Addressing FIDO Alliance's Technologies in Post Quantum World

January 2024

Contents

1. Introduction

There has been considerable press, a number of papers, and several formal initiatives concerned with quantum computing's impact on cryptographic algorithms and protocols. Most standards development organizations are addressing concerns about the impact on the security of the currently deployed cryptographic algorithms and protocols. This paper presents FIDO Alliance initiatives that address the impact of quantum computing on the Alliance's specifications and how the FIDO Alliance is working to retain the long-term value provided by products and services based on the FIDO Alliance specifications.

This paper is directed to those who have or are considering FIDO-enabled products and solutions but have concerns about the impact of Quantum Computing on their business. This paper will focus, from a high-level approach, on the FIDO Alliance's acknowledgment of issues related to Quantum Computing and explain how the FIDO Alliance is taking appropriate steps to provide a seamless transition from the current cryptographic algorithms and protocols to new PQC (or quantum-safe) algorithms in a timely manner.

2. Challenges Introduced by Quantum Computers

2.1 General

Quantum computers have the potential to solve certain hard mathematical problems, on which cryptographic algorithms are based, much faster than classical computers (e.g. solving discrete logarithm equations for Elliptic-Curve Cryptography). These improvements affect current cryptographic algorithms and protocols used by the FIDO Alliance's specifications. While for some cryptographic algorithms this threat may be addressed by simply increasing the sizes of the keys (i.e. symmetric cryptography such as AES) or the size of the digest of the message (i.e. hash or mac such as SHA-3 or HMAC), for others, a change to the cryptographic algorithm (i.e. asymmetric algorithms such as RSA or ECDSA or ECDH) is required.

> ***Note: This affects not just implementations based on FIDO Specifications but will impact all aspects of computing that rely on cryptographic algorithms.***

The timeline for the availability of quantum computers capable of "breaking" a classical cryptographic algorithm is debatable even by the experts, with some anticipating an impact within 10 years. But as migration takes time, and security agencies are requesting to plan for protection now, a post-quantum strategy for migration is necessary.

2.2 FIDO Alliance's Approach

FIDO Alliance's specifications use cryptographic algorithms and protocols for authentication, attestation, confidentiality, integrity, authenticity, provisioning and other security functions. These functions are implemented through either asymmetric cryptography or symmetric cryptography. Quantum computing mostly impacts the security of asymmetric cryptography. The only impact on the other types of algorithms is the potential increase in the size of the keys or of the size of the digests.

Several organizations and agencies have been investigating new PQC-resistant asymmetric cryptographic algorithms resistant in a post quantum era. These new algorithms are based on several mathematical problems such as lattices, hash, code, etc. The United States National Institute of Standards and Technology (NIST) is a leader in this effort, having issued a request for proposed post-quantum cryptography (PQC) algorithms as a "challenge" to the public (See [1] and [2]). But other organizations or countries have also started working on this topic, by either publishing new algorithms, or giving recommendations, see Section 7.

Currently, several algorithms have been selected for standardization by NIST and by ISO. Other algorithms are being reviewed for another round of selection expected in 2024. The rational for having multiple algorithms is to provide a selection of these new algorithms implementors to choose from and to mitigate the risk of a discovery of a vulnerability on one of these new algorithms. This means that crypto-agility is a major requirement for post quantum standards. Crypto-agility is the ability to manage multiple algorithms for the same function, and to be able to shift from one algorithm to another one if a major vulnerability is discovered.

3. Dependency and Tracking External Efforts

As mentioned above, there are several industry and government agencies defining or making recommendations for PQC algorithms, notably NIST [3] and ISO. Draft [4] have been released by NIST on their selected choice (FIPS 203 for Dilithium, FIPS 204 for Kyber and FIPS 205 for SPHINCS+, missing FIPS for Falcon) and by ISO (ISO/IEC JTC 1/SC 27, FrodoKEM). These standards are expected to be published in 2024. In addition, NIST is reviewing three code-based key exchange algorithms for selection in 2024 (Bike, HQC and McEliece) as well as standardization. Last, NIST has opened a new request for both signatures [5] and KEMs [5], although this effort will take time.

FIDO Alliance's specifications also rely on standards developed by other standards organizations – which are also tracking PQC algorithms and any impact PQC algorithms have on their own specifications.

