#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **SAT-W09**

Time is Running Out:
Post Quantum Cryptography Call to Action
SAFECode/NIST panel discussion

MODERATOR: **Janet Jones**
Principal Security Program Manager – SAFECode/Microsoft Corporation

PANELISTS:

Dr. Dustin Moody
Mathematician
National Institute of Standards and Technology

Judith Furlong
Distinguished Engineer
SAFECode/Dell EMC

Souheil Moghnie
Technical Director/Security Architect
SAFECode/NortonLifeLock

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

MODERATOR:

Janet Jones

Principal Security Program Manager
SAFECode/Microsoft Corporation

PANELISTS:

Dr. Dustin Moody

Mathematician
National Institute of Standards and Technology

Judith Furlong

Distinguished Engineer
SAFECode/Dell EMC

Souheil Moghnie

Technical Director and Security Architect
SAFECode/NortonLifeLock

Agenda

- Introductions
- Post Quantum Cryptography (PQC) – Why the rush?
- NIST PQC Standardization Update
- Preparing for the PQC transition – immediate recommendations
- Q&A
- Summary

Q&A

Summary

- Inventory where and how your product/code uses cryptography
- Implement crypto agility to minimize code changes
- Begin to pilot-use of the candidate quantum-safe algorithms
- Prepare to use different algorithms for encryption, key exchange, and signatures
- Test your code for impact of large key sizes, ciphers, and signatures
- Participate in standardization efforts and foster awareness

Resources

- Post Quantum Crypto – SAFECode (https://safecode.org/category/post-quantum-crypto/)
- Start the Countdown Now: Your Cryptography's Time is Running Out (https://safecode.org/blog/start-the-countdown-now-your-cryptographys-time-is-running-out/)
- Preparing for PQC: Roadmap & Initial Guidance (https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/)
- Identifying Your Cryptographic Dependencies (https://safecode.org/blog/identifying-your-cryptographic-dependencies/)
- How Agile Is Your Cryptographic Strategy? (https://safecode.org/blog/how-agile-is-your-cryptographic-strategy/)
- Strategies for Achieving Crypto Agility (https://safecode.org/blog/strategies-for-achieving-crypto-agility/)
- The Implications of Post Quantum Cryptography for Software Supply Chain Security (https://safecode.org/blog/the-implications-of-post-quantum-cryptography-for-software-supply-chain-security/)

Thank you!