




Update on Privacy Engineering Program and Privacy Enhancing Technologies Updates



NIST Privacy Engineering Program

Presented by Naomi Lefkowitz

Privacy Framework



Total Downloads

124,246



Top 10 Countries

USA
Canada
U.K.
India
Australia
Brazil
Germany
Netherlands
Japan
China

Presentation Title



Top 3 Resources

PF/CSF Crosswalk
PF/GDPR Crosswalk
PF/27701 Crosswalk

NIST Privacy Workforce Public Working Group (PWWG)



Over 900 members from around the world



Currently drafting content for the
NIST Privacy Workforce Taxonomy



3 Project Teams active

Integrating Privacy Guidance

- Draft SP 800-60, Revision 2, Guide for Mapping Types of Information and Systems to Security Categories
- Draft SP 800-50, Revision 1, Building a Cybersecurity and Privacy Learning Program
- Draft SP 800-63-4, Digital Identity Guidelines
- Final SP Cybersecurity Practice Guide, 1800-22, Bring Your Own Device will be published in August



The US-UK PETs Prize Challenges 2023



Financial Crime

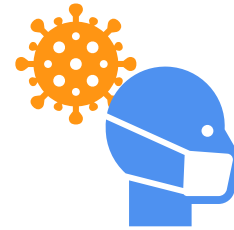
Task: Develop privacy-preserving federated learning solution to detect potentially anomalous payments

Given:

- Transaction information
- Bank account flags

Predict:

Probability of transaction being fraudulent



Public Health

Task: Develop privacy-preserving federated learning solution to forecast an individual's risk of infection

Given:

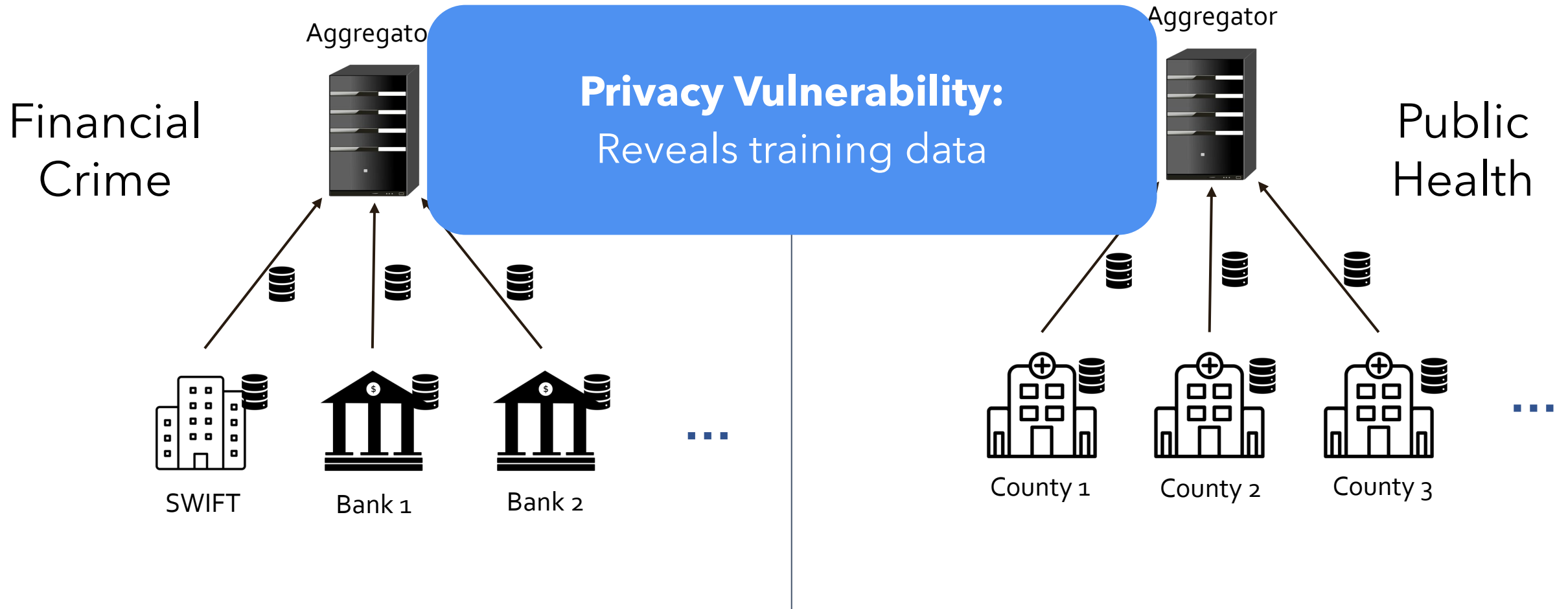
- Demographic information + location/activity
- Population Contact Network (up to time t)
- Infection status (up to time $t-7$ days)

