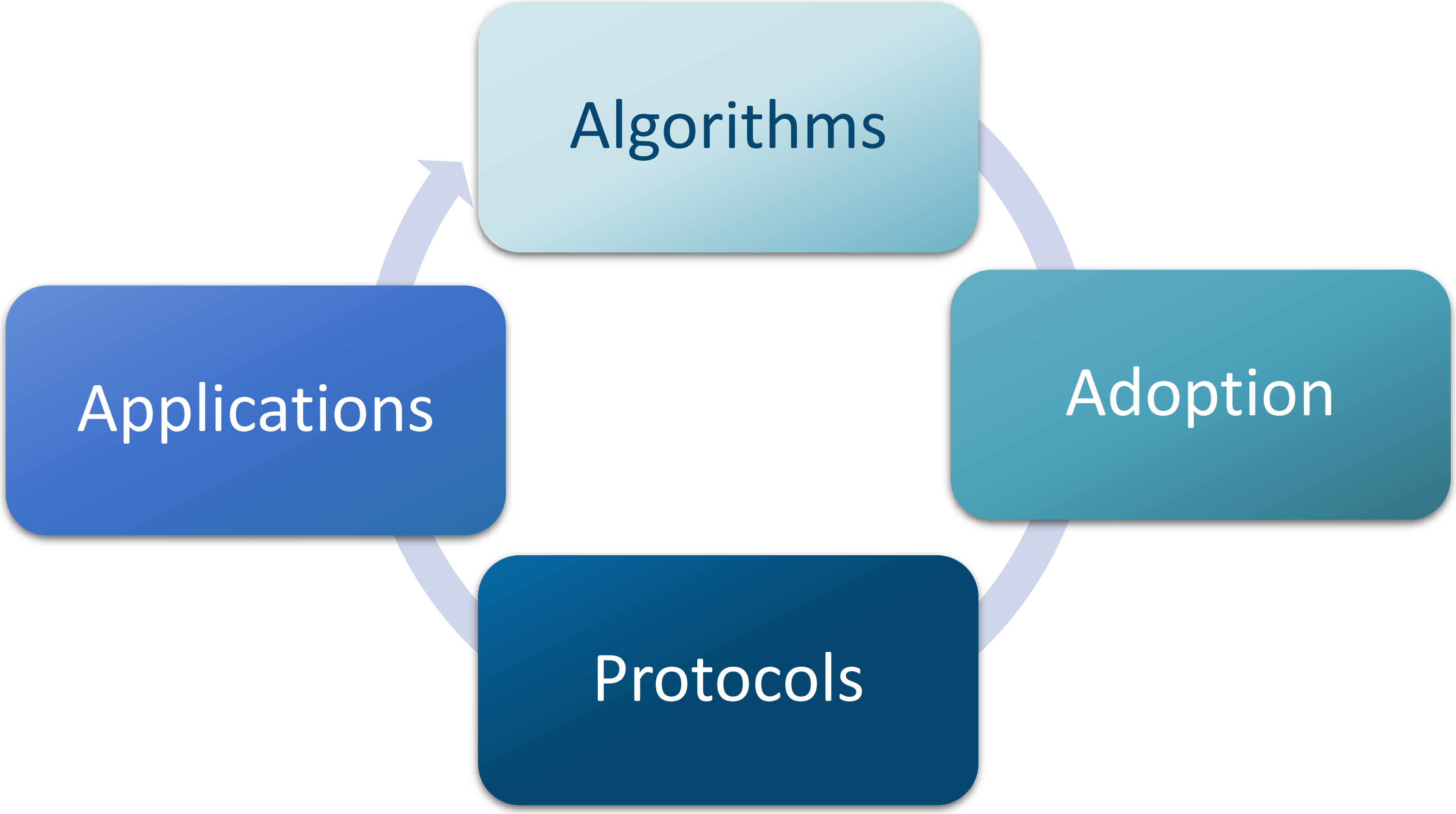
Security Conference 2022

# Post-quantum: Next steps

Peter Campbell, UK NCSC

05/10/2022

# Post-quantum: Next steps



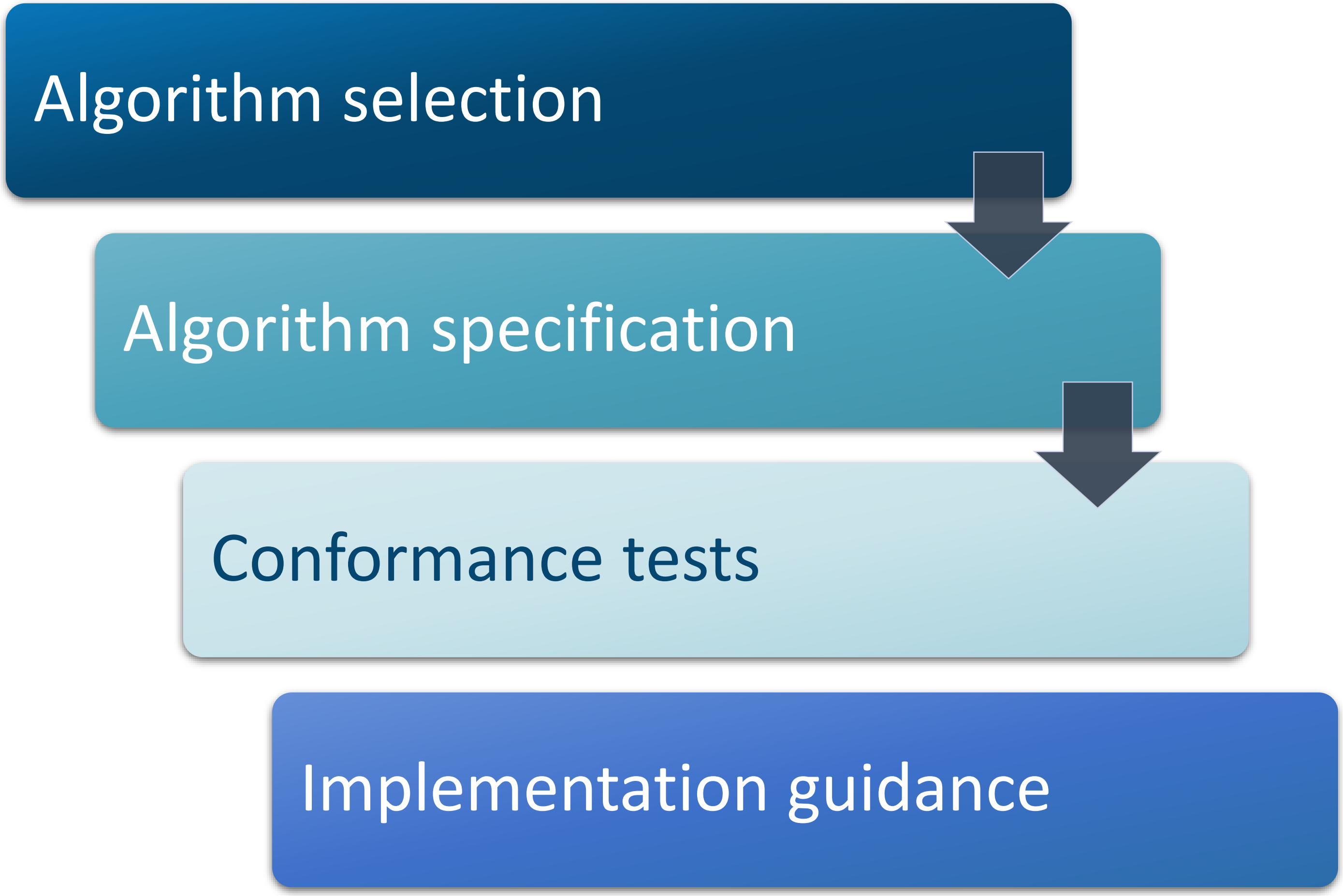
