The Second International Conference on Cross-Domain Security in Distributed, Intelligent and Critical Systems
CROSS-SEC 2027
March 7 - 11, 2027 - Barcelona, Spain

http://www.iaria.org/conferences2027/CROSS-SEC27.html

www.iaria.org

Important deadlines:

Submission (full paper)	November 16, 2026
Notification	January 3, 2027
Registration	January 17, 2027
Camera ready	January 31, 2027

Tracks:

Security Foundations and Architectures

- Trust frameworks, access control, and zero-trust models
- Governance, compliance, and security management
- Secure design for distributed systems
- Security in virtualised, containerised, or Cloud-native environments
- Identity and access across hybrid/multi-clouds
- Monitoring and observability for threat detection

Database Security

- Secure architectures for relational and non-relational databases
- Access control, encryption, and key management, Multitenant scenarios
- Threats and defenses against injection, inference, and data leakage
- Privacy, compliance, and secure data lifecycle management

IoT, OT, and Critical Infrastructure Security

- Security for edge, fog, and hybrid architectures
- Security for IIoT, smart home, and smart grid protection
- Firmware updates, device onboarding, and identity provisioning
- Threats and countermeasures in critical infrastructure systems
- Forensics in constrained environments
- Future-proof crypto life-cycle in long-lived devices

Artificial Intelligence and Security

- AI for threat and anomaly detection
- Attacks on AI: adversarial, poisoning, model theft
- Robust and trustworthy AI systems
- Privacy-preserving machine learning

Cryptographic and Privacy-Enhancing Technologies

- Post-quantum cryptography and migration
- Homomorphic encryption, secure multiparty computation
- Scalable identity and key management
- Blockchain or distributed ledgers for integrity and coordination
- Crypto-agility by design and secure reconfiguration

Application Domains and Human Factors

- Cybercrime analysed via culture, linguistics, history, and ethics
- Security in health, energy, mobility, public sector
- Usability and awareness in secure systems