COLORADO
Governor’s Office of
Information Technology
Serving People. Serving Colorado.

Comments to the National Institute of Standards and Technology

The Second Draft of the Fourth Revision to the Four-Volume Suite of Special Publication 800-63, *Digital Identity Guidelines*

To: National Institute of Standards and Technology, Digital Identity Guidelines, 100 Bureau Drive, Gaithersburg, MD 20899
Submitted electronically to: dig-comments@nist.gov
Submitted by: Colorado Governor’s Office of Information Technology
Date: October 7, 2024
Re: NIST SP 800-63-4

Dear Digital Identity Guidelines Authors,

The Colorado Governor’s Office of Information Technology thanks you for the opportunity to provide public comment on the fourth revision of NIST’s Special Publication 800-63, *Digital Identity Guidelines*.

We appreciate the effort invested to deliver practical, user-friendly guidance. This provides a resource for us to develop and implement robust digital identity solutions. We find multiple areas especially valuable and usable.

The guidance is clear, concrete, and actionable, providing a much-needed roadmap for both strategy and implementation in a space that has been fraught with fear and uncertainty. We commend the user-centric and vendor-agnostic approach.

The inclusion of the risk management framework is incredibly helpful, offering a valuable tool for assessment and decision-making. Strong security controls are crucial for protecting sensitive citizen data and maintaining public trust in government services.

The standardization of assurance levels and proofing taxonomy is a significant contribution, and we anticipate incorporating these directly into our policy. The inclusion of remote identity proofing options is a welcome addition, as it expands access to digital services for citizens in remote areas and those with limited mobility.

We appreciate the acknowledgment of the evolving digital landscape and the flexibility for adopting new authentication technologies and methods, such as passwordless authentication and federated identity management. This allows us to explore innovative solutions that improve security and user experience.

In that vein, we appreciate the emphasis on continuous evaluation, monitoring, and adaptation. This allows us to measure effectiveness, identify areas for improvement, and ensure long-term security and resilience.

We applaud the focus on usability, accessibility and inclusivity, aligning with our goal of providing user-friendly, inclusive and accessible government services for all Coloradans, regardless of technical skills or disabilities.

Introducing user-controlled wallets into the federation model raises concerns about key management, vulnerability to attacks, privacy concerns and potential for misuse. We welcome clear guidelines and standards, including requirements for key management, vulnerability testing and data protection to mitigate these risks before widespread adoption within state agencies.

We'd welcome additional discussion or recommendations regarding building interoperable approaches to digital identity across and between jurisdictions. Overall, we believe that the fourth revision of NIST's Special Publication 800-63 provides a strong foundation for modernizing and securing digital identity systems. The comprehensive and detailed framework for digital identity management has demystified a complex, rapidly evolving, and high-risk area. It equips us with a clear path to enhance service delivery in support of our mission to provide secure digital services that put Coloradans first.

Important Aspects

Stronger Security Controls: The updated guidelines emphasize stronger security controls and risk-based approaches, which are crucial for protecting sensitive citizen data and maintaining public trust in government services.

Privacy Enhancements: The focus on privacy-enhancing technologies and data minimization principles aligns with our commitment to safeguarding citizen privacy and ensuring responsible data handling practices.

Usability Considerations: The emphasis on usability and accessibility is critical for ensuring that digital identity solutions are user-friendly and inclusive for all citizens, regardless of their technical skills or disabilities.

Addressing the Digital Divide: The guidelines acknowledge the importance of addressing the digital divide and promoting equitable access to digital services, which aligns with our goal of providing inclusive and accessible government services for all.

Performance Measurement: The introduction of continuous evaluation metrics provides a valuable framework for measuring the effectiveness of our digital identity systems and identifying areas for improvement.

Adapting to Evolving Threats: The emphasis on continuous monitoring and adaptation helps us stay ahead of evolving threats and ensure the long-term security and resilience of our digital identity infrastructure.

Areas of Concern

1. Increased Complexity and Costs:

Higher Assurance Levels: The guidelines seem to push for higher assurance levels across the board, even for services with lower risks. This could significantly increase the cost and complexity of implementing and maintaining digital identity systems for all state agencies, many of whom have limited budgets and resources.

Expanded Fraud Requirements: While combating fraud is crucial, the expanded requirements could be overly burdensome, especially for smaller agencies. Balancing fraud prevention with usability and accessibility for all citizens is critical, and the guidelines may need further clarification on achieving this balance.

2. User-Controlled Wallets in Federation:

Security and Privacy Risks: Introducing user-controlled wallets into the federation model raises concerns about key management, vulnerability to attacks, and potential for misuse. We welcome clear guidelines and standards to mitigate these risks before widespread adoption within state agencies.

Interoperability Challenges: Ensuring seamless interoperability between different wallet implementations across various agencies and services will be a significant challenge. The guidelines should provide clear standards and recommendations to address this.

3. Continuous Evaluation Metrics:

Implementation Guidance: While the inclusion of continuous evaluation metrics is welcome, the guidelines need to provide more specific guidance on how to implement and measure these metrics effectively across different agencies with varying levels of technological maturity.

Resource Implications: Continuous evaluation requires ongoing monitoring and assessment, which could strain resources for some agencies. The guidelines should offer practical advice on resource allocation and prioritization for effective implementation.

4. Equity and Accessibility:

Digital Divide: The guidelines should emphasize the importance of addressing the digital divide and ensuring that digital identity solutions are accessible to all citizens, regardless of their socioeconomic status, technological literacy, or disabilities.

Bias Mitigation: Clear guidance is needed on mitigating potential biases in identity proofing and authentication processes to ensure fairness and equity for all users.

5. **Impact on Legacy Systems:**

Transition Strategies: Many state agencies rely on legacy systems. The guidelines should provide clear transition strategies and support for agencies to modernize their digital identity infrastructure without disrupting essential services.

Recommendations:

Flexibility and Scalability: The guidelines should offer more flexibility and scalability to accommodate the diverse needs and resources of different state agencies.

Practical Implementation Guidance: More detailed and practical guidance is needed on implementing the guidelines, including best practices, risk assessment frameworks, and technical specifications.

Collaboration and Support: NIST should foster collaboration among state agencies and provide ongoing support for implementing the guidelines effectively.

Thank you for the opportunity to submit these comments. Colorado is working to enable easy, secure digital identity as part of our Digital Government Strategic Plan and are grateful for NIST's guidance as we continue this important work.

Sincerely,

Sarah Tuneberg

Sarah Tuneberg
Colorado Digital Service Director
Governor's Office of Information Technology