Public Comments on NIST IR 8547 (ipd),
Transition to Post-Quantum Cryptography Standards

Comment period: November 12, 2024 – January 10, 2025

On November 12, 2024, NIST published NIST IR 8547 (Initial Public Draft), Transition to Post-Quantum Cryptography Standards. NIST solicited public comments to be sent by email until January 10, 2025.

Including Ascon family in NIST IR 8547

From Sonmez Turan, Meltem (Fed) [redacted]
Date Fri 1/10/2025 9:27 AM
To Moody, Dustin (Fed) [redacted]; Perlner, Ray A. (Fed) [redacted]; Regenscheid, Andrew R. (Fed) [redacted]; Robinson, Angela Y. (Fed) [redacted]; Cooper, David (Fed) [redacted]
Cc lightweight-crypto <lightweight-crypto@nist.gov>

Dear authors of NIST IR 8547,

I am forwarding the Ascon team's email regarding NIST IR 8547. We can work together to make sure that Ascon AEAD and the hash functions (currently draft) are mentioned in the final version.

As the lightweight crypto group, we would appreciate receiving an early copy of our publications involving symmetric cryptography before they are published. (Apologies if we have overlooked the email.)

Best,
Meltem

From: Martin Schläffer [redacted]
Sent: Wednesday, January 8, 2025 10:45 AM
To: lightweight-crypto <lightweight-crypto@nist.gov>
Cc: ASCON [redacted]
Subject: Re: Draft Ascon standard v1

Dear NIST LWC team,

...

NIST IR 8547 ipd (Transition to Post-Quantum Cryptography Standards): We have read the document with great interest, but miss Ascon in the list of algorithms. We think adding Ascon will help industry adoption. Ascon-AEAD128 should have level 1 security, which can likely be increased by nonce masking. Ascon-Hash256, Ascon-XOF128 and Ascon-CXOF128 should have level 2, like SHAKE-128. We would appreciate it if you could discuss this with the authors of NIST IR 8547. We could also make an official comment if you think this might be helpful?

Best regards,

The Ascon team

#	Type	Line #	Comment	Suggested Change
1	T	Table 3, row 1	FIPS 204 allows the security category of ML-DSA-44 to vary based on the security strength of the RBG used to generate the seed (section 3.6.1p. 12): "For ML-DSA-44, the RBG **should** have a security strength of at least 192 bits and **shall** have a security strength of at least 128 bits. If an approved RBG with at least 128 bits of security but less than 192 bits of security is used, then the claimed security strength of ML-DSA-44 is reduced from category 2 to category 1." Of course this only applies to key generation, and not signature generation / verification, but it might still be useful to mention in a footnote.	Add a footnote to the security category "2" for ML-DSA-44 stating that "The security category for ML-DSA-44 is reduced to category 1 if an approved RBG with less than 192 bits of security is used."
2	E	499	Pre-hash ML-DSA and SLH-DSA don't necessarily need separate entries in the table, but it might be useful to mention that the digest algorithm used needs to provide at least the same classical security strength as the ML-DSA or SLH-DSA parameter set.	Add the following sentence: "FIPS 204 and FIPS 205 specify pre-hash versions of ML-DSA and SLH-DSA. As explained in these standards, the digest algorithm used to perform pre-hashing must provide at least the same classical security strength as the ML-DSA or SLH-DSA parameter set."
3	E	Table 5, row 2	"ML-DSA-768" should be "ML-KEM-768"	Change to "ML-KEM-768"
4	E	Table 5, row 3	"ML-DSA-1024" should be "ML-KEM-1024"	Change to "ML-KEM-1024"
5	E	592	The dot after “Digital Signature standard.” has gray background but rest of the text does not.	Remove the background color for the dot.

Comment on draft NIST IR 8547

From [redacted]
Date Wed 11/27/2024 4:39 AM
To pqc-transition <pqc-transition@nist.gov>

Hello,

I would like to submit a comment on the initial public draft, dated November 2024, of the document NIST IR 8547 “Transition to Post-Quantum Cryptography Standards”.

START OF COMMENT

Section 3.2 discusses hybrid schemes for both key establishment and digital signature, combining a classical algorithm and a PQC algorithm into a composite mechanism, intended to be secure as long as at least one of the component algorithms is secure. It states that such hybrid approaches may be used in the initial transition to PQC.

Section 4.1 then proposes dates after which classical algorithms will be deprecated or disallowed – but here there is no guidance about hybrid schemes. If, after a certain date, a classical algorithm is disallowed (or deprecated), is that algorithm also disallowed (or deprecated) as a component of a hybrid scheme? I suggest that the document needs greater clarity on this point.

END OF COMMENT

Best regards,

Prof. Steve Babbage
BabbageWorks Limited
[redacted]

Feedback on NIST IR 8547 ipd

From Bartelt Andreas (C/CYG-GP) [redacted]
Date Fri 1/10/2025 3:58 PM
To pqc-transition <pqc-transition@nist.gov>

Hello,

I'm responsible for the internal policy on cryptography at Bosch. The special publications from NIST in scope of cryptography are among the most relevant and valuable sources for deriving this Bosch-internal crypto policy. Use cases in Enterprise IT as well as Bosch products are in scope.

I've looked into various sources which try to estimate the timeline if/when a CRQC could be practically built. My current understanding is that we can't rule out that a CRQC could be practically built at some point in the future. Nevertheless, the gap between the current state of quantum computers and a future CRQC is still exceedingly large (e.g., many orders of magnitude with regard to physical qubit scaling as well as the error rate at the level of logical qubits). It's also still unclear if it actually will be possible to solve all the many remaining challenges in the future in order to practically build a CRQC.

Due to the "harvest now, decrypt later" scenario, I agree with the assessment that addressing confidentiality in scope of PQC is typically relatively more urgent than addressing authenticity. Luckily, the engineering tradeoffs for integrating ML-KEM (e.g., as a hybrid solution) are typically acceptable for most use cases. Unfortunately, the same is not true for the relatively less urgent problem in scope of PQC migration (e.g., integration of ML-DSA into TLS would typically result in an additional round-trip during handshake due to the commonly used initial window size for TCP which is also determined at a different network layer). Consequently, in my understanding, it would only be a reasonable tradeoff to integrate PQC signature schemes into protocols like TLS if it's foreseeable that a CRQC could likely be practically realized in the next couple of years. I don't see this kind of urgency at the moment.

I fully agree with the consideration from sections 3.1.2 and 3.1.3. Unfortunately, this prioritization doesn't seem to be sufficiently reflected yet in table 2 since quantum-vulnerable digital signature algorithms will generally be disallowed after 2035. In my understanding, starting in 2030+, for a significant fraction of use cases it would be a more adequate strategy to keep quantum-vulnerable digital signature algorithms at deprecated until the CRQC threat is more imminent. The document already acknowledges that migration timelines may vary based on the specific use case or application [441-448]. However, the current revision of the document isn't very specific about the kinds of use cases which would warrant a longer migration timeline. My concern is that without a more clear differentiation, generally disallowing quantum-vulnerable digital signature algorithms after 2035 will result in a lot of unneeded PQC migration efforts and solutions with significantly worse engineering tradeoffs (e.g., in scope of embedded use cases; signatures during crypto protocol handshakes; protection of short-lived data; protection of low-value data; etc.).

Mit freundlichen Grüßen / Best regards

Andreas Bartelt

Cyber Security - Governance Product IT (C/CYG-GP)
Robert Bosch GmbH | Postfach 30 02 20 | 70442 Stuttgart | GERMANY | www.bosch.com
Tel. | Mobil [redacted]

Sitz: Stuttgart, Registergericht: Amtsgericht Stuttgart, HRB 14000;
Aufsichtsratsvorsitzender: Prof. Dr. Stefan Asenkerschbaumer;
Geschäftsführung: Dr. Stefan Hartung, Dr. Christian Fischer, Dr. Markus Forschner,
Stefan Grosch, Dr. Markus Heyn, Dr. Frank Meyer, Katja von Raven, Dr. Tanja Rückert

Feedback on "Transition to Post-Quantum Cryptography Standards" (NIST IR 8547)

From (Abel C. H. Chen) [redacted]
Date Thu 12/19/2024 3:16 AM
To pqc-transition <pqc-transition@nist.gov>
Cc (Austin Lin) [redacted]; (Abel C. H. Chen) [redacted]

Dear NIST Information Technology Laboratory,

My name is Abel C. H. Chen, and I am writing from Chunghwa Telecom Laboratories.

It has been a great privilege to review the document Transition to Post-Quantum Cryptography Standards (ID: NIST IR 8547 ipd). The content provides comprehensive and thorough guidance, which I found extremely insightful and valuable.

During my review, I noticed a few minor issues that I would like to bring to your attention for reference:

Page	Line	Comment
10	399	Consider formatting "Z" in italics.
17	552	Suggest adding the full name of IKE as "Internet Key Exchange."

If there is anything further I can assist with in the future, please do not hesitate to let me know.

Thank you for your time and consideration.

