Privacy-enhancing cryptography at NIST

Luís Brandão and René Peralta [1]

[1]National Institute of Standards and Technology (Gaithersburg MD, USA)

Presented at the 2nd ZKProof Workshop
April 11, 2019 (Berkeley, USA)

Contact email: crypto-privacy@nist.gov

Outline

1. Crypto Standards at NIST
2. Privacy-Enhancing Crypto
3. Our perspective on ZKProof
4. Conclusions

Outline

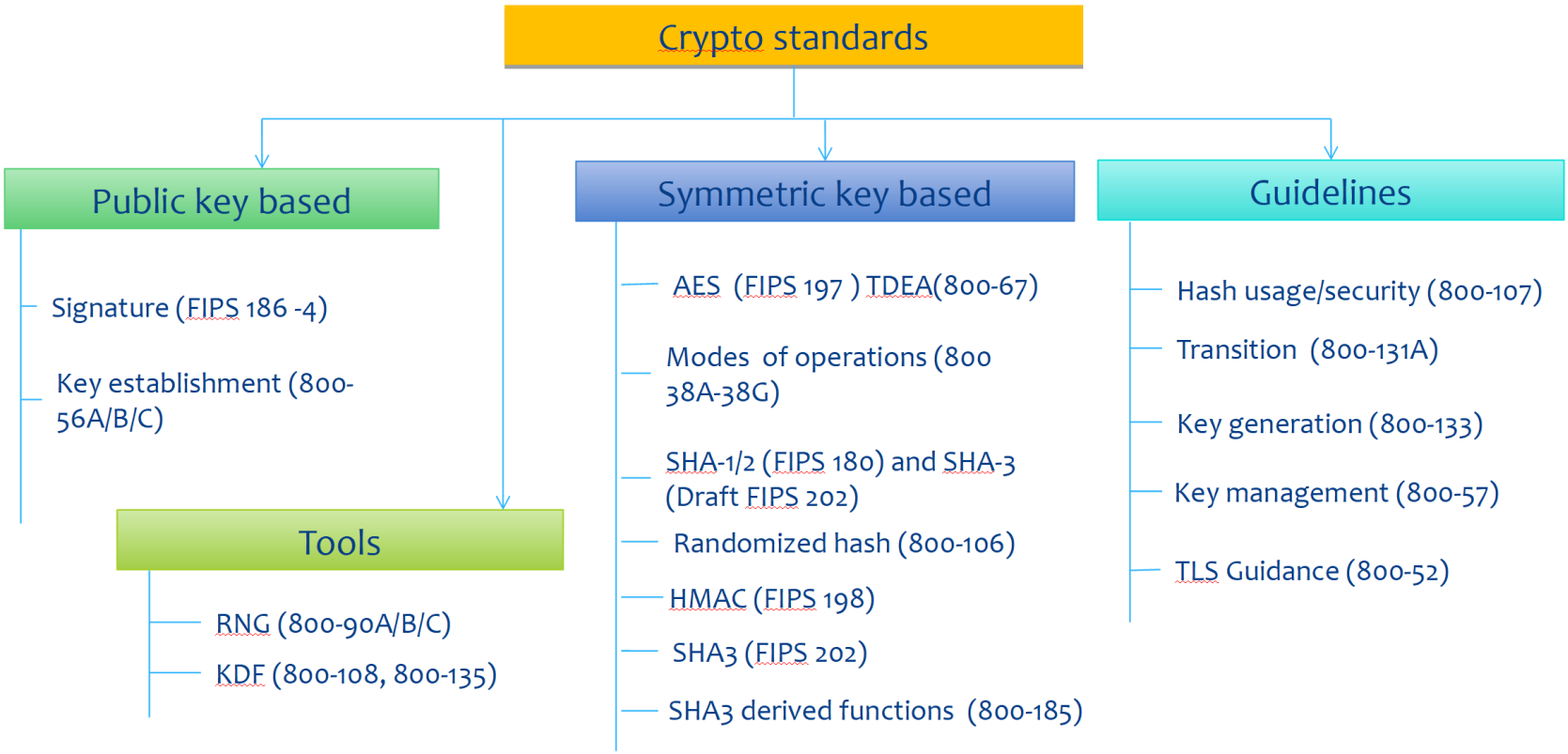
Some history

- 1977: FIPS 46 "Data Encryption Standard (DES)"
- 1990s: Public–key Cryptography (FIPS 186, SP 800-56A/56B)
- 2001: FIPS 197 "Advanced Encryption Standard (AES)"
- Dual_EC_DRBG episode
- 2015: FIPS 202 "SHA-3" (Secure Hash Function 3)
- Ongoing standardization projects
  - Post-Quantum Cryptography (PQC)
  - Lightweight Cryptography (LWC)
  - Threshold Cryptography

