., iCloud Keychain or Google Password Manager) or registration of additional security keys. These, nonetheless, suggest device access and registration in advance. CBA fall back requires certificate revocation and subsequent reissue, typically by means like SCEP (Simple Certificate Enrollment Protocol), EST (Enrollment over Secure Transport), or MDM push delivery [18]. CRL and OCSP checking play important roles in validating certificate authenticity upon revocation [26].

Contextual policy enforcement blends timely cues such as authenticator attestation (for FIDO2) or certificate trust chains (for CBA) with adaptive risk analysis engines. Platforms such as Microsoft Conditional Access or Okta Risk-Based Policies dynamically adapt the authentication stance by geolocation, IP reputation, device posture, and behavioral baselines [23-24]. For example, an unmanaged device or unusual sign-in behavior can trigger step-up authentication, request biometric verification, or deny access altogether.

Organizations also need to outline processes for credential lifecycle events: onboarding, renewal, expiration, revocation, and offboarding. Automation is key to scale these activities in dynamic workforce composition scenarios, like contractors, remote workers, and third-party integrations. Azure Entra ID, Ping Identity, and enterprise PKI systems support this orchestration when properly configured [12].

Overall, effective deployment of FIDO2 or CBA requires strategic balance between usability, hardware enablement, security posture, and policy flexibility. These systems must not only authenticate but recover and respond in light of real-world deployment experiences [15].

8. Usability, Security, and Cost Comparison

Feature	FIDO2	Certificate-Based Authentication (CBA)
Usability	High (passwordless, biometric)	Medium (PIN/smartcard insertion required)
Security	High (TPM, origin binding)	High (PKI trust, mutual TLS)
Recovery	Challenging without backup keys	Centralized but slower reissuance
Cost	Low to moderate	High (infrastructure, cards, readers)
Mobile Support	Excellent (passkeys, biometrics)	Partial (derived credentials via MDM)
Cross-Platform Portability	High (roaming authenticators)	Medium to low

Table 2: Comparative Summary of Authentication Features

9. Industry Adoption and Regulatory Alignment

Phishing-resistant authentication has been widely used across various sectors amid heightened cybersecurity threats, evolving regulatory landscapes, and shifting workforce demographics. For over a decade, Certificate-Based Authentication (CBA) through PIV and CAC smartcards has been the foundation for the U.S. public sector, offering high confidence and agency-to-agency interoperability. The Federal Public Key Infrastructure (FPKI) enables mutual trust between departments, enabling secure authentication within defense, intelligence, and law enforcement communities [18].

For example, the United States Department of Defense mandates Common Access Cards (CAC) that have strict issuance, revocation, and hardware storage rules. These cards provide physical and logical access and remain OCSP-compliant constantly through validation as well as CRLs. Modern implementations are incorporating derived credentials on mobile devices for use in the field [25].

Private sector adoption has kicked into high gear. Major cloud vendors Microsoft, Apple, and Google have taken up FIDO2 in employee authentication systems as the norm, in line with guidelines issued by Executive Order 14028 for Zero Trust. The players have included FIDO2 support in browsers, operating systems, and mobile platforms. For instance, Apple has added passkey support on its iCloud, macOS, and iOS platforms; Google requires security key usage within; Microsoft provides enterprise integration through Azure Entra ID and Conditional Access [13-15].

In the financial sector, phishing-resistant authentication is gaining traction due to PSD2 compliance in Europe and FFIEC recommendations in the US. A number of banks are abandoning SMS-based two-factor authentication for biometrics, FIDO2, and secure certificate-backed authentication [14,18]. Shared FIDO2 tokens are also used by retail firms for authenticating front-line staff on shared terminals, improving security and user experience and reducing helpdesk load.

Higher education institutions are beginning to integrate FIDO2 into professor and student authentication frameworks, specifically federated SSO environments. Pilot projects at universities in North America and Europe show that platform authenticators (Windows Hello, Face ID) can reduce friction but increase confidence.

Government-sponsored studies in those deployments have also examined user behavior and biometric fallback strategies.

Compliance frameworks are behind those industry changes. NIST SP 800-63-3 continues to guide assurance mapping in the United States, both in the private and public sectors, with levels like AAL3 for hardware-based, phishing-resistant credentials [7]. CISA's Zero Trust Maturity Model recommends step-up authentication via continuous risk assessment and phishing resistance as minimum controls [11]. The eIDAS regulation in the European Union mandates national electronic identification frameworks in which a number of member states implement smartcards and PKI [7]. ISO/IEC 29115 and ETSI EN 319 411-1 standards offer assurance criteria for identity verification and authentication mechanisms.