Best regards,
Dr. Abel C. H. Chen

Senior Member of IEEE.
Senior Research Fellow, Chunghwa Telecom Laboratories
Google Scholar: https://scholar.google.com/citations?user=8sofsmgAAAAJ
E-mail: [redacted]

本信件可能包含中華電信股份有限公司機密資訊,非指定之收件者,請勿蒐集、處理或利用本信件內容,並請銷毀此信件. 如為指定收件者,應確實保護郵件中本公司之營業機密及個人資料,不得任意傳佈或揭露,並應自行確認本郵件之附檔與超連結之安全性,以共同善盡資訊安全與個資保護責任.
Please be advised that this email message (including any attachments) contains confidential information and may be legally privileged. If you are not the intended recipient, please destroy this message and all attachments from your system and do not further collect, process, or use them. Chunghwa Telecom and all its subsidiaries and associated companies shall not be liable for the improper or incomplete

transmission of the information contained in this email nor for any delay in its receipt or damage to your system. If you are the intended recipient, please protect the confidential and/or personal information contained in this email with due care. Any unauthorized use, disclosure or distribution of this message in whole or in part is strictly prohibited. Also, please self-inspect attachments and hyperlinks contained in this email to ensure the information security and to protect personal information.

Comments on NISTIR 8647, Transition to Post-Quantum Cryptography Standards

From Deirdre Connolly [redacted]
Date Thu 11/14/2024 10:55 AM
To pqc-transition <pqc-transition@nist.gov>

Please clarify the hybrid constructions that will comply with the 'allowed schemes' and parameters as listed in tables 3 and 5, and that hybrid constructions whose 'primary' algorithm (the equivalent of the producer of Z in section 3.2.1) is one of the algorithms w/ appropriate parameter set in tables 3 and 5 are considered compliant as of the deprecated and disallowed dates.

Please clarify the hybrid/composite signature constructions mentioned in section 3.2.2 that are allowed/compliant. Section 3.2.1 leverages concrete techniques from SP 800-56A to guide how hybrid key-establishment may be done in an allowed manner, section 3.2.2 is more vague and leaves room for possibly too much diversity and filling in the gaps.

Deirdre Connolly

Submitter or Submitting Organization				Crypto4A Technologies Inc.	
Page #	**Starting Line #**	**Ending Line #**	**Section #**	**Comment/Rationale**	**Proposed Change**
1	89	90	1	Need to safeguard both confidentiality and integrity.	Change "confidential electronic" to "both the confidentiality and the integrity of electronic". Change "access" to "accesses".
3	167	167	2.1.1	The comment that the S-HBS private key consists of a large set of OTS keys should include a comment regarding the use of a seed-based PRNG-generated OTS keyset as an alternative implementation.	
4	208	208	2.1.3	You may want to provide an example for the key-hash construction item to clarify it.	Add the text "(e.g., Message Authentication Codes or MACs)" to the end of the line.
6	254	258	2.2.3	Hardware modules are both the providers of cryptographic services (the updating of which is nicely stated here) and the consumers of cryptographic services which is not discussed. We think there should be some language indicating the internal processes/components of the modules need to transition to quantum-safe mechanisms/methods as well (e.g., FW update, secure boot process(es), object transfer between modules, object wrapping for external storage, etc.).	Add text to capture the need for the devices themselves to migrate to quantum-safe internal processes/components to ensure the module is PQC-compliant.
6	264	269	2.2.4	Question: should we mention the notion of composite/hybrid certificates at some point in this section? We could refer them to section 3.2 for additional information.	If necessary, add some text broaching the topic of composite/hybrid certificates and refer the reader to section 3.2 for details.
7	281	295	3	The section would benefit from a more general perspective where it's not just data at risk but both data and roots of trust as long-lived signatures should be a concern, even if Mosca's theorem didn't explicitly mention non-data elements. We're doing a disservice by ignoring this aspect of the problem as it oversimplifies things by making it seem like we just need to address the harvest-now-decrypt-later aspect when we should be assessing non-data elements using the same X + Y >= Z metric as a silicon root of trust that needs to provide assurance for Y years better have been implemented by (Z - X) or we may have a serious issue.	Add some text to ensure the long-lived signature aspect is adequately addressed and added to the prioritization discussion.
7	292	295	3	There should be a mention of long-lived signatures as they need to be addressed sooner rather than later so they should be prioritized as such, along the same urgency as addressing the harvest-now-decrypt-later problem.	Add text referencing the long-lived signature requirement(s).
8	333	337	3.1.3	Suggest splitting this paragraph into two so that the last sentence becomes its own paragraph.	Split paragraph at start of last sentence ("The cryptographic...").
8	339	347	3.1.4	This section should include some discussion around the length of lifetime of some of these document signatures as those documents may need to persist for a very long time. This should in turn lead into the discussion of long-lived signatures and the need to prioritize their PQC transition too as only the harvest-now-decrypt-later aspect seems to be discussed.	Add some text discussing the missing elements.
8	349	352	3.2	Is there any consideration being given to hybrids composed from two quantum-safe algorithms or is this strictly addressing only one quantum-safe + one quantum-vulnerable combinations?	If necessary, add some text mentioning other types of potential hybrids.
9	381	381	3.2.1	Simple typo.	Change "composite" to "composition".
11	450	450	4.1	Simple typo.	Remove one of the two references to "[SP800131A]".
17	550	552	4.2	The prioritization discussion only mentions harvest-now-decrypt-later but it should include long-lived signatures as there are a number of use cases (e.g., satellites, certain document records, silicon-based secure boot w/limited space for trust anchors, etc.) where we need to transition authentication roots-of-trust as urgently as we need to address the harvest-now-decrypt-later concerns.	Add some text discussing the need to prioritize certain long-lived signature use cases.

All	1	742	All	In general, this document seems to be overly fixated on the harvest-now-and-decrypt-later problem when discussing priorities. The long-lived signature concern is just as important for use cases where the those signature lifetimes exceed the time remaining until we're being told is Q-day (i.e., 5 or 10 years depending on a 2030 or 2035 deadline). There will be numerous use cases where this threshold will be violated, making the migration of the associated roots of trust as important, if not more important, than the harvest-now-decrypt-later scenario -- we need to migrate those over BEFORE that condition occurs. In the civilian space it's all about identity/authentication/integrity so we need to ensure we're including these use cases in the cold calculus of prioritizing the PQC transition. We feel that is not being done in this document, whereas other agencies/entities (e.g., BSI et.al. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf) have acknowledged the concern and are ensuring it is highlighted appropriately. It would be nice to see stronger language drawing attention to this concern to ensure it doesn't get overlooked/ignored in the transition discussion.	If necessary, add language throughout the document that ensures the long-lived signature use case is properly accounted for in all analyses and prioritization activities.
All	1	742	All	We believe the traditional approach of gradually phasing out cryptographic algorithms based on anticipated advances in computational power is fundamentally flawed in the context of the Quantum Era. Unlike the gradual erosion of safety margins seen with classical cryptographic attacks, the advent of Cryptographically Relevant Quantum Computers (CRQCs) presents a sudden and catastrophic risk, a "cliff function," so to speak. While classic digitial signatures used in short-lived real-time authentication protocols can continue to function securely up until the 2035 PQC transition deadline, long-lived digital signatures and roots of trust needeed to be transitioned immediately.	We strongly recommend that NIST reflect this “paradigm shift” in its guidance by providing readers and practitioners with clear and robust strategies to prepare for this rapidly approaching future. Additionally, we suggest that NIST consider addressing the fundamental change in techniques for managing the demise of classical algorithms at the very beginning of the document. Providing a series of examples to clarify this new concept would further enhance the document’s value for its audience.

January 10, 2025

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930
VIA Email
pqc-transition@nist.gov

Re: *NISTIR 8547: Transition to Post-Quantum Cryptography Standards*

To whom it may concern,

CTIA[1] is pleased to submit this letter regarding the initial public draft of NISTIR 8547, Transition to Post-Quantum Cryptography Standards (Draft), which provides target dates for deprecation and disallowance of quantum-vulnerable cryptographic algorithms in existing NIST and Federal Information Processing Standards (FIPS) publications.[2] While NIST's proposals are focused on standards that are applicable to federal agencies, these deprecation and disallowance timelines will also impact government contractors that provide services or capabilities that must adhere to NIST or FIPS standards, and may indirectly impact the private sector, as NIST intends this guidance to "inform…stakeholder's efforts and timelines for migrating information technology products, services, and infrastructure to PQC."[3]

With these comments, CTIA reiterates the unique challenges that the transition to quantum-resistant algorithms pose for the wireless industry and urges NIST to: (1) more clearly explain the applicability of the proposed timelines in the Draft NISTIR 8547 and how its latest guidance fits together with other federal workstreams; (2) adopt a risk-based approach that acknowledges the complexities inherent in the transition to quantum-resistant cryptography and incorporates flexibility for non-federal information systems; (3) defer to global industry-led standards bodies on developing quantum-resistant cryptography transition timelines for non-federal information systems; and (4) expand

[1] CTIA – The Wireless Association® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless providers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. CTIA represents a broad diversity of stakeholders, and the specific positions outlined in these comments may not reflect the views of all individual members. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] NISTIR 8547 Initial Public Draft, Transition to Post-Quantum Cryptography Standards, NIST, at 3 (Nov. 2024), https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf ("Draft NISTIR 8547") ("Section 4.1 provides the transition plan for the quantum-vulnerable algorithms in [FIPS and NIST SP 800-series] standards.").

