

Identiverse® 2027 Call for Presentations — Proposal Guidance

Welcome to the Identiverse® 2027 Call for Presentations!

As always, the Identiverse agenda will be community-driven, assembled from proposals submitted by identity professionals like you and selected by our independent Content Committee.

Identiverse has long been known for bringing together practitioners, architects, engineers, business leaders, policymakers, researchers, and innovators from across the digital identity ecosystem. We are looking for presentations that help our audience better understand today's challenges, prepare for tomorrow's opportunities, and learn from the experiences of others.

WHO SHOULD SUBMIT A PROPOSAL?

We welcome proposals from a broad range of perspectives, including:

Identity Professionals

Individuals with first-hand technical, operational, architectural, governance, or implementation experience from real-world identity deployments in the enterprise, public sector, education, healthcare, financial services, and other industries.

Business and Technology Leaders

Professionals responsible for strategy, product direction, organizational transformation, business outcomes, or digital modernization initiatives where identity plays a critical role.

Industry Representatives

Individuals working for technology providers, consultancies, research organizations, standards bodies, or analyst firms. Vendor participation is welcome; however, proposals must focus on industry learning and practical insights rather than product promotion.

Researchers, Policymakers, and Community Leaders

Individuals exploring emerging technologies, governance models, public policy, regulatory developments, social impacts, or future directions for digital identity.

WHAT KIND OF PRESENTATION SHOULD I PROPOSE?

Identiverse offers several presentation formats:

Session Presentations

The foundation of the conference agenda. Sessions are 25 minutes long, including approximately 20 minutes of presentation and 5 minutes of Q&A.

Masterclasses

Longer-form educational sessions that allow presenters to explore a topic in greater depth. Masterclasses are 50 minutes long, including approximately 45 minutes of presentation and 5 minutes of Q&A.

Panel Discussions

Selected panel discussions may be scheduled in masterclass-length slots. Panel proposals should clearly identify the intended panelists and explain why multiple perspectives are necessary for the discussion.

Keynotes and General Sessions

Main-stage presentations are by invitation only and are not part of the Call for Presentations.

Presentations may be delivered by an individual speaker, multiple presenters, or in interview-style formats when appropriate.

To encourage a diverse agenda and focus submissions on presenters' strongest ideas, each individual may submit a maximum of three (3) proposals.

WHAT SHOULD I TALK ABOUT?

Identityiverse attendees consistently tell us they value practical experience, honest lessons learned, thoughtful analysis, and forward-looking perspectives.

We are particularly interested in presentations that:

- Share lessons from real-world deployments
- Explain how identity technologies, standards, or architectures work in practice
- Present original research, data, or industry analysis
- Explore emerging challenges and opportunities
- Examine business, regulatory, operational, or technical implications of identity decisions
- Offer thoughtful, evidence-based perspectives on where the industry is heading

We encourage speakers to discuss not only successes, but also obstacles, failures, trade-offs, and lessons learned along the way.

IDENTIVERSE 2027 CONTENT TRACKS

1. Architecture, Standards & Engineering ("ASE")

This track focuses on how identity technologies and systems are designed, standardized, integrated, and implemented. It covers protocols, architecture patterns, interoperability, platform behavior, engineering tradeoffs, and the practical realities of turning specifications into working systems. This is about the technical machinery of identity itself.

Strong sessions will explain how components fit together, where architectural or protocol assumptions break down, and how design choices affect interoperability, security, scalability, and user experience.

Sessions belong in Identity Infrastructure & Access Control when their primary focus is how authorization or access decisions are modeled, evaluated, delegated, enforced, or audited. If the session is primarily about the design, evolution, implementation, or interoperability of a protocol or standard used to support those functions, it belongs in Architecture, Standards & Engineering.