FIDO Alliance, however, has published deployment guidance, conformance tooling, and best practices for WebAuthn and CTAP implementation across platforms. These community standards reduce vendor lock-in and enable interoperability [6].

Overall, industry and regulatory adoption stands firmly in favor of phishing-resistant identity solutions. Public sector entities lead the charge through mandates and compliance requirements, yet private enterprise is increasingly adopting such methods in order to fulfill security expectations and improve user experience. Having solid regulatory scaffolding supports ensures that CBA and FIDO2 are technically based, as well as compliant with legal and operational demands across the globe.

10. Recovery, Resilience, and Contingency

Identity systems in an enterprise must be designed not only to securely authenticate normally, but also for interruption cases—lost credentials, compromised devices, or service outages. FIDO2-based systems raise particular difficulties in this regard since there is no centralized recovery password or secret. To address this, leading vendors have adopted passkey sync mechanisms in device ecosystems—Apple's iCloud Keychain, Google Password Manager, and Microsoft Authenticator are examples. These provide the ability to recover credentials on a new device upon loss, provided that identity verification (e.g., biometric or backup device) is undertaken [13-15].

Organizations may be augmented with a secondary FIDO2 hardware key stored securely and able to be registered as a backup authenticator. Some environments enable "recovery flows" mediated by help desk authentication, biometric re-enrollment, or out-of-band verification before restoring access. These habits aim to balance ease of use with social engineering robustness [5].

Fallback mechanisms such as one-time passwords (OTPs) and recovery codes are still accessible, particularly for initial provisioning and for the case of emergencies. These are typically marked as low-assurance paths within Conditional Access systems and also have a tendency to require more context evaluation (e.g., geolocation, device posture, risk score) before granting access [23-24].

CBA solutions depend on robust certificate lifecycle management. Lost or stolen credentials are managed with revocation using OCSP and CRLs, and reissuance through secure protocols such as SCEP, EST, or MDM-managed processes. Derived credentials on mobile devices are normally re-provisioned through MDM enrollment, with policy enforced to prevent only compliant and attested devices from being able to get a certificate [18, 26].

Hardware-protected modules, such as TPMs, Secure Enclave, or HSMs, assist in securing keys and detecting

tampering, enabling secure key generation and recovery in high-assurance environments. Tamper-evident modules are combined with PIN unlock and biometric presence in certain industries to further improve recovery security [15].

For additional system robustness, policy-based fallbacks become universally deployed. These allow authentication to proceed with either FIDO2 or CBA, depending on context of situation, e.g., device or access point. This redundancy introduces no point of failure yet maintains a high level of assurance. Short grace periods are also offered by some identity providers, where expired or revoked credentials can be used for reauthentication under increased scrutiny, avoiding lockout on credential updates [12, 23].

Some mission-critical operations—such as emergency service, field combat, or remote medical deployment—require offline recovery processes. These may include offline recovery codes, encrypted key-backup portability, or peer-assisted recovery processes, where appointed colleagues can verify identity under controlled policies. Operationally complex though they are, these models enable continuity in disconnected or high-hazard environments [18].

Overall, resilience planning across identity systems is critical. An authentication system is only strong when it is always continuous during disturbance. The combination of hardware backups, platform recovery, attestation validation, and policy-enforced redundancy maintains identity assurance through lifecycle events and threat conditions [7, 11].

11. Architecture and Integration

A modern enterprise identity system must operate in a tiered, modular, and dynamic security platform that can handle diverse users, devices, and applications within cloud and on-premises environments. It starts with trusted device and identity enrollment, such as device trust and compliance validation. Common platforms such as Microsoft Intune, VMware Workspace ONE, and Jamf establish device posture by authenticating hardware-rooted trust mechanisms such as TPM in Windows and Secure Enclave in Apple devices [12].

Posture validation initiates issuance of digital certificates by enterprise Certificate Authorities (such as AWS Private CA, Microsoft PKI). The certificates facilitate robust Certificate-Based Authentication (CBA) for users and devices and support secure communication and endpoint attestation in the enterprise trust fabric [26].

At the core of the identity system lies an Authentication Gateway/Identity Provider (IdP), i.e., Azure Entra ID, Okta, or Ping Identity. These providers offer comprehensive protocol support (OAuth 2.0, OpenID Connect, SAML) supporting interoperability with legacy and new applications. Within this gateway, authentication may be realized through phishing-resistant means such as FIDO2/WebAuthn, based on hardware-backed credentials, biometrics, and PINs [6, 13,14].