[3] *Id*. at 2.

its information sharing and collaboration efforts with industry and global standards bodies on quantum-resistant federal standards development.

I. QUANTUM-RESISTANT CRYPTOGRAPHY POSES CRITICAL OPERATIONAL AND TIMING CHALLENGES FOR THE WIRELESS INDUSTRY.

The development of quantum computing promises many benefits, including for the wireless communications industry. For example, quantum search algorithms could possibly increase the energy efficiency of wireless networks.[4] Some have speculated that quantum algorithms could improve other aspects of telecommunications, such as finding the optimal route in a classical wireless network.[5] As companies race to develop quantum computers, even more wireless use cases may emerge. At the same time, the advent of quantum computing also poses critical challenges for the wireless industry with respect to developing and transitioning to quantum-resistant algorithms and standards. As CTIA has previously advised NCCoE, the impact of new quantum-resistant algorithms will be acute for the wireless industry, and the transition will present operational and timing challenges and will require ongoing coordination among various stakeholders.

One of the primary operational hurdles to incorporating quantum-resistant algorithms into wireless protocols is key length. For example, Level 5 of the CRYSTALS-Dilithium algorithm chosen for digital signature standardization is about 18 times the size of the standard 256-byte RSA algorithm used today. Existing applications may be unable to deploy large algorithms, and existing infrastructure will likely need to be adjusted to address performance and scalability issues. Shifting to new algorithms will also be disruptive to the communications supply chain. Purchasers will need to begin examining their procurement processes to ensure that components can use new algorithms, as well as consider crypto-agility strategies for their supply chains.

There must also be sufficient lead time to implement quantum-resistant algorithms. The process to develop, standardize, and implement quantum-resistant algorithms will be lengthy and complex. Once algorithms are standardized, the standards will need to be built into Internet and wireless protocols through work by IETF and 3GPP. For example, IETF's Transport Layer Security (TLS) protocol standard will need to be updated, as will the associated public key infrastructure. Integration of these quantum-resistant cryptographic algorithms will also impact other standards, such as Wi-Fi and VoLTE. Addressing these timing issues will require close coordination among industry, 3GPP, IETF, ITU-T, and NIST, as well as other standards stakeholders.

Given the unique and critical impact of quantum computing and quantum-resistant cryptography on wireless, as well as the broader Communications Sector, the industry has been proactively planning and preparing for the transition, especially to ensure that the transition does not disrupt the 5G ecosystem. To this end, the CSCC published an Impact Report on Post Quantum Cryptography ("CSCC

[4] Comments of CTIA, Study to Advance a More Productive Tech Economy, Docket No. NIST-2021-0007, at 27 (filed Feb. 15, 2022), available at https://www.regulations.gov/comment/NIST-2021-0007-0059.

[5] *Id.*

Report") in July 2023.[6] The CSCC Report—available here—outlines the impact of this impending transition for the Communications Sector, focusing on the inherent challenges posed by the scale of deployments, the performance requirements of key protocols, and the international coordination required for any changes to protocol standards.

II. NIST'S GUIDANCE SHOULD BE CLEAR, RISK-BASED, AND FLEXIBLE.

A. NIST Should Clarify the Scope of Its Guidance and How the Draft Fits with Other Federal Workstreams.

To promote clarity, NIST should more clearly state that its proposed transition timeline—as outlined in the Draft—applies only to NIST and FIPS standards for federal information systems. While the underlying NIST and FIPS standards discussed in the Draft are mandatory for federal agencies, some language in the Draft discusses these standards being used for nonfederal systems[7]—a statement that could be read to inadvertently confuse the scope of these documents. To avoid confusion, NIST should state clearly, as it does in relevant FIPS publications, that its guidance is voluntary for non-federal organizations.[8]

Additionally, NIST should consider adding context for NISTIR 8547 to explain its interaction with other ongoing quantum-resistant cryptography workstreams within the federal government. CTIA applauds NIST for including a glossary of terms in NISTIR 8547 as such a resource provides clarity and promotes standardized terminology across an emerging ecosystem that often uses different definitions. Building from this and including an explanation of NISTIR 8547's role within the broader federal post-quantum federal workstreams would add even more clarity.

B. The Draft Should More Fully Acknowledge the Complexities Inherent in the Transition to Quantum-Resistant Cryptography.

As illustrated above with respect to the Communications Sector, the transition to post-quantum cryptography will be lengthy and multifaceted. NIST should more explicitly acknowledge these operational and timing challenges, in order to appropriately account for them. NIST should also consider adding a discussion about other complexities that will be critical to understand and account for during the transition. For example, NIST should acknowledge that there various "options to take systems from quantum vulnerable to quantum resistant,"[9] acknowledging that each path presents unique issues and may require different timelines. As the CSCC Report details, "given the magnitude of the

---

[6] *The Engineer Who Cried Quantum: Emerging Technologies Committee Impact Report on Post Quantum Cryptography*, Communications Sector Coordinating Council, available at https://www.comms-scc.org/2023/07/31/the-engineer-who-cried-quantum/ (last visited Jan. 9, 2025) ("CSCC Report").

[7] Draft NISTIR 8547 at 11 ("NIST's cryptography standards provide comprehensive guidance on a broad spectrum of cryptographic mechanisms that are essential for securing sensitive information across both federal and nonfederal systems.").

[8] FIPS 197: Advanced Encryption Standard, NIST, at iii, (updated May 9, 2023), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf ("Federal Information Processing Standards apply to information systems used or operated by federal agencies, a contractor of an agency, or other organization on behalf of an agency…This Standard may be adopted and used by non-Federal Government organizations.")

[9] CSCC Report at 6.

[post-quantum] transition, a one-size-fits-all approach is not viable;" rather, there are several migration options, including one-time migration and hybrid solutions.[10] NIST should also acknowledge that there are complex interdependencies throughout any given ecosystem, and these interdependencies may complicate or extend timelines for certain transitions. For example, there will be interdependencies with respect to a company and its third-party vendors, including third-party cloud service providers. Other complexities include competing security priorities that may affect the investment and deployment schedules for Post-Quantum Cryptography ("PQC").

In addition to discussing the various challenges, NIST should consider providing a high-level description of the steps that would be involved in implementing the new algorithms by the 2030 and 2035 target dates, to ensure that it is fully accounting for the various complexities.

C. NIST's Guidance Should Be Risk-Based and Flexible.

NIST has been a champion for a risk-based approach to emerging technologies, including through landmark work products such as the Cybersecurity Framework and the AI Risk Management Framework. NIST's PQC standards should be no different; however, NIST's timeline by which certain standards are disallowed or become deprecated is broad and does not appear to account for different levels of risk for different types of information. For example, while NIST's proposed 2035 timeline for disallowing identified quantum-vulnerable cryptographic standards is generally consistent with other timing expectations for some of the most sensitive data to transition to fully quantum-resistant cryptography[11]—NIST should not apply this same timeline to all federal systems. Instead, NIST should acknowledge in NISTIR 8547 that the risk profile of National Security Systems differs from civilian federal agencies' systems (and it will also differ from non-federal systems, which may be impacted by NIST's guidance, as well).

CTIA concurs with NIST's statements that "flexibility in migration planning is essential,"[12] and to this end, NIST should bolster its focus on flexibility, especially with respect to applying its guidance voluntarily to non-federal systems. As mentioned above, the wireless sector will have specific hurdles in its transition to quantum-resistant algorithms. Other sectors will face their own unique challenges, and, even at the organizational level, there will be various novel considerations. NIST should consider explicit statements that the goal timelines may be subject to change depending on the progress of technological implementation.

III. NIST SHOULD COORDINATE WITH AND DEFER TO STANDARDS BODIES ON PQC TRANSITION TIMELINES.

NIST is a key player in developing the PQC standards and implementation guidance. However, when applying guidance to the private sector, NIST should defer and coordinate with standards-setting

[10] CSCC Report at 2; *See also* Draft NISTIR 8547 at 9 (CTIA also concurs with NIST's intent to "accommodate the use of hybrid techniques in its cryptographic standards to facilitate the transition to PQC where their use is desired.").

[11] *See The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ*, Version 2.0, NSA (April 2024), available at https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF.

[12] Draft NISTIR 8547 at 11.

bodies on updating relevant global industry-led standards to harmonize its approach with similar ongoing efforts. Standards bodies with proven and reliable track records, such as 3GPP in the wireless space, should take the lead when it comes to incorporating quantum-resistant algorithms into relevant standards, including wireless standards. This standards-based approach is preferable to any top-down regulation of emerging technologies. It is also consistent with longstanding U.S. policy that has championed standards-setting bodies that emphasize transparency, consensus, and technical innovation.[13] NIST should move quickly to collaborate closely with those standards bodies because, as noted above, coordinating and updating multiple standards across numerous applications will take many years.

