

DOI: https://doi.org/10.48009/4_iis_2026_153

The Identity Trust Chain: A governance framework for attribute-level identity provenance and assurance in higher education

Felix Jelen, *Mercer University*, [Jelen f@mercer.edu](mailto:f@mercer.edu)

Johnathan Yerby, *Mercer University*, Yerby jm@mercer.edu

Abstract

This paper develops the Identity Trust Chain (ITC), a standards-informed governance framework for attribute-level identity provenance and assurance in higher education enrollment systems. Motivated by ghost-student and FAFSA-related fraud patterns, the paper argues that institutional identity risk is broader than authentication. The central problem is whether the attributes composing a student identity have known sources, validation histories, assurance levels, freshness conditions, and permitted uses when relied upon for institutional decisions. Using an abstracted enrollment stack composed of identity providers, customer relationship management systems, student information systems, learning management systems, financial-aid systems, payment systems, and federated services, the paper identifies where identity trust is created, transformed, propagated, degraded, and revalidated. The ITC synthesizes NIST digital identity guidance, REFEDS assurance concepts, W3C provenance modeling, federation trust practices, zero trust principles, and NIST Cybersecurity Framework 2.0 governance logic into a conceptual model for institutional decision-making. The contribution is not a new authentication technology or forensic method, but a governance framework for improving attribute trust, auditability, decision justification, and fraud resistance across higher education identity workflows.

Keywords: identity attributes, assurance, identity provenance, federation, identifier governance

Introduction

Higher education institutions increasingly make enrollment, aid, access, recovery, payment, and credentialing decisions through interconnected digital identity systems. Ghost-student and FAFSA-related fraud have made this issue visible, but the underlying challenge is broader than any single fraud pattern. Institutions routinely rely on student identity attributes that originate in different systems, are validated through different processes, and are later reused for decisions carrying very different levels of risk.

This paper argues that institutional identity risk is not limited to whether a student, applicant, or claimant can authenticate to a portal. Authentication can show control of an account or authenticator, but it does not necessarily show that the legal name, date of birth, enrollment status, financial-aid attribute, payment detail, recovery attribute, or federated identifier connected to that account is accurate, current, validated, or appropriate for a specific institutional decision.

The purpose of this paper is to develop the Identity Trust Chain (ITC), a standards-informed governance framework for attribute-level identity provenance and assurance in higher education enrollment systems. The framework synthesizes concepts from NIST digital identity guidance, REFEDS assurance practices, W3C provenance modeling, federation trust practices, zero trust principles, and NIST Cybersecurity Framework 2.0 governance logic.

The paper first defines the scope and key concepts needed to discuss attribute-level identity trust. It then reviews literature and standards related to higher education identity risk, trust propagation, digital identity assurance, federation, provenance, and cybersecurity governance. After that review, the paper states the specific governance problem addressed by the ITC, presents the research questions and methodology, develops the eight-domain ITC framework, and summarizes implications, limitations, and future research opportunities.

Scope and Research Contribution

This study focuses on institutional governance levers that can improve identity trust across higher education enrollment systems: (1) identity attributes, (2) provenance metadata, (3) assurance interpretation, (4) identity proofing, (5) federation, (6) identifier governance, (7) recovery and continuity, and (8) exception handling. The paper does not conduct incident-specific technical analysis or provide prescriptive configuration recommendations for systems or vendors. Instead, it aligns with the governance logic of NIST CSF 2.0 by proposing a framework that institutions can adapt to their enrollment stacks, risk appetites, and technological maturity. Although ghost-student fraud motivates the study, the governance problem is broader. Weak attribute provenance can affect admissions decisions, account recovery, payment processing, credential issuance, compliance reporting, and institutional reputation. The paper's contribution is the Identity Trust Chain, an eight-domain governance framework for managing student identity as a collection of governed attributes rather than as a single monolithic account record.

Key Concepts and Definitions

Several concepts are used throughout the ITC. Student identity refers to the collection of attributes, identifiers, records, and claims that represent a student across institutional systems. An identity attribute is a discrete data element associated with the student, such as legal name, date of birth, institutional identifier, address, financial-aid status, payment detail, LMS activity signal, or federated identifier. Attribute provenance refers to the documented origin, validation history, transformation path, and decision-use context of an identity attribute as it moves through institutional systems. Assurance refers to the level of confidence that an attribute is accurate, current, validated, and appropriate for a specific institutional use. Freshness refers to whether the validation attached to an attribute remains current enough for the decision being made. Permitted use refers to the institutional decisions or workflows for which an attribute may appropriately be used.

The enrollment stack refers to the connected systems through which student identity attributes are created, stored, transferred, and used. In this paper, an identity provider (IdP), such as Microsoft Entra ID, Okta, Google, or another SAML/OIDC service, authenticates users and may assert identity claims. A customer relationship management system (CRM), such as an admissions or applicant-management platform, supports recruitment and admissions workflows. A student information system (SIS), such as Banner, Anthology, or PeopleSoft, serves as the central administrative student record. A learning management system (LMS), such as Canvas or Blackboard, supports course access and activity records. Federated services rely on identity assertions or attributes shared across organizational or technical boundaries. InCommon is a U.S. research and education federation operated by Internet2 that supports federated identity trust among participating institutions, identity providers, service providers, and related research and education services. For example, a prospective student may begin in an admissions portal, have application attributes promoted into the SIS after admission, authenticate through the IdP, and then appear in the LMS after course registration. A financial aid or payment workflow may then rely on legal identity, enrollment status, FAFSA/ISIR data, and refund-routing information drawn from several systems rather than from one unified identity source.

