InCommon®

Powered by INTERNET2®

Beyond Authentication: Working Together on Identity Verification Thread Meetup

Report

Virtual Session:

October 22, 2025

Table of Contents

Overview

The October 2025 Identity Assurance Thread Meetup brought together over sixty IT leadership, security professionals, and members of IAM teams from across higher education and research to address the growing challenges of identity verification. The meeting followed up on InCommon's Identity Verification Survey and built upon years of work around implementing identity assurance standards. Participants represented a range of institutional roles, from IT and security leadership to IAM teams, library services, and admissions, reflecting the cross-functional nature of identity verification challenges.

The discussion revealed that institutions are grappling with fragmented, decentralized processes across different departments, each with varying requirements and data collection needs. Participants shared experiences ranging from manual verification procedures to emerging concerns about deepfake technology compromising video-based verification methods. The conversation highlighted tensions between the desire for standardized cost-effective solutions and the reality of diverse use cases and decentralized business processes. Institutions must balance regulatory compliance requirements from federal financial aid programs with practical considerations for different populations like international students, alumni, contractors, and traveling nurses.

Survey results indicated a strong community interest in finding a vendor solution that could meet multiple remote compliance requirements while remaining affordable and scalable. Participants expressed a desire for continued collaboration through various formats including live discussion groups, structured learning programs, self-paced guides, and peer-to-peer support channels. The meeting identified a clear need for community support with identity verification through discussion groups, guides, peer learning, and vendor comparisons.

Conversation Highlights

- **Vendor Solution Exploration:** Institutions are researching commercial identity verification services, with participants discussing various providers they're evaluating or considering. Significant variation exists in vendor pricing and requirements, with institutions conducting RFPs and evaluating which providers might offer government certifications for federal compliance requirements.

- **Deepfake Technology Concerns**: An attendee from Carnegie Mellon University raised a critical security issue, noting that deepfake video capabilities could compromise current video-based verification methods, highlighting the need for more robust verification approaches beyond simple video calls.

- **Data Challenges, Contractor Verification and Duplicates**: Another attendee from from Harvard University emphasized the difficulty of verifying contractor identities during onboarding because they need to verify basic identity

information like legal name and birthdate to determine whether there is an existing identity in the system or need to create a new one. Without proper identity verification at the point of onboarding, there is a lack of confidence in the accuracy of the foundational data that drives the entire identity and access management system.

- **Implementation Strategy Debate:** An attendee from Rochester Institute of Technology shared their phased approach, focusing on individuals where identity verification is needed to meet regulatory requirements before expanding to all users. This sparked discussion about whether identity verification should be implemented universally from the start or target strategically at specific high-risk use cases.

- **Request for Guidance**: Another attendee from Ithaca College articulated a key need for practical guidance, requesting example ID verification methods mapped to specific Identity Assurance Levels with clear limitations spelled out, moving beyond abstract NIST guidelines to actionable implementation options.

Survey Findings

- **High-Level Leadership Engagement:** The survey received strong participation from senior leadership, with 40 IT Leadership, 36 Security Leadership, and 36 IAM Team members participating. The survey also included representation from 18 other IT teams, 17 security operations, 2 library staff, and 1 admissions representative, demonstrating broad institutional interest in identity verification across multiple departments.

- **Physical Access and ID Card Issuance as Top Priorities:** Survey results showed that physical access to buildings and ID card issuance were among the highest areas already being addressed by institutions (over 50% for each), indicating these are established use cases where identity verification is actively implemented.

- **Strong Interest in Commercial Identity Proofing Services:** Approximately 90% of respondents indicated they are using government-issued identity documents for verification and about 75% are looking at commercial identity proofing services. Many institutions reported they're in various stages of investigating or implementing vendor solutions.

- **Most Institutions Don't Store Identity Proofing Status:** Nearly 47% of respondents indicated they do not store identity proofing status information in

their databases, with only about 32% currently storing this data. This suggests a significant gap in institutional record-keeping around verification activities and inability to leverage a proofing event for multiple purposes. .

- **Overwhelming Support for NET+ Service:** Approximately 73% of respondents expressed interest in having identity verification available as a NET+ service, with only about 4% saying no, and 23% uncertain. This demonstrates strong community desire for a collective purchasing and evaluation approach to identity verification services.

Next Steps

- **Engage with InCommon's Support Programming**: Participate in the educational resources and discussion forums that InCommon will develop based on poll results. Take advantage of live discussion groups and structured learning experiences designed to get peer-to-peer support and learn from institutions facing similar challenges.

- **Evaluate Vendor Solutions Systematically**: Review the commercial service providers being considered by peers and consider attending an upcoming EDUCAUSE Demo Day on Fraudulent Application Detection Systems scheduled for April 8, 2026. Stay tuned for a potential Net+ identity proofing service that would allow institutions to leverage collective purchasing power and shared requirements, potentially avoiding the need for individual campuses to duplicate RFP efforts.

- **Review InCommon's Implementation Guidance**: Access the existing RAF IdP implementation guidance resources that were shared during the meeting to understand concrete approaches for meeting different Identity Assurance Levels. Use these materials as a starting point for developing your institution's identity verification strategy.

APPENDIX

Meeting Recording & Assets

Select the following links to access the recording and slides:

Zoom Recording Passcode: GKV&23r^

Please note that audio and chat transcripts are available within the recording.

Meetup Slides