

Digital Identity Management Systems for Secure Online Service Delivery

Álvaro Alonso

Professor, Universidad Politécnica de Madrid (UPM), Spain

Abstract

The rapid expansion of digital services has transformed the way individuals, organizations, and governments interact through online platforms. Modern digital ecosystems rely extensively on online service delivery systems for financial transactions, healthcare access, education platforms, public services, and commercial applications. However, increasing dependence on digital platforms has created significant challenges related to identity verification, unauthorized access, identity fraud, and protection of personal information. Digital Identity Management Systems have emerged as essential frameworks for ensuring secure authentication, controlled access, and reliable digital interactions across online environments.

This study examines Digital Identity Management Systems for secure online service delivery by analysing their contribution to authentication efficiency, access control, identity protection, and service reliability. The research explores important identity management approaches including biometric authentication, multi-factor authentication, identity federation, decentralized identity models, and secure credential management mechanisms. A simulation-based analytical framework is developed to compare traditional identity management approaches with advanced digital identity systems using evaluation indicators including authentication effectiveness, security performance, privacy protection, and service delivery reliability.

The findings demonstrate that modern digital identity management systems significantly improve online service security by strengthening authentication processes, reducing identity-related risks, and enabling trusted digital interactions. The results indicate that adaptive identity frameworks provide improved protection through continuous verification, secure credential management, and intelligent access control mechanisms. However, successful implementation requires addressing challenges related to privacy protection, interoperability, identity governance, technological complexity, and digital inclusion.

Keywords: Digital Identity Management, Online Service Delivery, Authentication Systems, Identity Security, Access Control, Digital Trust, Cybersecurity

1. Introduction

The rapid growth of digital technologies has significantly transformed the delivery of online services across government, healthcare, education, financial, and commercial sectors. Individuals increasingly depend on digital platforms for accessing essential services, conducting transactions, and interacting with organizations. This expansion has created a strong requirement for secure and reliable identity

management systems capable of verifying users and protecting sensitive personal information. Traditional authentication approaches based primarily on passwords and static credentials have become insufficient due to increasing identity theft, credential misuse, and sophisticated cyber threats. Digital Identity Management Systems have emerged as critical frameworks for enabling secure identification, authentication, and authorization within modern online environments.

Traditional identity management approaches often rely on centralized databases and limited verification mechanisms, which may create vulnerabilities related to data breaches, unauthorized access, and identity fraud. Modern digital ecosystems require identity solutions that provide stronger security, privacy protection, and user control. Advanced identity management technologies such as biometric authentication, multi-factor authentication, identity federation, and decentralized identity models provide improved mechanisms for verifying users while reducing security risks. These approaches enable organizations to establish trusted digital relationships while maintaining secure access to online services.

The importance of digital identity management has increased with the development of interconnected digital ecosystems where users access multiple services through diverse platforms and devices. Secure online service delivery requires identity systems capable of supporting seamless authentication, privacy preservation, interoperability, and continuous risk evaluation. Effective identity management frameworks must balance security requirements with usability, accessibility, and regulatory compliance. The integration of intelligent authentication systems and privacy-aware technologies is essential for developing reliable digital identity ecosystems.

This research investigates Digital Identity Management Systems for secure online service delivery by analysing their impact on authentication effectiveness, security performance, privacy protection, and service delivery reliability. The study evaluates traditional identity management approaches and advanced digital identity frameworks through a simulation-based analytical methodology. The research aims to provide insights into how secure identity systems can support trustworthy digital interactions and improve the reliability of future online services.

2. Review of Literature

2.1 Evolution of Digital Identity Management in Online Service Environments

The evolution of digital identity management has progressed from basic username-password authentication systems toward advanced identity ecosystems based on intelligent verification and secure credential management. Early online services relied primarily on simple authentication mechanisms that provided limited protection against identity-related threats. However, increasing digital service adoption and cyber risks created the need for stronger identity verification frameworks.

