THE OVERALL CLASSIFICATION OF THIS BRIEFING IS: UNCLASSIFIED

HYBRID DESIGNS

LAMPS - IETF 112
ALISON BECKER, REBECCA GUTHRIE, DAPHANIE NISBETH
CENTER FOR CYBERSECURITY STANDARDS, NSA
11/8/2021
PQ MIGRATION

GOALS

- Crypto agility
  - Rigorous, effective algorithm vetting is a must, NSA has confidence in the NIST PQC process
- NSA will not require a hybrid design for security purposes
- NSA only anticipates using hybrid solutions to maintain interoperability during the transition (or where direct drop-in is not feasible)
  - Any hybrid method adopted should allow for a quick transition to PQ-only solutions
- Ensure interoperability with PQ-only systems is included for forward compatibility and to allow for use of direct drop-in of PQ
**HYBRID DESIGNS**

**Hybrid** - The use of two or more algorithms simultaneously such that the desired security property holds if and only if at least one of the component algorithms remains unbroken.

### GOALS
- Backwards compatibility
- Forwards compatibility
- High performance
- Low latency
- Allow for PQ-only migration

### TERMINOLOGY
- Composite signatures
- Dual signatures
- Multi-certs
- Combined negotiation
- Multiple key shares
- Algorithm pairs
HYBRID SOLUTIONS (TERMINOLOGY)

DEFINING A FRAMEWORK FOR PQ MIGRATION

COMPOSITE DESIGN

A solution in which the traditional and PQ algorithms function together, as one entity

NON-COMPOSITE DESIGN

A solution in which the traditional and PQ algorithms function discretely, as individual entities

These concepts arise in multiple parts of a protocol, including but not limited to the negotiation of algorithms, key exchange, KDF, or authentication.
• Support non-composite hybrid designs for interoperability during transition to PQ-only

• Non-composite certs put most of the work on protocols to implement
  • Backwards and forwards compatibility is straightforward
COMPOSITE SOLUTIONS

DESIGN CHARACTERISTICS

PROS

• Often no new protocol logic needed for negotiation, etc.
• Matching security levels of algorithms is built into composite pairs

CONS

• Requires new composite OIDs
• Can require reworking of certificate validation
• Maintenance concerns surrounding deprecated algorithms
• Requires another transition and set of standards from hybrid to PQ
NON-COMPOSITE SOLUTIONS

DESIGN CHARACTERISTICS

PROS

• Computational processes remain unchanged (but perhaps multiple iterations)
• UDP-based protocols potentially avoid fragmentation issues
• Ease of use for backward compatibility
• Facilitates seamless transition to PQ-only, no new standards needed
• Requires support for only two types of structures (traditional and PQ)

CONS

• Often requires new protocol logic for negotiation, etc.
• May send duplicate info (header of cert, etc.)
NEXT STEPS

• Get feedback on the list
• Technical report in progress
  • Analyzing several protocols to compare composite/non-composite certificate design
• Introduce composite/non-composite hybrid design terminology