NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

DRAFT - NIST Identity and Access Management Roadmap: Principles, Objectives, and Activities

April 21, 2023

Note to Reviewers

This Identity and Access Management (IAM) Roadmap provides a consolidated view of NIST's planned IAM efforts over the coming years. It singles out strategic objectives, aligns efforts with nationally defined priorities, and supports long-term planning. It is informed by advances in the technology landscape, current policies and strategies, feedback on NIST's existing identity and access management guidance, and engagement with public and private stakeholders.

This Roadmap is an initial draft to gain further input to inform our plans. We especially seek specific input on the following:

1. Are the guiding principles clear? Are any important principles missing?
2. Do any of the strategic objectives need clarification? Are any key objectives missing?
3. Are there specific activities, research, or guidance which should be included, and if so, why?
4. Which strategic objectives are most likely to have an impact and should be prioritized?
5. What additional outputs would be useful to accompany the Roadmap?

Feedback and comments should be directed to digital_identity@nist.gov by June 16th, 2023. All relevant comments, including attachments and other supporting material, will be made publicly available on the IAM program page. Personal, sensitive, or confidential business information should not be included. Comments with inappropriate language will not be considered. Marketing materials will not be accepted.

Table of Contents

Introduction

Identity and Access Management (IAM) is the foundation of digital services. It represents the complex orchestration of multiple technologies, standards, and protocols to enable an individual to access the services, benefits, and data to which they are entitled. It also allows organizations and agencies to mitigate risks associated with fraud and unauthorized access. As such, IAM sits at the nexus of cybersecurity and customer experience, making it a key component to creating trusted, modern digital services.

NIST has long played a leadership role in advancing critical research, standards, and technology in support of IAM efforts, including through development of the Digital Identity Guidelines (Special Publication 800-63). This role continues today with refreshed emphasis driven by federal legislation and priorities such as the CHIPS and Science Act (CHIPS) and the National Cybersecurity Strategy (NCS).

NIST's IAM Roadmap aims to provide coordination and strategic alignment to a diverse set of NIST initiatives that collectively drive towards providing a more private, secure, interoperable, and equitable Identity Ecosystem. It also communicates NIST's role and priorities within a broader network of federal, commercial, international, and academic partners all seeking to improve the identity landscape and better deliver digital services – ideally enabling continued and effective collaboration towards common outcomes.

Purpose

This document provides a consolidated view of NIST's planned IAM efforts over the coming years. It singles out strategic objectives, aligns efforts with nationally defined priorities, and supports long-term planning. Specifically, this document seeks to achieve the following outcomes:

- Achieve strategic alignment across NIST IAM Projects.
- Illustrate alignment with national and administration priorities.
- Provide long-term IAM planning capabilities.
- Share strategic focus areas and principles with internal and external stakeholders.

Scope

This Roadmap covers NIST IAM programs and projects that collectively address identity proofing, fraud mitigation, authentication, authorization, biometrics, digital credentials (e.g., mobile driver's licenses), and federation for both enterprise and public-facing use cases. It is a strategic planning document and not a detailed project or delivery plan.

Program Overview

IAM is a complex set of concepts that touch on different technologies and standards. As a result, NIST's efforts reflect an equally diverse set of programs contributing to our overall strategic objectives and bringing a cross-functional set of capabilities to address IAM challenges and desired outcomes.

To advance the state of Identity and Access Management, the NIST IAM program:

- Conducts foundational and applied research to better understand new and emerging technologies, their impact on existing standards, and the implementation of Identity and Access Management solutions;
- Leads in the development of national and international Identity and Access Management standards, guidance, best practices, profiles, and frameworks to create an enhanced, interoperable suite of secure, privacy-enhancing solutions;
- Develops and enhances Identity and Access Management standards, guidelines and resources;
- Advances measurement science and methodologies for evaluating the performance of identity related technology; and
- Enables transition to practice by producing example solutions that bring together the identity management, privacy, usability, and cybersecurity requirements needed to address specific business cybersecurity challenges.