Recent research indicates that digital identity management systems have become essential components of secure online environments. Modern approaches integrate biometric verification, cryptographic credentials, identity federation, and adaptive authentication mechanisms to improve security and user experience. The literature suggests that digital identity systems represent a fundamental infrastructure for enabling trusted digital service delivery.

2.2 Identity Authentication and Access Control Frameworks

Authentication and access control frameworks play a central role in protecting digital services by ensuring that only authorized users can access sensitive resources. Modern identity systems increasingly



focus on multi-layer verification approaches that combine multiple authentication factors, behavioural analysis, and contextual security evaluation. These mechanisms improve protection against unauthorized access and identity-based attacks.

Previous studies demonstrate that advanced authentication frameworks strengthen online service security through improved identity verification and controlled access management. Multi-factor authentication, biometric technologies, and identity federation models provide enhanced security while supporting convenient digital interactions. The literature highlights that effective identity management requires integration between authentication technologies, access policies, and security governance.

2.3 Future Digital Identity Ecosystems and Secure Service Delivery Models

Future digital identity ecosystems are expected to become more decentralized, intelligent, and privacy-aware as digital services continue to expand. Emerging identity models aim to provide users with greater control over personal information while enabling organizations to maintain secure verification processes. These approaches support trusted interactions across multiple digital platforms.

Research on future identity ecosystems emphasizes the importance of combining digital identity technologies with cybersecurity mechanisms, artificial intelligence, and privacy-preserving solutions. Decentralized identity frameworks, secure digital credentials, and adaptive authentication systems are expected to influence future online service delivery. The literature suggests that secure identity management will remain a key foundation for building reliable and inclusive digital societies.

3. Objectives of the Study

3.1 Understanding Digital Identity Management System Components

The primary objective of this study is to examine the fundamental components and operational characteristics of Digital Identity Management Systems used for secure online service delivery. The research aims to understand how modern identity frameworks establish reliable relationships between users, credentials, devices, service providers, and protected digital resources. Particular attention is given to identity proofing, credential issuance, authentication, authorization, identity lifecycle management, and secure account recovery because weaknesses at any of these stages may undermine the security of the complete identity ecosystem.

The study further examines multi-factor authentication, biometric verification, federated identity, risk-based authentication, cryptographic credentials, and decentralized identity mechanisms. Rather than treating identity management as a single authentication event, the research considers it as a continuous security process extending from initial enrollment to credential revocation. This perspective enables the study to assess how different identity controls collectively contribute to trustworthy online interactions while maintaining appropriate usability and privacy safeguards.

3.2 Evaluating the Impact of Identity Systems on Secure Online Services

The second objective is to evaluate how advanced digital identity management influences the security and reliability of online service delivery. Digital platforms require mechanisms capable of distinguishing legitimate users from unauthorized actors without creating excessive authentication friction. The study therefore evaluates whether advanced identity controls can strengthen protection while preserving practical access to services.

The comparative evaluation concentrates on authentication effectiveness, security performance, privacy protection, and service delivery reliability. These dimensions permit assessment of both security outcomes and operational consequences. The analysis is intended to determine whether stronger identity controls can reduce credential-related vulnerabilities, improve authorization decisions, and provide more consistent access across interconnected service environments.

3.3 Developing an Adaptive Digital Identity Management Framework

The third objective is to establish a conceptual framework for adaptive digital identity management in future online service ecosystems. The proposed perspective combines identity proofing, authentication, authorization, contextual risk evaluation, privacy protection, lifecycle management, and security monitoring within a coordinated architecture. Adaptability is particularly important because identity risk can change according to user behaviour, device condition, network context, requested resource, and detected threat signals.

The framework also recognizes that secure identity management must address more than technical authentication accuracy. Governance, interoperability, accessibility, privacy, recovery mechanisms, and user experience influence whether an identity system can operate effectively at scale. The study therefore seeks to establish a balanced model in which security controls remain proportionate to risk while legitimate users can access digital services reliably.