A transformation point is any moment where an attribute is created, asserted, validated, modified, promoted, transferred, federated, recovered, or interpreted for decision-making. A trust propagation amplifier is a system, such as an SIS, that can increase the institutional impact of weak or stale attributes by distributing them to downstream systems. Recursive lifecycle governance refers to the idea that identity trust must be revisited across the student lifecycle rather than established once and assumed indefinitely.

Literature Review

This literature review situates the Identity Trust Chain within four bodies of work that are usually discussed separately: higher education identity and fraud risk, enrollment-system trust propagation, digital identity assurance standards, and provenance-based cybersecurity governance. Read together, these areas show why institutions need more than authentication controls. They need governance mechanisms that preserve the source, validation history, freshness, assurance level, and permitted use of identity attributes as those attributes move across institutional systems.

Higher Education Identity and Fraud Risk

Higher education institutions manage identity attributes that carry academic, operational, financial, and compliance significance. Student identity data are used to support admissions, enrollment, financial-aid eligibility, payment processing, account recovery, learning management access, credentialing, and institutional reporting. Because these workflows connect identity attributes to access, funds, records, and credentials, weaknesses in identity governance can create risks that extend beyond ordinary account compromise (Yerby & Floyd, 2018). In the context of ghost-student and FAFSA-related fraud, the central concern is not only whether a fraudulent actor can access a system, but whether weak or insufficiently validated identity attributes can move through institutional workflows long enough to support aid eligibility, enrollment activity, refund routing, or other high-risk decisions.

Federal and oversight materials have increasingly emphasized the importance of identity verification and fraud detection in student-aid processes. The U.S. Department of Education has reported improper or ineligible federal student-aid disbursements and later announced expanded anti-fraud efforts, including real-time FAFSA fraud-detection controls and additional identity confirmation steps for applicants flagged for further review. The Office of Inspector General has similarly identified risks associated with FSA ID account creation and FAFSA-related fraud indicators. These sources demonstrate that identity risk in higher education is not limited to institutional authentication systems. Instead, it involves the broader enrollment and aid ecosystem in which identity attributes are collected, validated, transmitted, interpreted, and relied upon for decisions (Federal Student Aid, 2026; U.S. Department of Education, 2025a, 2025b; U.S. Department of Education, Office of Inspector General, 2024, 2026).

Enrollment Systems and Trust Propagation

A recurring problem in these environments is that student identity attributes are often asserted in one system, validated or modified in another, promoted into an official record in a third, and reused later by downstream systems for decisions that carry greater risk than the original collection context. When the source authority, validation history, freshness condition, assurance level, or permitted-use context is not visible, attributes become semantically flat data fields rather than governed identity claims.

Higher education enrollment workflows are supported by interconnected systems rather than a single authoritative identity environment. These systems collectively form the enrollment stack: the set of platforms that create, store, transfer, and use student identity attributes across the student lifecycle. Common components include identity providers, customer relationship management systems, student information systems, learning management systems, financial-aid systems, payment systems, recovery

workflows, and federated services. These systems may be self-hosted, cloud-based, vendor-managed, or delivered through software-as-a-service arrangements. Higher education identity and access management commonly involves the policies, processes, and technologies used to establish user identities and enforce access rules across campus systems and digital resources (EDUCAUSE, n.d.). Each system may perform its local function effectively, while still contributing to broader governance problems when identity attributes move across systems without visible source authority, validation history, assurance level, freshness condition, or permitted-use context. A wide range of users have a wide range of permissions and awareness of security behaviors related to the interconnected systems (Yerby & Floyd, 2018).

Identity providers serve as access gateways by supporting authentication and the assertion of identity claims. However, authentication should not be treated as equivalent to proof that all attributes associated with an account are accurate, current, or appropriate for later institutional use. In early recruitment or application workflows, low-friction access may be reasonable because prospective students need to request information, begin applications, or interact with admissions systems. The governance problem emerges when attributes collected or associated with these low-risk interactions are later reused for higher-risk decisions involving financial aid, payment changes, official records, or account recovery.

Customer relationship management systems often serve as the first sustained institutional interface for prospective students. At this stage, identity attributes may be self-asserted by applicants, supplied through documents, or received through external integrations. Legal, academic, financial, and contact attributes can therefore enter the institution with different levels of source reliability and validation. These attributes may be adequate for recruitment communication or application support, but they should not automatically be treated as sufficient for financial-aid disbursement, refund routing, compliance reporting, or credentialing.

Student information systems often become the central operational record for student administration. Once applicant data are promoted from the CRM into the SIS, downstream systems may treat those attributes as official, even when the original source, validation method, or assurance level is unclear. The SIS can therefore function as a trust propagation amplifier: attributes that enter with weak provenance or stale assurance may be distributed to LMS, financial-aid, payment, reporting, and federated workflows as though they carry institutional authority. This creates a systems-governance problem in which local records appear trustworthy because of their placement in the institutional stack rather than because their trust conditions are known.

Learning management systems introduce another interpretive challenge. LMS login records, course access, assignment submission, and participation signals may provide useful evidence of engagement, but they do not independently prove legal identity or validate high-risk identity attributes. In fraud contexts, activity signals may help sustain the appearance of legitimate enrollment. Therefore, LMS data should be treated as corroborating evidence rather than as primary proof of identity or eligibility.