Simply put, with its focus on foundational and applied research and standards, the NIST Identity Program seeks to ensure the right people and things have the right access to the right resources at the right time.

Principles

The NIST IAM program imbues all our work with the following guiding principles:

1. **Enhance privacy and security** by integrating confidentiality, integrity, and availability into our efforts alongside the core privacy engineering objectives of predictability, manageability, and disassociability.
2. **Foster equity and individual choice** by exploring the diverse socio-technical impacts of identity technology and integrating optionality and flexibility into our work products.
3. **Promote usability and accessibility** by assessing the impacts of technology on diverse communities with varying levels of technology access, knowledge, and capabilities.
4. **Enhance interoperability and standardization** by creating or contributing to accessible and technically viable standards, guidance, and specifications.
5. **Improve measurement and transparency** of identity technology by creating methodologies and metrics that enhance the fundamental understanding of how technologies perform and are open and available to the public.

These principles are not individual projects or efforts. Instead, they are concepts to be integrated into all our efforts – from guidance, to research, to reference implementations. The intent is to improve the broader ecosystem of identity technology, solutions, and services. Furthermore, these efforts help set the conditions for **responsible innovation** the idea of driving towards new technologies and solutions (but with an understanding of the broader impacts associated with technological change).

Drivers

Our IAM Roadmap is driven by business, policy, legislative, technical, and environmental factors, including:

- **Increasing fraud and sophistication of attackers:** Attackers are leveraging increasingly complex attacks to enable fraud and unauthorized access including phishing, ransomware, synthetic identities, automated attacks, and the use of industrialized criminal forums and marketplaces. They also have greater motivation and opportunity than ever before with the rapid transition of traditionally analog or offline services to the digital realm.
    - **Impact:** NIST's guidance must constantly evaluate and understand the threat environment and include updates – in a timely manner – to address emerging threats and attacks.
- **Changing public expectations and sentiments**: Surging awareness and concern around data privacy, bias, and usability are substantially shifting how organizations view risk and placing greater emphasis on the needs of individuals. This has been brought into clear view because of public response to some uses of biometrics, the increasing frequency of breaches, and ongoing concerns over lack of user control and accountability for data usage.
    - **Impact:** NIST must continue to adapt and evolve guidance to reflect the changing public views. This includes providing additional options for identity controls to account for different circumstances, capabilities, and access levels. Security is only one aspect of our research and guidance: privacy, bias, and usability mandate equal attention and investment.
- **Agency and Industry Capabilities:** NIST supports the needs of the public and individuals, but government agencies and industry remain the primary consumers of the materials we produce. New technologies, new capabilities, and improvements to our own outputs are defined by this community.
    - **Impact:** To provide valuable and easily adopted guidance, NIST must maintain continuous engagement with these stakeholders to integrate their feedback and address shifting capabilities and needs within the IAM space.
- **CHIPS & Science Act**: Among other things, the Act, which passed in 2022, authorizes NIST to conduct digital identity research and to develop a voluntary framework for digital identity management; expands NIST's Biometrics Identification research and testing programs; and directs NIST to develop performances standards and guidelines for high-risk federal biometric identification systems.
    - **Impact:** This statute requires NIST digital identity efforts to produce specific outcomes. It mandates the creation of a "voluntary framework" for digital identity and expanded biometric testing. The Act also mandates a digital identity technical roadmap that is made available to stakeholders.
- **Administration Policies and Directives:** Emerging administration and policy initiatives with implications for NIST's IAM efforts include the *National Cybersecurity Strategy, the White House's Initiative on Identity Verification, Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government, The Federal Zero Trust Strategy, Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government*, and *OMB Memo 19-17 Enabling Mission Delivery through Improved Identity Credential and Access Management*.

- **Impact:** These policies and directives provide taskings, priorities, and deliverables specifically for NIST, while also defining administration priorities to which the execution of initiatives will align.

