World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(Review Article)

Check for updates

Automated fibre channel device onboarding using FIDO protocol: Transforming SAN infrastructure management

Derek Asir Muthurajan Caleb *

Broadcom Inc., USA.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(02), 2530–2539

Publication history: Received on 28 March 2025; revised on 08 May 2025; accepted on 10 May 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.2.0657

Abstract

The onboarding of Fibre Channel (FC) devices in Storage Area Network (SAN) environments presents significant operational challenges for data center administrators, involving multiple manual configuration steps that create bottlenecks in infrastructure expansion. This article explores how adapting the FIDO protocol—originally developed for IoT device authentication—can revolutionize FC device provisioning by enabling automated, secure onboarding processes. Through a comprehensive article of current onboarding workflows and their limitations, it presents a technical framework for implementing FIDO-based zero-touch provisioning that eliminates the need for manual IP assignment, firewall configuration, management system discovery, monitoring setup, and switch parameter synchronization. The proposed methodology substantially reduces deployment timeframes while maintaining security compliance and operational consistency across SAN infrastructures.

Keywords: Zero-Touch Provisioning; Fibre Channel Automation; Fido Protocol Adaptation; San Device Onboarding; Storage Infrastructure Management

1. Introduction

In contemporary enterprise data centers, Storage Area Networks (SANs) represent a critical infrastructure component supporting mission-critical workloads. According to Enterprise Storage Systems Tracker, Fibre Channel (FC) technology remains predominant in high-performance storage environments despite the emergence of alternative networking protocols [1]. The manual onboarding process for these sophisticated FC devices creates significant operational inefficiencies that directly impact business agility and IT resource allocation.

1.1. Current Manual Provisioning Challenges

The traditional FC device provisioning workflow requires sequential execution of multiple configuration tasks that cannot be easily parallelized. SAN administrators must methodically allocate management IP addresses, update perimeter security controls, register devices within management platforms, configure monitoring parameters, and synchronize fabric settings to maintain operational integrity. Research indicates that this process represents a substantial portion of storage administration overhead, particularly as data center infrastructures scale to accommodate exponential data growth demands [1]. The time investment required for these manual processes directly correlates with increased operational expenditure and reduced deployment agility across enterprise environments.

1.2. Business Impact of Provisioning Delays

The ramifications of protracted FC device onboarding extend beyond immediate administrative burdens. Research published in the Journal of Information Processing and Development demonstrates that infrastructure provisioning

* Corresponding author: Derek Asir Muthurajan Caleb

bottlenecks create cascading delays throughout the application deployment pipeline [2]. These delays materially impact time-to-market for business initiatives, especially in sectors where competitive advantage relies on rapid infrastructure scalability. The journal's analysis of enterprise operations identifies a direct correlation between storage provisioning efficiency and overall business responsiveness to market opportunities, with particular significance in financial services, healthcare, and e-commerce verticals [2].

1.3. Security Compliance Considerations

Manual device onboarding introduces substantial security vulnerabilities through configuration inconsistencies. The Journal of Information Processing and Development research emphasizes that storage networks require particularly rigorous security controls due to their access to sensitive organizational data [2]. The security protocols necessary during FC device provisioning frequently necessitate coordination across multiple administrative domains, including network security teams, compliance officers, and storage administrators. This cross-functional dependency introduces additional procedural complexities that further extend provisioning timelines while still failing to eliminate the potential for security-compromising human error in the configuration process.

2. Understanding FIDO Protocol and Its Adaptation for FC Environments

The FIDO (Fast Identity Online) protocol represents a paradigm shift in authentication methodology that holds significant promise for addressing the complex challenges of Fibre Channel device onboarding in enterprise storage environments. Originally developed to solve the "password problem" in consumer authentication, FIDO's architectural principles offer a compelling foundation for secure device provisioning in mission-critical infrastructure. According to the FIDO Alliance, the protocol has been specifically designed to address the fundamental weaknesses of traditional authentication methods while providing strong cryptographic security that can be adapted across diverse technological domains [3].

2.1. FIDO Core Architecture and Security Principles

The FIDO protocol architecture fundamentally transforms the traditional authentication paradigm by eliminating shared secrets and leveraging public key cryptography to establish strong device identity. This architecture operates on a challenge-response model where authenticators (which would be the FC devices in our adaptation) generate and securely store prate keys while sharing only public keys with the relying party (the SAN management infrastructure). What makes this approach particularly valuable is that authentication credentials never leave the authenticator device, dramatically reducing the attack surface available to malicious actors. The FIDO Alliance emphasizes that this architecture provides phishing resistance by design, as there are simply no shared secrets to be compromised through deceptive techniques [3].

