PST 2027
Privacy, Security & Trust





2027 24th Annual International Conference on Privacy, Security and Trust (PST 2027)

August 25–27, 2027, Sheffield, United Kingdom

https://pstnet.ca

Hosted by
University of Sheffield, UK
Organized with
PST Network & Canadian Institute for Cybersecurity, UNB

Committees
General Co-Chairs
Prosanta Gope
University of Sheffield, UK
Weizhi Meng
Lancaster University, UK
TPC Co-Chairs
Rongxing Lu
Queen's University, Canada
Syed Rafiul Hussain
Pennsylvania State University, USA
Steering Committee Chair
Ali Ghorbani
University of New Brunswick, Canada
Advisory Committee
Biplab Sikdar
National University of Singapore
Security Track Co-Chairs
Aryan Pasikhani
Zhou Li
Privacy Track Co-Chairs
Behzad Abdolmaleki
Alessandro Brighente
Trust Track Co-Chairs
Imtiaz Karim
Zengpeng Li
Emerging Tech Co-Chairs
Neetesh Saxena
Daisuke Mashima
Publication Co-Chairs
Xichen Zhang
Yongqiang Cheng
Publicity Co-Chairs
Shancang Li
Meltem Kurt Pehlivanoğlu
Workshop & Tutorial Chair
Jinku Li
Poster Chair
Mahshid Delavar
Sponsorship Co-Chairs
Jack Miskelly
Sridhar Adepu
Artifact Evaluation Co-Chairs
Fei Hongming
Yang Yang
Local Chair
Andrei Popescu
Web Chair
Michael Mills

Scope of the Conference

The 24th Annual International Conference on Privacy, Security and Trust (PST 2027) provides a premier forum for researchers, practitioners and industry experts to share advances in cybersecurity research and security applications. PST 2027 will be hosted by the University of Sheffield at The Diamond, Sheffield, United Kingdom, from August 25 to 27, 2027. The programme features one industry day followed by two days of keynotes and technical presentations on privacy, security and trust, together with a special track on Emerging Technologies and Trends. The conference is held in person, and speakers who are unable to travel may present remotely.

Papers are solicited in three main tracks, **Privacy, Security and Trust**, and in the **Emerging Technologies and Trends** special track. Topics of interest include, but are not limited to:

- Access Control and Capability Delegation
- Anonymity and Privacy vs. Accountability
- Biometrics, National ID Cards, Identity Theft
- Cloud Security, Web Security and Privacy
- Critical Infrastructure Protection
- Cryptographic Technologies
- Digital Forensics
- Digital Rights Management
- Generative AI Security, Privacy and Trust
- Human Computer Interaction and PST
- Identity and Trust Management
- Lawful Surveillance: Implications and Technologies
- Internet of Things (IoT) Security and Privacy
- Intrusion Detection / Prevention Technologies
- Network and Wireless Security
- PST in Practice, Society, Policy and Legislation
- Operating Systems Security
- Post-Quantum Cryptography
- Privacy Preserving / Enhancing Technologies
- Privacy, Traceability and Anonymity
- PST Challenges in e-Health, e-Government, e-Commerce
- Quantum Cryptography beyond QKD
- Quantum Key Distribution (QKD) Protocols
- Recommendation, Reputation and Delivery Technologies
- Secure Software Development and Architecture
- Security Analytics and Data Mining
- Security and Privacy in Blockchain and its Applications
- Trust and Reputation in Self-Organizing Environments
- Technologies for Building Trust in e-Business
- Zero-Day Vulnerabilities, Continuous Authentication

Submission of Papers

High-quality original papers that are not under review and have not been published or accepted for publication elsewhere are invited. Regular papers may be up to 10 pages and short papers up to 6 pages, including references and appendices, in the standard IEEE two-column conference format. Up to 2 additional pages are allowed in each category with over-length charges. Authors must select the track (Privacy, Security or Trust) most relevant to their work. Reviewing is **double-blind**: submissions must be properly anonymized, with no author names, affiliations or acknowledgments, and self-citations in the third person. At least one author of each accepted paper must register for the conference and present the paper.
Submission Web Site: https://easychair.org/conferences/?conf=pst2027

Publication

All submissions will be peer reviewed by the Technical Program Committee for originality, significance, relevance, technical quality and clarity. Accepted regular and short papers will be published in the conference proceedings. Accepted papers will be posted for review, pending approval. An optional Artifact Evaluation process allows accepted papers to earn IEEE reproducibility badges (Available, Reviewed, Reproducible). Selected papers will be recommended, after significant extension, for special issues of SCI-indexed journals.

Contact

PST 2027 Organizing Committee, University of Sheffield, Sheffield, United Kingdom
https://pstnet.ca

Important Dates

April 10, 2027	Paper submission due
June 7, 2027	Author notification
June 16, 2027	Early-bird registration
August 25–27, 2027	Conference & workshops