Financial-aid and payment systems are where identity trust failures become especially consequential. These systems rely on legal identity, eligibility, enrollment, financial, and payment-routing attributes to support aid decisions, disbursement, refund processing, fraud flagging, and account updates. Attributes originally collected for lower-risk purposes may become problematic if they are later reused for high-risk financial decisions without revalidation. This makes financial aid and payment workflows key decision points for risk-based assurance escalation.

Digital Identity Assurance Standards

Existing digital identity standards provide essential vocabulary for distinguishing among forms of trust, but they do not by themselves provide a higher-education-specific governance model for attribute movement

across enrollment systems. NIST SP 800-63-4 and its companion documents distinguish identity proofing, authentication, authenticator management, federation, and assertions. This distinction is important because authentication establishes control of an authenticator, while identity proofing and assurance address the relationship between a claimant, evidence, and identity attributes. For higher education, this distinction helps clarify why a student's ability to log in should not automatically validate the attributes attached to that student's record (Temoshok et al., 2025a).

The Research and Education Federations group, commonly known as REFEDS, develops guidance for identity federations that support universities, research organizations, and related service providers. Its Assurance Framework 2.0 provides a useful model for evaluating identity trust in research and education environments because it separates identifier uniqueness, identity assurance, and attribute assurance. This distinction allows institutions to interpret trust more precisely. For example, a university may have confidence that an identifier is unique within a system but still lack confidence that a specific attribute, such as legal name, date of birth, address, aid eligibility, or payment detail, is current and validated for a particular decision. REFEDS therefore supports this paper's argument that institutions need attribute-level assurance rather than a single generalized trust status attached to an account (REFEDS, 2023).

Federation further complicates identity assurance because claims and attributes may move across organizational, administrative, and technical boundaries. NIST federation guidance describes the role of assertions, relying parties, federation assurance, and protections for assertion integrity. InCommon federation trust practices emphasize metadata accuracy, operational authority, security expectations, and incident readiness. Together, these sources show that trust in federated environments depends not only on whether a claim can be exchanged securely, but also on whether the receiving institution can interpret what the claim means, what assurance it carries, who is accountable for it, and what decisions it can appropriately support. For higher education, this distinction is critical because an attribute received through a trusted federation may still require contextual evaluation before it is used for enrollment, financial aid, account recovery, payment processing, or other high-impact decisions (Internet2, 2020; Richer et al., 2025).

Provenance and Governance Foundations

Provenance modeling provides a way to describe how identity attributes originate, move, change, and become associated with systems, processes, reviewers, and decisions. The World Wide Web Consortium, commonly known as W3C, develops technical standards for the web and related data practices. Its PROV model provides a vocabulary for representing provenance, or the history and context of how information was created, modified, attributed, and used. This vocabulary includes concepts such as entities, activities, agents, derivation, and time. Applied to higher education identity governance, an attribute can be treated as an entity, a proofing or transformation event as an activity, a system or reviewer as an agent, and timestamps or derivation records as evidence of how the attribute's trust context has changed over time. This provenance perspective is important because institutions often need to know not merely what value exists in a record, but where that value came from, who or what validated it, when it was changed, and what decision it was used to support (Moreau et al., 2013).

Zero trust guidance also informs the governance logic of the ITC. Zero trust is a cybersecurity model that rejects automatic or inherited trust and instead requires access decisions to be based on current, relevant context. NIST SP 800-207 emphasizes that trust should not be granted merely because a user has authenticated, a device is inside a network, or a system has been trusted in the past. Although zero trust is not a higher education enrollment framework, its core principle is relevant to identity governance: trust must be evaluated continuously and contextually. For identity attributes, this means that an attribute should not remain trusted simply because it entered the institution through a familiar system or was validated at some earlier point. Instead, attribute trust should be reassessed as data moves across systems and is used

for decisions with different levels of risk, such as enrollment, financial aid, account recovery, or payment processing (Rose et al., 2020).

NIST CSF 2.0 provides a broader governance foundation for connecting technical controls to institutional risk management, accountability, policy, recovery, and continuous improvement. This is important because identity provenance and assurance cannot be solved solely through authentication technology or fraud-detection tools. Institutions also need governance structures that define ownership, permitted use, escalation triggers, recovery expectations, and exception handling (Pascoe et al., 2024).

Taken together, the literature shows that the problem is not a lack of identity standards, provenance models, federation practices, or cybersecurity governance principles. Rather, the gap is that these concepts remain fragmented and are not integrated into a higher-education-specific framework for managing attribute trust across the enrollment lifecycle. The Identity Trust Chain addresses that gap by synthesizing assurance, provenance, federation, and governance concepts into a practical model for determining when student identity attributes can be trusted, when they require revalidation, when their use should be restricted, and how their provenance should be preserved for auditability, recovery, and fraud resistance.

Problem Statement

The literature and standards reviewed above establish a clear governance gap. Higher education institutions rely on identity attributes that move across admissions, student information, learning management, financial-aid, payment, recovery, and federated systems, yet those attributes are not always accompanied by metadata showing where they originated, how they were validated, whether they remain fresh, what assurance level they carry, and which decisions they are permitted to support.

This creates a trust problem rather than only a technical authentication problem. An institution may know that an attribute exists in a system of record, but not whether that attribute is trustworthy for a particular decision at a particular point in time. Low-risk recruitment communication may reasonably rely on self-asserted or lightly validated attributes, but high-risk actions such as aid disbursement, payment changes, legal identity updates, account recovery, or credential issuance require stronger evidence of source authority, validation, freshness, and auditability.

