

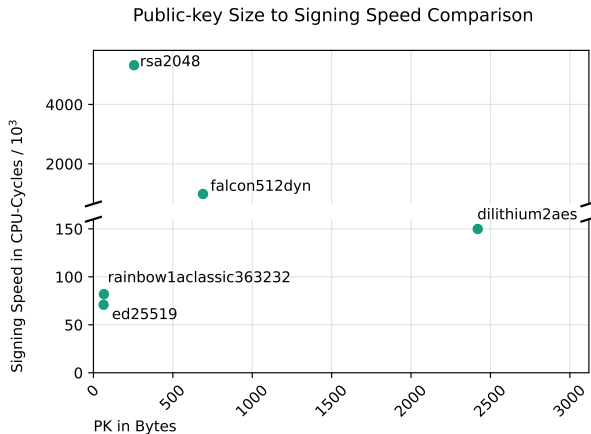
Post-Quanten-PKIs in Anwendungen

Post-Quantum Cryptography

Die Suche nach quantenresistenten Verfahren:

- Gitter-basierte Kryptographie
- Multivariate Kryptographie
- Code-basierte Kryptographie
- Isogenien in supersingularen elliptischen Kurven
- Hash-basierte Signaturen
- ...

Alles wird immer schneller und kleiner - nicht



by Gerhard Cenko, Fraunhofer AISEC

And it goes on and on and on and on...

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST
COMPUTER SECURITY
RESOURCE CENTER
CSRC

PROJECTS

Post-Quantum Cryptography: Digital Signature Schemes



Overview

[Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process](#) (PDF)

NIST announced that the PQC standardization process is continuing with a fourth round, with the following KEMs still under consideration: BIKE, Classic McEliece, HQC, and SIKE. However, there are no remaining digital signature candidates under consideration. As such, **NIST is calling for additional digital signature proposals to be considered in the PQC standardization process. Submission packages must be received by NIST by June 1, 2023.**

PROJECT LINKS

Overview

News & Updates

ADDITIONAL PAGES

Standardization of Additional Digital Signature Schemes

[Call for Proposals](#)

[Example Files](#)

<https://csrc.nist.gov/projects/pqc-dig-sig>

Hash-basierte Signaturen

- Verfahren:
 - XMSS / XMSS^{MT} (RFC 8391)
 - LMS / HSS (RFC 8554)
 - SPHINCS+ (NIST TBD)
 - Pyramid, ...
- Empfehlungen
 - BSI TR-02102-1
 - NIST SP 800-208
 - NSA CNSA 2.0
- Vieles mehr:
 - *State Management for Hash-based signatures*, McGrew et al., 2016
 - ETSI, ISO, ...

PQ-X.509-Zertifikat (gekürzt)

Personenname

C (Land): DE

CN (Vorname): FLOQI-Sub-06_01_DILI_4x4

Name des Herausgebers

C (Land): DE

CN (Vorname): FLOQI-Root-06_DILI_6x5

Zertifikat des Herausgebers

Version: 3

Seriennummer: 01 83 A8 F4 29 F8

Nicht gültig vor: 2022-10-05

Nicht gültig nach: 2025-12-31

Informationen zum öffentlichen Schlüssel

Schlüssel-Algorithmus: 1.3.6.1.4.1.2.267.7.4.4

SHA1-Fingerabdruck des Schlüssels: F6 A3 0D 48 87 D1 59 B1 95 9F 7E 2D 6D 73 E9 FF 19 63 CF B9

Öffentlicher Schlüssel: 0D D4 AF F8 D0 94 99 74 9F 10 20 70 50 90 AA 82 E0 88 3A 92 C3 7C AA 16 D8 F1 8F 98 AA 0F F1 18 0D A6 EA D2

Neue Zertifikatsarten

Transition

Zertifikat	
PK	<u>UniqueID</u>
	Issuer
	Algorithmus
	...