The FIDO Alliance has developed multiple technical specifications, including FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF), and FIDO2, which includes the W3C Web Authentication (WebAuthn) specification. These specifications collectively establish a comprehensive framework that can be adapted to specialized enterprise environments, including storage infrastructure. The latest FIDO specifications have been designed with interoperability as a core principle, enabling integration with existing enterprise security architectures while providing the flexibility to accommodate domain-specific requirements such as those presented by Fibre Channel fabrics and SAN infrastructure [3].

2.2. Security Implications for SAN Infrastructure

Adapting FIDO for Fibre Channel environments addresses critical security vulnerabilities inherent to traditional device onboarding approaches. Research on enterprise network security indicates that configuration management during device provisioning represents one of the most significant attack vectors in infrastructure environments, with inadequate authentication mechanisms creating exploitable security gaps during the initial deployment phase [4]. Traditional SAN infrastructure often relies on default credentials and shared management passwords during commissioning, creating substantial exposure windows that can persist long after initial deployment.

The strong authentication principles of FIDO provide a robust solution to these challenges by establishing cryptographically verifiable device identity from the moment of initial network connection. Security analysis of enterprise networks emphasizes that authentication mechanism strength represents a critical control point for infrastructure protection, with hardware-backed credentials providing orders of magnitude greater resistance to compromise compared to traditional password-based approaches [4]. In the context of FC device onboarding, the attestation capabilities inherent to the FIDO protocol enable verifiable proof of device authenticity and integrity, effectively eliminating the risk of rogue device insertion that has historically plagued SAN environments.

2.3. Implementation Framework for FC Environments

Implementing FIDO-based authentication for FC device onboarding requires careful consideration of the unique architectural characteristics of storage networks. Research on enterprise security planning emphasizes the importance of authentication boundary definition, particularly in specialized network segments containing high-value assets such as storage infrastructure [4]. For Fibre Channel environments, this authentication boundary must encompass not only the management plane but also extend security assurances to the fabric configuration to prevent potential data path compromise.

The adaptation process necessitates establishing a root of trust within the storage infrastructure that can validate FIDO attestations from newly connected devices. This typically involves modifications to existing SAN management platforms to support public key verification and challenge issuance. Security planning research indicates that successful implementation of advanced authentication systems requires integration with existing security information and event management (SIEM) infrastructure to enable comprehensive visibility and maintain security posture awareness across all technology domains [4]. For FC environments specifically, this integration must accommodate the unique characteristics of fabric-based networking while providing seamless administrator experiences that reduce rather than increase operational complexity.

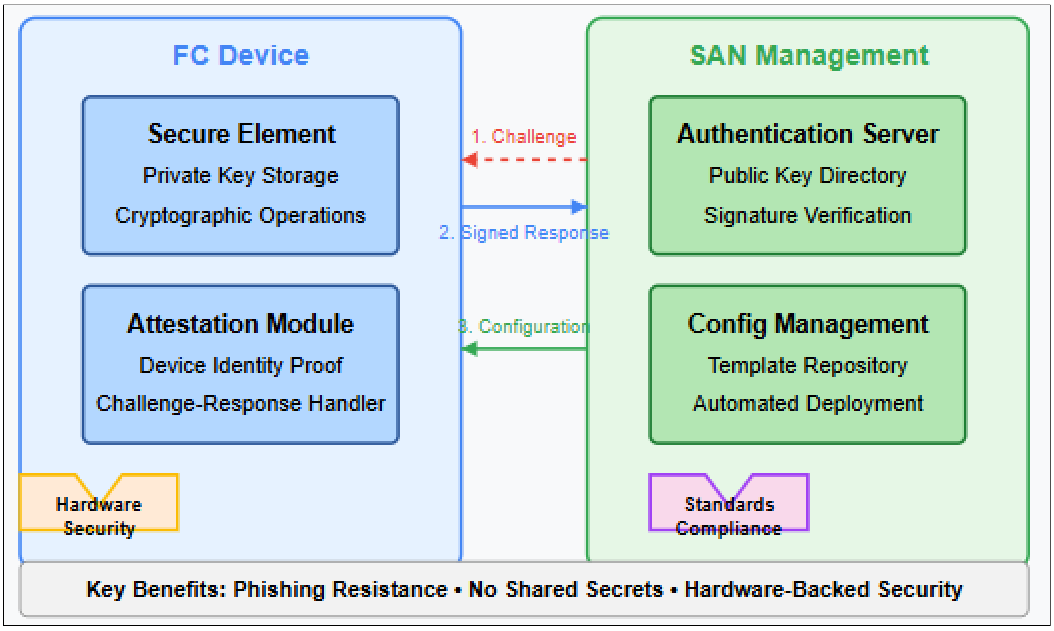

Figure 1 FIDO Protocol Adaptation for FC Environments [3, 4]