Algorithms

Adoption

Protocols

Applications

# Algorithms



Algorithm selection

Algorithm specification

Conformance tests

Implementation guidance

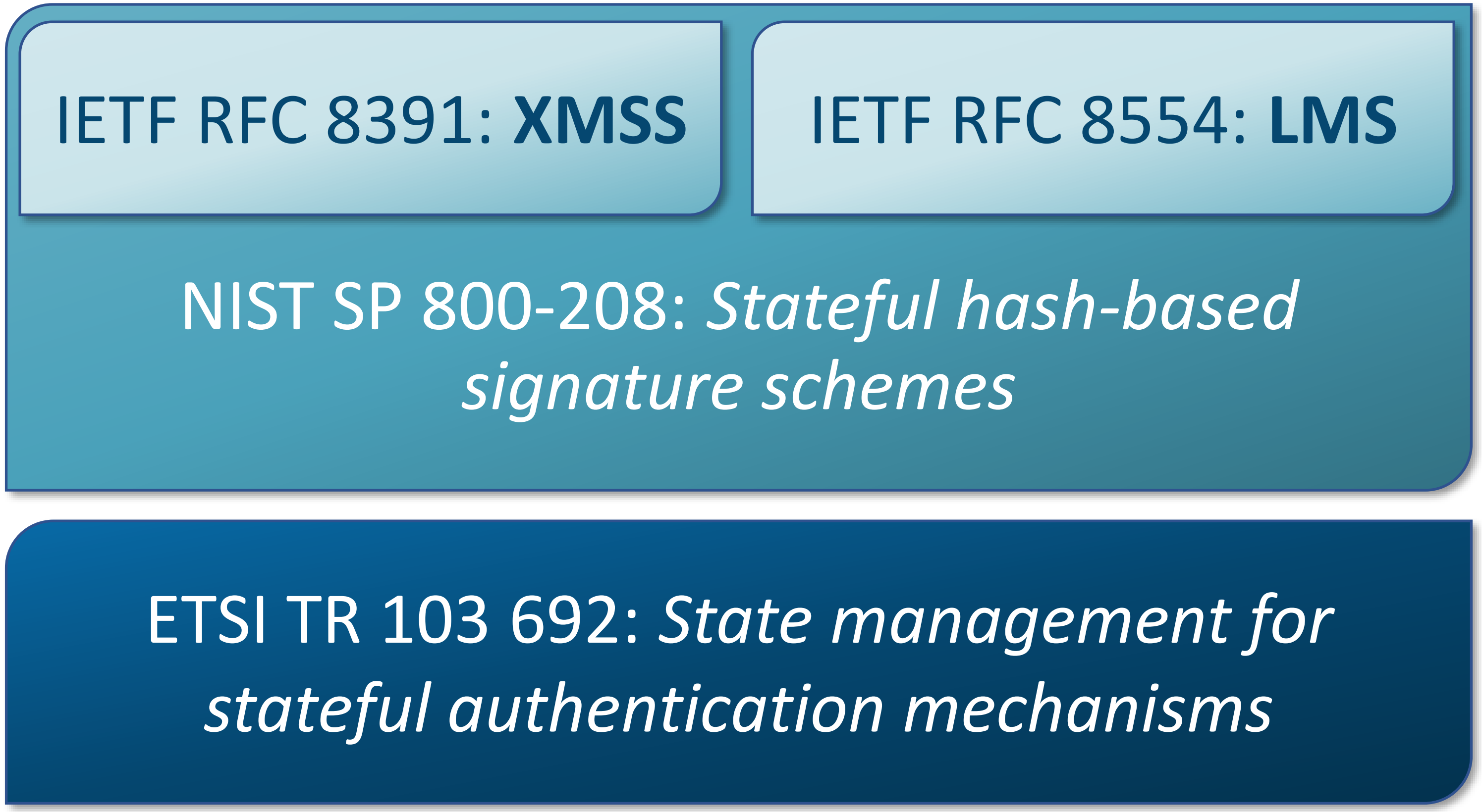
KYBER