Predict:

Probability of individual x being infected at time t

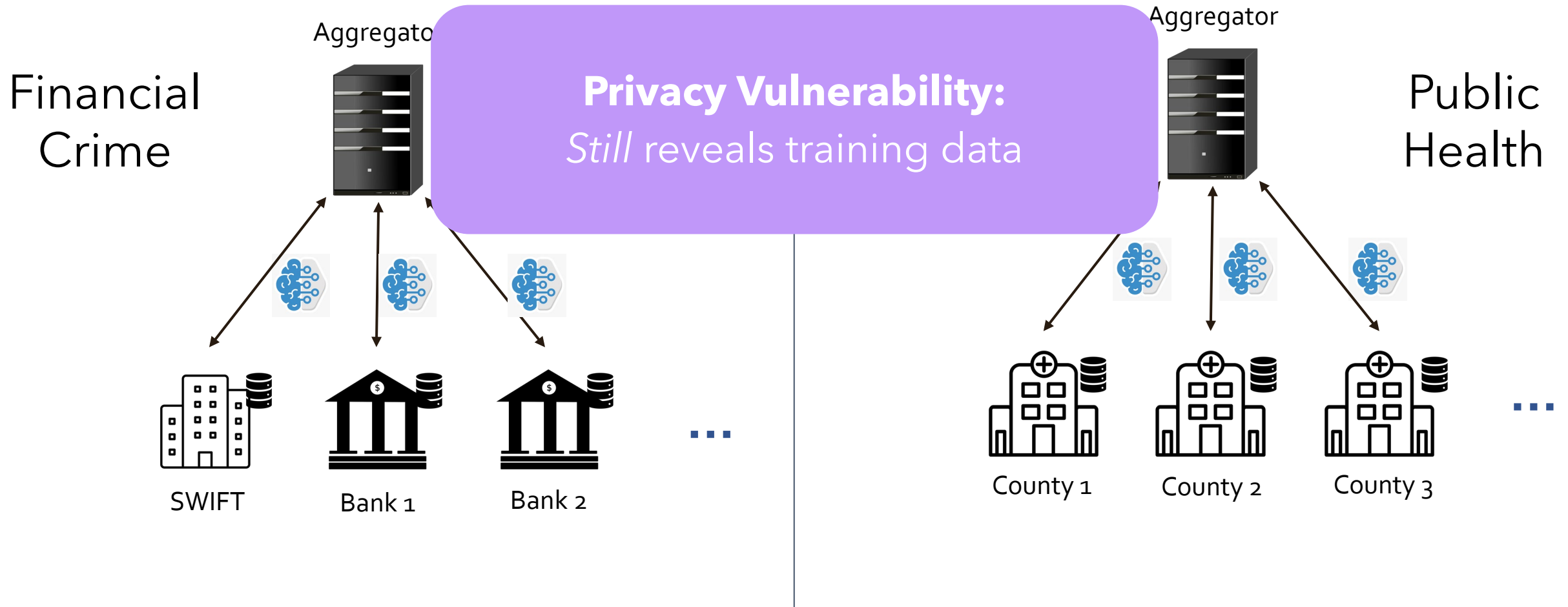
Centralized Learning

Participants send data to aggregator, who trains model

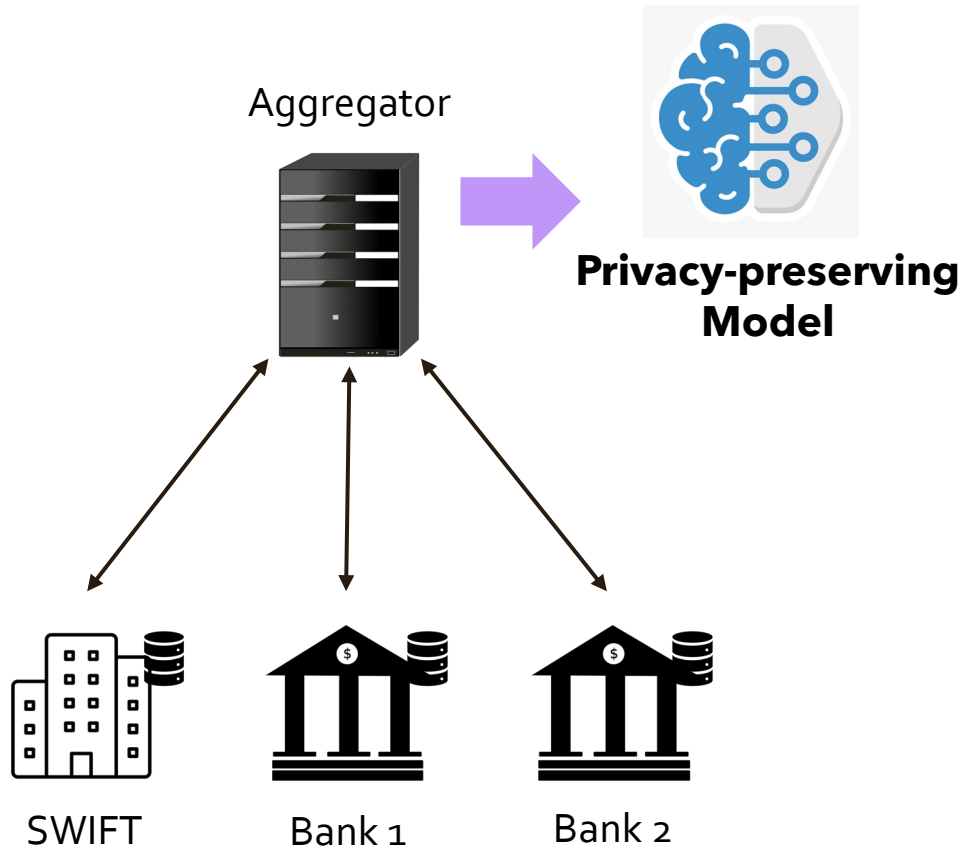


Federated Learning