3. The Technical Framework for FC Device Auto-Discovery

The implementation of auto-discovery mechanisms for Fibre Channel devices represents a transformative approach to SAN infrastructure management that can dramatically reduce administrative overhead while enhancing security posture. Traditional onboarding methodologies require extensive manual intervention, creating operational inefficiencies that impact both deployment timelines and configuration consistency. By adapting frameworks similar to those used in enterprise security storage, organizations can establish automated discovery processes that significantly streamline device onboarding while maintaining robust security controls.

3.1. Zero-Touch Provisioning Architecture

Zero-touch provisioning for FC devices necessitates a comprehensive architectural framework that encompasses discovery, authentication, and configuration components. Research on ZTP models identifies four essential infrastructure components required for successful implementation: device connectivity, authentication mechanisms, configuration repositories, and orchestration services [6]. Within FC environments specifically, this architecture must accommodate the unique characteristics of fabric-based networking while providing seamless integration with existing management platforms. The orchestration component holds particular significance in fabric environments, as it must coordinate configuration deployment across multiple interdependent devices while maintaining fabric consistency and preventing potential segmentation.

Intel's FIDO Device Onboard (FDO) implementation provides a valuable architectural reference for zero-touch provisioning that can be adapted to FC environments. The Intel FDO architecture establishes a multi-phase device onboarding process that begins with initial attestation and progresses through ownership transfer and configuration deployment without requiring direct administrative interaction [13]. While designed primarily for IoT devices, this architectural approach offers compelling parallels for FC device onboarding, particularly in the establishment of verifiable device identity as the foundation for secure automated provisioning. The FDO Rendezvous Server concept could be particularly valuable when adapted to FC environments, providing a secure intermediary for device discovery and authentication before integration with management infrastructure.

Authentication represents the foundational security mechanism within this architecture, providing assurance regarding device identity and preventing unauthorized network access. As outlined in research on enterprise secured data storage, hardware-based authentication leveraging device-specific cryptographic materials offers substantially greater security assurance compared to software-based approaches, particularly for infrastructure components within high-security environments [5]. This finding aligns perfectly with FIDO implementation for FC devices, where hardware security modules can securely store authentication credentials throughout the device lifecycle while preventing potential extraction or compromise.

3.2. Authentication Flow and Security Mechanisms

The authentication flow within automated FC device discovery adapts established security principles to address the unique requirements of storage infrastructure. Research on enterprise secured data storage emphasizes the importance of maintaining distinct authentication zones with appropriate trust boundaries, particularly when implementing multi-factor authentication for high-value infrastructure components [5]. For FC environments, these authentication zones must encompass both the management plane and data path, with appropriate segmentation to prevent potential lateral movement in the event of compromise.

Intel's FDO implementation demonstrates this principle through its structured ownership transfer protocol, which establishes cryptographically verifiable chain of custody from device manufacturer through to the end-user organization [13]. This approach provides a valuable model for FC device onboarding, where establishing trusted provenance represents a critical security requirement. By adapting the FDO ownership voucher mechanism to FC environments, organizations can validate device authenticity before integration with production infrastructure, significantly reducing the risk of unauthorized device insertion or spoofing attacks.

The implementation of certificate-based authentication provides particularly compelling security benefits for FC device onboarding. As demonstrated in research on authentication mechanisms for enterprise secured data storage, certificate-based approaches dramatically reduce the administrative overhead associated with credential management while simultaneously enhancing security posture through elimination of shared secrets [5]. This approach aligns precisely with FIDO implementation for FC environments, where device-specific certificates can establish cryptographic identity without relying on potentially vulnerable shared credentials or default passwords commonly associated with traditional onboarding methodologies.

3.3. Integration with Multi-Domain Environments

The integration of automated discovery mechanisms with multi-domain SAN environments presents unique challenges that must be addressed through appropriate architectural considerations. Research on zero-touch provisioning models emphasizes that successful implementations must establish clear demarcation boundaries between service providers and resource consumers, with appropriate abstraction layers to accommodate diverse infrastructure components [6]. Within FC environments, these boundaries typically manifest as distinctions between fabric managers, device element managers, and higher-level orchestration platforms, each requiring appropriate integration points to facilitate seamless discovery and configuration workflows.