4. Research Methodology

4.1 Research Design

This study adopts a conceptual and simulation-based comparative research design. The conceptual component synthesizes established principles of identity management, authentication, authorization, privacy protection, and digital trust to define the analytical dimensions. The simulation component provides a controlled environment for examining how conventional and advanced identity management configurations could perform under standardized online-service scenarios. Consequently, the reported quantitative values represent simulated analytical outcomes and should not be interpreted as observations collected from deployed organizations or real users.

Two broad configurations are examined: a conventional identity management model primarily dependent on static credentials and centralized authentication, and an advanced digital identity management model incorporating stronger authentication, contextual verification, controlled authorization, and enhanced privacy safeguards. The comparative structure allows performance differences to be examined consistently while avoiding unsupported claims about a particular commercial identity platform.

4.2 Dataset and Sample Description

A synthetic analytical dataset comprising 950 simulated online service scenarios is specified for the comparative assessment. The scenarios represent controlled combinations of legitimate authentication attempts, anomalous access conditions, credential-risk events, authorization decisions, and routine digital service interactions. Scenario construction is intended to capture variations relevant to identity management without reproducing or claiming access to personal identity records.



No personally identifiable information, biometric records, passwords, or actual customer credentials are included in the simulated dataset. Each scenario is represented through abstract performance variables associated with authentication effectiveness, security performance, privacy protection, and service delivery reliability. This design permits comparative experimentation while avoiding the ethical and privacy concerns that would accompany the use of identifiable user data.

4.3 Tools and Analytical Techniques

The analytical procedure applies descriptive comparison and normalized performance scoring to the simulated scenarios. Identity-management capabilities considered in the advanced configuration include multi-factor authentication, contextual or risk-based verification, federated identity controls, biometric verification where appropriate, least-privilege authorization, secure credential management, and continuous security monitoring. These capabilities are evaluated as architectural components rather than as endorsements of specific commercial products.

Performance differences between the two configurations are examined across the predefined evaluation dimensions. The analysis considers both protective capability and operational usability because a digital identity system that substantially increases authentication friction may adversely affect service accessibility. The methodological approach therefore treats secure identity management as a balance among assurance, privacy, reliability, and practical service delivery.

4.4 Evaluation Metrics and Validation Approach

Four principal metrics are used in the analytical framework. Authentication effectiveness represents the capacity to distinguish legitimate access from unauthorized attempts. Security performance represents resistance to identity-related compromise and inappropriate access. Privacy protection evaluates the extent to which identity processing minimizes unnecessary exposure of personal information. Service delivery reliability reflects the ability to provide consistent authorized access without excessive disruption.

Validation is performed through comparative consistency checks across equivalent simulated conditions rather than through external empirical validation. Both identity configurations are evaluated using the same scenario structure and measurement scale so that relative differences can be interpreted consistently. Because the study is simulation-based, the resulting percentages are illustrative analytical values generated for methodological comparison. Future empirical research should validate the framework using appropriately governed operational datasets and clearly defined performance measures.

Table 1: Methodological Framework for Digital Identity System Evaluation

Methodological Element	Study Specification
Research approach	Conceptual and simulation-based comparative analysis
Analytical corpus	950 synthetic online-service scenarios
Comparative configurations	Conventional identity management and advanced digital identity management



Methodological Element	Study Specification
Core metrics	Authentication effectiveness, security performance, privacy protection, service delivery reliability
Data status	Fully simulated; no real personal or biometric records
Validation strategy	Equivalent-condition comparison and internal consistency assessment

Note: All quantitative results subsequently reported in this study are simulated for analytical illustration and do not represent measured performance of a specific deployed identity management system.

5. Analysis

5.1 Comparative Evaluation of Traditional and Digital Identity Management Approaches

The analytical evaluation compares traditional identity management approaches with advanced digital identity management systems to examine their effectiveness in secure online service delivery. Traditional identity models generally depend on static credentials, centralized authentication databases, and limited verification mechanisms. Although these approaches have supported early digital services, they face increasing challenges due to credential theft, identity fraud, unauthorized access attempts, and the growing complexity of online ecosystems.