Drivers for NIST's IAM efforts will continue to change over time. This Roadmap will be revised as needed – and reflecting stakeholder inputs – to ensure that the evolving strategic environment continues to be reflected in our IAM program.

Strategic Objectives and Activities

Strategic Objectives reflect NIST's priorities and define specific areas of focus. They address the drivers previously defined in this document and provide a means to evaluate our work for alignment with national and organizational goals.

Accelerate Implementation and Adoption of Mobile Driver's Licenses (mDL) and User Controlled Digital Credentials

Advance international standards, implementation guidance, and interoperability efforts to promote increased and accelerated adoption of mDL and other forms of interoperable digital credentials. Initial efforts will focus on advancing mDL in line with the National Cybersecurity Strategy, but will progress to evaluation and integration of other standards-based credentials (such as verifiable credentials) into an interoperable wallet.

Short Term	Long Term (pending resources)
Develop Privacy and Security Considerations for mDL Implementation	**Execute NCCoE Project – Accelerating adoption of Mobile Driver's License Technology**
Contribute to ISO/IEC 18013-5, mDL Reference Implementation	**Execute NCCoE Project – Implementing Multiple Interoperable Credential Types**
Contribute to ISO/IEC 23220 Building Blocks for Identity Management via Mobile Devices	**Develop Draft Guidance for use of Digital Wallets and Portable Digital Credentials**
Contribute to ISO/IEC 18013-7, mDL for Unattended Use Cases	

Expand and Enhance Biometric and Identity Measurement Programs

Expand and enhance efforts to measure, test, and improve the accuracy, usability, and inclusivity of biometric and identity technologies. To date, biometrics are the most measurable component of the Identity Ecosystem, with standards, methods, and processes to evaluate their performance. NIST will continue to enhance our existing face, fingerprint, and iris activities while conducting foundational research to understand how best to apply metrology to new and emerging identity technologies and processes.

Short Term	Long Term (pending resources)
Expand Biometric Technology Evaluations to Support Face Recognition PAD	**Develop Considerations for Evaluating the Performance Identity Proofing Services**
Expand Biometric Technology Evaluations to Support Face Recognition Twin Detection Track	**Re-establish and Maintain NIST's Fingerprint Evaluation Program**
Develop Guidance for Certifying Contactless Fingerprint Capture Devices	**Expand Evaluation Program for Iris Technology**
	Maintain and Enhance the FRVT Program

Promote Technology that Enables Authoritative Attribute Validation

Establish architectures, requirements, and implementation guides to promote authoritative validation of user attributes and verifiable, user-controlled representations of validated attributes such as verifiable credentials. Our intent is to set the foundation for agencies and organizations that may choose to offer attribute services at varying levels.

Short Term	Long Term (pending resources)
Analyze Attribute Validation Services & Architectures	**Develop a Privacy Preserving Distributed Ledger Technology**
	Execute NCCoE Project to Create Reference Architecture and Implementations for Attribute Validation Services

Advance Secure, Privacy-Protective, and Equitable Identity Proofing and Fraud Mitigation Options

Strengthen and improve the privacy, security, and equity of identity proofing, verification, and fraud prevention methods used in identity management systems through research, analysis, and evaluation of emerging technology. We will focus on evaluating emerging techniques for potential integration into guidance, such as NIST SP 800-63A, applying privacy enhancing technologies, and providing guidance for agencies on how best to integrate such technologies into their identity management processes.

Short Term	Long Term (pending resources)
Update NIST SP 800-63A Digital Identity Guidelines – Enrollment & Identity Proofing	**Execute NCCoE Project - Analyzing Emerging Identity Verification Technologies**
Foundational Research into Emerging Identity Proofing and Identity Verification Technologies	**Joint Collaboration with NIST Privacy Engineering Program to Test Privacy-Preserving Federated Learning Models for Fraud Detection**
Update NIST SP 800-63A Implementation Guidance	**Develop Considerations for Continuous Improvement and Program Integration of Identity Systems**
	Develop Considerations for Fraud Management in a Federated Identity Model

Accelerate the Use of Phishing Resistant, Modern Multi-Factor Authentication

Conducting research and providing implementation guidance and the standards necessary to accelerate the adoption of more secure and phishing-resistant authenticator options across the enterprise and public-facing use cases within government. Specifically, we will focus on the integration of phishing resistance into existing guidance, while also seeking to develop new and highly consumable implementation guidance that can provide a wider audience with a clear understanding of different authenticators. That includes the risks they mitigate, the value they bring to transactions, and common implementation patterns.