Intel's FDO implementation provides valuable insights into multi-domain integration through its ownership transfer mechanism, which facilitates secure handoff between manufacturing, distribution, and operational domains [13]. The cryptographic attestation chain maintained throughout this process offers a compelling model for FC environments, where similar ownership boundaries often exist between infrastructure providers, storage administrators, and security governance teams. By implementing comparable attestation mechanisms for FC devices, organizations can maintain appropriate separation of duties while enabling streamlined device onboarding across administrative domains.

Standardization of integration interfaces represents a critical success factor for multi-domain implementations. Research on ZTP infrastructure components identifies the need for standardized APIs and data models to enable interoperability across diverse technology domains [6]. For FC environments specifically, these standardization efforts must accommodate both legacy management protocols and emerging REST-based interfaces to ensure comprehensive coverage across modern and traditional infrastructure components. Through appropriate abstraction and interface standardization, organizations can establish unified discovery frameworks that seamlessly span diverse management domains while maintaining consistent security controls and operational workflows.

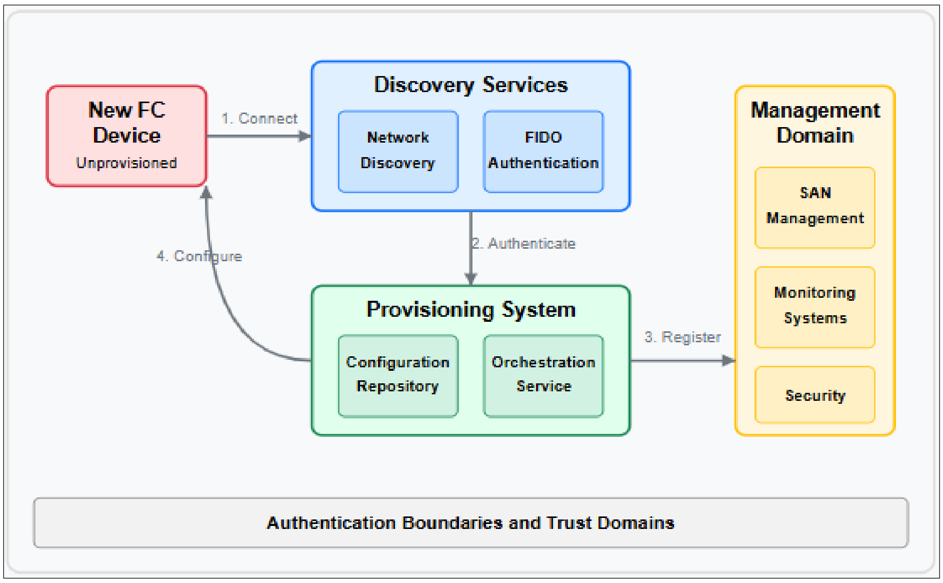

Figure 2 Technical Framework for FC Device Auto-Discovery [5, 6]

4. Automated Configuration Components and Workflow

The deployment of automated configuration mechanisms represents a fundamental requirement for establishing efficient FC device onboarding processes. The traditional approach to device configuration involves multiple manual steps that introduce significant operational overhead and potential for error. Implementing structured automation within this domain requires careful consideration of enterprise network architectural principles and corresponding security frameworks to ensure both efficiency and infrastructure integrity.

4.1. Network Configuration Automation Architecture

Enterprise network configuration automation requires a comprehensive architectural framework that addresses both operational and security requirements. Research on enterprise network configuration identifies three distinct topology-based configuration models: centralized, decentralized, and hierarchical, each presenting unique considerations for automated FC device provisioning [7]. The centralized model establishes a single authoritative configuration repository and deployment mechanism, providing enhanced consistency but potentially introducing single points of failure. Conversely, the hierarchical model establishes a structured delegation approach that accommodates organizational complexity while maintaining appropriate governance controls, making it particularly suitable for large-scale FC environments with distributed administrative responsibilities.

The implementation of automated configuration for FC devices necessitates careful consideration of technological parameters beyond basic connectivity. As outlined in research on enterprise network configuration, the automation architecture must incorporate "intelligent configuration mechanisms" that adapt deployment processes based on device-specific requirements and environmental context [7]. For FC environments specifically, these mechanisms must comprehend fabric topology constraints, inter-switch parameter dependencies, and potential cascading impacts of configuration changes. This capability becomes particularly critical during switch parameter deployment, where inappropriate configuration sequencing can potentially trigger fabric segmentation events that impact production workloads.

4.2. Security Policy Enforcement and Validation

The integration of security controls represents a critical component of automated FC device onboarding. Research on enhanced data security architecture emphasizes the requirement for "multi-layered security measures" that establish comprehensive protection across all infrastructure components, particularly within high-value domains like storage networks [8]. The implementation of these measures within automated workflows requires systematic policy definition and translation capabilities that convert organizational security requirements into device-specific configuration parameters. For FC environments, these parameters encompass both management plane controls and data path security mechanisms, including zoning enforcement, LUN masking, and fabric access controls.