Focus areas:

- Wallets, verifiable digital credentials, mobile credentials, and passkeys
- Identity system design patterns, including centralized, federated, and decentralized models
- Protocol implementation challenges, including OIDC, OAuth, SCITT, WIMSE, SPICE, and related work
- Browser and platform shifts affecting identity architecture
- Developer experience, tooling, testing, and deployment of identity protocols and components
- Interoperability gaps and implementation tradeoffs
- Standards adoption, deployment challenges, and migration paths
- Technical debt and legacy constraints affecting identity architecture and protocol adoption

2. Consumer Identity & Digital Experience (CID)

This track focuses on customer-facing identity systems: authentication, registration, account recovery, consent, user experience, accessibility, and scale. Sessions should address how organizations design and operate identity journeys for consumers while balancing usability, security, fraud prevention, privacy, and business outcomes.

This is the primary home for CIAM content. Regulation, fraud, and wallets may appear in this track, but only when the session centers on the consumer experience, product design, adoption, or operational impact.

Focus areas:

- Authentication UX and conversion
- Account creation, recovery, and lifecycle
- Cross-device and cross-channel identity journeys
- Wallet and passkey adoption from the user perspective
- Consent and preference management
- Accessibility and inclusion in consumer identity
- Identity orchestration for consumer journeys
- Balancing friction, privacy, fraud prevention, and business outcomes
- Operating consumer identity systems at scale
- Customer trust, retention, and account security

3. Regulated Identity, Privacy & Governance (REG)

This track focuses on identity systems shaped by legal obligations, public policy, assurance requirements, privacy expectations, and formal accountability. Sessions should examine how organizations and ecosystems assign responsibility, establish trust, interpret requirements, and translate regulatory or policy goals into practical identity decisions.

In this track, governance means the structures through which identity programs, credential ecosystems, and data practices are directed and held accountable. It does not mean workforce identity governance and administration, entitlement management, access reviews, or joiner-mover-leaver processes; those belong in Enterprise & Workforce Identity.

Strong sessions should connect regulation, privacy, assurance, liability, or ecosystem governance to concrete choices about system design, data use, legal reliance, operating models, or accountability.

Focus areas:

- Regulatory impacts on identity systems
- Privacy governance and accountable data use
- Data minimization, selective disclosure, and purpose limitation
- eIDAS, age assurance, KYC, AML, mobile credentials, and digital wallets
- Identity proofing, assurance levels, liability, and legal reliance
- Public-sector and public-private identity programs
- Relying-party trust and legal acceptance of digital identity assertions
- Cross-border identity and data-sharing challenges
- Oversight, accountability, and decision-making models for identity programs, credential ecosystems, and trust frameworks
- Organizational accountability, risk ownership, and decision rights
- Aligning standards, regulation, and operational practice
- Internal policies governing identity data, automated identity decisions, assurance, and privacy-sensitive uses of AI
- Measuring whether privacy, assurance, and accountability mechanisms work in practice

4. Enterprise & Workforce Identity (EWI)

This track focuses on identity for employees, contractors, partners, administrators, developers, and other workforce users. Sessions should address the realities of managing enterprise identity across complex organizations, including lifecycle management, access governance, federation, SaaS sprawl, privileged access, and Zero Trust initiatives.

This track should prioritize practical enterprise experience. Strong sessions will address organizational constraints, legacy systems, integration challenges, and lessons learned from real deployments.

Focus areas:

- Workforce IAM, including SSO, lifecycle management, identity governance and administration, access reviews, and entitlement management
- SaaS sprawl and identity orchestration
- Zero Trust implementations and lessons learned
- Developer, administrator, and privileged identity
- Enterprise federation realities
- Joiner, mover, leaver processes
- Identity governance and administration
- Managing identity across mergers, acquisitions, reorganizations, and distributed workforces
- Enterprise identity modernization
- Workforce identity metrics, ownership, and operating models

5. Identity Threats, Fraud & Trust Signals (TFT)

This track focuses on attacks against identity systems and the signals, controls, and response practices used to detect, prevent, and reduce harm. Sessions should examine identity-centered threats across consumer, workforce, and machine environments, with attention to both technical defenses and the economics of abuse.