DILITHIUM

FALCON

SPHINCS$^+$

# Algorithms: Stateful hash-based signatures



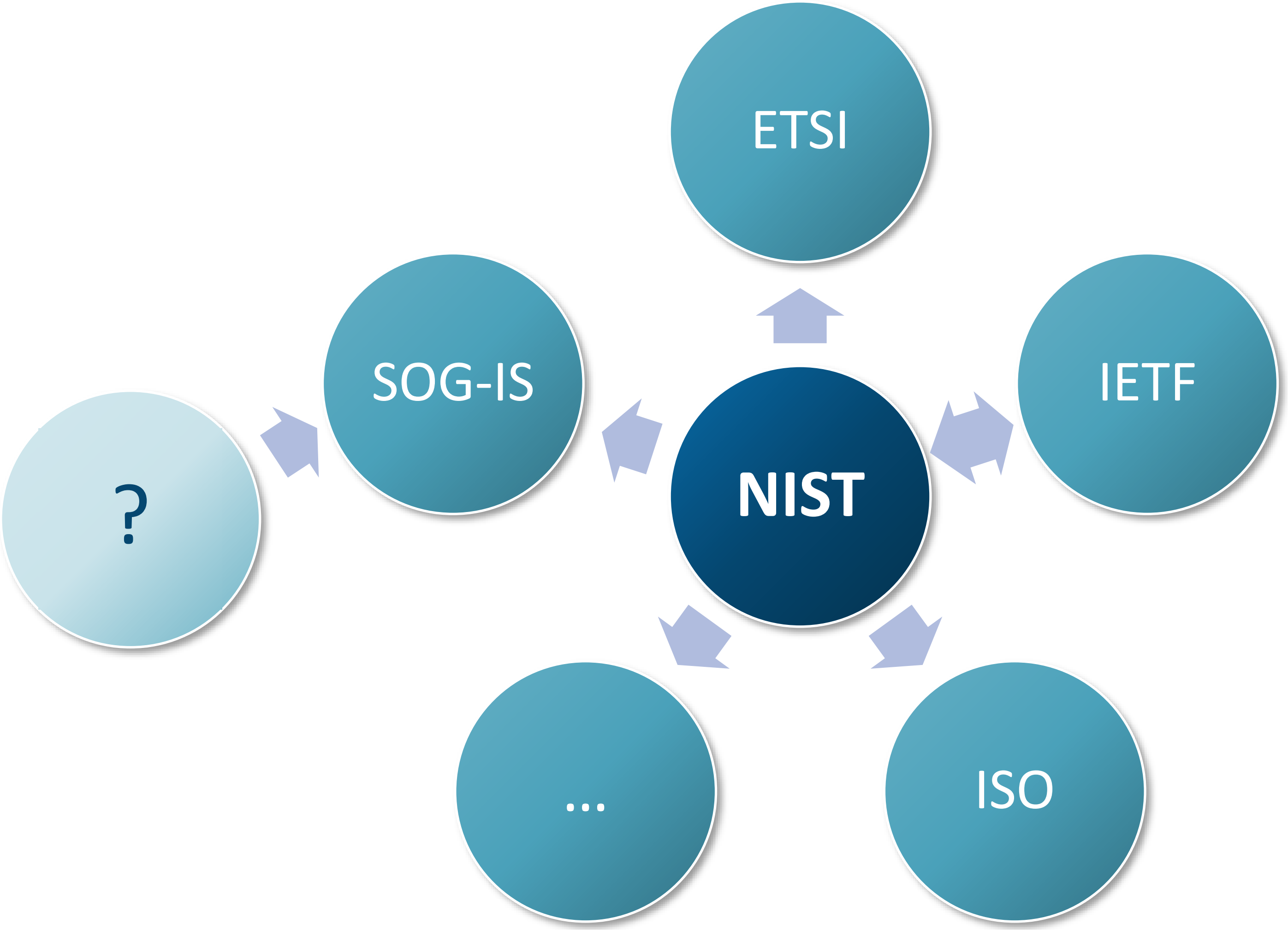
IETF RFC 8391: **XMSS**

IETF RFC 8554: **LMS**

NIST SP 800-208: *Stateful hash-based signature schemes*

