Overview of NIST Cryptographic Standards Development Processes

Andy Regenscheid

NIST

Outline

- Standards development processes
  - Overview of current processes
  - Example: SHA-3 Competition and Standardization
- Crypto Program Review
  - Review of Standards Development Process
  - Review of Existing Crypto Standards and Guidelines
  - Example: NIST Elliptic Curves
- Open Discussion

Who We Work With

- ***Researchers***
  - Development of new algorithms/modes/schemes
  - To advance science of cryptography
- ***Industry***
  - On adoption of strong cryptographic algorithms
  - Feedback mechanism on standards
- ***Standards Organizations***
  - Adoption and development of new standards
- ***Government***
  - Core user community
  - Collaboration with NSA on standards and guidelines

Principles

- *Transparency*
- *Inclusivity*
- *Balance*
- *Integrity*
- *Technical Merit*
- *Continuous Improvement*

Standards and Guidelines

- Types of Standards and guidelines
  - Algorithm specifications
  - General guidance on use of cryptography
  - Guidelines in application-specific areas
- Publications
  - Federal Information Processing Standards
  - 800-Series Special Publications
  - NIST Interagency Reports
  - ITL Bulletins

Standards Development Processes

- International Competitions
  - Engage community through an open competition
  - *e.g., AES, SHA-3*
- Adoption of Existing Standards
  - Collaboration with accredited SDOs
  - *e.g., RSA, HMAC*
- Development of New Standards
  - Used if no suitable standard exists
  - e.g., DRBGs

Public Review and Outreach

- Solicit public feedback on draft standards
- Public workshops and forums
- Involvement in Standards Development Organizations
- Engaging community at industry/academic conferences, meetings, and other events

Discussion

- What kind of changes should be make to our program?
- How can be better engage the community?
  - Academia
  - Standards Development Organizations
- Improvements to development procedures

Break

SHA-3

NIST Cryptographic Standards Process Review

Andy Regenscheid

NIST

Process Review & Update

- Document and publish NIST process
- Invite public comment on NIST process
- Independent evaluation to review the process ands to suggest improvements
- NIST will update process as necessary to:
  - Maximize openness and transparency
  - Support the development of the most secure, trustworthy guidance practicable
  - Maintain confidence of all stakeholders

Review of Existing Work

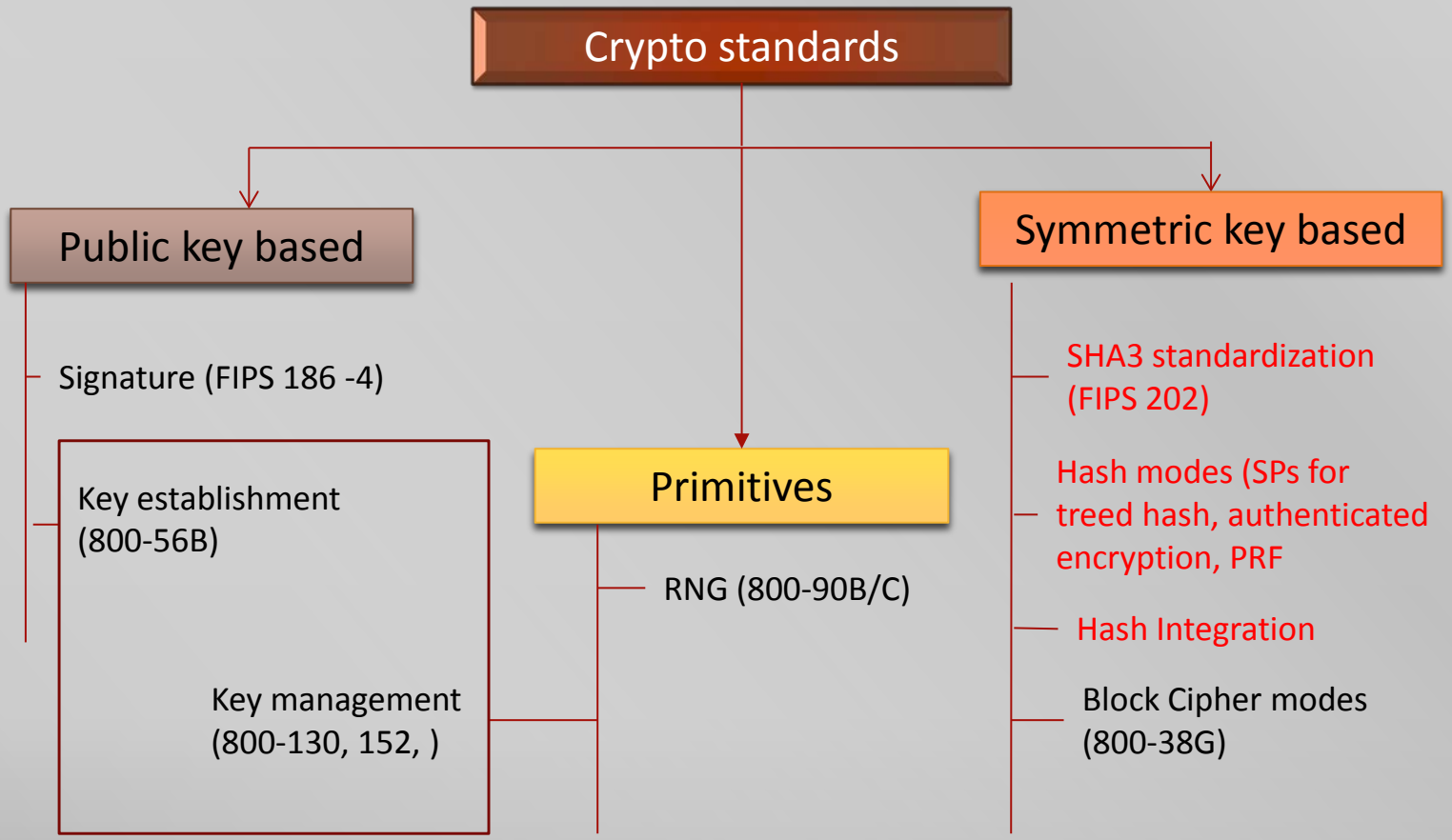
- NIST will also review existing body of cryptographic work and the process through which it was developed
- NIST will invite new public comments and withdraw standards or guidance that do not meet these standards