The specific problem addressed by this paper is the absence of a higher-education-specific governance framework for managing attribute-level identity provenance and assurance across the enrollment lifecycle. Without such a framework, weak, stale, or insufficiently validated attributes can be elevated, propagated, or overinterpreted by downstream systems. The Identity Trust Chain is proposed to help institutions determine when student identity attributes can be trusted, when they require revalidation, when their use should be restricted, and how their provenance should be preserved for decision justification, recovery, and fraud resistance.

Research Questions

This study is guided by three framework-development questions: (1) which identity attribute transformation points in the higher education enrollment stack create risks of trust degradation, assurance mismatch, or fraud exposure; (2) what minimum provenance metadata and audit artifacts are necessary to support defensible enrollment decisions and investigations; and (3) what governance and control components can help universities manage identity provenance and assurance across the enrollment stack?

Methodology

This study uses a standards-informed conceptual framework development method to analyze identity provenance and assurance across the higher education enrollment stack. The purpose of this paper is framework development and conceptual integration, not empirical validation. The study develops a governance framework by identifying recurring identity trust problems in enrollment workflows and synthesizing relevant concepts from established identity, provenance, federation, and cybersecurity governance standards. This approach is appropriate because identity risk emerges through the movement, transformation, reuse, and interpretation of student identity attributes across interconnected institutional systems.

The unit of analysis is the digital student identity as a collection of governed attributes rather than a single account, profile, or institutional record. These attributes may include legal identity information, contact information, academic records, financial-aid data, payment details, institutional identifiers, federated identifiers, LMS activity signals, recovery information, and exception or fraud flags. At the granular level, each attribute is assumed to have a source, assertion method, validation history, assurance level, freshness condition, transformation history, permitted-use context, and decision-use history, although institutions may vary in their ability to capture this metadata.

The framework development process followed six steps. First, the study defined an abstracted higher education enrollment stack composed of systems commonly involved in student identity creation and use, including identity providers, customer relationship management systems, student information systems, learning management systems, financial-aid systems, payment systems, recovery workflows, and federated services. This abstracted model was used to represent common identity movement patterns without assuming that every institution uses the same vendors, architectures, or integration methods.

Second, the study identified identity attribute transformation points within that stack. Transformation points were defined as moments where student identity attributes are created, asserted, validated, modified, promoted, transferred, reused, federated, recovered, or interpreted for institutional decisions. Examples include IdP-to-CRM account creation, CRM application intake, CRM-to-SIS attribute promotion, SIS-to-LMS enrollment feeds, financial aid and payment decision points, federated attribute release, and account recovery or fraud exception handling.

Third, each transformation point was examined for identity trust risks. These risks included authentication being mistaken for identity proofing, self-asserted attributes being reused for higher-risk decisions, weak or stale attributes being promoted into official records, LMS activity being overinterpreted as proof of identity, financial-aid and payment workflows relying on insufficiently validated attributes, federated claims being interpreted without adequate assurance context, and recovery workflows bypassing normal proofing controls. The purpose of this step was to identify where identity trust is created, transferred, amplified, degraded, or revalidated across the student lifecycle.

Fourth, the study extracted relevant concepts from established standards and guidance documents. NIST SP 800-63 and its companion documents were used to distinguish identity proofing, authentication, authenticator assurance, federation, and assertion management. REFEDS Assurance Framework 2.0 was used to incorporate research-and-education-specific concepts related to identifier uniqueness, identity assurance, and attribute assurance. W3C PROV was used to structure provenance through entities, activities, agents, derivation, and time. NIST SP 800-207 informed the ITC's use of continuous contextual evaluation by rejecting implicit trust and emphasizing access decisions based on available identity, device, system, and behavioral context (Rose et al., 2020). NIST Cybersecurity Framework 2.0 was used to ground

the framework in governance, risk management, accountability, recovery, and continuous improvement. InCommon federation trust practices were used to inform the treatment of metadata accuracy, operational trust, and cross-organizational identity interpretation.

Fifth, these concepts were synthesized into the Identity Trust Chain. Concepts were not imported as standalone compliance requirements. Instead, they were translated into governance domains suitable for higher education identity workflows. NIST's separation of proofing, authentication, and federation informed the ITC distinction between authenticator control and attribute trust. REFEDS informed the treatment of identifier uniqueness and attribute assurance. W3C PROV informed the provenance model for documenting attribute source, validation, transformation, and use. Zero trust concepts informed the requirement that attribute trust be reassessed across context and time rather than assumed because an attribute appears in a system of record. NIST CSF 2.0 informed the broader governance logic of policies, ownership, recovery, exception handling, and continuous improvement. InCommon informed the ITC's treatment of federated identity, metadata accuracy, and cross-organizational trust. This synthesis produced the eight ITC domains: authoritative source hierarchy, provenance modeling, identity proofing, identity assurance mapping, federated identity governance, identifier governance, continuity and recovery, and incident response and exception governance.

Sixth, the framework was conceptually checked by mapping each ITC domain back to the framework-development questions. The framework identifies enrollment-stack transformation points where identity trust can be weakened, misinterpreted, or exploited; identifies minimum provenance metadata and audit artifacts needed to support defensible identity decisions and investigations; and defines governance and control domains that institutions can adapt to operationally manage attribute trust, assurance, and provenance across the student lifecycle. This conceptual validation does not establish empirical effectiveness, but it demonstrates internal alignment among the research questions, standards base, transformation-point analysis, and resulting governance framework. Because the ITC is conceptual, empirical testing through case studies, expert validation, or pilot implementation remains necessary.