Several approaches

- Cryptographic algorithm competitions.
  - Advanced Encryption Standard (AES).
  - Secure Hash Algorithm – 3 (SHA-3).
- Adopt standards from other standardization organizations.
- Develop new standards.
  - In-house development based on well-accepted research results (e.g. SP 800-56C).
  - Selected among submissions (e.g. modes of operations in SP 800-38 series).
- Not a competition, but based on call for submissions.
  - PQC, LWC.
- Open to other approaches...

Overview of NIST Crypto Standards



(1) This is not a complete list

Privacy at NIST

NIST Privacy Framework

https://www.nist.gov/privacy-framework

- Envisioned to be a voluntary enterprise risk management tool to help organizations manage individuals's privacy risk
- Drafting the NIST Privacy Framework: Workshop #2 in Atlanta, May 13–14

Data de-identification challenges

e.g. https://www.herox.com/UnlinkableDataChallenge/community

Privacy-enhancing Cryptography. This presentation.

Outline

The NIST PEC project

Privacy-Enhancing Cryptography (PEC):
https://csrc.nist.gov/Projects/Privacy-Enhancing-Cryptography

- It's been dormant ... now getting revived.
- Fundamental role for SMPC and zero-knowledge proofs.
- An important goal: develop useful **reference materials**.

Reference materials

In order to

- **Assess** the state of things in a particular area.
- **Motivate** real-use applications or proofs of concept.
- **Frame** development of standards and future discussions.
- **Enable** interoperability for companies doing things now.

Reference materials

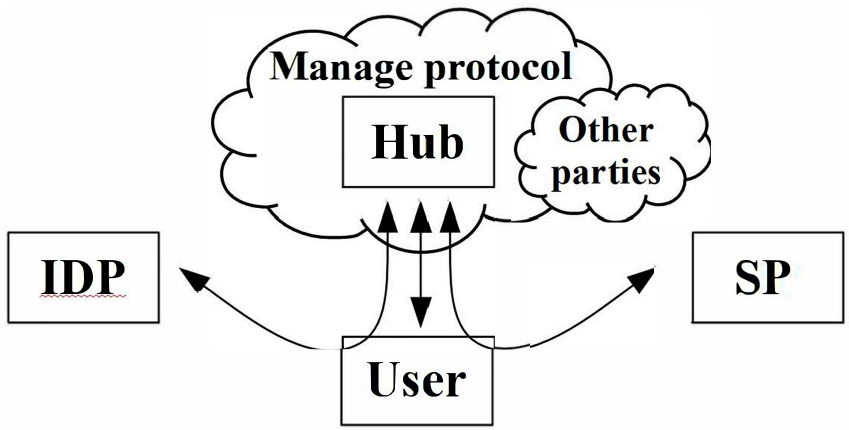
In order to

- **Assess** the state of things in a particular area.
- **Motivate** real-use applications or proofs of concept.
- **Frame** development of standards and future discussions.
- **Enable** interoperability for companies doing things now.

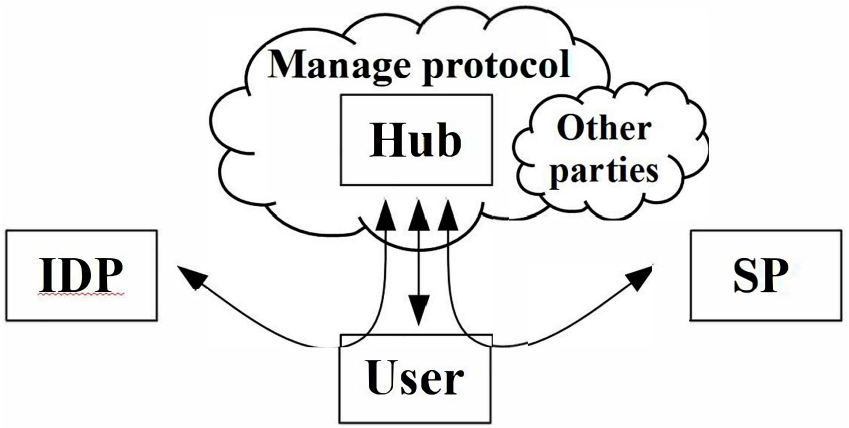
Context is PEC use-cases:

- Brokered identification
- "Students' right to know"
- Privacy-preserving public auditability

Use-case: Brokered identification in FCCX (1/2)

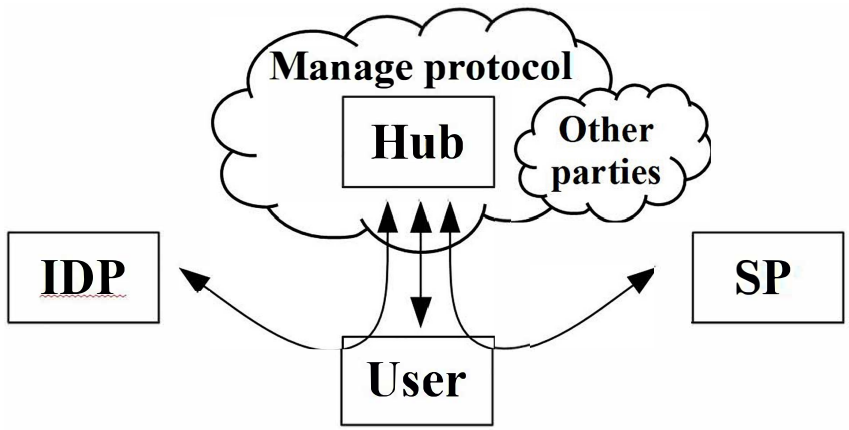


Use-case: Brokered identification in FCCX (1/2)



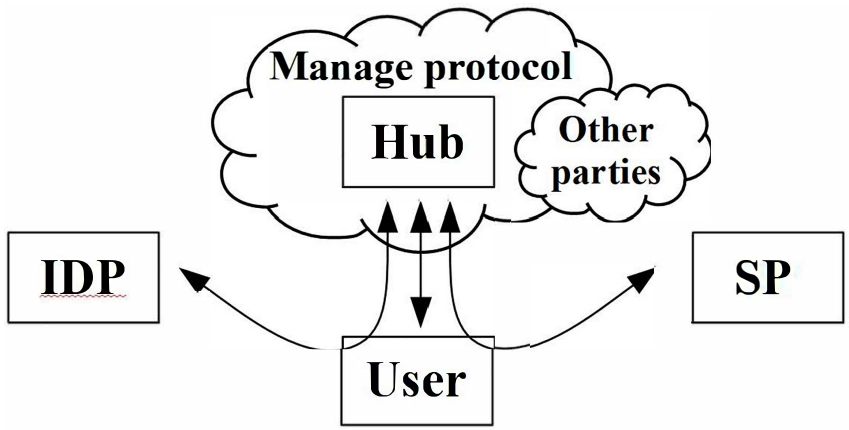
- Why this example? It relates to privacy; relates to the identity framework use-case in the ZKProof docs.

Use-case: Brokered identification in FCCX (1/2)