Short Term	Long Term (pending resources)
Develop Implementors Guide to Modern Authentication Technology	**Build Identity Innovation and Modernization Lab in the NCCoE**

Update NIST SP 800-63B Digital Identity Guidelines - Authentication & Lifecycle Mgt	
Update NIST SP 800-63B Implementation Guidance	

Promote Greater Interoperability of Identity Solutions

Develop, contribute to, and enhance technical and process standards that promote and support greater interoperability among the federal enterprise, other parts of the public sector, and the private sector. This includes multilateral and bilateral engagements to promote pre-standardization research and common standards development goals.

Short Term	Long Term (pending resources)
Update NIST SP 800-63 Base Document – Digital Identity Guidelines	**Develop Considerations and Tools for Conducting a Digital Identity Risk Assessment**
Update NIST SP 800-63C – Federation and Assertions	**Provide Considerations, Guidance, and Profiles for Verifiable Credentials in Government**
Update NIST SP 800-63C Implementation Guidance	**Develop Government profiles for Federation and Digital Credential (e.g., OIDC, SAML, VC, mDL)**
Update NIST SP 800-63-4 Conformance Criteria	**Update Guidance for the Use of Electronic Signatures**
	Research machine readable version of conformance criteria

Advance Dynamic Authorization and Access Control Schemes

Develop standards, guidance, implementation guides, and technical solutions that support agencies' efforts to deploy dynamic and contextual authorization in support of Zero Trust Architectures, within federal and commercial enterprises. Our efforts will build from existing standards – such as Next Gen Access Control (NGAC) – to provide additional layers of research and tools to support fine-grained authorization capabilities in multiple scenarios.

Short Term	Long Term (pending resources)
Develop A Zero Trust Architecture Model for Access Control in Cloud Native Applications in Multi-Cloud Environments	**Research Embedded ABAC in Database**
Develop a Federated System to Share Granular Data Among Disparate Database Resources	**Develop Next Generation Access Control: A comprehensive Approach to Multi-Cloud Environments**

Modernize the Federal PIV Architecture and Guidance

Develop, update, and improve PIV standards and guidelines to facilitate the implementation of flexible architectural models, support additional authentication methods for interagency use, advance greater identity and lifecycle management capabilities, address emerging threats, and prepare for strategic shifts such as the need to migrate quantum-resistance cryptographic algorithms.

Short Term	Long Term (pending resources)
Update NIST SP 800-157 Guidelines for Derived PIV Credentials	**Stand-up NCCoE PIV Modernization Lab**

Develop NIST SP 800-217 Guidelines for PIV Federation	**Update NIST SP 800-79-3 PIV Card and DPC Issuer Accreditation**
Update SP 800-78-5 PIV Cryptographic Guidelines	**Update SP 800-85A PIV Card Test Requirements**
Update NIST SP 800-73-5 PIV Card and Middleware Spec	**Update NPIVP PIV Card Test Runner for Testing labs**
Update SP 800-76-3 Biometric Specifications for Personal Identity Verification	

Conclusion

This draft Roadmap is a mechanism to gain feedback on the strategic direction of NIST's IAM program. It is important to note that this Roadmap is a multi-year endeavor, with the completion of projects spread through the next several years. NIST will revisit this Roadmap on an annual basis to reevaluate, prioritize, and refresh our efforts and to ensure alignment with advances in technologies and new policy directives. We welcome all input on how best to prioritize our efforts, suggestions about new objectives or activities, and areas where clarification would be helpful.