IV. NIST SHOULD EXPAND ITS COOPERATION AND INFORMATION SHARING EFFORTS WITH INDUSTRY.

NIST should continue to expand its cooperation and information sharing efforts on PQC migration with key private sector stakeholders and provide more transparency on those efforts. NIST acknowledges that it plans to "coordinate with standards-developing organizations and industry to ensure that critical security protocols and technologies are updated to support PQC in a timely manner,"[14] but does not discuss details on its efforts or a method for industry to engage. A collaborative approach that incorporates feedback from a range of stakeholders will allow NIST to understand and address the challenges associated with implementing quantum-resistant cryptography. NIST should specifically take steps to engage with industry beyond the specified private-sector collaborators and support additional information sharing efforts, as more rapid information sharing related to the project will allow industry to be better poised for future adoption of new algorithms.

* * *

CTIA appreciates NIST's efforts to create and implement quantum-resistant cryptography and looks forward to future collaboration on this important issue.

Sincerely,

/s/ Justin C. Perkins

Justin Perkins
Director, Cybersecurity & Policy

CTIA
1400 16th Street, NW
Washington, DC 20036
202-736-3200
www.ctia.org

[13] *See U.S. Government National Standards Strategy for Critical and Emerging Technologies Implementation Roadmap*, White House (July 2024), available at https://www.whitehouse.gov/wp-content/uploads/2024/07/USG-NSSCET_Implementation_Rdmap_v7_23.pdf.

[14] Draft NISTIR 8547 at 17.

Comments from the Department of Veterans Affairs

NIST IR 8547 Transition to Post Quantum Cryptography Standards

Comments Due: January 10, 2025Email Comments to: pqc-transition@nist.gov

Section	Line Number(s)	Comments
2.2 Cryptographic Technologies and Components	N/A	It would be beneficial to put in guidance around Legacy systems/mainframe systems that may not have the capacity or capability to transition to PQC algorithms. Per the White House's Report on Post-Quantum Cryptography (July 2024) these systems, and those with cryptography embedded within their firmware will likely be the most difficult and most costly systems to address for PQC. Guidance that specifically addresses these types of systems would help create a more standardized approach to transitioning them.
3.1 Use Cases	N/A	With processing and memory limitations, transitioning to PQC on embedded systems/IoT/IoMT devices may not be feasible. Adding a sub-section that talks about lightweight/hybrid solutions to enhance crypotographics to better secure the sensitive data on these embedded systems would be helpful.

ERICSSON

Date: January 10, 2024

Ericsson AB
Group Function Technology
SE-164 80 Stockholm
SWEDEN

Comments on NIST IR 8547
Transition to Post-Quantum Cryptography Standards

Dear NIST,

Thanks for your continuous efforts to produce open-access security documents. Please find below our comments on the initial public draft of IR 8547:

The US government has been the clear thought leader in PQC migration with excellent advice [1–3] such as:

> *"Create migration plans that prioritize the most sensitive and critical assets."*
>
> *"prioritize the assets that would be most impacted by a CRQC, and that would expose the organization to greater risk"*
>
> *"Prioritization should be given to high impact systems, industrial control systems (ICSs), and systems with long-term confidentiality/secrecy needs."*
>
> *"This prioritization schema ensures that agency will focus their resources on defending the cryptography, functions, and data most vulnerable to a CRQC. Once migration begins, agencies will continuously re-assess their prioritization and timelines."*

The new requirement in NIST IR 8547 to deprecate ECC and RSA by 2030 is in stark conflict with the above recommendations. FIPS 203–205 are just hot off the press, and it will take several years until hardened and certified hardware and software implementations are available, and even more years before they can be deployed in practice. As NIST correctly states, cryptographic migration has in the past often taken 20 years after standardization, the transition to PQC is unprecedented in scale, and for many applications the new PQC algorithms are not a drop-in replacement. Almost 100% of all

existing hardware as well as hardware that are deployed in the next few years needs to be replaced in industries, health care, education, transport, telecom, and homes. For many use cases, turning off ECC and RSA by 2030 means that no prioritizations whatsoever are possible and that later standards such as FN-DSA, Classic McEliece, BIKE, HQC, MAYO, UOV, HAWK, FEAST, etc., are not even an option.

One implication of this new 2030 deprecation in NIST IR 8547 is that most industries will go for 100% hybrids aligning with ANSSI's and BSI's requirements that "*Post-quantum algorithms must be hybridized*" [4] and "PQC only in hybrid solutions" [5]. When SIKE was presented at the first PQC workshop, Shamir said: *"I don't think this should be deployed in the next 20 years".* Similar things can be said about early implementations, many of them have severe implementation bugs and side-channels. The 2030 deprecation date for RSA and ECC means that industry need to pick the very first available implementations of ML-KEM and ML-DSA and use them in production systems, which without hybrid schemes creates unacceptable risks.

NSA expects the transition to quantum-resistant algorithms for NSS to be complete by 2035 [6]. It is hard to understand why the US government thinks that Mr. Arkko's connected toaster [7] should follow the same timeline as US national security systems protecting highly classified data that need to be confidential for many decades. Formulated differently, it is hard to understand why the US national security systems do not have harder requirements than Mr. Arkko's connected toaster.

We suggest that NIST IR 8547 is rewritten with a strong focus on prioritization. Firm dates for deprecation and disallowment of quantum vulnerable algorithms are better handled in future revisions of SP 800-131A [8]. Both prioritization and timelines should be continuously re-assessed.

A rewritten NIST IR 8547 focusing on prioritization should include:

- Different recommendations for federal agencies, industries, and the general public, which are the groups NIST states its recommendations are for.
- Different recommendations depending on use case (long-term roots-of-trust for firmware update, binding signatures for non-repudiation, short-term signatures for authentication, encryption of classified data, encryption of metadata, etc.).
- Different recommendations based on the required protection lifetime of the node or data.
- Different recommendations based on how long-time migration takes (already deployed hardware vs. easily updatable software)
- Value of the protected node or data. Early CRQCs will most likely be very expensive, meaning that early attackers will focus on very high-value targets [9].

The rewritten NIST IR 8547 can, for example, define four categories (ranging from most time-sensitive, Category I, to least critical, Category IV) with differing migration timelines and provide guidance on how to identify the appropriate category. The actual assessments should be deferred to industry-led standardization bodies, which have the in-depth knowledge of how NIST algorithms are utilized, the required protection lifetimes, the value of the protected node or data, and the timelines for

system upgrades driven by other factors. Such an industry-led, standards-based approach is vastly preferable to top-down regulation and fosters technical innovation and economic growth.

The broad-brush approach required by NIST IR 8547 can have severely negative consequences.

- A broad-brush approach without prioritization may lead to that highly prioritized systems are updated later than they should be. In case of delays due to complication in the migration, which does not seem unlikely, some of the most prioritized systems might miss the 2030 deadline.

- If and when a CRQC will be developed is still uncertain. Already now deciding that almost all deployed hardware in all industries need to be replaced comes with astronomical economical costs. It is not unlikely that we in 2035 are still very far from building a CRQC. Nvidia CEO Jensen Huang recently said that the quantum computers won't be "very useful" for 15–30 years [10]. And even a very useful quantum computer is far from being a CRQC.

- NIST is the de facto global crypto SDO driving long-term cryptographic standards. NIST requirements have always been seen as very reasonable taking practical security and existing deployments into account. Requirements that are seen as unreasonable, like replacing all existing hardware and downgrading constrained IoT to symmetric group keys without PFS, might lower trust in NIST as a global SDO.

Comments:

- The report should clarify early on that "deprecated" and "disallowed" also apply to already deployed hardware, much of which cannot be updated. Organizations striving to use only "acceptable" cryptography will need to replace almost all existing hardware, as well as hardware deployed over the next few years, before January 1, 2031.

- The report should emphasize that migration of algorithms for firmware signing is urgent. CNSA 2.0 requires that the first use case to migrate to PQC should be the asymmetric algorithm used for digitally signing firmware and software [11]. We agree with the NSA. Hardware is often in use for many decades, and unlike software implementations, the algorithms for firmware signing typically cannot be updated once deployed.

- *"These guidelines had projected that NIST would disallow public-key schemes that provide 112 bits of security on January 1, 2031. However, based on the need to migrate to quantum-resistant algorithms during this timeframe, NIST intends to instead deprecate classical digital signatures at the 112-bit security level."*

  SP 800-57 disallow 112 bits of security from 2031 minus the lifetime of the protected data. For most encryption use cases 112-bits is already disallowed. We are strongly against NIST changing the previously required timeframe. Changing the timeframe distorts market competition and unfairly benefits companies that have neglected their cryptographic hygiene. While it is very uncertain when or if CRQCs will be built, it is very certain that hostile nation states will be able to break 112-bit security in a few decades.

- *"Cryptographic algorithms … future quantum computing may be able to break these algorithms"*

  Quantum computing will never be a practical threat to any symmetric crypto [12–13]. As explained in the keynote at CHES 2024, a quantum computer breaking a single AES-128 key would require qubits covering the surface area of the Moon [14].