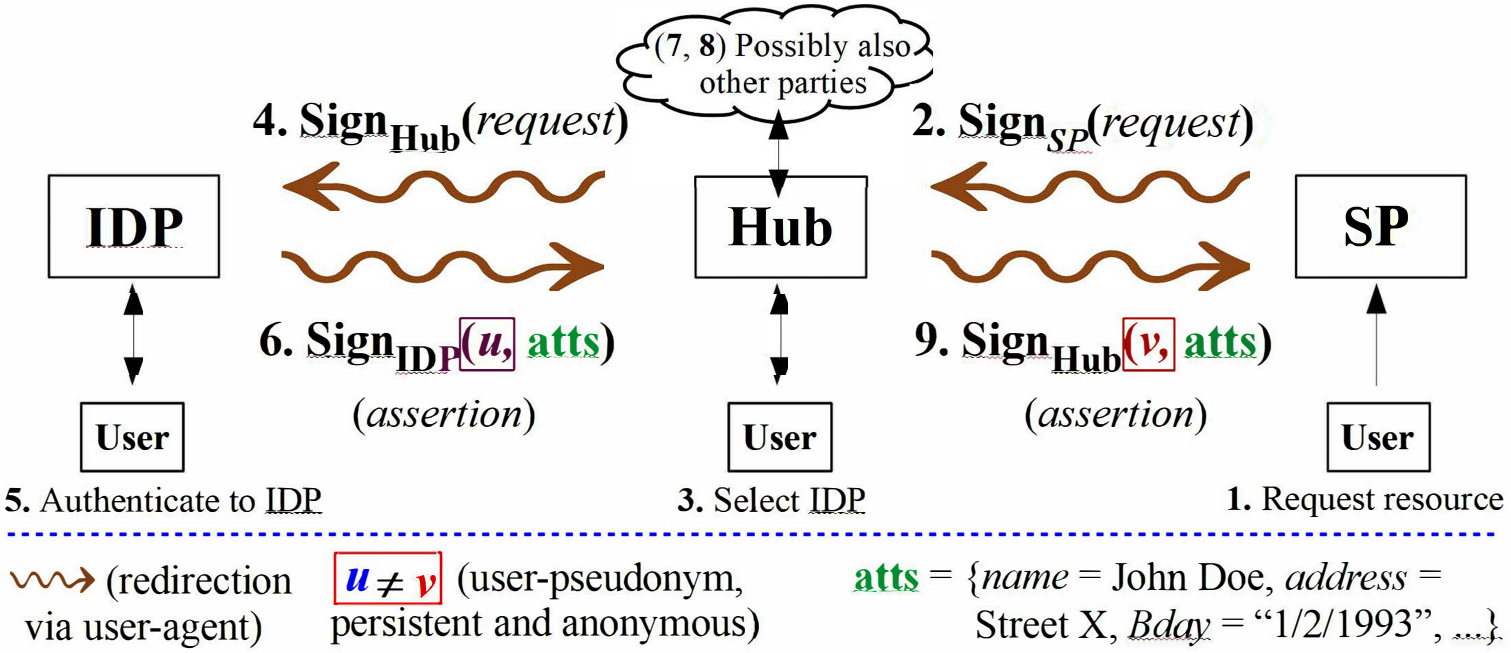
- Why this example? It relates to privacy; relates to the identity framework use-case in the ZKProof docs.
- **Design constraints** in place: mostly-passive user; broker must exist. (We can't always chose the optimal solution paradigm)

Use-case: Brokered identification in FCCX (1/2)