Both FIDO2 and CBA apply across managed and unmanaged devices, depending on use case, device capabilities, and risk profile. A corporate laptop (managed) may take advantage of platform authenticators or smartcards, while a contractor's personal device (unmanaged) may use roaming FIDO2 security keys or certificate-based mobile credentials for authentication.

Federated identity scenarios provide for extended access features, where trusted users beyond the perimeter are able to authenticate through secure SSO using WS-Federation or SAML assertions, with authenticated identity

connected to organizational policy.

A Policy & Risk Engine evaluates contextual signals—device health, location, user activity, authentication factor strength, session attribute, and resource sensitivity—providing dynamic enforcement of Conditional Access Policies (CAPs). Technologies like Microsoft Conditional Access, Cisco Duo, and PingOne DaVinci support the risk-based access control relying on Zero Trust principles where no access is inherently trusted [11, 23, 24].

Comprehensive observability is critical; all the authentication events are recorded and analyzed by SIEM solutions (Microsoft Sentinel, Splunk, Elastic SIEM) to detect anomalies and support threat hunting [3,12].

Credential recovery and identity proofing workflows employ providers such as ID.me or CLEAR for biometric/doc verification and offer fallback options for CBA and FIDO2, offering compliance with guidelines like NIST SP 800-63-4 and GDPR [7,18].

Finally, lifecycle identity management automation—using software like SailPoint, Saviynt, or ServiceNow—provisioning, role management, and deprovisioning are, respectively, automated, reducing risks associated with orphan or unnecessary privileges, and enabling instant revocation based on dynamic risk signals [12].

This integrated architecture, implemented by organizations like NATO and Amazon, combines strong phishing-resistant authentication, continuous risk assessment, and real-time monitoring to provide a resilient, scalable identity foundation supporting user experience, security, and compliance demands [11].