ETSI TR 103 692: *State management for stateful authentication mechanisms*

# Adoption

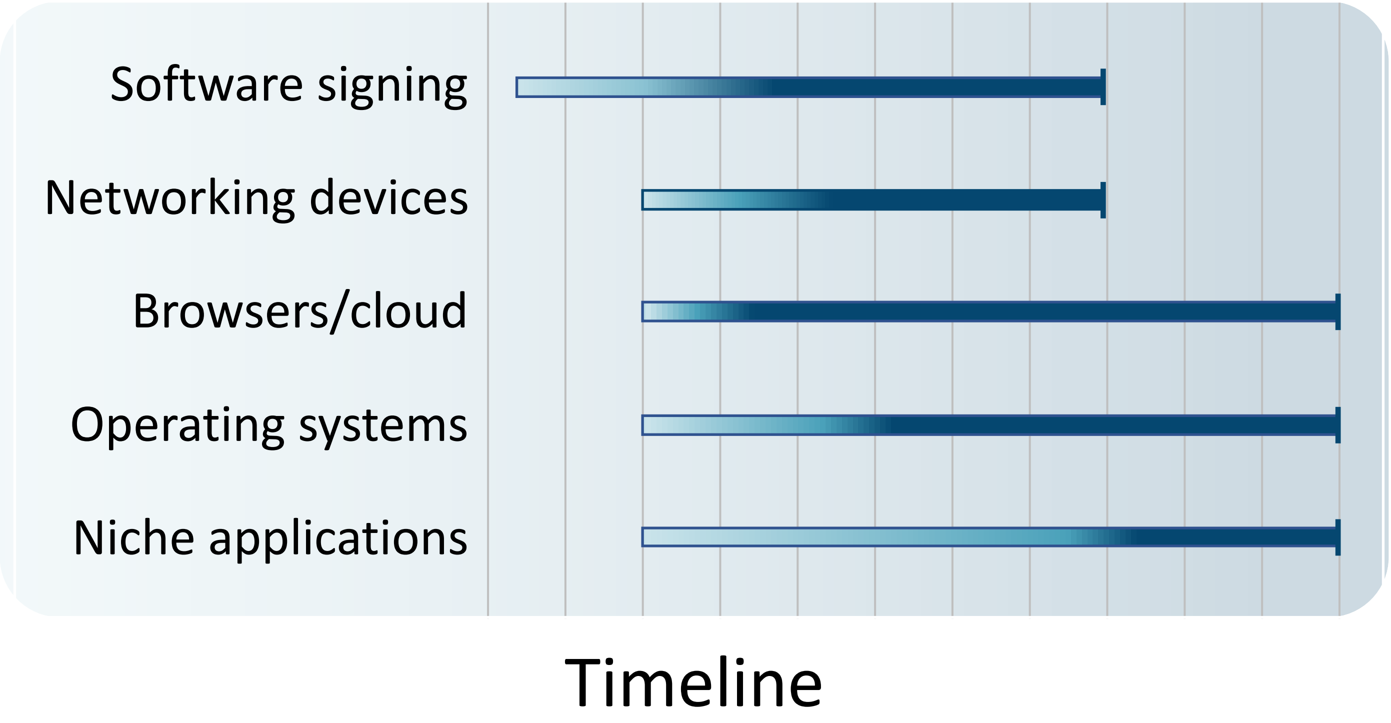


# Adoption: CNSA 2.0

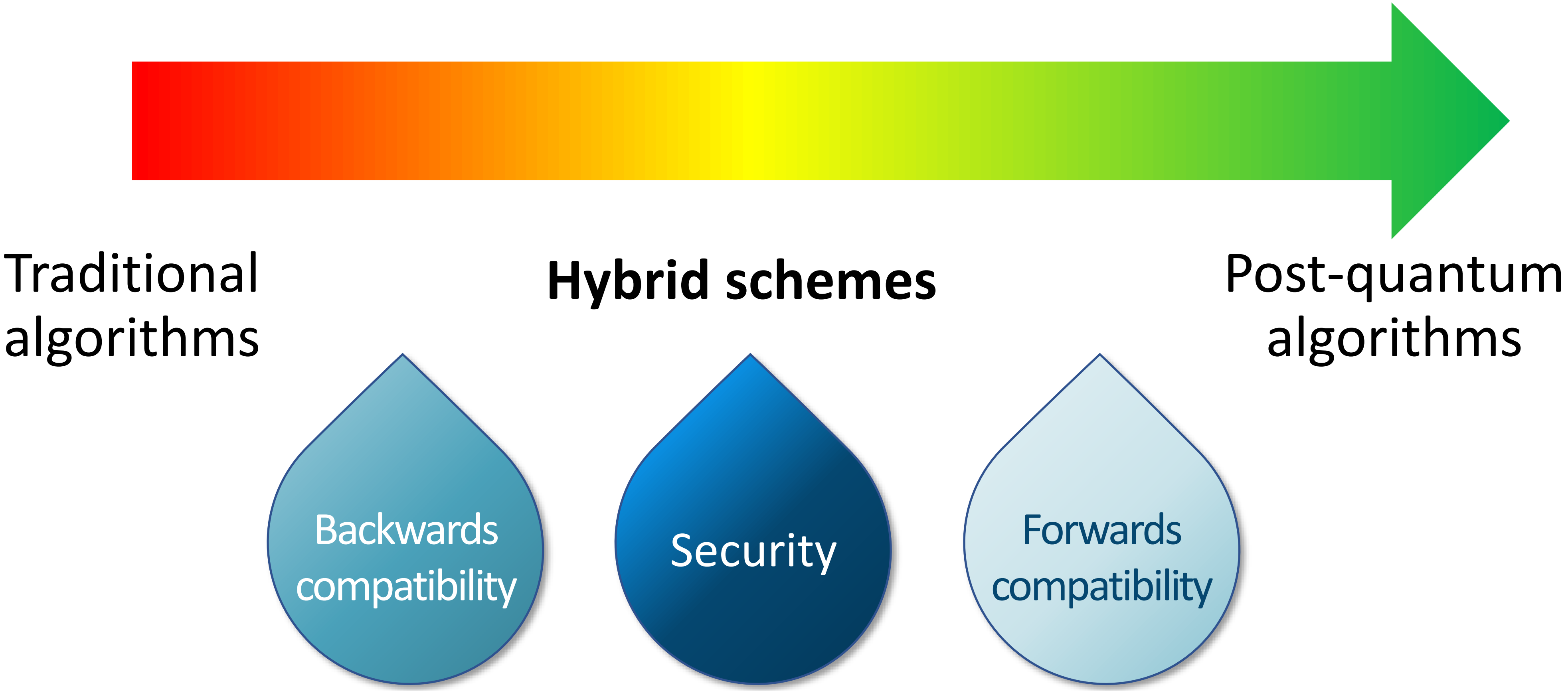
