August 11, 2025

Call for U.S. Guidelines on Advanced Digital Security (Threshold Signature Schemes) to Reduce Risks and Encourage Innovation

Executive Summary

To counter cryptocurrency attacks and threats by adversaries, including DPRK, it is critical that the U.S. Government support an effort to close gaps in standardization around cryptographic key management systems (KMS) – and prevent single point of failures used to exploit U.S. financial actors and U.S. retail users.

New cryptographic technologies, such as Multi-Party Computation (MPC), have been used for almost a decade to secure trillions of dollars and have become a de facto standard in the digital assets and crypto payments ecosystem. However, their adoption in U.S. financial institutions is slowed down by a lack of proper supporting standardization and defined best practices for traditional finance participants.

We commend the U.S. Government's efforts to improve cyber resilience by reviewing this issue in an MPC Interagency Report (IR). We are eager to partner with the Administration on these efforts. Specifically, we recommend the Commerce Department engage through National Institute of Standards and Technology (NIST) to speed up (and invest in) a new Special Publication (SP) for MPC, and specifically, the widely used Threshold Signatures Schemes (TSS), which serve as the backbone for the most advanced cryptocurrency operators such as custodians and technology providers.

To achieve the goals of meeting institutional requirements at the scale needed for global adoption, we suggest a Special Publication on TSS to be issued within 12 months, and to incorporate the SP into Federal Information Processing Standards (FIPS) standards in 18 months through direct industry engagement. Doing so will support future-proofing American technology and have U.S. standards form the blueprint for the future of cryptocurrency innovation globally. Such an approach also allows for standardization and benchmarking of MPC and related primitives on a parallel (if shorter) timeline to ongoing efforts related to more aspirational post-quantum distributed signature schemes and other research areas that are included in the Threshold call class S.

Key Reasons to Prioritize These Security Guidelines:

1. <u>Enshrining National Security and Consumer Protection:</u> The digital asset landscape faces persistent and sophisticated cyberattacks. Threshold Signature Schemes (TSS) are a proven best-in-class security approach, which all major U.S. institutions should be able to choose. The absence of official standards for TSS inhibits this choice, in some instances, and risks inferior deployment, in others. As digital assets become more integrated in the U.S. financial system, and as policymakers provide legal permissibility for such activities, government action to standardize TSS will bolster U.S. defenses

against threat actors, contribute to financial system stability and help protect consumers from financial losses.

2. Fostering Innovation and Competitiveness: Official guidelines would provide a trusted, standards-based approach to security, fostering U.S. innovation and global competitiveness. NIST standards drive regulatory permissibility globally, which would allow U.S. institutions to scale securely. Particularly given potential concerns around supply chain risk and prevalence of foreign-owned hardware security modules (HSMs), the delivery of standards supporting MPC-based solutions offers an improved security posture through a more decentralized security architecture. In particular, financial institutions such as banks may be more hesitant to adopt MPC absent some form of recognition by NIST even as this technology has been proven for this field.
3. Securing Current Systems While Preparing for Future Technologies: Preparing for post-quantum cryptography is critical; however, current systems using widely deployed algorithms (e.g., ECDSA, EdDSA, BLS) require immediate, robust security. Since blockchain network algorithm adoption is not centrally controlled by individual institutions, official NIST guidelines for current TSS implementations would provide vital, endorsed security practices during this interim period, and facilitate a smoother transition to post-quantum solutions. Additionally, as MPC becomes a more common industry tool in additional non-financial use cases, including, for example, in digital identity applications, setting a standard for such usage will be critical to safeguard sensitive personal data.
4. Leveraging Proven Industry Expertise for Rapid Guideline Development: Threshold Signature Schemes are not theoretical; they are currently deployed by several large organizations to secure billions of dollars in digital assets, and transfer trillions of dollars. The digital asset industry possesses considerable operational expertise, proven know-how, and established best practices with TSS, and there is wide alignment on established approaches that can serve as a base for this work.
5. An Expedited, Phased Approach for Optimal Impact: Current timelines for broader government reports (e.g., targeting 2027 for an initial MPC IR) are misaligned with immediate institutional security needs. We strongly recommend developing specific TSS guidelines via special publication (for ECDSA, EdDSA, and BLS) rapidly, potentially concurrently with or preceding other reports, to deliver immediate security benefits.

Broad Ecosystem Alignment and Commitment to Contribute:

The undersigned organizations constitute a broad representation of the digital asset ecosystem and are deeply committed to dedicating significant resources to support NIST with an expedited standardization process, including active participation in all processes related to this standardization, from proposal of schemes to comments, reviews, and workshops, and publication. We are aligned in our goal to enhance security and foster responsible innovation within the U.S. digital asset space.

Respectfully Submitted by the Undersigned:

Pavel Berengoltz
Chief Technology Officer, Co-Founder
Fireblocks, Ltd.

Dan Boneh
Co-Director of the Stanford Center for Blockchain Research
Stanford University

Jacques Boschung
CEO
Halborn

Ran Canetti
Wang Professor of Computer Science
Director of the Center for Reliable Information System and Cyber Security
Boston University

George Kadianakis
Cryptography Research Team Lead
Ethereum Foundation

Yehuda Lindell
Head of Cryptography
Coinbase

Redwan Meslem
Executive Director
Ethereum Enterprise Alliance

Jim Miller
Engineering Director, Cryptography
Trail of Bits

Nelly Porter
Director of Product Management, Encryption and Confidential Computing, Google Cloud
Google LLC

Jay Prakash
CEO & Co-Founder
Silence Laboratories

Javed Samuel
Practice Leader, Cryptography Services
NCC Group

Sarah Wilson
General Counsel & Corporate Secretary
Circle, Inc.

Alex Zinder
Chief Product Officer
Blockdaemon