Authentication mechanisms play a central role in establishing appropriate security boundaries during device onboarding. Research on enterprise data security architecture emphasizes that "authentication represents the cornerstone of network security," with robust mechanisms providing the foundation for all subsequent security controls [8]. This principle aligns with FIDO implementation for FC device onboarding, where strong device authentication establishes the trust basis necessary for automated configuration deployment. By validating device identity through cryptographic attestation before deploying configuration, organizations can prevent potential security compromise through rogue device insertion while maintaining appropriate separation of administrative domains.

4.3. Configuration Consistency and State Management

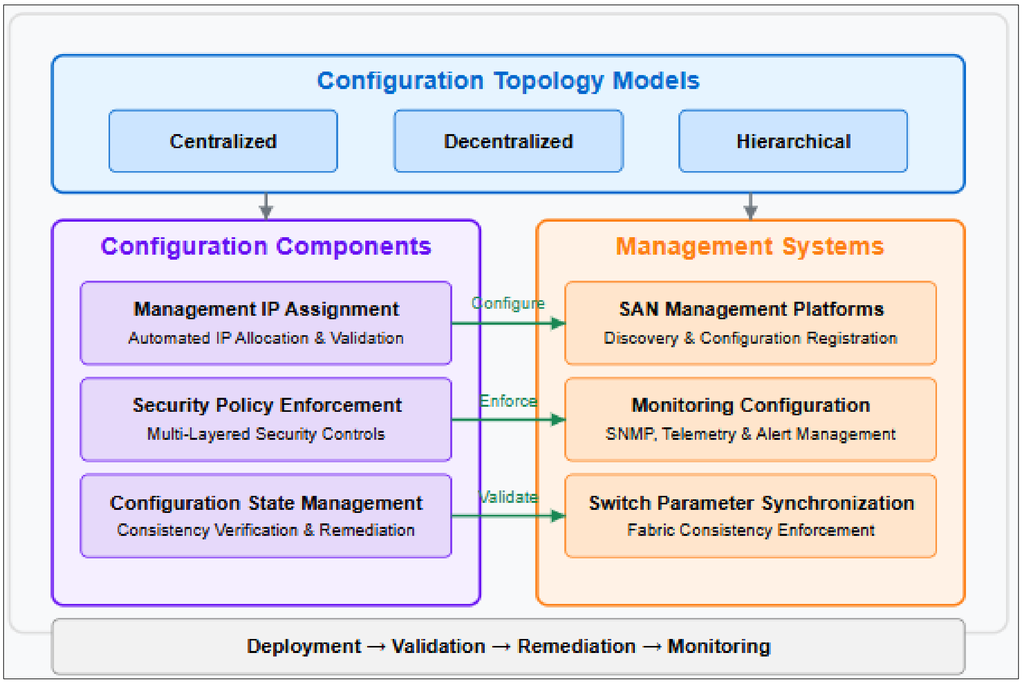
Configuration Topology Models
Centralized
Decentralized
Hierarchical
Configuration Components
Management IP Assignment
Automated IP Allocation & Validation
Security Policy Enforcement
Multi-Layered Security Controls
Configuration State Management
Consistency Verification & Remediation
Configure
Enforce
Validate
Management Systems
SAN Management Platforms
Discovery & Configuration Registration
Monitoring Configuration
SNMP, Telemetry & Alert Management
Switch Parameter Synchronization
Fabric Consistency Enforcement
Deployment → Validation → Remediation → Monitoring

Figure 3 Automated Configuration Components and Workflow [7, 8]

Maintaining configuration consistency across complex FC environments represents a significant challenge that impacts both operational stability and security posture. Research on enterprise network configuration indicates that inconsistent implementation of configuration parameters across infrastructure components represents one of the primary sources of operational incidents within enterprise environments [7]. This challenge becomes particularly pronounced in SAN infrastructure, where fabric integrity depends on precise parameter alignment across multiple interconnected switches. Automated configuration mechanisms address this challenge through systematic parameter deployment and validation, ensuring consistent implementation across all fabric components without relying on error-prone manual processes.

The implementation of state-based configuration management provides particular value for FC environments. As outlined in research on enhanced security architecture, "maintaining awareness of current and desired configuration states" enables systematic validation and remediation to address potential configuration drift [8]. This capability proves especially valuable during device provisioning, where automated comparison between desired configuration templates and actual device configuration can identify potential misalignments before they impact production services. By validating configuration accuracy as part of the automated deployment process, organizations can dramatically reduce post-deployment troubleshooting requirements while ensuring consistent security policy implementation across the infrastructure.