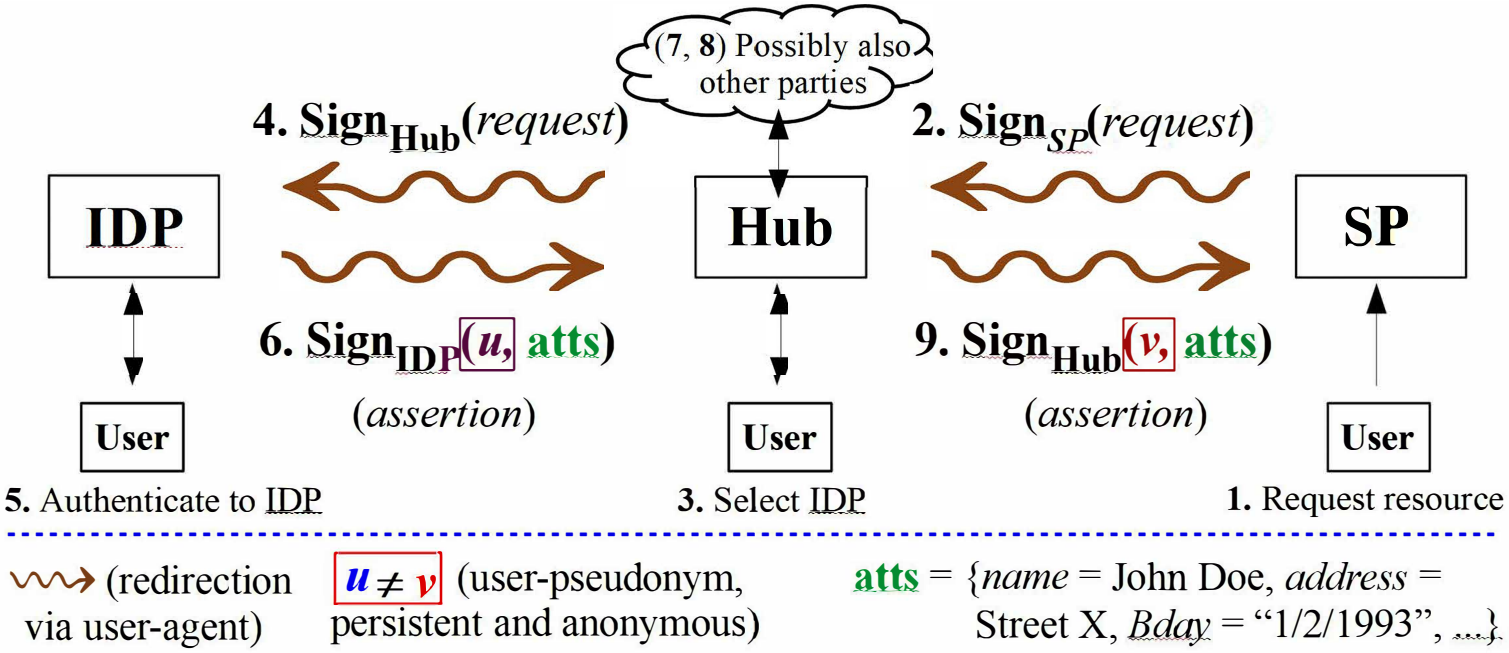


- Why this example? It relates to privacy; relates to the identity framework use-case in the ZKProof docs.
- **Design constraints** in place: mostly-passive user; broker must exist. (We can't always chose the optimal solution paradigm)
- Not enough privacy-preserving **reference material** for engineers.

Use-case: Brokered identification in FCCX (2/2)



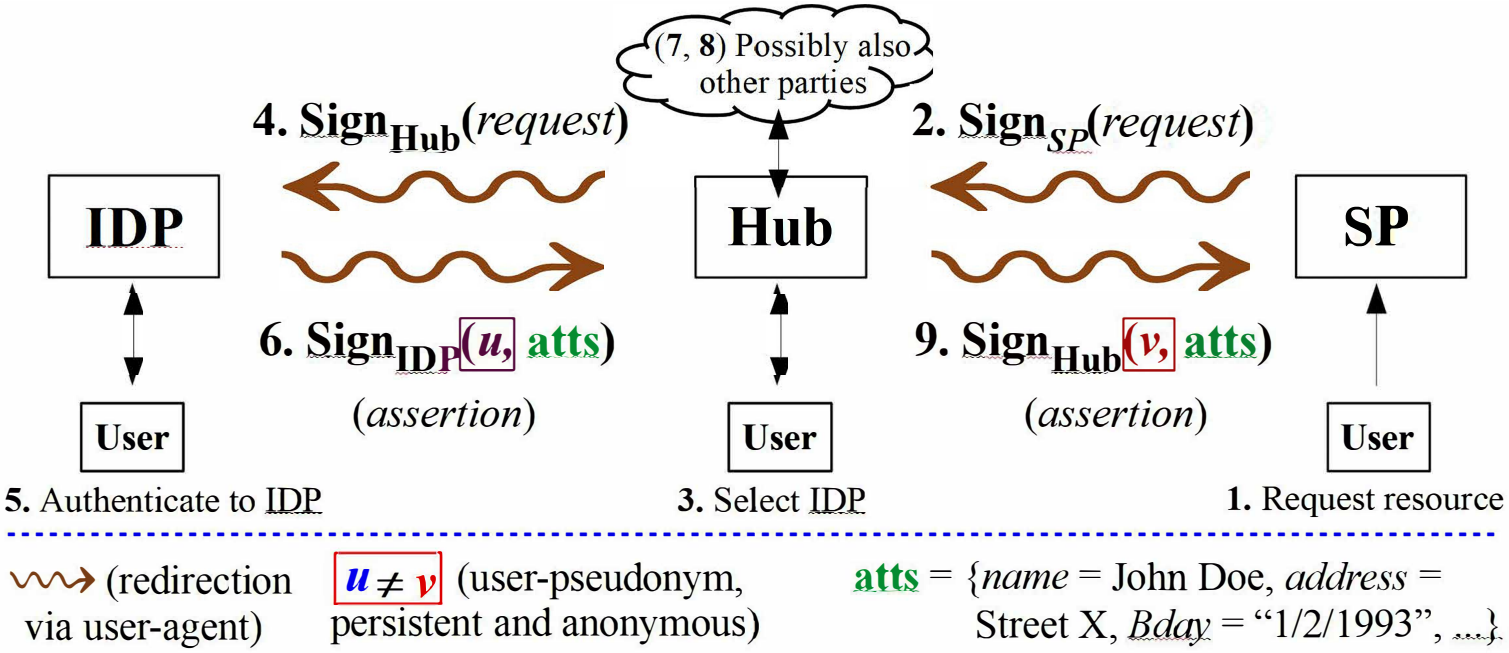
Use-case: Brokered identification in FCCX (2/2)



