STPPA#4 Welcome

Cryptographic Technology Group
National **I**nstitute of **S**tandards and **T**echnology

November 21, 2022 @ Virtual meeting

Special **T**opics on **P**rivacy and **P**ublic **A**uditability (STPPA) event #4

Hosted by the **P**rivacy-**E**nhancing **C**ryptography (PEC) project

This short presentation

1. **The STPPA series**
2. **Today's event**
3. **Attendance**
4. **The PEC project**
5. **Resources**

Special Topics on Privacy and Public Auditability (STPPA)

Series of half-day events with talks and/or panel(s)

- Emphasis on **privacy-enhancing cryptography** (PEC) tools
- Topics relating to **privacy** and **public auditability** (and their duality)
- **Content:** basic technical background; research questions; applications.
- **Reference material:** record talks and panels to support further reflection
- **Recurring:** a series of events will cover the role of diverse PEC tools

https://csrc.nist.gov/projects/pec/stppa

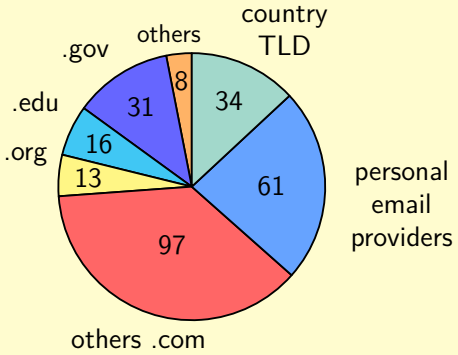
Today's event: STTPA#4 (October 31, 2022)

Featured topics: anonymous credentials, blind signatures, private authentication

- 09:00–09:10: ***STPPA#4 Welcome.*** (Eastern Daylight Time: UTC-4)
- 09:10–09:55: ***Anonymous Credentials***
  Anna Lysyanskaya (Brown University, USA)
- 09:55–10:40: ***Blind Signatures: Past, Present, and Future.***
  Julian Loss (CISPA, Germany)
- 10:40–10:55: Break
- 10:55–11:40: ***Challenges and New Features for Anonymous Credentials: Revocation and Decentralization.***
  Foteini Baldimtsi (George Mason University, USA)
- 11:40–12:30: ***Panel: PEC for privacy and public auditability.***
  Panelists: All speakers. Moderators: the PEC team.

Video-conference logistics/registrations

- **Virtual registrations:** 260
  (To be updated after the event)
- **Video:** Audio and video are being recorded (posting will be announced in PEC-forum)
- **Questions:** Attendees can use the virtual Q&A (to be considered as time permits)



The Privacy-Enhancing Cryptography (PEC) project

- A project within the NIST Cryptographic Technology Group (CTG).
- **PEC:** broadly refers to **c**ryptography (that can be) used to **e**nhance **p**rivacy.

Goals:

1. Accompany the progress of emerging PEC tools [emphasis on non-standardized tools]
2. Develop reference material that can support the use of crypto to enable privacy.
3. Preliminary work on evaluating the potential for standardization of PEC tools.

(Tools $\approx$ primitives, protocols, techniques, technologies)

https://csrc.nist.gov/projects/pec/

PEC webpage resources

PEC webpage

https://csrc.nist.gov/projects/pec/

STPPA subpage

https://csrc.nist.gov/projects/pec/stppa

Webpage within the NIST Computer Security Resource Center (CSRC)

Thank you for your attention!

We welcome feedback/questions about ongoing PEC activities:

- Join the PEC forum: https://csrc.nist.gov/projects/pec/email-list
- PEC project email: crypto-privacy@nist.gov
- STPPA specific email: pec-stppa@nist.gov
- PEC website: https://csrc.nist.gov/projects/pec
- STPPA resources: https://csrc.nist.gov/projects/pec/stppa
- The PEC team: Luís Brandão, René Peralta, Angela Robinson

Enjoy today's STPPA event