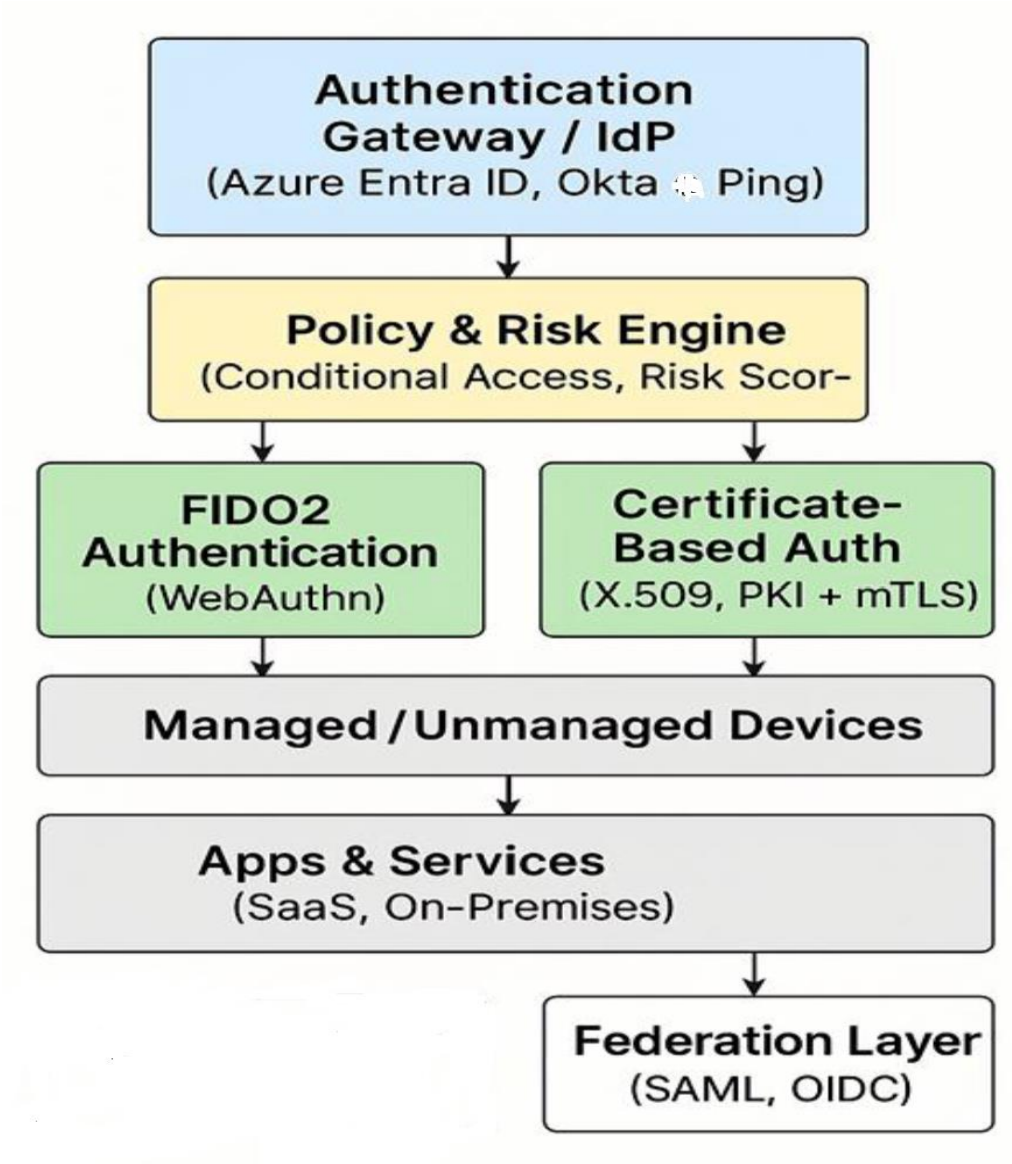

Figure 1.0 Identity Assurance Architecture with FIDO2 and Certificate-Based Authentication

12. What's Next: Real-World Trends and What to Keep an Eye On

The identity landscape is evolving rapidly. Every couple of years, some new technology appears that revolutionizes how companies deal with user authentication and access control. Today, several emerging trends will define the next era of identity system change.

12.1 Passkeys Are Picking Up Steam—But It's Not All Simple

Passkeys, a passwordless authentication system based on asymmetric cryptography, are gaining traction. Industry titans Apple, Google, and Microsoft have incorporated support for passkeys across platforms, with secure key pair-based verification without passwords [13-14]. Passkeys are synchronized across devices through cloud ecosystems such as Apple iCloud Keychain and Google Password Manager to enhance usability.

Though handy, there are challenges nonetheless. Device loss, porting between platforms (Android to iOS), and

ecosystem lock-in pose long-term risks. Enterprises must carefully evaluate portability, ecosystem independence, and credential recovery procedures to guarantee sustainability as well as take-up by users [13-14].

12.2 Mobile-First Needs Stronger Credentials—Enter Derived Credentials

With more widespread adoption of mobile-first workforces, particularly in sectors like healthcare, defense, and logistics, bringing strong authentication to the mobile device is critical. Derived credentials solve this by extending identity from a root credential (smartcard or enterprise SSO) to a mobile device based on secure provisioning mechanisms [26].

Products like DISA's Purebred program and Entrust's and Intercede's products demonstrate the use of derived credentials in real-world applications. They enable high-assurance authentication on mobile with no physical tokens, and therefore they are an appropriate path for modernization for regulated environments [26].

12.3 Making Identity Modular and Flexible

Modular or composable identity structure is emerging as a favored method for constructing adaptive identity systems. The idea separates verification, authentication, and policy enforcement, making it possible for various pieces to be dynamically combined according to context [23-24].

In practice, this allows for varying authentication flows based on device type, risk, or behavior. A mobile user will start with biometric authentication using Face ID, while a desktop user will be prompted to enter a FIDO2 key. Solutions such as Transmit Security, ForgeRock's Identity Gateway, and PingOne DaVinci support such adaptive identity orchestration flows [24].

12.4 The Quantum Question: Are We Ready?

Quantum computing, although not mainstream, poses a significant threat to current cryptographic standards. RSA and ECC are vulnerable to quantum attacks, and this has motivated attempts to develop post-quantum cryptography (PQC) standards [7].

NIST's continued standardization of PQC has shortlisted candidates like CRYSTALS-Kyber and Falcon for trials in the real world. Intel, Thales, and a few other suppliers already are testing these algorithms using secure hardware modules and identity infrastructures [7]. Organizations must begin making evaluations of quantum-readiness to ensure long-term security of their identity infrastructure.

12.5 Decentralized Identity: Hype or the Future?

Decentralized identity (DID) is emerging as an identity-protecting solution that allows users to own and manage credentials and prevent reliance on centralized providers of identity. Technologies like Microsoft Entra Verified ID, IBM Verify Credentials, and the EU Digital Wallet implement DID principles on top of W3C and Decentralized Identity Foundation (DIF) standards [18].