Participants send *model updates* instead of data



Privacy-Enhancing Technologies for Federated Learning



Input Privacy



Hide model updates *during training*

Output Privacy



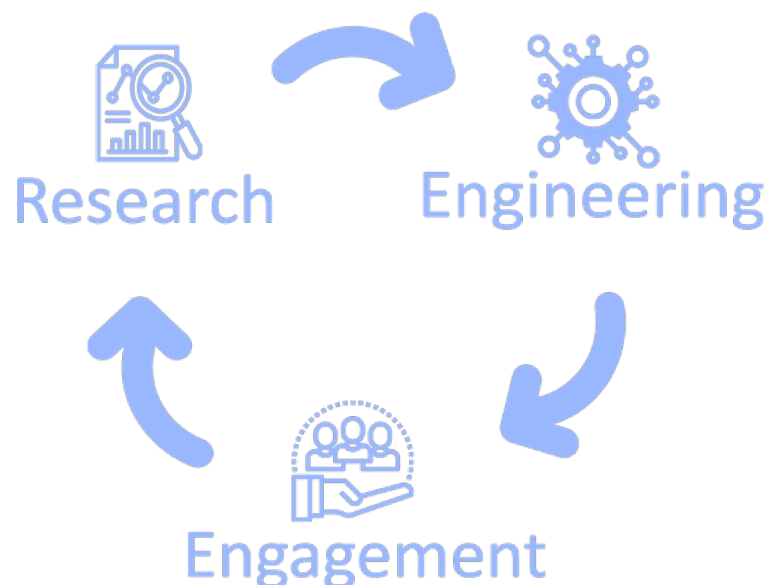
Prevent privacy attacks on trained models