5. Implementation Case Study: Reducing Weeks to Minutes

The implementation of FIDO-based onboarding for FC devices represents a transformative approach to infrastructure management that can dramatically reduce provisioning timelines while enhancing security posture. Documented implementations provide compelling evidence of operational improvements achievable through systematic automation of the onboarding process. By analyzing these implementations through formal enterprise architecture assessment methodologies, organizations can develop realistic expectations and implementation strategies for their environments.

5.1. Enterprise Architecture Assessment Framework

The implementation of automated onboarding solutions requires comprehensive architectural evaluation to ensure alignment with broader enterprise infrastructure objectives. Research on quantitative analysis of enterprise architectures emphasizes the importance of multi-dimensional assessment frameworks that consider both technical and business dimensions when evaluating potential implementations [9]. These frameworks typically incorporate multiple viewpoints including business architecture, application architecture, data architecture, and technology architecture, with appropriate metrics for each dimension. For FC device onboarding specifically, the technology architecture assessment holds particular significance, as it directly impacts operational efficiency and infrastructure agility.

The assessment of potential implementation approaches should leverage formal modeling techniques to predict operational improvements before committing to specific implementations. As outlined in research on enterprise architecture analysis, modeling techniques including "scenario-based, simulation-based, and calculation-based approaches" provide complementary insights into potential operational impacts [9]. For FC device onboarding automation, simulation-based approaches offer particular value by enabling organizations to quantify potential time savings and administrative workload reductions across diverse deployment scenarios. By establishing comprehensive assessment frameworks before implementation, organizations can identify optimal architectural approaches while establishing appropriate success metrics for post-implementation validation.

5.2. Distributed System Implementation Considerations

The implementation of automated onboarding for FC devices typically necessitates a distributed system architecture that can accommodate geographically dispersed infrastructure while maintaining consistent security controls. Research on distributed systems implementation emphasizes that "system reconfiguration plays a critical role in maintaining service availability" across distributed environments, with formal verification mechanisms ensuring appropriate implementation of security policies despite geographic distribution [10]. This consideration holds particular relevance for global organizations implementing automated onboarding across multiple data centers, where consistent policy enforcement must be maintained despite network latency and potential connectivity limitations.

The implementation architecture must incorporate appropriate fault tolerance and recovery mechanisms to ensure operational resilience. As outlined in research on distributed systems, "the ability to reason about consistency under potential failures" represents a critical capability for enterprise implementations, particularly those supporting mission-critical infrastructure [10]. For FC environments specifically, this resilience extends beyond the onboarding system itself to include the configuration state of provisioned devices, ensuring that interruptions during the onboarding process do not result in inconsistent fabric configurations that could potentially impact production services. By implementing appropriate transaction management and state verification within the onboarding workflow, organizations can ensure consistent outcomes even when process interruptions occur.

5.3. Operational Transformation and Governance

The successful implementation of automated onboarding solutions requires careful consideration of operational governance to ensure appropriate oversight despite reduced manual intervention. Research on enterprise architecture emphasizes that operational transformations must establish appropriate "control structures and control flows" that maintain governance requirements while enabling automation benefits [9]. For FC device onboarding specifically, these governance mechanisms typically include structured approval workflows, compliance validation, and comprehensive audit logging to document the provisioning process despite its automated nature.

The implementation of automated onboarding solutions necessitates corresponding evolution of operational practices and administrator skill requirements. As outlined in research on distributed systems, successful implementations require "careful resource planning" that addresses both technical and operational dimensions [10]. For SAN administrators specifically, the transition from manual configuration to automation oversight requires significant skill development in areas including policy definition, template management, and exception handling. Organizations implementing automated onboarding should establish comprehensive training programs that enable administrators to effectively transition from direct configuration responsibilities to automation governance roles, ensuring appropriate utilization of specialized knowledge despite reduced direct intervention requirements.

6. Future Directions and Best Practices

The integration of FIDO protocol for automated FC device onboarding represents a significant advancement in SAN infrastructure management, but continued evolution will further enhance security and operational efficiency. Emerging trends in enterprise automation and cybersecurity frameworks offer valuable insights for organizations implementing or planning FIDO-based solutions for their storage infrastructure.

