Post-quantum cryptography migration use cases

draft-vaira-pquip-pqc-use-cases

PQUIP – IETF 120 – July 23rd 2024

Hendrik Brockhaus
Siemens

John Gray
Entrust

Mike Ounsworth
Entrust

Alex Railean
Siemens

What is it?

Systematize migration strategies for digital signature use cases

Aims

- Help choose fitting algorithms and parameters
- Start a discussion

What changed since IETF 119?

- Incorporate feedback
- Wording around hybrids
  - Better supporting argumentation, bias for action
  - Acknowledge potential downsides
- Revised decision tree
  - removed subjective component

What next? Explore “pessimistic migration”

- Assumption: CRQC-attacks start sooner than standardization or migration is complete. How about tomorrow?

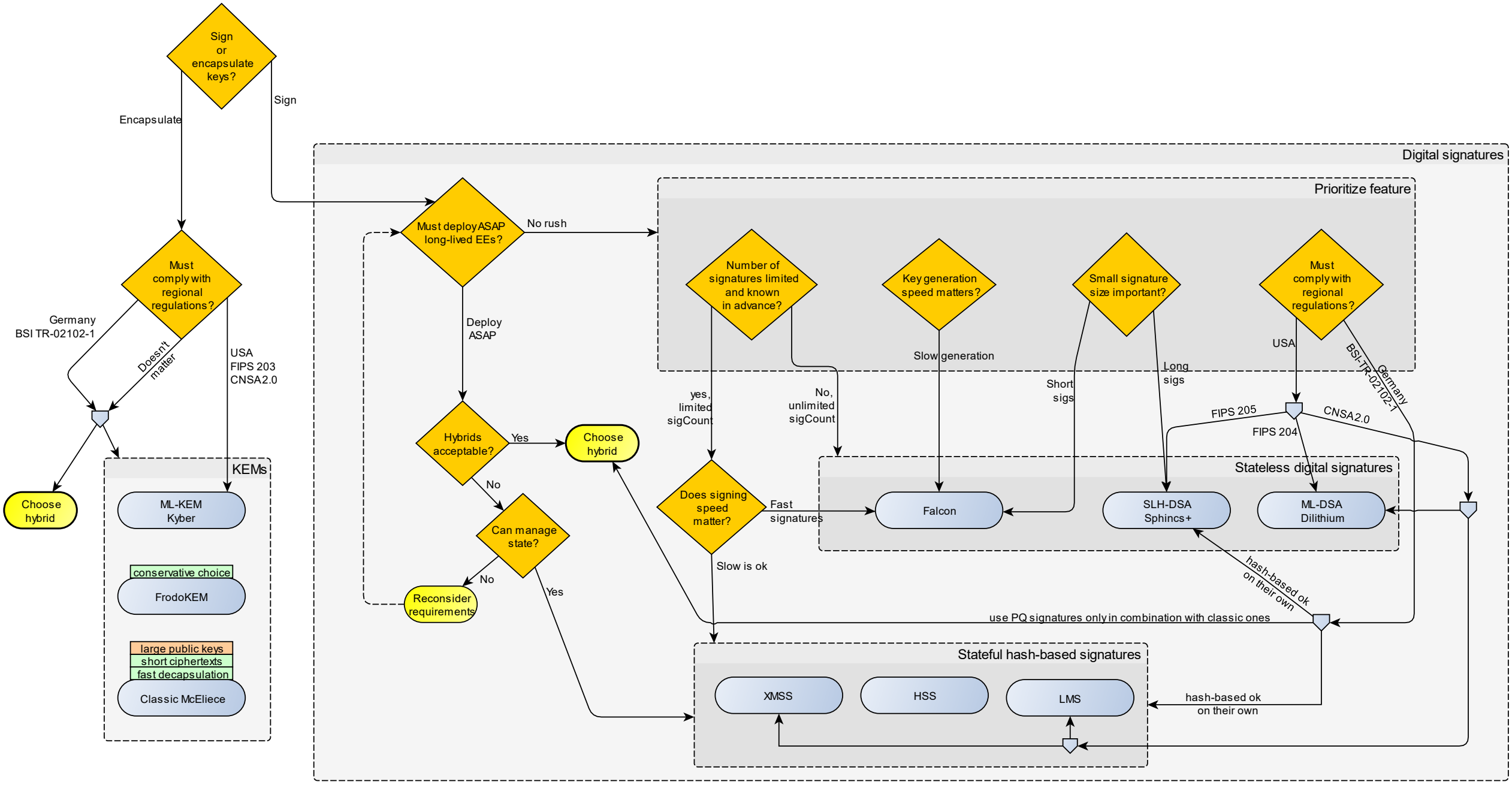
- What can one do today to
  - not be an easy target tomorrow
  - and buy time on Q-day

- Some techniques
  - Wrap legacy communications (e.g., SSH tunnels with NTRU/x25519)
  - Symmetric ciphers with pre-shared keys without handshakes (e.g., shadowsocks)

What next?

- Find me and let’s talk
  - Challenges
  - Questions

- Feedback
  - IETF channels
  - https://github.com/avaira77/pq-ietf-usecase


Sign or encapsulate keys?
Encapsulate
Sign
Must comply with regional regulations?
Germany BSI TR-02102-1
Doesn't matter
USA FIPS 203 CNSA2.0
Choose hybrid
KEMs
ML-KEM Kyber
conservative choice
FrodoKEM
large public keys
short ciphertexts
fast decapsulation
Classic McEliece
Digital signatures
Must deploy ASAP long-lived EEs?
No rush
Deploy ASAP
Prioritize feature
Number of signatures limited and known in advance?
Key generation speed matters?
Small signature size important?
Must comply with regional regulations?
yes, limited sigCount
No, unlimited sigCount
Slow generation
Short sigs
Long sigs
USA
BSI-TR-02102-1
Germany
FIPS 205
CNSA2.0
FIPS 204
Hybrids acceptable?
Yes
Choose hybrid
No
Can manage state?
No
Reconsider requirements
Yes
Does signing speed matter?
Fast signatures
Slow is ok
Stateless digital signatures
Falcon
SLH-DSA Sphincs+
ML-DSA Dilithium
hash-based ok on their own
use PQ signatures only in combination with classic ones
Stateful hash-based signatures
XMSS
HSS
LMS
hash-based ok on their own