*Key establishment*
**Kyber**

*General signature*
**Dilithium**

*Software signature*
**LMS** or **XMSS**



# Protocols



Traditional algorithms

**Hybrid schemes**

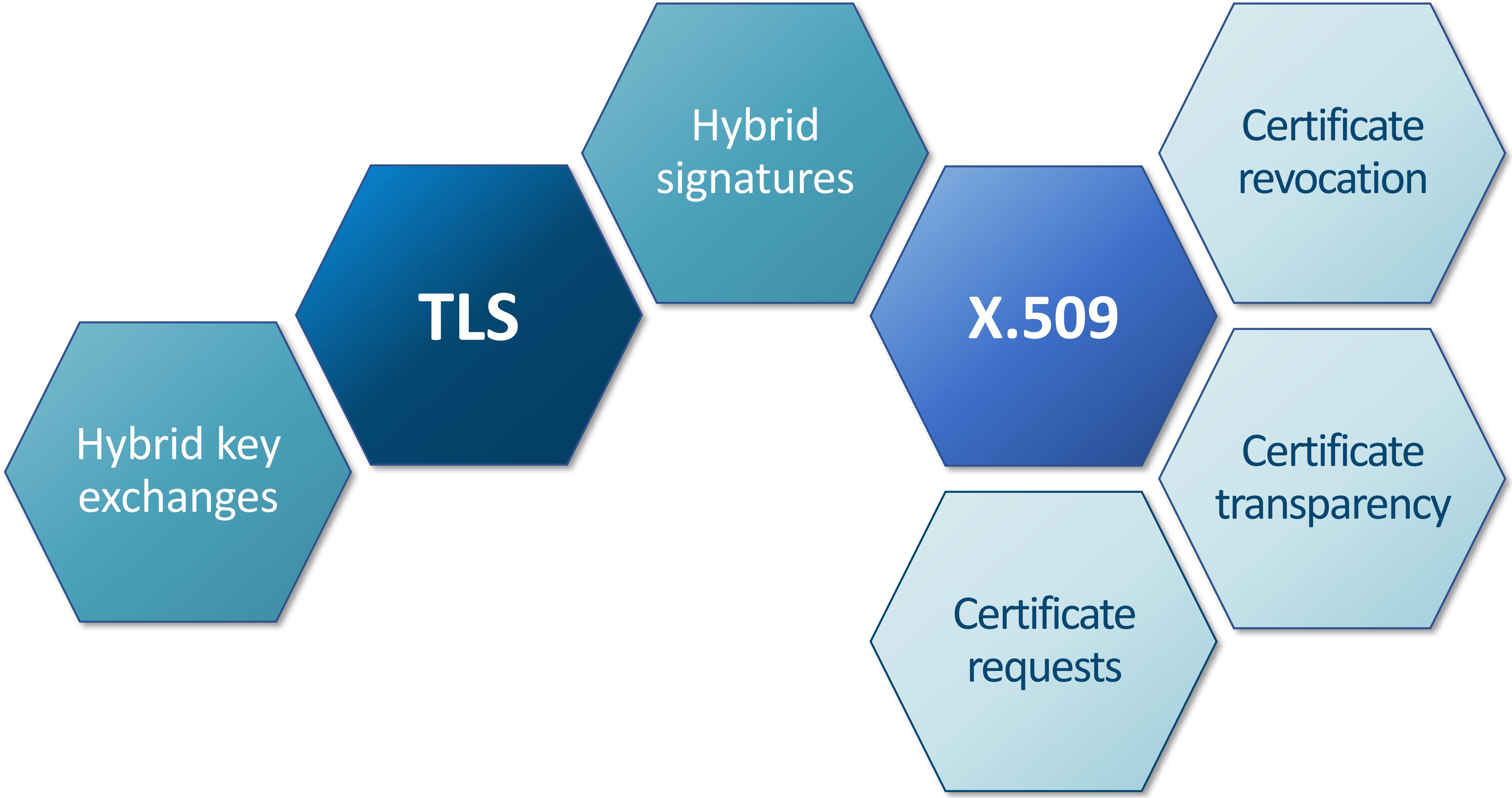