6.1. AI-Enhanced Configuration Management

The incorporation of artificial intelligence into infrastructure configuration represents a transformative opportunity for FC device onboarding. Research on enterprise automation indicates that AI-based technologies are increasingly being deployed to "identify patterns, anomalies, and optimization opportunities that human operators might miss," particularly in complex infrastructure environments [11]. For FC device onboarding specifically, machine learning algorithms can enhance configuration validation by analyzing historical deployment data to identify potential fabric segmentation risks or security vulnerabilities before they impact production environments. These capabilities become particularly valuable in large-scale deployments where traditional rule-based validation may struggle to identify subtle configuration interdependencies across diverse fabric components.

Intel's FIDO Device Onboard (FDO) implementation demonstrates how standardized onboarding protocols can establish the foundation for future AI-enhanced management by generating consistent, structured device interaction data [13]. The well-defined phases in Intel's FDO protocol—from initial attestation through ownership transfer and configuration—create distinct data collection points that could feed machine learning models for process optimization. By adapting similar structured approaches to FC device onboarding, organizations can establish the data foundation necessary for future AI enhancements while delivering immediate operational benefits through basic automation.

The implementation of AI-enhanced configuration management typically evolves through progressive capability maturation rather than immediate comprehensive deployment. As outlined in research on enterprise automation, organizations typically begin with "supervised learning models trained on historical configuration data" before progressing to more sophisticated approaches including reinforcement learning for optimization and natural language processing for intent-based configuration [11]. In FC environments, this evolutionary approach enables progressive enhancement of automated onboarding capabilities while minimizing operational risk through controlled introduction of advanced functionality. By establishing appropriate data collection mechanisms during initial implementation, organizations can build the foundation for future AI enhancement while delivering immediate operational benefits through basic automation.

6.2. Framework-Based Security Implementation

The integration of comprehensive security frameworks represents a critical best practice for organizations implementing FIDO-based FC device onboarding. Research on cybersecurity frameworks emphasizes that effective security implementations require structured approaches that address "identifying, protecting, detecting, responding, and recovering" across all infrastructure components [12]. For FC device onboarding specifically, this framework-based approach ensures that security considerations extend beyond basic authentication to encompass the complete device lifecycle from initial provisioning through operational management and eventual decommissioning.

Intel's FDO implementation provides a valuable reference model for framework-based security through its comprehensive approach to device lifecycle management. The FDO protocol explicitly addresses multiple security dimensions including supply chain validation, secure bootstrapping, and operational attestation [13]. This comprehensive approach aligns well with established cybersecurity frameworks, demonstrating how automated onboarding can enhance rather than compromise security posture. By adapting similar lifecycle-focused security principles to FC device onboarding, organizations can establish robust governance mechanisms that maintain appropriate oversight despite reduced manual intervention.

The implementation of framework-based security requires careful consideration of both technical and governance dimensions. As outlined in cybersecurity framework research, organizations must establish appropriate "categories and subcategories that address specific outcomes" associated with each security function [12]. For FC environments, these categories should encompass critical aspects including firmware validation, configuration baseline enforcement, continuous monitoring, and incident response capabilities. By aligning FIDO implementation with comprehensive security frameworks, organizations can ensure that automated onboarding enhances rather than compromises their overall security posture while establishing appropriate measurement mechanisms to validate ongoing effectiveness.

6.3. Standardized Implementation Methodologies

The adoption of standardized implementation methodologies represents a critical success factor for organizations deploying FIDO-based FC device onboarding. Research on enterprise automation emphasizes that successful transformations require "comprehensive change management that addresses both technological and organizational dimensions" rather than focusing exclusively on technical implementation [11]. This holistic approach encompasses capability development, process redesign, and cultural adaptation to ensure sustainable operational improvements beyond initial deployment.

Table 1 Cybersecurity Framework Implementation Guide [11, 12]

Framework Function	FC Onboarding Application	Implementation Requirement	Success Indicator
Identify	Asset inventory and fabric topology mapping	Automated discovery with cryptographic device identity	Comprehensive visibility of all fabric components
Protect	Authentication and configuration baseline enforcement	FIDO attestation and template-based configuration	Elimination of default credentials and consistent security parameters
Detect	Continuous monitoring of device configuration state	Configuration drift detection	Real-time alerts for unauthorized changes
Respond	Automated remediation of configuration anomalies	Self-healing configuration capabilities	Minimal time between detection and correction

Intel's FDO implementation provides valuable insights into standardized methodologies through its phased implementation approach and comprehensive documentation. The detailed process workflows, reference architectures, and implementation guides available for Intel FDO demonstrate the importance of structured knowledge transfer in successful deployments [13]. By establishing similar implementation resources for FC environments, organizations can accelerate adoption while ensuring consistent outcomes across deployment teams. These standardized methodologies should address not only technical configuration but also operational processes, governance mechanisms, and skills development to ensure comprehensive organizational readiness.