- *"FIPS 186 specifies the Elliptic Curve Digital Signature Algorithm (ECDSA) and adopts the RSA algorithm specified in RFC 8017 and PKCS 1 (version 1.5 and higher)"*

  RFC 8017 is the latest version of PKCS #1. FIPS 186 does not refer to any earlier versions of PKCS #1. RSASSA-PKCS1-v1_5 is included in PKCS #1 Version 2.2. Suggestion:

  "FIPS 186 specifies the Elliptic Curve Digital Signature Algorithm (ECDSA) and adopts the RSA algorithm specified in RFC 8017 (PKCS #1 Version 2.2)"

- *"These algorithms are vulnerable to Shor's Algorithm on a cryptographically relevant quantum computer."*

  Might be good to inform the reader about the existence of the new state-of-the-art Ekerå-Håstad and Regev algorithms, which are based on Shor's algorithm and significantly improves it [9].

- *"Due to this need to maintain state, HBS schemes are not intended for general use".*

  We think the document should state the intended use case instead of writing what it is not for.

- *"However, hybrid solutions add complexity to implementations and architectures, which can increase security risks and costs during the transition to PQC."*

  We think NIST should also emphasize the security risks of deploying early implementations of cryptographic algorithms. Early implementations often have implementation bugs and side-channels.

  NIST has done a truly excellent work with the standardization of ML-KEM and ML-DSA. ML-DSA offer strongly unforgeability (SUF-CMA), and both ML-KEM and ML-DSA exclusively utilize SHA-3, which has superior properties to SHA-2, and is much easier to protect against side-channel attacks. NIST should caution readers about the limitations of hybrid solutions that only achieve EUF-CMA or combine ML-KEM and ML-DSA with SHA-2.

- *"Such approaches are not considered hybrid solutions if each session only uses a single cryptographic algorithm"*

  Very good that NIST highlights this issue. We have seen unserious companies promoting such solutions as hybrid implantations. Related to this, NIST should also emphasize the differences in migrating to PQC within protocols that do or do not support algorithm negotiation. For protocols with algorithm negotiation, such as TLS, IKEv2, and EDHOC, adding support for PQC algorithms can significantly enhance security. However, for protocols without algorithm negotiation, such as

S/MIME and firmware updates, security improvements are only realized when RSA and ECC are fully disabled on the receiving side.

John Preuß Mattsson,
Expert Cryptographic Algorithms and Security Protocols
MSc Engineering Physics/Theoretical Computer Science
MSc Business Administration and Economy

[1] Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/

[2] Quantum-Readiness: Migration to Post-Quantum Cryptography
https://www.cisa.gov/sites/default/files/2023-08/Quantum Readiness_Final_CLEAR_508c%283%29.pdf

[3] Report on Post-Quantum Cryptography
https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

[4] ANSSI plan for post-quantum transition
https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_jerome-plut_anssi_anssi-plan-for-post-quantum-transition.pdf

[5] Post-Quantum Policy & Roadmap of the BSI
https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_stephan-ehlen_bsi_post-quantum-policy-and-roadmap-of-the-bsi.pdf

[6] Announcing the Commercial National Security Algorithm Suite 2.0
https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[7] Now, Even Granny's Fuzzy Slippers Are Texting You
https://www.wsj.com/articles/SB10001424052702303544604576434013394780764

[8] Transitioning the Use of Cryptographic Algorithms and Key Lengths
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

[9] On factoring integers, and computing discrete logarithms and orders, quantumly
https://www.wsj.com/articles/SB10001424052702303544604576434013394780764

[10] Quantum Computing Stocks Dive After Nvidia CEO Says Tech 15-30 Years Away
https://www.msn.com/en-us/news/technology/quantum-computing-stocks-dive-after-nvidia-ceo-says-tech-15-30-years-away/ar-AA1x8Tix

[11] Announcing the Commercial National Security Algorithm Suite 2.0
https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[12] IETF Statement on Quantum Safe Cryptographic Protocol Inventory
https://datatracker.ietf.org/liaison/1942/

[13] 3GPP Statement on PQC Migration
https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_118_Hyderabad/docs/S3-244307.zip

[14] Quantum Attacks on AES
https://www.youtube.com/watch?v=eB4po9Br1YY&t=3227s

Lightweight Crypto and PQC Effort Plans?

From Figueroa, Wilson [redacted]
Date Wed 11/13/2024 10:49 AM
To Moody, Dustin (Fed) [redacted]
Cc Figueroa, Wilson [redacted]

Hello Mr. Moody.

NIST recently released the public draft - Lightweight Cryptography Ascon family in SP 800-232.

NIST also recently released a for comment NISTR for the PQC Transition (NIST IR 8547).

Would the Ascon algorithms meet the Security Category level 1 (AES-128) in the NISTR?

Are the Ascon algorithms considered quantum – safe since I only see a specific Ascon-80pq?

Are all the Ascon family algorithms considered quantum safe at Security Level 1?

If so, should they be part of the NISTR as we are seeing an explosion in IoT / IIoT and D2D devices and such things also require cryptography?

Lastly, previous crypto specs included human readable summaries with a small example. Will anything like this be done for the new PQC algorithms as they are much more challenging for those of us not familiar with the math used and even reading the specs is difficult?

Thank you for this wonderful NISTR document.

~Wilson

Wilson Figueroa
Deputy Chief Information Security Officer
Government Systems
[redacted]
T.
Viasat

wrong reference in NIST.IR.8547.ipd.pdf

From Hippler Marco, EE-441[redacted]
Date Tue 11/19/2024 8:23 AM
To pqc-transition <pqc-transition@nist.gov>

Dear NIST Team,

On page 15 DSAs are referenced instead of KEMs:

Table 5: Post-quantum key-establishment schemes

Key Establishment Scheme	Parameter Sets	Security Strength	Security Category
ML-KEM [FIPS203]	ML-KEM-512	128 bits	1
	ML-DSA-768	192 bits	3
	ML-DSA-1024	256 bits	5

Regards,
Marco Hippler

CONFIDENTIAL

NIST IR 8547 and hybrid mechanisms

From Paul Hoffman [redacted]
Date Wed 11/13/2024 6:41 AM
To pqc-transition <pqc-transition@nist.gov>

Thank you for the opportunity to comment on the draft of NIST IR 8547.

Section 3.2 talks extensively about hybrid protocols, but hybrid protocols are not discussed at all in Section 4. This omission from Section 4 needs to be rectified before the final version is published.

--Paul Hoffman

IDEMIA comments about the NIST IR 8547

From GONZALVEZ Alexandre [redacted]
Date Fri 1/10/2025 4:16 AM
To pqc-transition <pqc-transition@nist.gov>
Cc GIRAUD Christophe [redacted]; LE DU Fabien [redacted]; DOTTAX Emmanuelle [redacted]; BOUDINEAU Jerome [redacted]; DISCHAMP Paul [redacted]; BETTALE Luk [redacted]

Dear Dustin,

Please find below IDEMIA comments about the NIST IR 8547 document named “Transition to Post-Quantum Cryptography Standards”:

- Clarification on the requirements for the hybrid signature mechanism in paragraph 3.2.2. are kindly requested to ensure practical implementation. The document fails to clearly specify whether both signatures (pre-quantic and post-quantic) are required to be binding collectively and whether they must be generated together rather than independently.
- Regarding section 4, algorithms acceptable between 2030 and 2035 are marked baldly disallowed in 2035 without any transitional state. Continuing to use something as if it were acceptable just a few months before it becomes prohibited seems unusual. Additionally, users (decision maker, stakeholder,…) might not understand the need to transition to more secure algorithms, or they may be reluctant to make the change before the deprecation. Perhaps the document should suggest a smoother transition to be more realistic between 2030 and 2035, as described in the following example:

Year	≤ 2030	2031	2032	> 2035
112-bits	Acceptable	Deprecated	Deprecated	Disallowed
128-bits	Acceptable	Acceptable	Deprecated	Disallowed

Kind regards,

Alexandre

January 10, 2025

National Institute of Standards and Technology (NIST)
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

Submitted via email: pqc-transition@nist.gov

RE: ***Transition to Post-Quantum Cryptography Standards***
NIST IR 8547 ipd (Initial Public Draft)

Dear NIST Authors:

Infineon Technologies Americas Corp. ("Infineon") is pleased to comment on the National Institute of Standards and Technology ("NIST") effort to address the timely transition to Post-Quantum Cryptography ("PQC") standards.

Infineon designs, develops and manufactures a broad range of semiconductors and system solutions. Our semiconductors enable smart mobility, energy efficiency and secure connectivity. Infineon makes secure chips for credit cards and contactless payment, as well as Trusted Platform Modules ("TPM"s) which help to secure data on computers and also for connected vehicles, as well as Internet of Things devices ("IoT") devices. Infineon is a long-term, trusted partner of the federal government providing security technology for the e-Passport, a leader in international security standards-setting bodies, and works closely with device manufacturers on a variety of hardware-based security solutions.