The Identity Trust Chain Framework

The Identity Trust Chain is a student lifecycle governance model for determining how trust in student identity attributes is created, preserved, interpreted, transferred, degraded, recovered, and investigated across the institutional enrollment stack. The ITC rejects the treatment of identity as a flat account record in which all attributes carry the same trust value. Instead, it treats student identity as a dynamic collection of attributes whose trust depends on source authority, validation history, assurance level, freshness, transformation history, and decision context.

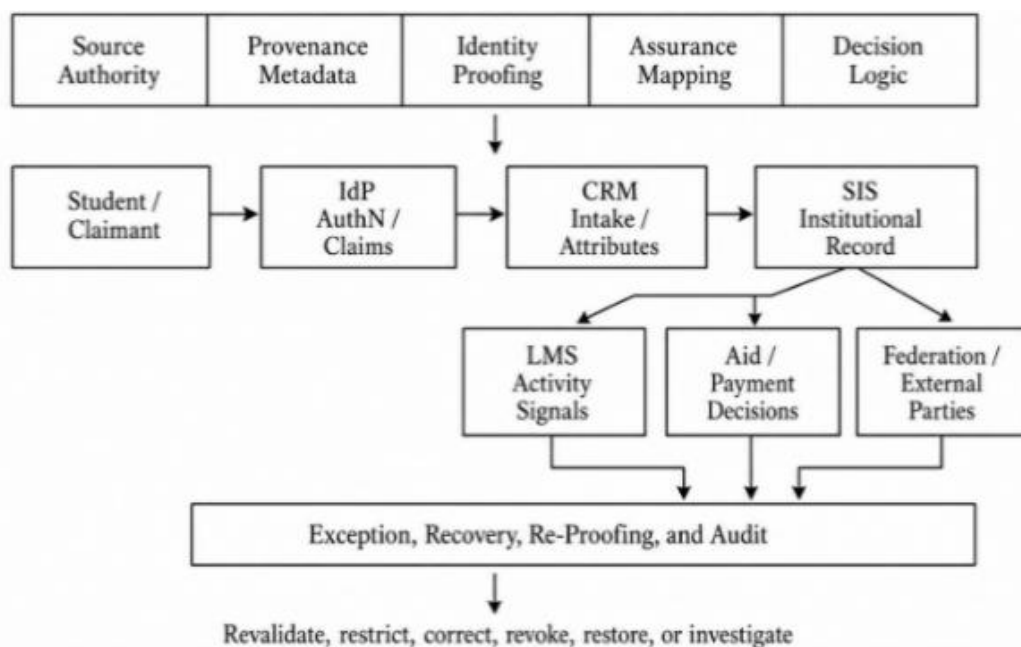


Figure 1. Overview of the Identity Trust Chain

In this model, identity assurance is not established once and then assumed indefinitely. Rather, assurance changes as attributes move through institutional systems, are transformed by integrations, reused for new decisions, made stale, modified, merged with other records, or recovered after disruption. Dynamic trust is therefore essential to decision-making in the higher education enrollment stack. The ITC provides a framework, vocabulary, and governance structure for identifying when identity attributes can be trusted, when they require revalidation, and when their use should be restricted.

The ITC domains are presented sequentially for readability, but the model is recursive rather than strictly linear. Trust conditions may need to be revisited at multiple points in the student lifecycle, especially when attributes are promoted into official records, reused for higher-risk decisions, released through federation, recovered after disruption, or flagged through an exception process. This recursive approach is consistent with governance and zero trust principles that emphasize continuous evaluation, risk management, and contextual decision-making (Pascoe et al., 2024; Rose et al., 2020).

Authentication remains necessary under the ITC, but it is treated as one component of identity trust rather than as a substitute for attribute assurance. A central control principle in the ITC is proportionality: the assurance required for an attribute should match the risk of the decision it supports. Low-risk actions, such as recruitment communication or initial portal access, may rely on lower assurance states. Higher-risk decisions, such as aid disbursement, payment changes, legal identity updates, account recovery, or credentialing, should require stronger source authority, validation, freshness, and auditability.

The Eight ITC Governance Domains

The ITC is organized around eight governance domains that define how student identity attributes should be sourced, validated, interpreted, transferred, recovered, and investigated across the enrollment stack. These domains are presented separately for clarity, but they function recursively across the student lifecycle rather than as a strictly linear sequence.

Authoritative Source Hierarchy

The authoritative source hierarchy establishes which system, office, or external authority is permitted to speak authoritatively for a specific identity attribute. This is a governance function rather than a single technical system. An institution should define the authoritative source, responsible steward, validation requirements, and propagation conditions for high-risk attributes before those attributes are reused by downstream systems. This is necessary because student identity is assembled from heterogeneous sources. Legal identity attributes may be self-asserted or drawn from government records; academic attributes may come from transcripts or credential evaluators; financial-aid attributes may come from federal aid records or financial documents; and activity signals may originate in the LMS. Without a defined source hierarchy, these attributes can appear equally trustworthy even when their origins and validation histories differ substantially.

Provenance Modeling

Provenance modeling records the history and trust context of identity attributes as they move through the enrollment stack. In the ITC, provenance is not limited to document metadata. It applies to attributes, profiles, validation events, transformations, assertions, decisions, and exceptions. A provenance-aware attribute should allow the institution to determine where the attribute came from, who or what validated it, when it was validated or changed, how it was transformed, what system used it, and for what decision. W3C PROV provides a useful conceptual basis because it models entities, activities, agents, derivation, and time (Moreau et al., 2013). In the ITC, the attribute functions as the entity, proofing or transformation events function as activities, systems or reviewers function as agents, and timestamps or derivation records explain how the attribute's trust context changes over time. The ITC does not require institutions to preserve every piece of data, but it does require enough provenance to support defensible decision-making, targeted investigation, recovery, and revalidation.