Challenge goal:

Drive development of *practical PETs* for federated learning

Collaborative Research Cycle

Community challenge to evaluate de-identification algorithms

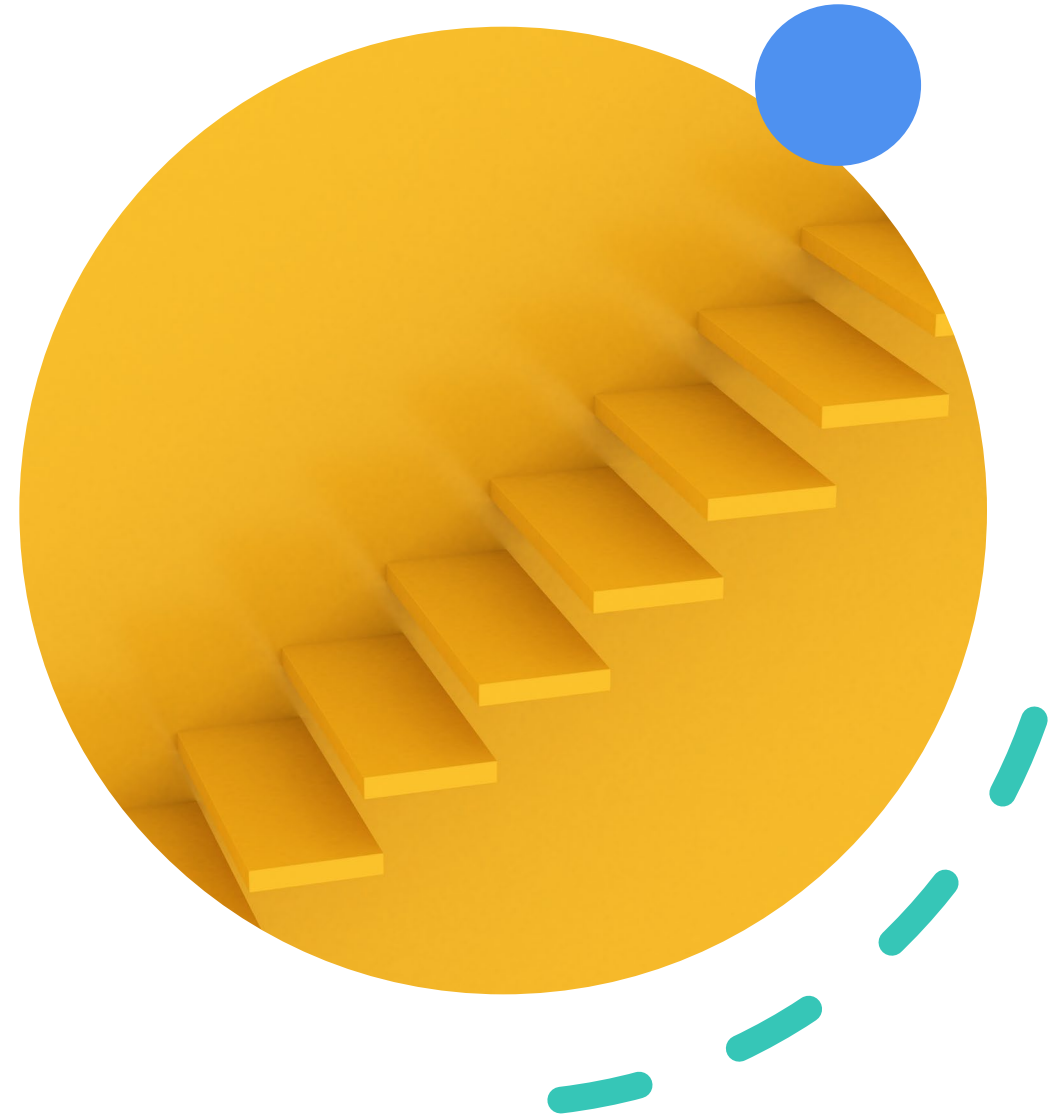


- NIST released 'Diverse Communities Excerpt Data'
- Research community submits deidentified instances
- NIST evaluates deidentified data quality and releases the data and reports for research
- > 320 submissions using many types of techniques (e.g., differential privacy, synthetic data, statistical disclosure limitation)
- Hosting a workshop in November for research results



Next Steps

- Finalize and publish the PWWG taxonomy in early 2024 following a public comment period.
- Identify and support PETs pilots
- Update SP 800-30, *Guide for Conducting Risk Assessments*, to include privacy risk assessments



Resources



Websites