Regarding NIST IR 8547 ipd, Infineon is seeking clarity from NIST on what the disallowance of RSA/ECC after 2035 means for legacy devices, e.g., devices that are already deployed and not easily updatable. As a provider of security solutions in a wide variety of end uses, it is important to note that many of these devices can have long lifetimes; even devices built before the publication of the first PQC-standards might eclipse the proposed 2035 date, including but not limited to: automobiles (15-20 years of operation); Supervisory Control and Data Acquisition ("SCADA") systems (greater than 15 years of use); identity cards and passports (typically 10 years of use). Moreover, existing hardware security platforms may not have enough compute power and/or memory to accommodate a PQC transition (e.g., not updateable over the air). Equally, many of these embedded applications require interoperability specifications which are not currently in place for any of the proposed transition deadlines. Even when the various

Infineon Technologies Americas Corp.
2600 Virginia Ave. NW, Washington, DC 20037
www.infineon.com

interoperability specifications are available, there will need to be a transition plan as each "old" is rotated out of the field for the "new" updated PQC-capable device.

Infineon would encourage NIST to consider a hybrid approach where both new and old are supported to realistically facilitate a workable transition. In other situations (not PQC) there have been hybrid approaches to address the interoperability transition.

Separately, for certification schemes, such as the Federal Information Processing Standards ("FIPS"); usually a year prior to reaching "disallowed" status, the Cryptographic Module Validation Program ("CMVP") releases a transition policy explaining what happens with certificates. The certificate will likely end up on the "historical list", meaning that it can't be used for new designs, but existing products don't need to be updated. There is often a "revalidation" option which allows for the removal of the disallowed algorithm in the certificate.

Thanks again for your work on this important effort. I am happy to help facilitate access to Infineon experts in this space should you have questions or seek additional information.

Regards,

Patrick Thompson
Director, Government Relations
Infineon Technologies Americas Corp.

Comment to NIST IR 8547 - Transition to PQC Standards

From Anja Lehmann [redacted]
Date Fri 1/10/2025 2:23 PM
To pqc-transition <pqc-transition@nist.gov>
Cc Anna Lysyanskaya [redacted]

Dear NIST Team,

The NIST Internal Report NIST IR 8547 details its plans for the transition to post-quantum cryptography. For digital signatures it states that the classically secure algorithms ECDSA, EdDSA and RSA will be fully disallowed after 2035. The report is already more nuanced when it comes to user authentication (Sec 3.1.2) and states that authentication systems "may continue to use quantum-vulnerable algorithms until quantum computers that are capable of breaking current, quantum-vulnerable algorithms become available".

Nevertheless, we are concerned that the report can currently be misunderstood to indicate that *any* classically secure cryptography will be disallowed after 2035. This interpretation could have a negative impact on the Digital Identity systems that are currently being developed around the globe.

When building digital identity systems for people, it is essential that the secure authentication does not harm their privacy, and users can authenticate in a pseudonymous and unlinkable manner. In fact, the eIDAS regulation even mandates both features for the European Identity Wallet which must be available by the end of 2026. Therefore, there are currently serious efforts to create a privacy-preserving identity system, and the fear is that they will be abandoned if NIST declares that post-quantumness is required for everything starting in 2035.

At the moment, all practical and mature cryptographic solutions that are capable of providing the necessary privacy features rely on discrete-logarithm-based or RSA-based assumptions. And while the research on quantum-safe solutions has made great progress over the last few years, they are not ready for deployment yet, and will not be ready in the tight timeframe mandated by the eIDAS regulation.

We believe that building a privacy-preserving identity system with classically secure cryptography is currently the only feasible path to ensure that the protection of users' privacy is built into such a critical infrastructure. Bringing these cryptographic techniques to actual deployment will also fledge out the most essential properties and design criteria – which gives the research community a clear and concrete target of what has to be redeveloped in a quantum-safe manner.

Thus, to not harm this process we would suggest to clarify that transition to quantum-safe algorithms is only necessary for applications and requirements for which mature solutions exist and should not be

misunderstood as a general ban of all classically secure cryptography.

Best regards,
Anja Lehmann & Anna Lysyanskaya

--

Prof. Dr. Anja Lehmann

Hasso-Plattner-Institut für Digital Engineering gGmbH
Digital Engineering Fakultät | Universität Potsdam
Prof.-Dr.-Helmert-Straße 2-3, D-14482 Potsdam

Amtsgericht Potsdam, HRB 12184 P
Geschäftsführung: Prof. Dr. Tobias Friedrich
Prof. Dr. Ralf Herbrich, Dr. Marcus Kölling

Comments for NIST IR 8547

From Faye Loe [redacted]
Date Thu 1/2/2025 11:04 AM
To pqc-transition <pqc-transition@nist.gov>

Hello @pqc-transition@nist.gov,
I have read through your IPD for the Transition to Post-Quantum Cryptography Standards https://doi.org/10.6028/NIST.IR.8547.ipd and I have a number of items for discussion.

#1 Section 4.1.1: '*However, based on the need to migrate to quantum-resistant algorithms during this timeframe, NIST intends to instead deprecate classical digital signatures at the 112-bit security level.*'

AND

Section 4.1.2: '*Similar to the transition for digital signature algorithms, NIST intends to instead deprecate rather than fully disallow classical key-establishment schemes at the 112-bit security level.*'

Is my understanding correct based on these statements that on SP 800 57 part 1 rev 5 in Section 5.6.3, that the item in Table 4 below:

Table 4: Security strength time frames

Security Strength		Through 2030	2031 and Beyond
< 112	Applying protection	Disallowed	
	Processing	Legacy use	
112	Applying protection	Acceptable	Disallowed
	Processing		Legacy use
128	Applying protection and processing information that is already protected	Acceptable	Acceptable
192		Acceptable	Acceptable
256		Acceptable	Acceptable

Will instead be 'Deprecated' until 2035, and thereafter Disallowed?

My recommendation is that this is made clearer in the document.
For example, working at Jaguar Land Rover, especially with embedded hardware-based cryptography, planning for our upgrades often requires hardware replacements for our vehicle ECU's.
Therefore, if we can work with 'deprecated' until 2035 (with the acceptance of the risks involved) this certainly gives us more runway to address our transition timelines.

#2 Section 4.1.2: Minor editorial point for Table 4, it would be nice to have a line in between the 112 bits of security strength and >=128 bits of security strength to identify the Deprecated and Disallowed states. For example, the first row of Table 2 in Section 4.1.1 has this line for the ECDSA item and it is much easier to read.

#3 Section 4.1.3: Minor editorial point - the citations to the SP and FIPS standards for the hash functions, XOFs, block ciphers, KDFs, and DRBG's may be helpful. For example, it is useful to look at SP 800 108r1 upd1 to see that the PRF's are HMAC, CMAC, or KMAC based (i.e. no quantum vulnerable public-key cryptography is used), or for the DRBG's that SP 800 90A r1 is Hash or block cipher based (i.e. no longer any reliance on the Dual EC).

#4 Section 4.1.3: In Table 7, can I double check the pre-image security strength for SHAKE256. In the IPD you have this noted at 512 bits:

531 **Table 7: Hash functions and XOFs**

Hash/XOF Algorithm Family	Variants	Collision Security Strength	Collision Security Category	Preimage Security Strength	Preimage Security Category
SHA-1 [FIPS180]	SHA-1	80 bits	< 1	160 bits	1
SHA-2 [FIPS180]	SHA-224 SHA-512/224	112 bits	< 1	224 bits	3
	SHA-256 SHA-512/256	128 bits	2	256 bits	5
	SHA-384	192 bits	4	384 bits	5
	SHA-512	256 bits	5	512 bits	5
SHA-3 [FIPS202]	SHA3-224	112 bits	< 1	224 bits	3
	SHA3-256	128 bits	2	256 bits	5
	SHAKE128	128 bits	2	128 bits	2
	SHA3-384	192 bits	4	384 bits	5
	SHA3-512	256 bits	5	512 bits	5
	SHAKE256	256 bits	5	512 bits	5

532

However in FIPS 202 you have the pre-image security strength as >=min(d,256).

Function	Output Size	Security Strengths in Bits		
		Collision	Preimage	2nd Preimage
SHA-1	160	< 80	160	$160 - L(M)$
SHA-224	224	112	224	$\min(224, 256 - L(M))$
SHA-512/224	224	112	224	224
SHA-256	256	128	256	$256 - L(M)$
SHA-512/256	256	128	256	256
SHA-384	384	192	384	384
SHA-512	512	256	512	$512 - L(M)$
SHA3-224	224	112	224	224
SHA3-256	256	128	256	256
SHA3-384	384	192	384	384
SHA3-512	512	256	512	512
SHAKE128	d	$\min(d/2, 128)$	$\geq \min(d, 128)$	$\min(d, 128)$
SHAKE256	d	$\min(d/2, 256)$	$\geq \min(d, 256)$	$\min(d, 256)$

Thank you for taking the time to consider my comments ahead of the Jan. 10, 2025 deadline.