IETF specifications are used particularly heavily, and as the FIDO2 standard encompasses the W3C's WebAuthn protocol, there is a strong mutual dependence between our groups' efforts.

Note: Members of the FIDO Alliance are actively tracking and actively involved in these efforts.

4. FIDO Alliance's Objectives for Post-Quantum Cryptography

FIDO Alliance's objectives and approach to address post-quantum cryptography (PQC) include:

- Provide a seamless transition from the currently defined algorithm to PQC algorithms.
    - This applies to both providers and Relying Parties.
- Active tracking of PQC algorithm development.
    - Not all PQC algorithms may be suitable for FIDO Alliance specifications. Our intention is to track the various algorithms, and the security agency recommendations, to determine their effectiveness.
- Ensure that each FIDO Alliance working group understands the impacts of PQC algorithms and crypto-agility, define the migration strategy, and track the external dependencies of their standards (i.e., IETF efforts).
- Continue to provide guidance as PQC algorithms development and standardization progresses as well as the dependent standards.

5. Summary

Acknowledging the dynamic nature of PQC algorithm development, the FIDO Alliance has delegated the responsibility to each working group to understand the impacts of these algorithms and monitor the external dependencies of their respective specifications and processes. This includes tracking efforts in related organizations such as the IETF. Furthermore, as PQC-safe algorithms progress in development and standardization, the FIDO Alliance remains dedicated to providing ongoing guidance and ensuring alignment with dependent standards to maintain the security and efficacy of its work.

The FIDO Alliance has set a key objective in addressing PQC, aiming to facilitate a smooth transition from the currently defined algorithms to PQC alternatives. This objective encompasses authenticator providers, relying parties, and Internet of Things (IoT) device manufacturers. The organization is actively monitoring the development of PQC algorithms, recognizing that not all algorithms will be suitable for integration into FIDO Alliance processes. To effectively assess their viability, the FIDO Alliance is committed to tracking various PQC algorithms, evaluating their performance, and determining their applicability to its specifications and processes.

The FIDO Alliance Working Groups will align and enhance the FIDO Alliance Specifications to provide a seamless, compatible, and safe transition to the new algorithms for a consistent user experience.

6. Glossary of Terms

Term	Definition
CTAP	Client to Authenticator Protocol (all versions)
FDO	FIDO Device Onboarding
IETF	Internet Engineering Task Force
KEM	Key Encapsulation Mechanism
MDS	Metadata Service
NIST	United States National Institute of Standards and Technology
PQC	Post Quantum Cryptography

7. Standards, Agencies and Industry Organizations

Standards, Agencies or Industry Organizations	Example Effort
ANSSI	https://www.ssi.gouv.fr/uploads/2023/09/follow_up_position_paper_on_post_qua
BSI	https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Inform
China competition	https://www.cacrnet.org.cn/site/content/854.html
ETSI CYBER QSC	https://portal.etsi.org/tb.aspx?tbid=856&SubTB=856#/
IETF	https://wiki.ietf.org/group/sec/PQCAgility
ISO/IEC JTC1 SC27 WG2	https://committee.iso.org/files/live/sites/jtc1sc27/files/resources/sc27wg2-sd8-data.zip
NIST	Post-Quantum Cryptography | CSRC (nist.gov)
NSA	https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/
South Korea competition	https://www.kpqc.or.kr/competition.html

8. References

[1] NIST: NIST PQC: Looking Into The Future

https://csrc.nist.gov/csrc/media/Presentations/2022/nist-pqc-looking-into-the-future/images-media/session-1-moody-looking-into-future-pqc2022.pdf

[2] CISA: Quantum-Readiness: Migration To Post-Quantum Cryptography

Quantum-Readiness: Migration to Post-Quantum Cryptography (cisa.gov)

[3] NIST: Post Quantum Cryptography:

https://csrc.nist.gov/Projects/post-quantum-cryptography

[4] NIST: Comments Requested on Three Draft FIPS for Post-Quantum Cryptography:

https://csrc.nist.gov/news/2023/three-draft-fips-for-post-quantum-cryptography

[5] NIST: Post-Quantum Cryptography: Digital Signature Schemes:

https://csrc.nist.gov/projects/pqc-dig-sig/round-1-additional-signatures