<https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering>
<https://www.nist.gov/privacyframework>



Mailing List

[List.nist.gov/privacyframework](https://list.nist.gov/privacyframework)



Contact Us

Privacyeng@nist.gov
PrivacyFramework@nist.gov
[@NISTcyber](#) [#PrivacyFramework](#)



Update on Privacy Enhancing Technologies

Presented by Angela Robinson

Privacy Enhancing Technology

Privacy-enhancing technologies (PETs) enable utility/power of private data without

- disclosing the underlying data
- risking deanonymization of underlying data owners

General categories

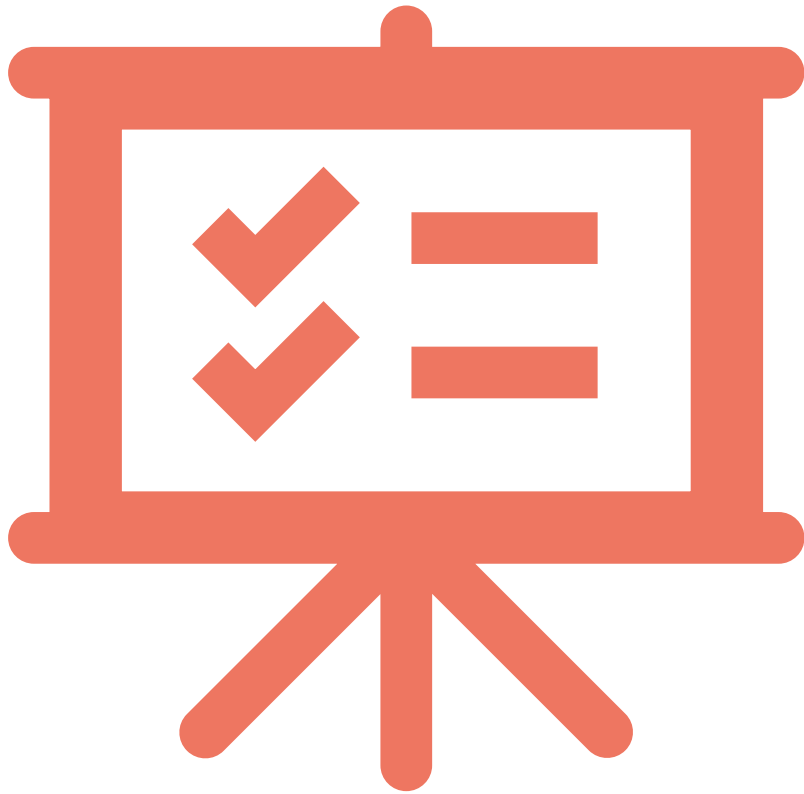
- Data masking approaches
- **Cryptographic approaches**
- Access control techniques

Privacy-Enhancing Cryptography project

Goal: accompany the progress of emerging technologies in the area of PEC and promote the use of cryptographic protocols that facilitate privacy goals