Identity Proofing

Identity proofing is the process through which trust enters the ITC. It connects a claimant and asserted identity attributes to evidence that supports those claims for a particular decision at a particular time. NIST SP 800-63A-4 treats proofing as a process involving identity resolution, validation, verification, and enrollment (Temoshok et al., 2025b). In higher education, proofing is distributed across admissions, financial aid, registrar, payment, recovery, vendor, and external data workflows. The ITC makes that distribution visible by treating proofing as an attribute-level process rather than a one-time account event. A proofing record should identify the evidence type, proofing modality, validation method, verification pathway, assurance level achieved, timestamp, reviewer or system, exception status, and attributes affected. This distinction matters because a document or profile may contain many data elements, while only some of them may have been validated for a specific use.

Identity Assurance Mapping

Identity assurance mapping translates provenance and proofing information into decision guidance. The central question is whether a specific attribute may be used for a specific decision at a specific time. Answering that question requires more than knowing whether a user has authenticated. It requires source authority, proofing level, validation method, freshness, provenance history, federation context, and action risk. NIST digital identity guidance separates identity proofing, authentication, and federation, while REFEDS separates identifier uniqueness, identity assurance, and attribute assurance (REFEDS, 2023; Temoshok et al., 2025a). The ITC applies these distinctions locally by requiring the assurance level of an attribute to match the risk of the decision. Low-risk actions may allow lower assurance states, while high-risk actions may require revalidation, escalation, restriction, or denial.

Federated Identity Governance

Federated identity governance addresses how identity claims and attributes remain interpretable when they cross organizational or technical boundaries. In higher education, federation may involve identity providers, service providers, transcript networks, aid systems, shared services, credential platforms, or external relying parties. NIST SP 800-63C provides guidance on federation, assertions, relying parties, federation assurance, and assertion integrity (Richer et al., 2025). REFEDS RAF 2.0 provides research-and-education vocabulary for identifier uniqueness, identity assurance, and attribute assurance (REFEDS, 2023). InCommon federation trust practices emphasize operational authority, metadata accuracy, security expectations, and incident readiness (Internet2, 2020). The ITC uses these concepts to require a local interpretation layer so that incoming or outgoing claims are evaluated according to source authority, assurance level, freshness, permitted use, and decision risk.

Identifier Governance

Identifier governance defines how institutional identifiers are created, assigned, reconciled, transformed, linked, retired, and recovered. Identifiers are high value because they connect attributes across systems in the enrollment stack. Weak identifier rules can lead to duplicate records, incorrect merges, stale attributes, improper permissions, failed recovery, or downstream misinterpretation. The ITC treats identifier governance as a core attribute-trust function. Institutions should define identifier ownership, uniqueness requirements, reconciliation rules, linkage between local and external identifiers, and authority requirements for identifier changes. This is especially important when identifiers are used across financial-aid systems, credential exchange platforms, federated services, and payment workflows.

Continuity and Recovery

Continuity and recovery preserve identity trust when systems are disrupted, restored, or suspected of compromise. Because HEIs rely on interconnected systems, recovery cannot focus only on restoring accounts, databases, or uptime. It must also preserve the provenance, assurance state, validation records, and decision history attached to identity attributes. If identity data are restored without their trust context, attributes may become stale, misaligned, or suspect after recovery. The ITC therefore treats continuity as an identity governance issue. Recovery plans should include authoritative-source restoration, identifier reconciliation, assurance-state preservation, audit-log recovery, re-proofing triggers for affected attributes, and communication procedures for affected systems and offices.

Incident Response and Exception Governance

Incident response and exception governance define how institutions manage suspicious, conflicting, stale, or compromised identity attributes. These conditions may arise when records do not match, a high-risk payment or recovery request is submitted; a federated source sends a fraud flag, or an investigation identifies questionable identity activity. The ITC requires institutions to define when attributes should be quarantined, escalated, revalidated, restricted, corrected, or denied. Exception handling should be proportionate to attribute risk. A low-risk inconsistency may require correction, while a high-risk financial aid, payment, legal identity, or account-recovery issue may require stronger proofing and documented approval. The goal is not to eliminate all uncertainty, but to prevent uncertain identity attributes from propagating through institutional systems without explicit review.

Table 1 applies the ITC to common identity transformation points in the higher education enrollment stack. The matrix is not intended as a prescriptive implementation checklist; rather, it illustrates how institutions can identify identity trust risks, preserve minimum provenance evidence, and apply proportionate governance controls.