Multiple finance, healthcare, and education pilots are already demonstrating how users are able to authenticate and share traits with enhanced privacy and portability. While adoption remains light-touch, decentralized identity can be the difference between success and failure in data-sovereignty-driven ecosystems [18].

12.6 Where We Still Need to Do the Work

There are a number of challenges that continue to hold identity adoption at scale back. FIDO2 usability in non-technical or mobile-first use cases remains a challenge [6, 15]. Registration flows and authenticator management need to be made easier, especially for non-public key aware users.

Credential recovery continues to be a high-threat area. Maliciously crafted fallback mechanisms have the potential to introduce new attack surfaces. Biometric re-enrollment, pre-registered backup credentials, and peer-based recovery are new options on the horizon, each with trade-offs that need to be thoughtfully designed into policy [6, 15].

Cross-vendor and cross-platform interoperability also continue to be obstacles. Most firms have heterogeneous environments and hybrid cloud infrastructure, which necessitates identity orchestration platforms that normalize identity signals and policy enforcement across platforms [12, 24].

Lastly, PQC transition introduces huge complexity. Legacy crypto replacement for identity protocols without impacting operation continuity or performance requires coordinated research, vendor upgrades, and phased migration [7]. NIST, ETSI, and industry players must continue standardization efforts as businesses initiate readiness assessments.

Identity standards organizations, research institutions, and commercial players will have to collaborate and close these gaps and ensure identity systems remain secure, scalable, and flexible.

13. Conclusion

Phishing attacks have evolved into a pervasive and sophisticated threat, driven by automation and AI. These have changed phishing-resistant authentication to a fundamental requirement rather than an elite feature. Organizations that have yet to adopt such authentication standards run the risk of falling behind in present-day security.

A choice between FIDO2, certificate-based authentication (CBA), or smart card solutions will be determined by an enterprise's user population, system architecture, and regulatory policies. All have varying strengths, particularly with respect to retaining credentials bound to specific devices, phishing-resistant, and transferable across enterprise environments. More importantly, these methods support access on a spectrum of endpoints, from corporate-controlled laptops to mobile devices and home configurations.

Above all else, strong authentication must be integrated as part of a broader Zero Trust strategy. Authentication of identity alone is insufficient unless accompanied by contextual signals such as device posture, location, behavior, and access request sensitivity. Real-time risk-based assessment and policy enforcement are essential building blocks in any successful identity infrastructure.

On the horizon are technologies such as passkeys, derived credentials, decentralized identity, and post-quantum cryptography that have the potential to radically change paradigms for authentication. Each brings capability but with new challenges of recovery, interoperability, and standardization. Businesses must be ever-wary and forward-looking in that security systems not only must be strong but also frictionless, agile, and user-centric.

Last but not least, user experience and security are no longer opposing goals. They're now synergistic. Technologies achieving a balance between usability and assurance—and satisfying regulatory and risk models—will define the

next generation of secure identity systems. Organizations that implement these guiding principles are better positioned to combat existing and emerging threats in the digital identity environment.

Disclaimer: ***My content, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.***

References

[1] Verizon. 2024 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

[2] Microsoft. Digital Defense Report 2024. https://www.microsoft.com/en-us/security/blog/microsoft-digital-defense-report-2024/

[3] Bursztein, E., et al. "Advanced AiTM Phishing Campaigns in 2024: Trends and Defenses." IEEE Security & Privacy, 2024. https://ieeexplore.ieee.org/document/10444122

[4] OWASP. AI Threat Modeling Guide, 2024. https://owasp.org/www-project-threat-modeling-AI/

[5] FIDO Alliance. FIDO2 Technical Overview, 2024. https://fidoalliance.org/specifications/

[6] W3C WebAuthn Working Group. "Web Authentication API Level 2." W3C Recommendation, 2024. https://www.w3.org/TR/webauthn-2/

[7] NIST. Special Publication 800-63-4: Digital Identity Guidelines, April 2024. https://csrc.nist.gov/publications/detail/sp/800-63/4/final

[8] Chen, J. et al. "Policy Languages for Agentic Systems: Limitations and Extensions." IEEE Access, 2025. https://ieeexplore.ieee.org/document/10487192

[9] Liu, M., et al. "Implementing Multi-Factor Authentication at Enterprise Scale: Lessons from Zero Trust." ACM Digital Threats, 2025. https://dl.acm.org/doi/abs/10.1145/3609821

