

About the Open Identity Summit

The **Open Identity Summit 2027** aims to connect diverse perspectives from academia, industry, and public administration to advance the state of digital identity, privacy, and trust. Identity Management (IDM) forms a cornerstone of secure, trustworthy digital infrastructures, thereby laying the foundation for trustworthy digital interactions.

Open standards, interoperable interfaces, and open-source technologies continue to define the IDM landscape. They are key enablers of secure and user-centric solutions in domains such as digital payments, e-health, e-government, manufacturing, AI data governance, and IoT ecosystems. While today's solutions already ensure authenticity, integrity, and confidentiality, emerging challenges demand new approaches to **transparency, accountability, user control, and privacy protection**.

The Summit welcomes interdisciplinary contributions that combine technical innovation with socio-technical insight, usability research, and empirical studies. We particularly encourage submissions addressing real-world deployments, governance frameworks, and open collaboration models in digital identity.

Researchers, practitioners, and policymakers are invited to submit papers presenting novel concepts, practical experiences, and theoretical foundations. Contributions may be:

- **Full papers** (up to 12 pages, excluding references)
- **Short papers** (up to 8 pages, excluding references)

All submissions will be peer-reviewed (double-blind) and, upon acceptance, published in the **GI-Edition** "Lecture Notes in Informatics (LNI)", indexed in *Scopus*. Please use the LNI template for your submissions, which can be found at https://gi.de/service/publikationen/lni/.

The LNI series is a peer-reviewed scientific publication channel ranked level 1 in the Norwegian publication channel list: kanalregister.hkdir.no/en/tidsskrift?id=469934

Previous conference's proceedings can be fond open access with the publisher: https://dl.gi.de/search?spc.page=1&query=open%20identity%20summit

Topics of Interest

Topics of interest include but are not limited to:

- Technical Foundations of Identity Management
- Governance and Regulation
- Cyber security, Trust Frameworks, Privacy Aspects
- Applications and Use Cases
- Human and Societal Dimensions
- Open Source and Collaborative Innovation
- Resilience of Identity Management

A more detailed list of topics of interest can be found at the end of the CfP below.

Organization and Committees

Conference Chairs

- Nurul Momen (Oslo Metropolitan University), nurul.momen@oslomet.no
- Lothar Fritsch (Oslo Metropolitan University), lotharfr@oslomet.no
- Heiko Roßnagel (Fraunhofer IAO), heiko.rossnagel@iao.fraunhofer.de
- Christian Schunck (Fraunhofer IAO) christian.schunck@iao.fraunhofer.de

Local Organisation

- Nurul Momen (Oslo Metropolitan University), nurul.momen@oslomet.no
- Lothar Fritsch (Oslo Metropolitan University), lotharfr@oslomet.no

The **program committee** is listed on: https://openidentity.eu/

Important Dates

- Paper Submission Deadline: **31st January 2027**
- Notification of Acceptance: **31st March 2027**
- Submission of Camera-Ready Copies: **23rd April 2027**

Detailed List of Topics of Interest

Technological Foundations and Security of Digital Identity

- Authentication protocols; federated, decentralized, and self-sovereign identity systems
- Verifiable credentials, digital wallets (e.g., EU Digital Identity/ Business Wallet)
- Trust infrastructures and machine-readable governance
- Cybersecurity of digital identity systems: resilience, risk, and counterintelligence
- Standards and interoperability for IDM and trust services
- Quantum-safe and post-quantum identity management

Governance, Privacy, and Trust Frameworks

- Privacy, unlinkability, and auditability in IDM systems
- Transparency, accountability, and user intervenability
- Zero Trust architectures and secure access management
- Certification, accreditation, and compliance of trust services
- Long-term preservation and evidential value of electronic data
- Legal and international aspects of digital identity governance
- Role of AI in identity management (e.g., fraud detection, deep fakes)

Applications and Domain-Specific Use Cases

- Secure credential systems and electronic attestations
- Identity and access management for IoT, OT, Industry 4.0, and critical infrastructure
- Digital identity in healthcare and clinical settings
- Identity and trust management in e-government and cross-border services
- Identity and trust management for AI agents

Human and Societal Dimensions of Digital Identities and IDM

- Usability, accessibility, and human factors in identity and trust systems
- Social engineering, identity fraud, and human-centered security
- Acceptance, adoption, and digital literacy in identity ecosystems
- Socio-economic and regulatory implications of digital identity frameworks

Open Source and Collaborative Innovation

- Open-source components and frameworks for identity, trust, and security
- Governance, interoperability, and assurance of open-source IDM projects
- Business models for open source in regulated environments (e.g., EUDI Wallets)
- Experiences and case studies from open-source communities and initiatives

Resilience of Identity Management

- Robustness of IDM-Infrastructure
- Strategies and Procedures for Post-Attack Recovery