Table 1. Identity Trust Chain Application Matrix

Enrollment transformation point	Identity trust risk	Minimum provenance / audit artifacts	ITC governance control
IdP → CRM account creation	Authentication may be mistaken for identity or attribute trust. A user may control an authenticator without having validated legal, academic, financial, or recovery attributes.	Identity assertion source; IdP/CSP used; account creation timestamp; authenticator assurance level; proofing level, if known; asserted identifier; initial attribute set; intake channel.	Separate authenticator trust from attribute trust. Treat early authenticated access as sufficient for low-risk engagement, but insufficient for aid, payment, recovery, or official-record decisions.
CRM intake / application record creation	Self-asserted and externally supplied attributes enter through low-friction workflows and may appear coherent before independent validation.	Attribute source; applicant-supplied or third party-supplied status; document or data type; validation method; validator or process; validation timestamp; permitted use.	Assign source authority and permitted-use tags at intake. Classify attributes by decision risk, ie recruitment, admissions review, record creation, compliance, financial aid, or payment use.
External artifact or data feed → CRM / SIS	Transcripts, IDs, FAFSA/ISIR data, credential evaluations, and other artifacts arrive with different assurance levels. Channel trust may be overread as content trust.	Sending authority; transmission channel; artifact type; attribute extracted; source-system identifier; validation method; freshness date; transformation log; exception notes.	Preserve provenance at the attribute level, not only the document level. Do not promote externally supplied attributes into high-risk use without validation and freshness checks.
CRM → SIS attribute promotion	Applicant attributes may become “official” by virtue of SIS placement, even when source, validation, freshness, or assurance is weak.	Field mapping; source CRM record; promotion timestamp; responsible process or integration; validation status; assurance state; transformation history; authoritative system designation.	Treat SIS ingestion as a trust elevation event. Require explicit promotion rules before CRM attributes become official SIS attributes.
SIS → LMS / downstream systems	The SIS can amplify trust errors because downstream systems may inherit attributes without seeing their original source or assurance condition. LMS activity may also be overread as proof of identity.	SIS field owner; source authority; last validation date; freshness condition; downstream recipients; change log; decision-use history; LMS enrollment and activity logs; linkage to SIS identifier.	Govern the SIS as a trust propagation amplifier. Treat LMS activity as corroborating evidence of engagement, not primary identity proof for aid, payment, recovery, or credential decisions.
Financial-aid / payment decision point	High-risk decisions may rely on attributes collected earlier for lower-risk purposes. Aid eligibility, refund routing, bank changes, and fraud flags require stronger assurance.	Legal/financial identity source; FAFSA/ISIR or aid record; fraud flag status; bank account change log; validation method; validation timestamp; assurance level; decision record; reviewer/approver; exception rationale.	Require risk-based assurance escalation. Financial aid and payment decisions should require current, validated, high-assurance attributes and auditable decision records before funds, refunds, or account changes are approved.

Enrollment transformation point	Identity trust risk	Minimum provenance / audit artifacts	ITC governance control
Federation / recovery / fraud exception	Ambiguous claims, account recovery, override requests, or fraud exceptions can bypass normal proofing or propagate low-assurance attributes across trust boundaries.	Assertion audience; attribute release set; identifier type; assurance claim; relying-party purpose; recovery trigger; claimant evidence; re-proofing method; affected systems; incident ticket; post-event review.	Map institutional attributes to explicit federation claims. Treat recovery and exception handling as identity re-proofing events requiring documented authority, revalidation, and auditability.

The matrix can be illustrated through a high-risk financial aid or refund scenario. A fraudulent or compromised user may authenticate to an admissions or student portal, provide self-asserted demographic information, generate LMS activity, and later trigger aid or payment workflows. Under the ITC, these signals would not be treated as equivalent forms of identity trust. Authentication would establish control of an authenticator, LMS activity would serve as corroborating evidence of engagement, and financial-aid or payment decisions would require stronger source authority, proofing records, freshness checks, and permitted-use validation before funds are released or payment attributes are changed.

Discussion

The ITC shows that identity risk in higher education is not confined to a single system or authentication event. It emerges when attributes collected for one purpose are transformed, promoted, federated, or reused for decisions carrying greater risk than the original collection context. The most significant transformation points are CRM intake, CRM-to-SIS promotion, SIS propagation to downstream systems, LMS activity interpretation, financial-aid and payment decisions, federated attribute release, and account recovery or fraud exception handling.

For provenance and auditability, the framework identifies a minimum set of metadata needed to support defensible identity decisions: source authority, assertion method, validation process, timestamp, freshness condition, evidence type, transformation history, assurance state, permitted use, decision record, and exception rationale. These metadata do not require institutions to re-proof every attribute for every action. Rather, they allow institutions to determine whether the assurance attached to an attribute is proportionate to the risk of the decision being made.

The primary governance contribution is the eight-domain ITC model. By combining source authority, provenance, proofing, assurance mapping, federation, identifier governance, continuity and recovery, and exception governance, the framework gives institutions a way to manage student identity as a collection of governed attributes rather than as a flat account record.

Implications for Practice

The ITC provides several practical implications for higher education institutions. First, institutions should inventory the identity attributes used in admissions, financial aid, payment processing, account recovery, LMS access, credentialing, and compliance reporting. Second, high-risk attributes should be assigned authoritative sources and permitted-use categories so that attributes collected for low-risk purposes are not silently reused for higher-risk decisions. Third, CRM-to-SIS promotion should be treated as a trust elevation

event because applicant-supplied attributes may become institutional records once they enter the SIS. Fourth, LMS activity should be treated as corroborating evidence of engagement rather than as primary proof of identity. Fifth, financial-aid, payment, legal identity, and account recovery workflows should include re-proofing triggers when attributes are stale, conflicting, newly changed, or connected to fraud indicators. Finally, continuity and recovery planning should preserve not only accounts and records, but also the provenance, assurance state, and decision history attached to identity attributes.

Limitations and Future Research

This paper presents a standards-informed conceptual framework rather than an empirically validated implementation. The ITC has not been tested through live deployment, institutional case study, or quantitative analysis of fraud reduction. The framework is institution-neutral, meaning that implementation would vary based on institutional size, staffing, vendor ecosystem, data governance maturity, regulatory environment, and risk appetite. The paper did not evaluate specific CRM, SIS, LMS, IdP, financial-aid, or payment platforms, or estimate implementation cost or operational burden. Some institutions may have legacy systems or vendor-managed platforms that limit their ability to capture provenance metadata, assign attribute-level assurance, or preserve decision-use history. For this list of limitations, it also demonstrates a need for a framework that can be broadly applied to complex, diverse environments with similar challenges.