- Various tools of interest:
 - Zero-knowledge proofs (ZKP)
 - Secure multiparty computation (SMPC)
 - Fully homomorphic encryption (FHE), private set intersection (PSI), etc.
- Development of reference material
- Preliminary work on evaluating the potential for standardization of PEC tools

Special Topics on Privacy and Public Auditability



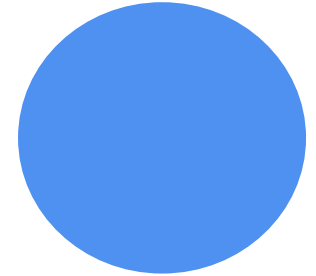
- Virtual seminar series that focuses on various PEC tools
- Initiated in January 2020
- Features presentations by SMEs and panel discussions
- All slides and video recordings available at https://csrc.nist.gov/Projects/pec/st_ppa

STPPA #6

Focus: Community efforts on various advanced cryptography techniques (ZKP, MPC, FHE, ABE)

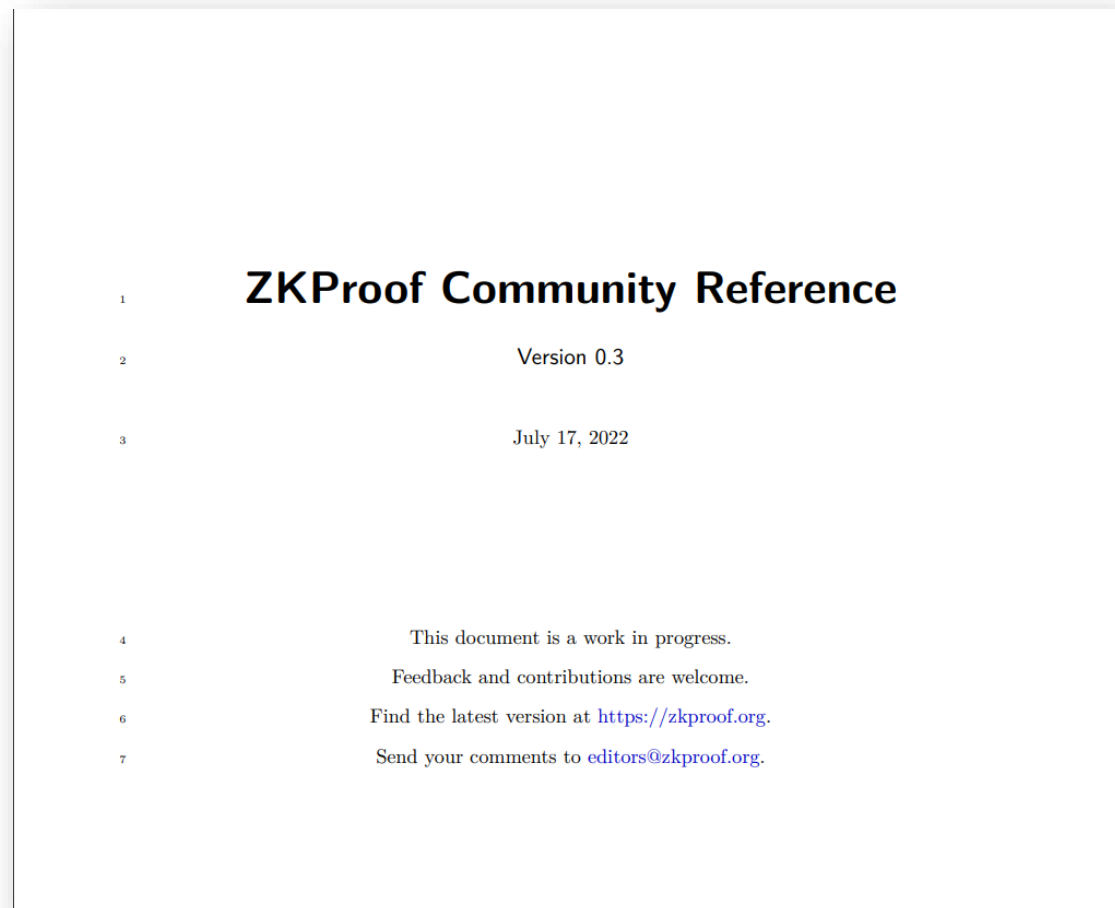
- ZKProof.org
- HomomorphicEncryption.org
- MPCAlliance
- ETSI on development of ABE standards
- ISO on development FHE standards

