Preliminary announcement on 2020-Aug-14
(Typo correction on 2020-Aug-27)

NIST Workshop on Multi-Party Threshold Schemes (MPTS 2020)

Virtual event, November 4–6, 2020, 9am–1pm EST

Organized by the Threshold Cryptography project @ NIST, Gaithersburg USA

Register online at https://csrc.nist.gov/events/2020/mpts2020

We expect to have a preliminary program schedule available in September.

For questions or comments related to the workshop, please send an email to MPTS-2020@nist.gov.

Deadlines:

- September 30: early registration (free)
- September 30: *briefs* submission (title + short abstract)
- October 28: late registration (conditions TBA)

The workshop in a nutshell

The MPTS 2020 workshop is intended as an informal consultation step about the development of criteria for evaluating multi-party threshold schemes for the cryptographic primitives identified in NISTIR 8214A. The organizers are asking the community of stakeholders to participate by providing examples, suggestions and recommendations for the multi-party track of the standardization process considered by the NIST Threshold Cryptography (TC) project. The collected feedback will be taken into consideration in the development process.

- **What:** NIST workshop on multi-party threshold schemes.
- **Goal:** Collect feedback for the multi-party track of the TC project.
- **How:** Invited *talks* (~20 min each) + Q&A; and submitted *briefs* (~5 min).
- **Logistics:** Participation by video-conference; free attendance based on early registration.
- **When:** November 4–6 (3 days, up to 4 hours per day).

Primitives[*] (see NISTIR 8214A, Section 4.1):

- (1) RSA signing, (2) decryption, (3) keygen;
- (4) EdDSA signing;
- (5) ECDSA signing;
- (6) ECC-CDH primitive;
- (7) Keygen for ECC;
- (8) AES enciphering/deciphering.

Related topics (see NISTIR 8214A, Section 5):

- (1) configurability (threshold numbers, ...);
- (2) practical feasibility;
- (3) security models;
- (4) security properties;
- (5) gadgets and modularity;
- (6) validation suitability.

[*] **Acronym legend:** AES (Advanced Encryption Standard); Cofactor Diffie-Hellman (CDH); ECC (Elliptic Curve Cryptography); ECDSA (Elliptic Curve Digital Signature Algorithm); EdDSA (Edwards Curve Digital Signature Algorithm); Keygen (key generation); RSA (Rivest–Shamir–Adleman).

Preliminary announcement on 2020-Aug-14

(Typo correction on 2020-Aug-27)

MPTS 2020 — Call for participation

The **Threshold Cryptography (TC) project** at the National Institute of Standards and Technology (NIST) is exploring the potential for standardization of threshold schemes for cryptographic primitives. The goal of the **multi-party track** (see NISTIR 8214A) is to enable the distributed execution of key-based primitives when the keys are secret-shared across multiple parties. By applying a threshold scheme, the confidentiality of the original key is preserved even if some threshold number of parties are compromised. A threshold property can also extend to other security aspects, such as integrity and availability of the operation.

The current focus of the project is on devising criteria for evaluation of threshold schemes that may be proposed in the future for consideration in the TC multi-party track. To develop such criteria, it is essential to obtain meaningful and timely feedback from expert stakeholders. The **NIST Workshop on Multi-Party Threshold Schemes (MPTS 2020)** is organized as a step to enable the organizers to collect useful feedback from the community. The organizers ask the community to aim at recommendations that promote security, practicality and interoperability, under the umbrella of improving best practices and fostering innovation, within the scope of standardization.

Workshop structure. MPTS 2020 will be a virtual workshop. The presentations and comments will be recorded and made publicly available after the event. The workshop will last three days, with up to four hours per day. The program will be based on two types of contributions:

- **Talks:** Invited talks (~20 min each), focused on recommendations for criteria for threshold schemes or their elements (e.g., gadgets); each talk is followed by a short period of moderated comments and Q&A.
- **Briefs:** Short talks (up to 5 min each), related to the goal of the workshop (requires submitting a title and short description).

We invite the community of stakeholders to participate in the workshop and share their views on threshold schemes for the multi-party track of NISTIR 8214A, and give recommendations on criteria for their standardization. Whereas it may be difficult to pick a “best” approach or technique, given the diversity of possible methods, application scenarios, and tradeoffs, we find it useful to hear about multiple suitable alternatives. We will publish the collected feedback after the workshop.

Content scope. This workshop and the multi-party track of the TC project cover the cryptographic primitives highlighted in Section 4.1 of NISTIR 8214A. The organizers are interested in characterizing potential threshold schemes with respect to the features in Section 5 of NISTIR 81214A. See also the Sections 2.3–2.5, 6.1 and 7.2.

Disclaimer (standards). The use of the words “standards” and “standardization” in the TC project does not imply a goal of producing new *Federal Information Processing Standards (FIPS) publications.* For example, the final products may include Recommendations or implementation guidelines to be incorporated in other documentation, such as (but not necessarily) *Special Publications in Computer Security* (SP 800).