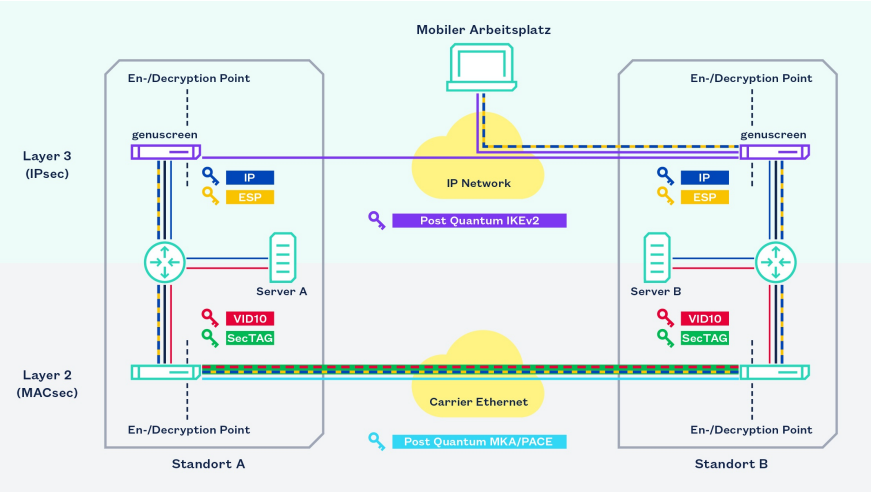


Composite

Zertifikat	
PK	<u>UniqueID</u>
	Issuer
	Algorithmus
	...

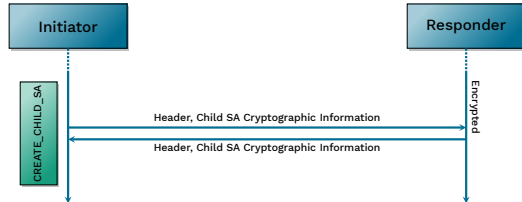
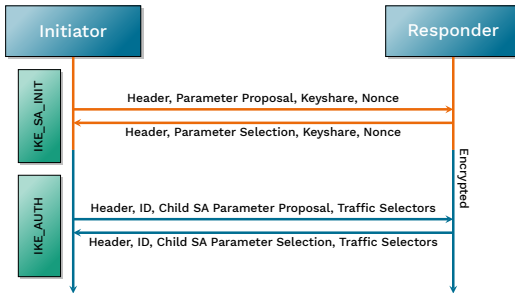


QuaSiMod0

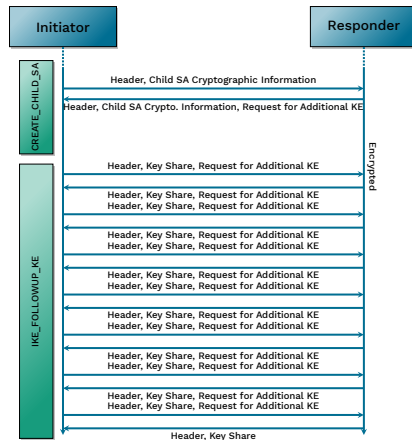


Internet Key Exchange (IKEv2)

What used to be complex enough...

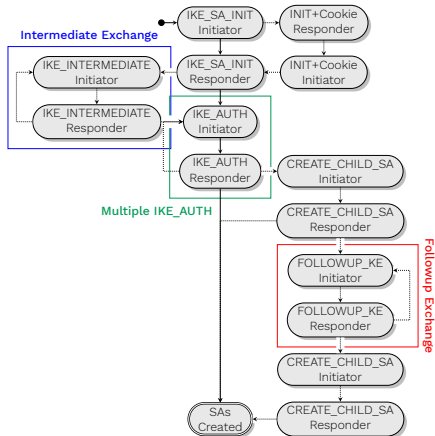
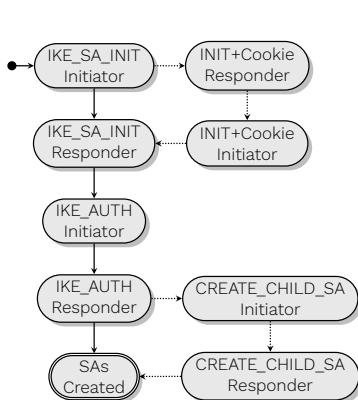


Full Post-Quantum Complexity



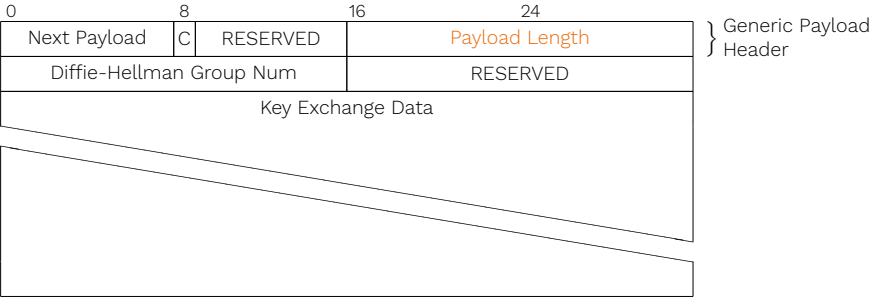
Internet Key Exchange (IKEv2)

State Machines



Internet Key Exchange (IKEv2)

Key Exchange Frame



Fragen?

Stefan-Lukas_Gazdag@genua.de

www.square-up.org

www.pq-vpn.de

www.genua.de