Kind Regards,

Dr Faye Loe (she/her/hers)
Head of Cryptography
Cryptography Centre of Excellence (CCoE)

T:
E: [redacted]

Base site address: Jaguar Land Rover Limited, Abbey Road, Whitley, Coventry, CV3 4LF, UK

Registered in England Number 1672070

CONFIDENTIALITY NOTICE: This e-mail message including attachments, is intended only for the person to whom it is addressed & may contain confidential information. Any unauthorised review; use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

typo in NIST IR 8547 draft

From Yann Loisel [redacted]
Date Thu 11/14/2024 8:00 AM
To pqc-transition <pqc-transition@nist.gov>

Hello
Table 5 refers to ML-KEM but two references are made to ML-DSA
Best regards

--

Yann Loisel
Principal Security Architect

SiF[redacted]

W: wwwsifive.com

comments on NIST IR 8547

From Matusiewicz, Krystian [redacted]
Date Fri 1/10/2025 3:34 PM
To pqc-transition <pqc-transition@nist.gov>
Cc Dobraunig, Christoph [redacted]; Sastry, Manoj R [redacted]

Hello,

I'd like to start with expressing gratitude for putting together this much needed document.
Please consider the following couple of comments on the text:

1/ The inclusion of hybrid solutions is very useful, in particular it aligns with the guidance issued by some European agencies (BSI, ANSSI).
It would be good to see it as part of FIPS 140, as mentioned in Section 3.2.2.
One aspect that could be clarified here is the question what would be the status of the hybrids after the 2035 cutoff date when the classical component of the scheme would be disallowed.

2/ The clear timeline for the transition, while recognizing that some use cases and industries might face adoption challenges, is greatly appreciated.
Perhaps a more fine-grained distinction between risk profiles where PQC transition is the top priority and those that may have extended transition period could alleviate some of the planning dilemmas for enterprises.

3/ Table 6 in Section 4.1.3 mentions only AES. It would be beneficial to include also ASCON (upcoming NIST SP 800-232) in that category.

4/ Section 4.1 mentions block ciphers, hash functions but does not have any explicit mention of MACs or modes of operation. It would be worth adding guidance regarding these constructions for completeness.

Thank you again for preparing this document and driving the PQC transition efforts.

With best regards,
Krystian Matusiewicz
Intel Product Assurance & Security

Intel Technology Poland sp. z o.o.

ul. Słowackiego 173 | 80-298 Gdańsk | Sąd Rejonowy Gdańsk Północ | VII Wydział Gospodarczy Krajowego Rejestru Sądowego - KRS 101882 | NIP 957-07 52 316 | Kapitał zakładowy 200 000 PLN

Spółka oświadcza, że posiada status dużego przedsiębiorcy w rozumieniu ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych

Ta wiadomość wraz z załącznikami jest przeznaczona dla określonego adresata i może zawierać informacje poufne W razie przypadkowego otrzymania tej wiadomości, prosimy o powiadomienie nadawcy oraz trwałe jej usunięcie; jakiekolwiek przeglądanie lub rozpowszechnianie jest zabronione

This e mail and any attachments may contain confidential material for the sole use of the intended recipient(s) If you are not the intended recipient, please contact the sender and delete all copies; any review or distribution by others is strictly prohibited

Comments on NIST IR 8547 ipd

From Arne Padmos [redacted]
Date Thu 1/9/2025 9:34 PM
To pqc-transition <pqc-transition@nist.gov>

Dear NIST PQC-transition team,

The 'Transition to Post-Quantum Cryptography Standards' draft report provides much-needed guidance for those planning their PQC transition. While there are some small errors already flagged on the pqc-forum, here I want to focus on two high-level points. One issue is the importance of highlighting the utility of hybrid KEMs, such as X25519MLKEM768, which are looking to become (or have already become) the de-facto standard for contemporary TLS and SSH implementations. This, together with examples such as PQ3 and PQXDH, evidences that initiating the transition to quantum-safe hybrid KEMs is feasible for general-purpose applications *starting today*.

Secondly, while the draft report correctly flags store-now-decrypt-later attacks as the primary issue, the transition deadlines for KEMs and signatures are the same. I find this peculiar and would have expected much much more aggressive timelines for encouraging the roll-out of (hybrid) KEMs and/or allowing organisations to make risk-based decisions regarding the timing of transitioning to quantum-safe signatures. As NIST has emphasised in the announcement accompanying the first set of PQC standards released on 13 August 2024, 'NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible'. This, in combination with the draft report flagging store-now-decrypt-later attacks as 'a pressing threat', would imply that section '4.1.2. Key Establishment' should at a minimum flag all KEMs listed in Table 4 as 'Deprecated' from the date of publication of NIST IR 8547. Based on the definition of the term 'Deprecated' in the draft report, this is exactly what all asset owners should already be doing when it comes to confidentiality requirements vis-a-vis quantum-vulnerable key establishment: 'Deprecated means that the algorithm and key length/strength may be used, but there is some security risk. The data owner must examine this risk potential and decide whether to continue to use a deprecated algorithm or key length.' This shouldn't be limited only to the application-specific guidance referred to in lines 508–511.

The situation with respect to quantum-vulnerable signatures is different (with some exceptions that are already flagged in the draft report). Especially in closed-loop systems where one organisation has end-to-end control of the full architecture, transitioning quantum-vulnerable signatures at a fixed date makes much less sense than allowing for a risk-based transition (provided solid implementations are available and a tested playbook is in place). Of course, one could state that cryptographic agility is a myth – e.g. see how the financial industry will likely continue to use 3DES for the foreseeable future – arguing

that a combined transition is the best approach. However, NIST has highlighted the virtue and importance of cryptographic agility in the 'Crypto-Transition and Agility' presentation last year. As such, it's a hard sell saying a two-pronged transition isn't possible.

I am aware that NSM-10 defines the explicit goal of 'mitigating as much of the quantum risk as is feasible by 2035'. Even so, it is critical that this goal be interpreted with a clear understanding of what constitutes quantum risk. As flagged in the draft report, data encrypted today is vulnerable to store-now-decrypt-later attacks. Unless (hybrid) ML-KEM is applied to data whose value extends beyond 2035 (or 2040 if using the estimates from BSI's recent report), the requirement to mitigate as much risk as possibly by 2035 is not met. As such, I would argue that NSM-10 actually requires NIST to base transition timelines on a clear risk assessment instead of shoehorning transition timelines into the magic number 2035. Interestingly, such a risk assessment is already present in NIST IR 8547 ipd, e.g. in lines 104–110, lines 290–295, lines 302–307, lines 314–319, lines 333–337, and lines 442–445. However, the outcome of this risk assessment is not (sufficiently) translated into the transition schedules of KEMs versus signatures specified in the last section of the draft report.

Finally, it should be noted that lines 283 and 284 appear needlessly fatalistic. While full migration will likely take over a decade and might never be completed, many applications can and should be encouraged to transition *now* to hybrid KEMs. This addresses inherent risk to data with long-term protection requirements, but it might also serve to increase the cost of identifying higher-value data in bulk intercepts as well as acting as a safety net in the not-uncommon scenario where asset owners aren't intimately familiar with the data they are tasked to protect (let alone the security requirements for said data).

Regards,
Arne

Comment on NIST IR 8547 initial public draft

From Bertram Poettering [redacted]
Date Fri 1/10/2025 4:34 PM
To pqc-transition <pqc-transition@nist.gov>

Dear authors of NIST IR 8547,
please find below three comments on the current draft of the document.

Regarding Sec 3.2.1 "Hybrid Key-Establishment Techniques":

Lines 383-387 suggest a specific way to construct a hybrid key establishment scheme. Lines 390-392 explain that "the desired property of hybrid techniques is that derived keys remain secure if at least one of the component schemes is secure". Together this suggests that the method of lines 383-387 meets this desired property. However, whether it does or not crucially depends on the security notion that is expected. In most practical applications the only acceptable notion is security against active adversaries (sometimes referred to as CCA security), and in this case the method of lines 383-387 does not represent a secure solution. (To see this, consider lines 383-387 used to construct a composite of (1) an IND-CCA secure KEM (e.g., ML-KEM) and (2) a KEM with malleable ciphertexts (e.g., a KEM where session keys do not depend on all ciphertext bits); this composite will have malleable ciphertexts as well, and in particular not be IND-CCA secure.)

Suggestion: (1) Remove details from lines 383-387 so that no specific construction method is suggested; instead point to SP 800-227 for technical details. (2) Reformulate lines 392-394, cautioning that, unless carefully implemented, the use of hybrid techniques may actually lead to reduced security.

Regarding Sec 3.2.2: "Hybrid Digital Signature Techniques"

Lines 402-406 suggest a dual-signature combiner where (composite) signatures are verified by verifying each component signature separately. However, whether this is secure or not depends on the security notion that is expected. If existential unforgeability is expected ("EUF"), this combiner is secure. But if strong unforgeability is expected ("SUF"), it is not. (To see this, consider ML-DSA combined with ECDSA: the well-known malleability attack on ECDSA will directly translate to also the composite scheme; in contrast to ML-DSA in isolation, the composite is hence is not SUF secure.)

Suggestion: In Sec 3.2.2, caution that, depending on the pursued security goal, dual signatures may be weaker than the stronger component.

Editorial remark:

While lines 411-416 discuss both hybrid key establishment and hybrid signatures, they are organized as a part of Sec 3.2.2 (which is only on signatures). Suggestion: Add an appropriate new section header ("Sec 3.2.3: ...") between lines 410 and 411.

