THE HYPERLEDGER IDENTITY SPECIAL INTEREST GROUP

Post Quantum Cryptography

NIST Special Publication 1800-38A

The Impact on Identity Solutions

Vipin Bharathan

Founder, dlt.nyc

Agenda

1. Why PQC?
2. NIST 1800-38A
3. Applicability to Identity solutions
4. Next Steps

Why PQC

1. Advances in Quantum Computing will break existi algorithms
2. RSA, ECDH, Elliptic Curve Digital Signature Algorithm (ECDSA) need updates
3. QC for breaking these algorithms (based on factoring)is it still “an Engineering Problem” a “Physics Problem”? Is it Real?
4. In the next 10-20 years?

NIST 1800-38A

1. An executive summary
2. New algorithms need to be resistant to classical & Quantum computers
3. Not a drop in replacement: differences in key size, signature size, error handling, number of execution steps, key establishment complexity etc.
4. Multiple touch-points, no control over algorithms

Identity solutions

1. Identify where, and how, public-key algorithms being used in Anoncreds, Indy, Aries, DIDComm e
2. Dangers due to store and break
3. Survey process and dangers for entire stack
4. Incorporate tools into identifying QV (Quantum Vulnerable) algorithms for cryptographic libs, network, applications.

Next Steps from NIST

1. Technology, security, and privacy program managers 1800-38B and IT professionals 1800-38C
2. Initial interoperability and performance testing will cover TLS, SSH, X.509 post-quantum certificate hybrid profiles to support traditional an post-quantum algorithms, and post-quantum-related operations of next-generation Hardware Security Modules (HSMs)

References

1. William Newhouse,Murugiah Souppaya, William Barker, Chris Brown NIST SPECIAL PUBLICATION 1800-38A Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography, Published April 24,2023, latest changes May 2 2023