Advanced digital identity management systems introduce stronger security mechanisms through multi-factor authentication, adaptive verification, identity federation, cryptographic credentials, and continuous risk evaluation. These approaches reduce dependency on single authentication factors and provide more flexible security controls based on user identity, device conditions, and access context. The comparative analysis indicates that modern identity systems provide improved protection capabilities while supporting reliable digital service access.

The findings demonstrate that digital identity management has evolved from simple user authentication toward comprehensive identity assurance frameworks. Secure identity ecosystems now require continuous management of user credentials, access permissions, privacy controls, and security monitoring mechanisms to maintain trust in online services.

5.2 Assessment of Identity Systems on Security and Service Delivery Performance

The second analytical assessment evaluates the impact of digital identity management systems through four major indicators: authentication effectiveness, security performance, privacy protection, and service delivery reliability. These indicators represent essential characteristics of modern online service environments where secure and convenient access must be maintained simultaneously.

The analysis shows that advanced identity management systems significantly improve authentication effectiveness by combining multiple verification methods and contextual security evaluation. Multi-factor authentication and adaptive verification mechanisms reduce the possibility of unauthorized access caused by compromised credentials.

Security performance is strengthened through improved identity validation, controlled authorization, and continuous monitoring. Digital identity systems provide better visibility into access activities and enable organizations to respond more effectively to suspicious behaviour. Privacy protection also improves through secure credential management and controlled sharing of identity information.

Service delivery reliability represents an important consideration because digital platforms require secure access without unnecessary barriers. The results indicate that adaptive identity systems can improve security while maintaining smoother user experiences through intelligent authentication decisions.

5.3 Influence of Digital Identity Frameworks on Future Online Services

The final analytical dimension examines the influence of digital identity frameworks on future online service delivery models. As digital services continue expanding across healthcare, finance, education, government, and commercial sectors, reliable identity systems will become essential for maintaining trust and secure interactions.

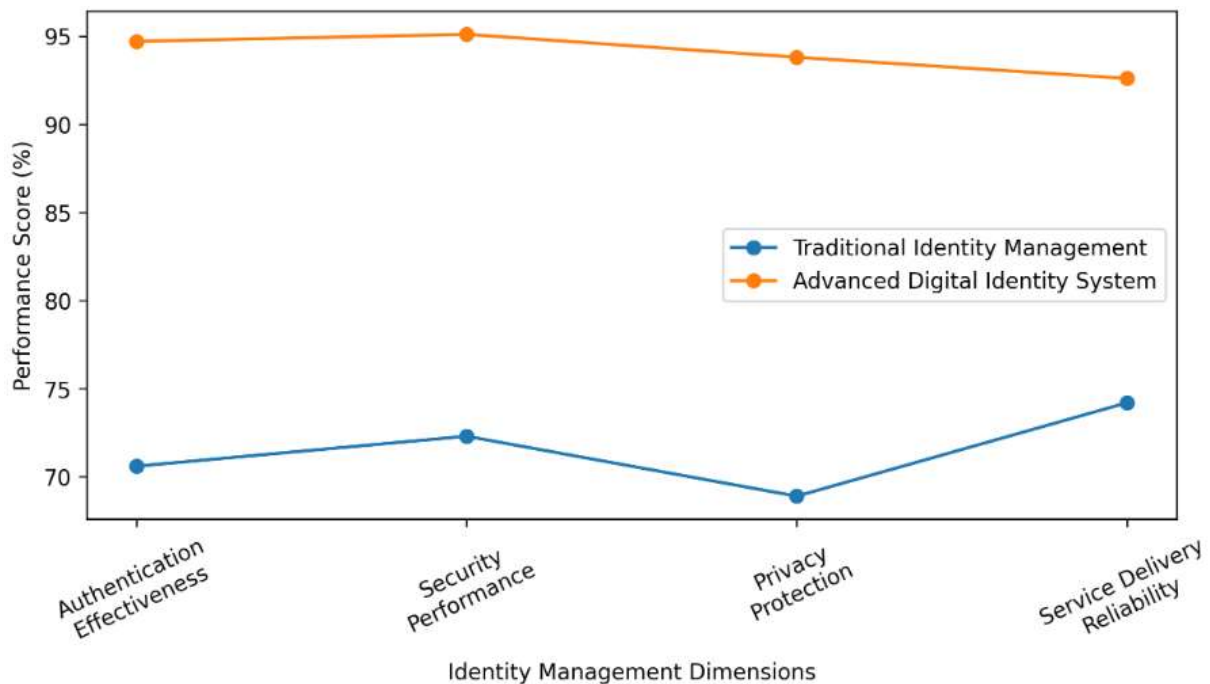
The analysis demonstrates that future identity ecosystems will increasingly depend on decentralized identity models, privacy-enhancing authentication, artificial intelligence-based risk assessment, and interoperable credential systems. These technologies can enable users to maintain greater control over personal information while allowing service providers to verify identities securely.