Future research should test the ITC through institutional case studies, expert validation, tabletop exercises, and pilot implementations. A Delphi study with higher education identity, cybersecurity, registrar, financial-aid, and compliance professionals could help refine the framework's domains and minimum metadata requirements. Additional research could develop an ITC maturity model, audit checklist, or implementation guide. Comparative studies could examine how the ITC aligns with or differs from existing identity and access management, identity governance and administration, zero trust, and fraud detection practices in higher education.

Summary

This paper introduced the Identity Trust Chain as a governance framework for attribute-level identity provenance and assurance in higher education enrollment systems. The ITC addresses the gap between authentication-centered security and the broader institutional need to know whether student identity attributes are sourced, validated, fresh, decision-ready, and auditable. By aligning source authority, provenance, proofing, assurance mapping, federation, identifier governance, continuity, and exception response, the framework gives HEIs a practical model for reducing identity-trust risk across the enrollment lifecycle.

The ITC does not claim to eliminate ghost-student fraud, FAFSA-related fraud, or other forms of identity misuse by itself. Instead, it strengthens the institutional conditions needed for fraud prevention, detection, and response. A fraudulent account, suspicious enrollment pattern, payment change, or aid-related flag becomes more actionable when the institution can determine which attributes were trusted, where they came from, how they were validated, when they became stale, and whether they were appropriate for the decision being made. In this way, the ITC helps institutions move from reactive investigation after funds, access, or credentials have already been misused toward earlier intervention at the points where identity trust is created, elevated, propagated, or degraded.

Ultimately, the ITC shifts the institutional identity question from “Can this user log in?” to “Can this attribute be trusted for this decision, at this time, in this system?” That shift is central to fraud-resistant enrollment governance because identity misuse often succeeds not merely through failed authentication, but through weak attribute provenance, over-trusted records, stale assurance, and unexamined reuse of identity data across connected systems.

References

- EDUCAUSE. (n.d.). Identity and access management.
<https://library.educause.edu/topics/cybersecurity/identity-and-access-management>
- Federal Student Aid. (2026, April 15). FAFSA real-time fraud detection. U.S. Department of Education.
<https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2026-04-15/fafsa-real-time-fraud-detection>
- Internet2. (2020, November 2). Baseline expectations for trust in federation. InCommon Federation.
<https://incommon.org/federation/baseline/security-requirements/>
- Moreau, L., Missier, P., Belhajjame, K., B'Far, R., Cheney, J., Coppens, S., Cresswell, M., Gil, Y., Groth, P., Klyne, G., Lebo, T., McCusker, J., Miles, S., Myers, J., Sahoo, S., & Tilmes, C. (2013). PROV-DM: The PROV data model. World Wide Web Consortium.
<https://www.w3.org/TR/prov-dm/>
- Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.CSWP.29>
- REFEDS. (2023). REFEDS Assurance Framework version 2.0. <https://refeds.org/wp-content/uploads/2023/12/RAF-2.0-Final-version.pdf>
- Richer, J. P., Fenton, J. L., Lefkovitz, N., Temoshok, D., Galluzzo, R., Regenscheid, A., & Choong, Y.-Y. (2025). Digital identity guidelines: Federation and assertions (NIST Special Publication 800-63C-4). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-63C-4>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-207>
- Temoshok, D., Choong, Y.-Y., Galluzzo, R., LaSalle, M., Regenscheid, A., Proud-Madruga, D., Gupta, S., & Lefkovitz, N. (2025a). Digital identity guidelines (NIST Special Publication 800-63-4). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-63-4>
- Temoshok, D., Choong, Y.-Y., Galluzzo, R., LaSalle, M., Regenscheid, A., Abruzzi, C., Fenton, J. L., & Lefkovitz, N. (2025b). Digital identity guidelines: Identity proofing and enrollment (NIST Special Publication 800-63A-4). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-63A-4>

- U.S. Department of Education. (2025a, May 28). U.S. Department of Education fights fraud in student aid to protect American taxpayers. <https://www.ed.gov/about/news/press-release/us-department-of-education-fights-fraud-student-aid-protect-american-taxpayer>
- U.S. Department of Education. (2025b, December 11). U.S. Department of Education prevents more than \$1 billion in federal student aid fraud this year, additional crackdowns expected in 2026. <https://www.ed.gov/about/news/press-release/us-department-of-education-prevents-more-1-billion-federal-student-aid-fraud-year-additional-crackdowns-expected-2026>
- U.S. Department of Education, Office of Inspector General. (2024, July 24). Federal Student Aid's actions to mitigate risks associated with the FSA ID account creation process (Report No. F23IT0138). <https://oig.ed.gov/reports/other/summary-report-federal-student-aids-actions-mitigate-risks-associated-fsa-id-account>
- U.S. Department of Education, Office of Inspector General. (2026, February 12). Fraud advisory: Potential fraud involving FAFSA from dependent students with unusual parent data. <https://oig.ed.gov/reports/other/fraud-advisory-potential-fraud-involving-fafsa-dependent-students-unusual-parent-data>
- Yerby, J., & Floyd, K. (2018, August). Faculty and staff information security awareness and behaviors. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 6, No. 1, pp. 23-23).