The "National Strategy for Trusted Identities in Cyberspace" wanted privacy properties for this, e.g.:

- End-to-end encrypted attributes
- Unlinkability of user-transactions by the Hub

Use-case: Brokered identification in FCCX (2/2)



The "National Strategy for Trusted Identities in Cyberspace" wanted privacy properties for this, e.g.:

- End-to-end encrypted attributes
- Unlinkability of user-transactions by the Hub

PEC can solve it ... but even a simple (semi-honest) Diffie-Hellman Key-Exchange was beyond vendors' capabilities.

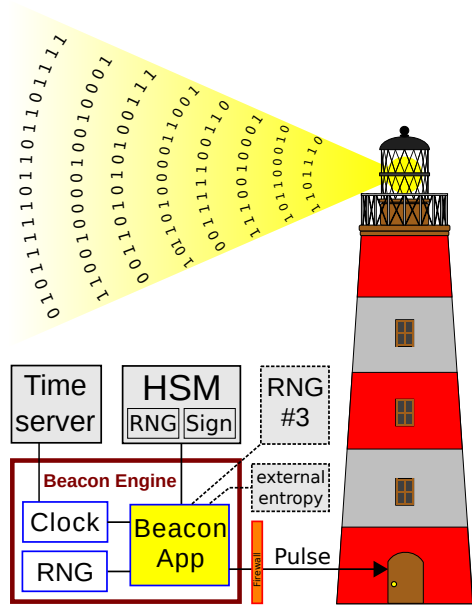
Use-case: Student's right to know

- Proposal to mandate the use of SMPC to calculate the monetary return on student's investment on education.
- Data is distributed among several entities. Because of privacy concerns, these entities cannot share the data.
- https://www.govtrack.us/congress/bills/116/s681/text

Use-case: public-auditability with randomness

The NIST Randomness Beacon

- Broadcasts a randomness pulse every 60 seconds
- Each pulse commits to a fresh 512-bit random string
- Each pulse is time-stamped and signed by NIST
- Hash-chained pulses for an immutable public record
- Cryptographic fields support strong trust assurance



Public randomness facilitates public auditability of randomized processes.

Enhancing them with privacy-preserving properties is a matter of PEC.

Research in multiplicative complexity (MC)

- Reference circuits for AES
- MC is relevant for ZK, SMPC, ..., since usually XOR gates are free and ANDs are expensive
- Intention to develop a circuit file format

Outline

ZKProof assessment

Our perspective of the ZKProof initiative:

- ZKProof is well within the reference materials approach
- Documentation can evolve to a useful reference
- Recent engagement: LaTeX porting, propose developing a reference, sent comments

ZKProof assessment

Do conceivable use-cases fit within the process being developed?

- Good scenario: spend time building things, and they turn out to be useful in achieving myriad functionalities.
- Bad scenario: spend 10 years on something and not enable something we now know is important.

Outline

Final Remarks

- NIST is interested in crypto development and interoperability
- That is achieved via standards and reference material
- NIST PEC wants to keep up to date with, and support, external initiatives
- NIST PEC is interested in supporting ZKProof

Thank you for your attention

The PEC team is

- Luís Brandão
- René Peralta
- Angela Robinson

email : crypto-privacy@nist.gov