Discussion

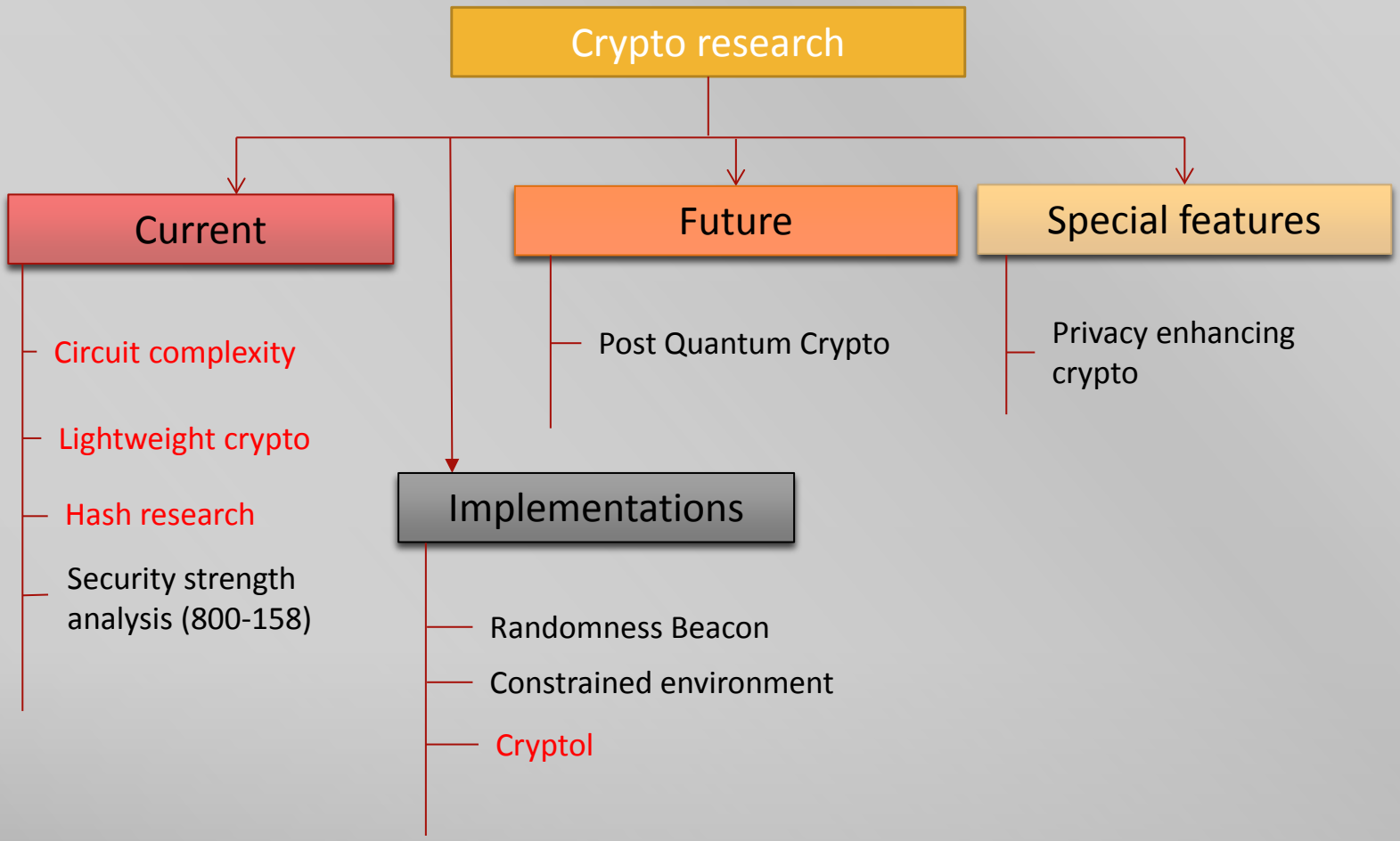
- Feedback on strategic approach
- Implementation of the review
  - How should we conduct the review?
  - What should be in scope?
  - Who should we involve?
- What other steps should we take?

Backup Slides

Crypto Standards



Crypto Research



Crypto Applications