This track combines identity security operations and fraud because many real-world attacks now cross those boundaries. Account takeover, phishing, session hijacking, synthetic identity, bot activity, deepfakes, and signal abuse all affect trust decisions. Strong sessions should connect the threat, the signal, the decision, and the operational response.

Focus areas:

- Account takeover, synthetic identity, and impersonation

- Session hijacking, token theft, and phishing-resistant authentication
- Identity threat detection and response
- Bot detection, abuse prevention, deepfakes, and liveness
- Signals, telemetry, behavioral analysis, and risk scoring
- Signal sharing ecosystems
- Incident response, forensics, and red/blue team lessons
- Fraud decisioning and adaptive controls
- Economics of fraud, including cost, friction, liability, and user harm
- Trust signals across consumer, workforce, and machine identity
- Recovery after identity compromise
- Measuring the effectiveness of detection and response programs

6. Identity Infrastructure and Access Control (IAC)

This track focuses on the decisions that determine what a person, workload, service, application, or agent is allowed to do. It covers authorization policy, access-control models, policy evaluation and enforcement, workload and non-human identity, delegation, secrets, and the infrastructure used to make and enforce access decisions across applications, APIs, cloud environments, and distributed systems.

Strong sessions will address how access decisions work in practice: where policy is defined, what identity and contextual information informs a decision, where evaluation and enforcement occur, how authority is delegated, and how decisions can be tested, explained, and audited.

The central question for this track is usually: who or what is allowed to do what, and how is that decision made or enforced? Sessions centered primarily on protocol design, standards development, interoperability, or general identity-system architecture belong in Architecture, Standards & Engineering.

Focus areas:

- Authorization models, including RBAC, ABAC, PBAC, and ReBAC
- Policy engines and externalized authorization
- Workload identity, including SPIFFE, service accounts, and non-human identities
- Runtime enforcement and access decision points
- Secrets management
- Delegation models for humans, services, workloads, and agents
- Access control for APIs, microservices, and cloud-native environments

- Policy lifecycle management and testing
- Auditing and explaining access decisions
- Infrastructure patterns for scalable, maintainable access control

7. Deployments & Leading Practices (DEP)

This track focuses on what worked, what failed, and what others can learn from real identity deployments. Sessions should be grounded in practical implementation experience and should include measurable outcomes, concrete lessons, or specific operational findings.

This track should be one of the primary homes for enterprise speakers. It should favor candid case studies over polished product stories. Strong sessions will explain the problem, the constraints, the decisions made, what broke, what changed, and what the organization would do differently next time.

The distinguishing feature of this track is that the value of the session comes from the experience and lessons of the deployment itself.

Focus areas:

- Case studies with measurable outcomes
- Migration stories, including passwords to passkeys and federation to wallets
- Build vs. buy decisions
- Organizational lessons from identity programs
- Failure analysis: what broke and why
- Deployment planning and sequencing
- Change management and adoption
- Identity modernization in complex environments
- Lessons from pilots, rollouts, and failed initiatives
- Metrics used to evaluate identity program success

8. Identity Strategy, Markets & Futures (SMF)

This track examines the business, economic, and strategic forces reshaping identity. Sessions should focus on how identity leaders make decisions amid changing market incentives, platform shifts, regulatory pressure, emerging technologies, and long-term infrastructure change.

This track should not become a dumping ground for speculative technology talks. Strong sessions should explain why a market, technical, regulatory, or ecosystem shift matters for identity decision-makers and what organizations should do in response.

Focus areas:

- Identity cost models and investment decisions
- Identity as a revenue driver, risk control, or cost center
- Vendor and platform market shifts
- Browser and platform control over identity flows
- Decentralization vs. centralization tradeoffs
- Identity and payments convergence
- Wallet ecosystems, marketplaces, and network effects
- Agentic systems, delegation, and future authorization models
- Long-term infrastructure shifts affecting identity architecture
- Build, buy, partner, or wait decisions
- Strategic planning for uncertain or immature identity technologies
- Market, regulatory, and ecosystem forces changing identity strategy

9. Professional Skills & Leadership (PSL)

This track focuses on the human, organizational, and leadership skills required to make identity programs successful. Sessions should address how identity professionals build influence, communicate tradeoffs, lead teams, work across functions, and grow their careers.