Scheduled for July 25, 2023. Event is free, registration required



Collaboration with ZKProof

- ZKProof: “an open industry/academia initiative to mainstream ZKP cryptography.”
- Annual workshops, with state-of-the-art proposals and presentations
 - Various talks from NIST-PEC
 - Working groups (developing standardization proposal).
- NIST-PEC collaboration since 2019, supporting the development of open reference material





Distributed trust

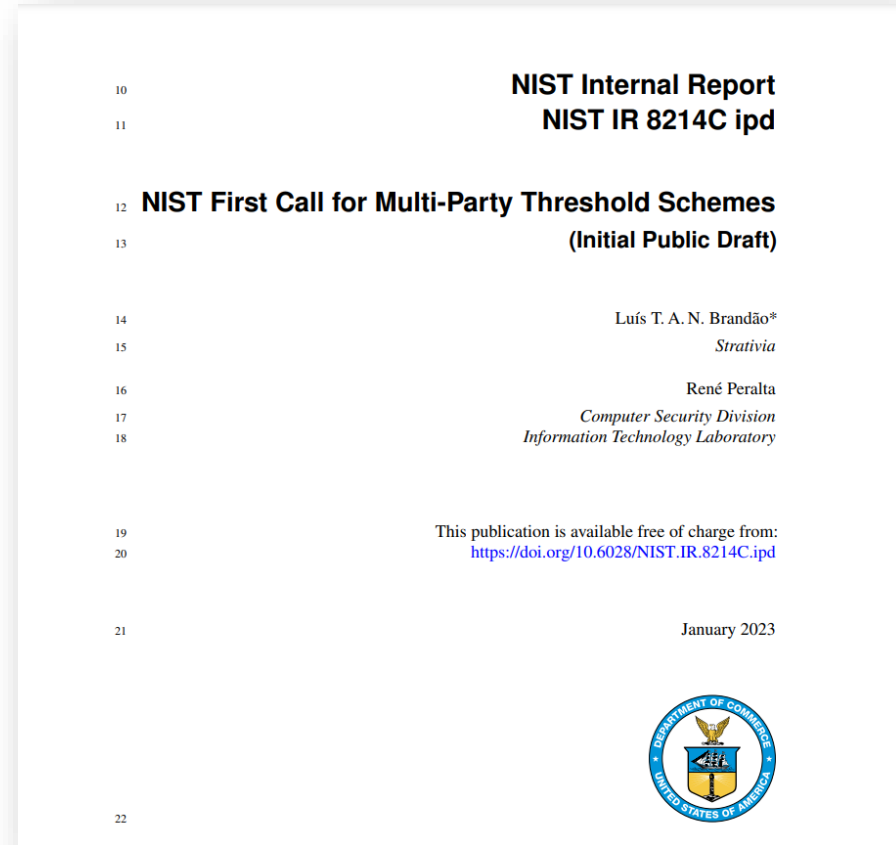
Solves the problem of individual untrustworthiness but trustworthy subsets

Distributed trust

Solves the problem of individual untrustworthiness but trustworthy subsets

Call for threshold schemes includes solutions which use:

- FHE
- SMPC





Summary

Pre-(NIST)-standards approach to PETs:

- Accompany progress and development of PETs
- Development of reference material
- Initial focus on threshold algorithms

NIST PEC Project

Webpage: <https://csrc.nist.gov/Projects/pec>

Contact the PEC team: crypto-privacy@nist.gov

PEC Forum: pec-forum+subscribe@list.nist.gov