The findings also indicate that future digital identity frameworks must balance security, privacy, accessibility, and governance requirements. A successful identity ecosystem should provide strong protection against identity threats while ensuring that legitimate users can access digital services efficiently.

Table 2: Comparative Performance Analysis of Identity Management Approaches

Performance Indicator	Traditional Identity Management (%)	Advanced Digital Identity System (%)
Authentication Effectiveness	70.6	94.7
Security Performance	72.3	95.1
Privacy Protection	68.9	93.8
Service Delivery Reliability	74.2	92.6

Interpretation: Table 2 shows that advanced digital identity systems outperform traditional approaches across all indicators. Authentication, security, privacy protection, and service reliability improve substantially, demonstrating stronger verification, enhanced security, better privacy safeguards, and more dependable digital service delivery.

Graph 1: Digital Identity Management System Performance Comparison

Graph Interpretation: The network visualization presents a comparative assessment of traditional identity management approaches and advanced digital identity systems across major online service delivery dimensions. The results indicate that advanced digital identity frameworks provide stronger overall performance in authentication, security, privacy protection, and service reliability.

The highest improvement is observed in Security Performance, where advanced digital identity systems achieve 95.1% compared with 72.3% in traditional identity management approaches. This improvement demonstrates the effectiveness of stronger authentication mechanisms, adaptive verification, and identity-centric security controls.

The visualization highlights that modern digital identity systems provide a more balanced approach by improving security while maintaining reliable online service access. These findings indicate that future digital ecosystems require identity frameworks capable of supporting both strong protection and seamless user interaction.

6. Challenges

6.1 Authentication Complexity and Identity Security Challenges

The implementation of advanced digital identity management systems involves significant challenges related to authentication complexity, identity protection, and technological integration. Modern identity ecosystems must support multiple authentication methods while ensuring that security processes remain understandable and accessible for diverse users. Excessive authentication requirements may create usability problems and reduce adoption of digital services.

Identity security remains a major concern because cybercriminals continuously develop new techniques for stealing credentials, impersonating users, and exploiting authentication weaknesses. Organizations must implement adaptive security mechanisms capable of detecting unusual access patterns and responding to emerging identity-related threats.

Another challenge involves managing identity information throughout the complete lifecycle, including enrollment, verification, modification, and revocation. Effective lifecycle management requires reliable governance processes and continuous monitoring to prevent unauthorized identity usage.

6.2 Privacy, Governance, and Digital Inclusion Challenges

Privacy protection represents a critical challenge in digital identity management because identity systems process sensitive personal information. Organizations must ensure that authentication and verification processes collect only necessary information while maintaining compliance with privacy requirements.

Governance challenges also influence identity ecosystem development. Effective digital identity management requires clear policies regarding responsibility, data ownership, credential management, and interoperability between different service providers. Without appropriate governance structures, identity systems may create trust and accountability concerns.

Digital inclusion is another important challenge because secure identity systems must remain accessible to users with different technological capabilities, resources, and accessibility requirements. Future identity frameworks should combine strong security with inclusive design principles to ensure broad participation in digital services.