Effective implementation methodologies incorporate structured governance mechanisms that maintain appropriate oversight despite reduced manual intervention. As outlined in cybersecurity framework research, organizations should establish processes that "enable cybersecurity activities to be managed as a risk management portfolio" rather than as isolated technical implementations [12]. For FIDO-based FC onboarding specifically, these governance mechanisms typically include structured approval workflows, compliance validation, and comprehensive audit logging that documents the automated provisioning process while maintaining appropriate separation of duties. By implementing robust governance alongside technical automation, organizations can achieve dramatic operational efficiency improvements while enhancing rather than compromising their overall control environment.

7. Conclusion

Adapting the FIDO protocol for Fibre Channel device onboarding represents a transformative approach to SAN infrastructure management that addresses longstanding operational inefficiencies. By implementing this zero-touch provisioning methodology, organizations can dramatically streamline the deployment process while simultaneously enhancing security posture and configuration consistency. The framework presented demonstrates that automation need not compromise enterprise security requirements or operational standards when properly architected. As data centers continue to scale and evolve, this FIDO-based approach provides a foundation for broader infrastructure automation initiatives that can extend beyond storage networks. Organizations adopting these methodologies will position themselves advantageously for managing increasingly complex hybrid environments where rapid, secure provisioning becomes a competitive necessity rather than merely an operational convenience.

References

[1] Viranart Chandarasanti, "Enterprise Storage Systems Market Insights," International Data Corporation, 28 March 2025. [Online]. Available: https://www.idc.com/promo/enterprise-storage-systems/

[2] Tanuj Tayeng et al., "Assessing the impact of infrastructure financing on economic growth in emerging markets," Journal of Infrastructure, Vol. 8, no. 15, 2024. [Online]. Available: https://systems.enpress-publisher.com/index.php/jipd/article/viewFile/9560/5013

[3] FIDO Alliance, "Alliance Overview," FIDO Alliance, 2025. [Online]. Available: https://fidoalliance.org/overview/

[4] Osama Hosameldeen et al., "Security Analysis and Planning for Enterprise Networks," ResearchGate, July 2024. [Online]. Available: https://www.researchgate.net/publication/382284571_Security_Analysis_and_Planning_for_Enterprise_Networks

[5] Nathanaël Cottin et al., "Authentication and enterprise secured data storage," ResearchGate, Feb. 2001. [Online]. Available: https://www.researchgate.net/publication/3944078_Authentication_and_enterprise_secured_data_storage

[6] Yuri Demchenko et al., "Zero-Touch Provisioning (ZTP) Model and Infrastructure Components for Multi-provider Cloud Services Provisioning," ResearchGate, Nov. 2016. [Online]. Available: https://www.researchgate.net/publication/309797547_ZeroTouch_Provisioning_ZTP_Model_and_Infrastructure_Components_for_Multi-provider_Cloud_Services_Provisioning

[7] Aleksandr M. Batkovskiy et al., "Configuration of enterprise networks," ResearchGate, Oct. 2018. [Online]. Available: https://www.researchgate.net/publication/328066378_Configuration_of_enterprise_networks

[8] Rashmi Shree V et al., "Enhanced Data Security Architecture in Enterprise Networks," ResearchGate, Jan. 2020. [Online]. Available: https://www.researchgate.net/publication/334845148_Enhanced_Data_Security_Architecture_in_Enterprise_Networks

[9] Maria-Eugenia Iacob and Henk Jonkers, "Quantitative Analysis of Enterprise Architectures," ResearchGate, July 2006. [Online]. Available: https://www.researchgate.net/publication/226236887_Quantitative_Analysis_of_Enterprise_Architectures

[10] Abhishek Hazra et al., "Distributed AI in Zero-touch Provisioning for Edge Networks: Challenges and Research Directions," arXiv:2311.17471v1, 29 Nov. 2023. [Online]. Available: https://dsg.tuwien.ac.at/~sd/papers/Bericht_2023_A_Morichetta_Distributed.pdf

[11] Sravanthi Gopala, "The Future of Enterprise Automation: AI as a Transformative Force," ResearchGate, Feb. 2025. [Online]. Available: https://www.researchgate.net/publication/389609236_The_Future_of_Enterprise_Automation_AI_as_a_Transformative_Force

[12] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology, 16 April 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[13] Intel, "Intel FIDO Device Onboard (Intel FDO) Documentation," Intel Corporation, 15 May 2023. [Online]. Available: https://www.intel.com/content/www/us/en/content-details/763447/intel-fido-device-onboard-intel-fdo-documentation.html