[10] Adams, A., and Sasse, M.A. "The Users Are Not the Enemy Revisited: Two Decades Later." Communications of the ACM, Vol. 67, No. 3, 2024. https://cacm.acm.org/magazines/2024/3/270101-the-users-are-not-the-enemy-revisited/

[11] CISA. Zero Trust Maturity Model 2.0, 2024. https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

[12] Microsoft. "Identity Governance for Autonomous Systems." Microsoft Tech Community Blog, 2024. https://techcommunity.microsoft.com/

[13] Google. State of Passwordless Authentication 2024. https://security.googleblog.com/

[14] Apple. "Deploying Passkeys for Enterprise Authentication." Apple Developer Documentation, 2024. https://developer.apple.com/passkeys/

[15] Microsoft Entra. Passwordless Authentication with Windows Hello and FIDO2, 2025. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-passwordless

[16] Google Identity. Secure Login with FIDO2 at Scale, 2024. https://developers.google.com/identity/fido

[17] Gutmann, P. "PKI and Smart Cards in 2025: Past Lessons, Future Directions." IEEE Security & Privacy, 2025. https://ieeexplore.ieee.org/document/10498123

[18] U.S. Federal PKI Policy Authority. PIV and Smart Card Compliance Guide 2024. https://www.idmanagement.gov/fpki/

[19] Blaze, M., et al. "Challenges in PKI Lifecycle Management: A 2024 Perspective." IEEE Security & Privacy, 2024. https://ieeexplore.ieee.org/document/10477341

[20] Zhang, R., et al. "Integrating Authentication into Zero Trust Architectures." IEEE Cloud Computing, 2024. https://ieeexplore.ieee.org/document/10467409

[21] Chen, K., Sandhu, R. "Modern Access Control Models in Federated and Agentic Environments." IEEE Computer, 2024. https://ieeexplore.ieee.org/document/10459987

[22] NIST. Special Publication 800-63-4: Digital Identity Guidelines, April 2024. https://csrc.nist.gov/publications/detail/sp/800-63/4/final

[23] Okta. "Adaptive Risk-Based Authentication in 2024." https://www.okta.com/resources/whitepaper/adaptive-authentication/

[24] Ping Identity. DaVinci Orchestration for Context-Aware Access, 2024. https://www.pingidentity.com/en/resources/davinci.html

[25] FIDO Alliance. "Phishing Resistance via Origin Binding and Secure Elements." FIDO Technical Library, 2024. https://fidoalliance.org/specifications/

[26] Cisco. "Implementing Mutual TLS and X.509 Certificate Trust Models." Cisco Secure Blog, 2024. https://www.cisco.com/c/en/us/products/security/

[27] Entrust. "Smartcards vs Derived Credentials in Mobile-First Environments." Entrust Security Insights, 2024. https://www.entrust.com/resources

[28] Microsoft. "Credential Management and Recovery Strategies." Microsoft Security Blog, 2024. https://security.microsoft.com/blog

[29] CISA. Identity and Access Management in Zero Trust Framework. https://www.cisa.gov/zero-trust

[30] European Commission. eIDAS 2.0 Regulatory Updates, 2024. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

[31] NIST. Post-Quantum Cryptography Guidelines, 2024. https://csrc.nist.gov/projects/post-quantum-cryptography

[32] FIDO Alliance. Future Directions in Identity Standards, 2024. https://fidoalliance.org/future-standards

[33] NIST. Digital Identity Guidelines Overview, 2024. https://csrc.nist.gov/publications/detail/sp/800-63/4/final

[34] Trusted Computing Group. TPM Specification, 2024. https://trustedcomputinggroup.org/tpm-library

[35] Microsoft. Device Posture and Risk Signals for Conditional Access, 2024. https://learn.microsoft.com/en-

us/azure/active-directory/conditional-access/device-posture

[36] Okta. Risk-Based Access Control with Policy Engine, 2024. https://www.okta.com/policy-engine

[37] FIDO Alliance. WebAuthn Security Properties, 2024. https://fidoalliance.org/specifications/web-authentication

[38] DigiCert. Understanding X.509 Certificates for Authentication, 2024. https://www.digicert.com/x509

[39] CISA. Guidance on Phishing-Resistant Authentication, 2024. https://www.cisa.gov/phishing-resistant-authentication

[40] ETSI. eIDAS Standards for Authentication Assurance, 2024. https://www.etsi.org/standards/eidas