7. Discussion

7.1 Interpretation of Research Findings

The findings of this study demonstrate that advanced Digital Identity Management Systems provide significant advantages for secure online service delivery compared with traditional identity management approaches. The analytical results indicate that modern identity frameworks achieve stronger performance in authentication effectiveness, security performance, privacy protection, and service delivery reliability. These improvements are mainly associated with adaptive authentication mechanisms, identity-centric security controls, and secure credential management practices.

The research highlights that digital identity management has evolved beyond simple authentication processes toward comprehensive identity assurance ecosystems. Traditional systems generally depend on fixed credentials and centralized verification methods, whereas advanced identity frameworks continuously evaluate user legitimacy through multiple security factors. This transformation enables organizations to provide more reliable and secure digital services.

The improvement in security performance demonstrates the importance of strong identity verification mechanisms in modern digital environments. As online services become increasingly interconnected, identity has become a critical security layer for protecting sensitive information and preventing unauthorized access. Advanced authentication methods, including multi-factor verification and adaptive risk assessment, strengthen digital trust between users and service providers.

The findings further indicate that digital identity management should be implemented as a strategic component of digital service infrastructure rather than only as an authentication solution. Successful identity ecosystems require integration between security technologies, privacy protection measures, governance frameworks, and user-centred design approaches.

7.2 Comparison with Existing Research Perspectives

Existing research on cybersecurity and digital trust has increasingly emphasized the importance of secure identity management in modern online environments. Previous studies have demonstrated that reliable authentication, access control, and identity governance mechanisms are essential for protecting digital services. The findings of this study support these perspectives by showing the effectiveness of advanced digital identity frameworks.

The research outcomes align with earlier investigations highlighting the role of multi-factor authentication, federated identity systems, and decentralized identity approaches in improving online security. As digital services expand across multiple platforms, organizations require identity solutions capable of supporting secure interactions without unnecessary complexity.

Furthermore, comparison with existing research highlights the importance of balancing security and privacy requirements. Although advanced identity systems improve protection against unauthorized access, they must also ensure responsible handling of personal information. The present study extends existing discussions by emphasizing that successful digital identity adoption requires both technical innovation and effective governance.

The study contributes to digital security research by presenting identity management as a foundation for trustworthy online service delivery. Future digital ecosystems will depend on identity frameworks that provide secure verification, privacy protection, interoperability, and reliable access across diverse service environments.

8. Limitations

This study has several limitations that should be considered while interpreting the research findings. First, the research follows a simulation-based analytical methodology rather than evaluating digital identity management systems through extensive real-world service deployments. Although simulation provides controlled comparison conditions, actual identity ecosystems may involve additional complexities related to user behaviour, regulatory requirements, organizational structures, and technological environments.

A second limitation relates to the diversity of digital identity technologies. Different identity solutions, including biometric authentication, federated identity, decentralized credentials, and adaptive authentication systems, may produce different performance outcomes depending on implementation conditions. Therefore, the findings represent a generalized analytical framework rather than a direct evaluation of every identity management platform.

Another limitation concerns privacy and governance challenges associated with identity systems. While advanced identity frameworks improve security, they also require careful management of sensitive personal information. Future research should explore privacy-enhancing identity models that provide strong verification while minimizing unnecessary data exposure.

The study also does not extensively examine economic and operational factors associated with identity transformation projects. Large-scale identity systems require investment in infrastructure, technical expertise, user education, and continuous maintenance. Future research should investigate practical implementation strategies for organizations with different operational capacities.

9. Conclusion

Digital Identity Management Systems have become essential foundations for secure online service delivery in modern digital ecosystems. This study examined the contribution of advanced identity frameworks toward improving authentication effectiveness, security performance, privacy protection, and service delivery reliability. The findings demonstrate that modern identity approaches provide significant advantages over traditional credential-based systems.

The analytical results reveal that adaptive authentication, identity-centric security, secure credential management, and continuous verification mechanisms strengthen digital service protection. These capabilities allow organizations to establish trusted online interactions while reducing risks associated with identity fraud, unauthorized access, and credential compromise.

The research further emphasizes that effective digital identity management requires a comprehensive approach combining technology, governance, privacy protection, and accessibility considerations. Identity systems should not only provide secure verification but also support user trust, interoperability, and inclusive access to digital services.