Post-quantum algorithms

Backwards compatibility

Security

Forwards compatibility

# Protocols: TLS



Hybrid key exchanges

TLS

Hybrid signatures

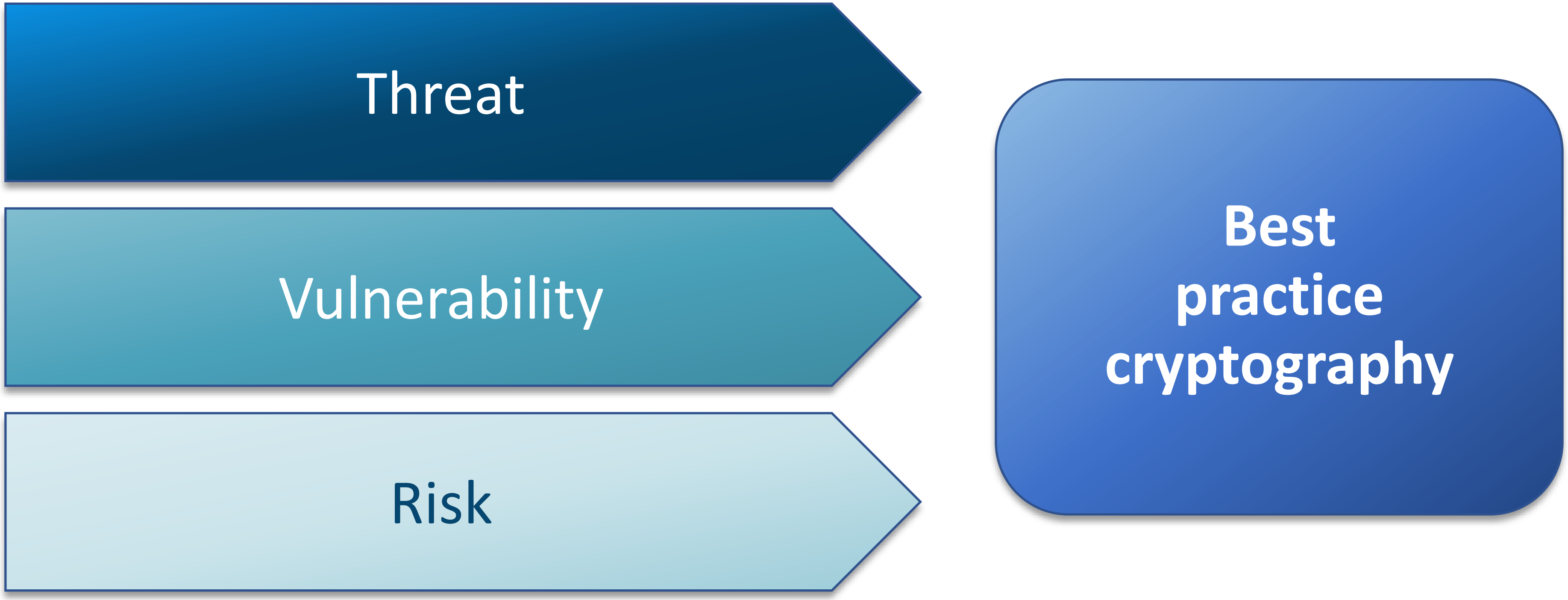
