Security Standardisation Research Conference 2023
@ Eurocrypt 2023, Lyon, France – 22-23 April 2023
ssresearch2023.github.io

* * * Call for Papers * * *

Papers offering research contributions to the area of security standardisation are solicited for submission to the SSR 2023 conference. SSR also invites Systematisation of Knowledge (SoK) papers and vision papers relating to security standardisation. Papers may present theory, applications or practical experience in the field of security standardisation, including, but not limited to:

Access control	History of standardization	Privacy regional and
Biometrics	Identity management	international standards
Blockchain	Industrial control systems security	RFID tag security
Cloud computing security/privacy	Internet of things security/privacy	Risk analysis
Critical national infrastructure protection	Internet security	Secure messaging
Standards consistency and	Interoperability of standards	Security controls
comparison critiques of standards	Intrusion detection	Security management
Cryptanalysis	Key management and PKIs	Security protocols
Cryptographic protocols	Standardisation process management	Security services
Cryptographic techniques	Mobile security	Security tokens
Data protection and law/regulation	Network security	Smart cards
Digital trust	Open standards and open source	Telecommunications security
Evaluation criteria	Payment system security	Trusted computing
Formal analysis of standards	Post-quantum security	Usability
		Web security

Submitted papers must comply with the guidelines communicated on the SSR 2023 website. In particular, they must be original, unpublished, anonymous and not concurrently submitted, written in English and at most 23 pages in Springer LCNS format incl. references, but not counting appendices. Accepted papers will be published via Springer's Lecture Notes in Computer Science (LNCS).

Important dates

Submission deadline:	5 January 2023	
Author notification:	9 February 2023	
Conference:	22–23 April 2023	(Eurocrypt: 23–27 April 2023)

Program committee

Nina Bindel (SandboxAQ)
Joppe Bos (NXP Semiconductors)
Sofía Celi (Brave)
Gareth T. Davies (Bergische Universität Wuppertal)
Jean Paul Degabriele (Cryptography Research Center, TII)
Benjamin Dowling (University of Sheffield)
Marc Fischlin (TU Darmstadt)
Scott Fluhrer (Cisco Systems)
Felix Günther (PC Chair; ETH Zurich)
Britta Hale (Naval Postgraduate School)
Julia Hesse (PC Chair; IBM Research - Zurich)
Christian Janson (TU Darmstadt)
Saqib A. Kakvi (Royal Holloway, University of London)
John Kelsey (NIST)
Markulf Kohlweiss (University of Edinburgh / IOHK)
Thalia Laing (HP Inc.)

Giorgia Azzurra Marson (NEC)
Catherine Meadows (Naval Research Laboratory)
Chris Mitchell (Royal Holloway, University of London)
Elisabeth Oswald (University of Klagenfurt)
Kenneth Paterson (ETH Zurich)
Christopher Patton (Cloudflare)
Bertram Poettering (IBM Research - Zurich)
Kazue Sako (Waseda University)
Stanislav Smyshlyaev (CryptoPro)
Christoph Striecks (AIT Austrian Institute of Technology)
Thyla van der Merwe (Google, Zurich)
Mathy Vanhoef (Katholieke Universiteit Leuven)
Gaven J. Watson (Meta)
Christopher Wood (Cloudflare)
Kazuki Yoneyama (Ibaraki University)