The emphasis should be on practical leadership within identity, not generic career advice. Strong sessions will help attendees become more effective inside their organizations and communities.

Focus areas:

- Building, scaling, and developing IAM teams
- Working across security, product, engineering, legal, compliance, and business stakeholders
- Standards participation, community engagement, and professional influence
- Communicating identity risk, cost, and tradeoffs to different audiences
- Leading identity programs through organizational change

- Career development paths for identity professionals
- Mentorship, hiring, retention, and skills planning
- Building credibility and influence without formal authority
- Translating technical identity issues for executives and non-technical stakeholders
- Developing the next generation of identity leaders

AI AND DIGITAL IDENTITY

Artificial intelligence is transforming nearly every area of digital identity. Rather than treating AI as a standalone topic, Identiverse considers it a cross-cutting theme that touches nearly every track.

We welcome proposals exploring the impact of AI on identity systems, security, governance, fraud, customer experience, business strategy, workforce identity, authorization, and related areas. Submit your proposal to the track that best reflects its primary focus.

WHAT DO I NEED TO PROVIDE?

Please have the following information ready:

- Presenter photograph (minimum 500 × 500 pixels)
- Presenter biography (150 words maximum)
- Presentation title
- Presentation abstract
- Additional supporting information that may help the Content Committee evaluate the proposal
- Bio and profile information for any co-presenters
- Bio and profile information for proposed panelists, if submitting a panel

CONTENT GUIDELINES

Identiverse is a professional conference for identity practitioners.

Attendees expect educational, informative, and thought-provoking content. They do not expect product demonstrations, sales presentations, or marketing pitches.

Vendor participation is welcome and encouraged, but accepted presentations must focus on lessons learned, industry insights, implementation experience, research findings, or technical education rather than product promotion.

All accepted presentations are subject to content review prior to the conference and will be expected to use the conference slide template.

HOW ARE PROPOSALS EVALUATED?

The Identiverse Content Committee is composed of experienced practitioners, architects, strategists, researchers, and industry leaders from across the identity ecosystem.

Proposals are evaluated based on factors such as:

- Relevance to the conference audience
- Quality and clarity of the proposal
- Originality and uniqueness
- Practical value and educational content
- Speaker expertise and perspective
- Fit within the overall conference program

The committee also strives to create a balanced agenda that reflects a broad range of experiences, viewpoints, industries, and voices.

IMPORTANT DATES

- CFP Opens: October 1st 2026
- CFP Closes: January 11th 2027
- Proposal Reviews: January 2027
- Acceptance Notifications: February 2027
- Agenda Publication: March 2027
- Conference: June 2027

WHAT HAPPENS IF MY PROPOSAL IS SELECTED?

Accepted speakers will receive additional information about presentation requirements, conference templates, content reviews, and deadlines.

All accepted presentations participate in a content review process designed to help speakers deliver the strongest possible session and ensure a high-quality experience for attendees.

Depending on presentation type and speaker category, presenters may receive discounted or complimentary conference registration.

Please note that Identiverse does not reimburse travel or accommodation expenses.

We look forward to seeing your ideas and helping shape another outstanding Identiverse agenda.

WAITLISTED PROPOSALS

Each year, the Content Committee identifies a small number of additional proposals that it would like to include in the conference if space becomes available. These proposals may be designated as waitlisted rather than accepted or declined.

Waitlisted proposals are not rejections. They are presentations the committee believes would be valuable additions to the agenda, but for which scheduling constraints, track balance, or other program considerations prevented immediate acceptance.

Should a slot become available before the conference, waitlisted proposals may be invited into the agenda. In some cases, waitlisted speakers may also be eligible for conference registration benefits normally associated with accepted presentations.