X.509

Certificate revocation

Certificate transparency

Certificate requests

# Applications



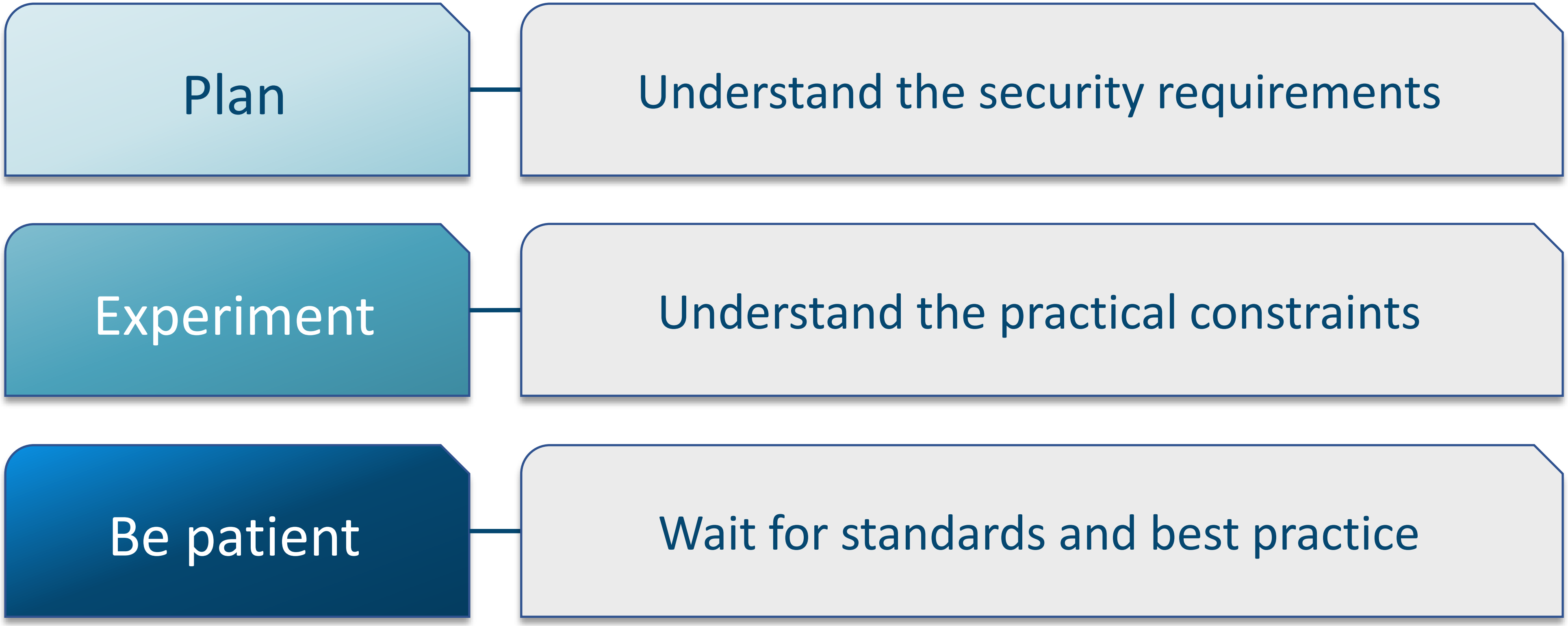
Threat

Vulnerability

Risk

**Best practice cryptography**

# Applications: Summary



| | |
|---|---|
| Plan | Understand the security requirements |
| Experiment | Understand the practical constraints |
| Be patient | Wait for standards and best practice |

# Questions?