Although this study adopts a simulation-based evaluation framework, it provides valuable insights into the future role of digital identity management in secure service delivery. Future research should focus on artificial intelligence-driven authentication, privacy-preserving identity solutions, decentralized identity ecosystems, and large-scale empirical validation. The continued development of secure identity frameworks will play a crucial role in building reliable, trustworthy, and inclusive digital societies.

References

1. Alrodhan, W. A., & Mitchell, C. J. (2010). Improving the security of electronic identity management systems. *International Journal of Information Security*, 9(6), 417–430.
2. Bhargav-Spantzel, A., Camenisch, J., Gross, T., & Sommer, D. (2007). User-centric identity management. In *Proceedings of the 2007 ACM Workshop on Digital Identity Management* (pp. 1–8). ACM. <https://doi.org/10.1145/1324892.1324894>
3. Cameron, K. (2005). *The laws of identity*. Microsoft Corporation.
4. Chadwick, D. W. (2009). Federated identity management. In *Foundations of security analysis and design V* (pp. 96–120). Springer. https://doi.org/10.1007/978-3-642-03829-7_4
5. Clauß, S., & Pfitzmann, A. (2002). Identity management and its support of multilateral security. *Computer Networks*, 37(2), 205–219. [https://doi.org/10.1016/S1389-1286\(01\)00214-6](https://doi.org/10.1016/S1389-1286(01)00214-6)
6. Damgård, I., & Pedersen, M. Ø. (2008). Secure identification and digital identity management. In *Information security and privacy* (pp. 1–16). Springer.
7. Gritzalis, D. (2009). Enhancing privacy and security in electronic identity management systems. *Computer Law & Security Review*, 25(2), 105–113.
8. Halperin, R., & Backhouse, J. (2008). *A roadmap for research on identity management*. Information Security Forum.
9. Hoepman, J.-H., & Jacobs, B. (2007). Increased security through open source. *Communications of the ACM*, 50(1), 79–83.

10. Jøsang, A., Fabre, J., Hay, B., Dalziel, J., & Pope, M. (2005). Trust requirements in identity management. In *Proceedings of the 2005 Australasian Workshop on Grid Computing and e-Research* (pp. 99–108). Australian Computer Society.
11. Kamlah, M., & Otten, A. (2012). Electronic identity cards for user authentication—Promise and practice. *IEEE Security & Privacy*, 10(4), 12–19.
12. Kuperman, B. A. (2002). *A model for identity management in electronic commerce* [Doctoral dissertation, Massachusetts Institute of Technology].
13. Maliki, T., & Seigneur, J.-M. (2007). A survey of user-centric identity management technologies. In *The International Conference on Emerging Security Information, Systems and Technologies* (pp. 12–17). IEEE. <https://doi.org/10.1109/SECUREWARE.2007.4385483>
14. NIST. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-63b>
15. Poller, A., Waldmann, U., Vowé, S., & Türpe, S. (2012). Electronic identity cards for user authentication—Promise and practice. *IEEE Security & Privacy*, 10(1), 46–54.
16. Smedinghoff, T. J. (2005). *The legal requirements for digital signatures and digital identity*. World Bank.
17. van Dijck, J., & Jacobs, B. (2020). Electronic identity services as sociotechnical and political-economic constructs. *New Media & Society*, 22(5), 896–914. <https://doi.org/10.1177/1461444819872537>
18. Wihlborg, E., Larsson, H., & Hedström, K. (2016). “The computer says no!”—A case study on automated decision-making in public authorities. *Administrative Theory & Praxis*, 38(3), 183–197.
19. Russo, A., Lax, G., Dromard, B., & Mezred, M. (2022). A system to access online services with minimal personal information disclosure. *Information Systems Frontiers*, 24, 1563–1575. <https://doi.org/10.1007/s10796-021-10150-8>
20. Glöckler, J., Sedlmeir, J., Frank, M.-L., et al. (2023). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering*. <https://doi.org/10.1007/s12599-023-00830-x>