Public Comment on IR 8547

From Pascal Schärli [redacted]
Date Sat 11/30/2024 9:10 AM
To pqc-transition <pqc-transition@nist.gov>

1 attachment (641 bytes)

[redacted] 0x936EDD58.asc;

Dear NIST PQC Team,

I am commenting on NIST IR 8547, Transition to Post-Quantum Cryptography Standards. I have two remarks:

1. HARVEST NOW DECRYPT LATER

I suggest adapting Table 4 to add deprecation of key establishment schemes also with >= 128 bits of security in 2030.

While harvest now decrypt later attacks are covered and explained throughout the report, these differences are not reflected in Tables 2 and 4, where both signature schemes and key establishment schemes have the same migration timeline. The timeline in Table 4 is fine when the established keys are used for short-lived encrypted data or message authentication codes. However, when used for encryption of data where "harvest now decrypt later" is applicable, the transition of these key establishment techniques should be prioritized. This nuance is only reflected in the text and is lost in Tables 2 and 4, which is realistically the main point of reference that most organizations will implement.

Either Table 4 should be adapted as per my suggestion, or the Table should differentiate what the established keys of these schemes are being used for. However, this might add too much complexity, hence my suggestion of simply adding depreciation in 2030 for all key establishment schemes listed in Table 4, regardless of their parametrization.

2. HYBRID MODE

I suggest clarifying in Tables 2 and 4, that deprecation and disallowment do not apply if schemes are used in hybrid mode (i.e., within SP 800-56C once it's updated). Furthermore, in Tables 3 and 5, I suggest specifying that post-quantum algorithms have to be used in hybrid mode with conventional algorithms of at least the same security category.

Quantum algorithms are still lacking maturity and face implementation flaws, such as those exploited by KyberSlash. While the report acknowledges that the migration to post-quantum cryptography may initially include hybrid solutions, this is not reflected in Tables 2-5. You present several arguments against using hybrid schemes, such as the complexity they add to implementations and architectures. I disagree with this argument, as the construction of hybrid modes for signatures or key encapsulation methods is not very complex. I also disagree with the argument that using hybrid modes will necessitate a second transition to tools that use Post-Quantum Cryptography algorithms only. There is no security gain in removing the pre-quantum algorithm, so there will be no need to migrate existing algorithms that use hybrid approaches.

By implementing these two suggestions, we can ensure that these important points are also reflected in the Tables, which will likely be the main point of reference for most readers. This will help provide clarity and guidance for organizations navigating the transition to post-quantum cryptography.

Regards, Pascal Schärli

[pqc-forum] concatenation of key-establishment schemes

From pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
on behalf of
Falko Strenzke [redacted]

Date Wed 11/13/2024 1:17 AM

To pqc-transition <pqc-transition@nist.gov>

Cc pqc-forum <pqc-forum@list.nist.gov>

Dear NIST PQC Team,

I have a comment regarding Section 3.2.1. There it says:

[[line 383]]
NIST currently allows a generic composite key-establishment technique described in SP 800-56C [SP80056C]. Assume that the value Z is a shared secret that was generated as specified by SP 800-56A or 800-56B and that a shared secret T is generated or distributed through other schemes. The value Z'=Z||T may then be treated as a shared secret and any of the key derivation methods given in SP 800-56C may be applied to Z' to derive secret keying material. NIST intends to update SP 800-56C so that the value Z may be generated as specified by any current and future NIST key-establishment standards.

If I read this correctly, then the concatenation of the two shared secrets allows only to achieve NIST-compliance with respect to the key-establishment scheme that produces the first part, namely Z. But the hybrid construction cannot be claimed to be NIST-compliant with respect to the key-establishment scheme that produces T.

My question is whether it is possible to allow the concatenation construction to be NIST-compliant with respect to both key-establishment schemes. In my view this would be useful when using two NIST approved schemes together.

Best regards,
Falko

--

MTG AG
Dr. Falko Strenzke

Phone: [redacted]
E-Mail: [redacted]
Web: mtg.de

MTG AG - Dolivostr. 11 - 64293 Darmstadt, Germany
Commercial register: HRB 8901
Register Court: Amtsgericht Darmstadt
Management Board: Jürgen Ruf (CEO), Tamer Kemeröz
Chairman of the Supervisory Board: Dr. Thomas Milde

This email may contain confidential and/or privileged information. If you are not the correct recipient or have received this email in error, please inform the sender immediately and delete this email.Unauthorised copying or distribution of this email is not permitted.

Data protection information: Privacy policy

Thales Cybersecurity & Digital Identity, Comments on NIST IR 8457.

From COSTA Graham [redacted]
Date Fri 1/10/2025 12:40 PM
To pqc-transition <pqc-transition@nist.gov>
Cc SecurityCertifications [redacted] JOHNSON Darren [redacted]; GARDINER Michael [redacted]

THALES GROUP LIMITED DISTRIBUTION to email recipients

Dear NIST Team,

We appreciate the opportunity to comment on your draft NIST IR. We've collated our comments from Thales DIS and where these can be found below.

This is an important document to the cryptographic community and where we view this as an important opportunity to work with NIST to minimize the impact transitions outlined in this document may have on consumers of cryptography not just within the US federal government but in many cases globally.

Should you wish to discuss any of the comments further, please do not hesitate to get in touch.

Kind Regards,

Graham Costa (on behalf of Thales CDI).

Comment Number	Section / Line Number	Comment Type	Comment	Proposed Resolution
Thales_1	3.2.1 / line 386.	Technical	In relation to the following statement we've identified a problem if this is read as the ordering of the inputs to the KDF MUST always include the primary CSP first. At the moment, we are being encouraged to add post quantum inputs to KDF as the 'additional input'. That means that at the moment they would fall under 'T'. We want to avoid a situation in 2035 where existing modules are forced to re order the inputs. "*Assume that the value Z is a shared secret that was generated as specified by SP 800 56A or 800 56B and that a shared secret T is generated or distributed through other schemes. The value Z'=Z||T*	This was discussed on the PQC Forum where Angela Robinson (NIST) confirmed that in particular, ordering of Z and T as inputs to a SP 800-56C KDF would allow either 'Z || T' or 'T II Z'. We'd propose this clarification be added to a footnote in NIST IR 8457 to avoid confusion and to provide certainty on this matter.

Comment Number	Section / Line Number	Comment Type	Comment	Proposed Resolution
			may then be treated as a shared secret and any of the key derivation methods given in SP 800 56C may be applied to Z' to derive secret keying material."	
Thales_2		Technical	We have a concern for modules implementing hybrid solutions that the transition to disallowed various algorithms in 2035 will immediately require them to stop being used including a need for all vendors to actively remove the disallowed component from already certified/deployed product. We strongly encourage NIST toallow for the continued ability to exercise implementations of quantum vulnerable algorithms (where paired with PQC safe equivalents) beyond 2035 but for disallowed algorithms to being able to be documented as 'no security claimed'. This avoids an immediate need to update products implementing hybrid solutions until the point where it is practical for a given product to remove the latent implementation of the post-2035 disallowed cryptography.	The following clarification was made by Andrew Regenscheid (NIST) on the PQC Forum: *"To clarify, the disallowance of ECC and other quantum-vulnerable public key algorithms after 2035 in NIST IR 8647 was not intended to apply to hybrid modes that incorporate an approved PQC algorithm alongside a quantum vulnerable or unapproved algorithm in a composite scheme.* *When an algorithm is "disallowed" according to SP 800-131A or NIST IR 8547, it may no longer be used "for the stated purpose." Essentially one must assume that a disallowed digital signature scheme is vulnerable to forgeries, a disallowed key establishment scheme is vulnerable to key recovery attacks, etc. This is no different from any other algorithm that is not "approved."* *Our current and planned approach to hybrid modes would accommodate the use of unapproved algorithms alongside approved algorithms, provided the scheme is designed to remain secure if only the approved algorithm is secure. This*

Comment Number	Section / Line Number	Comment Type	Comment	Proposed Resolution
				applies whether the unapproved algorithm is one that has never been approved or is one that was previously approved but has become disallowed." We propose the principles outlined in this response are added to a NIST IR 8547 to give developers clarity on how the 2035 transitions are expected to be handled for modules choosing to use hybrid implementations.
Thales_3	Section 4.1, line 364-466.	Technical	THIS IS A DUPLICATE OF A THALES COMMENT RAISED ON SP 800-131Ar3 - disposition of the comment is encouraged to be consistent across SP 800-131Ar3 and NIST IR 8547. -- Legacy use is defined in NIST IR 8547 as: "*The algorithm or key length may only be used to process already protected information (e.g., decrypt ciphertext data or verify a digital signature)*." This is problematic in that this has been interpreted by CMVP as meaning that all data used with a algorithm classed as 'legacy' needs to be provably have been protected by the algorithm ahead of the date the algorithm transitioned to legacy. Our original reading of 'legacy' was that NIST had pragmatically created this category to allow older cryptographic systems to interact with (or support migration to) new systems. In the case of moving long-term keys (which may be	Add the following footnote linked to 'already protected information': "already protected information may have either: • had protection applied prior to target algorithms transition to legacy; or • has had protection applied by an older module to support interoperability or migration of keys to a newer cryptographic module. In this second example, objects would be protected after the transition of an algorithm to legacy but where this occurs outside the boundary of a module compliant to all recommendations of this IR and is permitted exclusively for module interoperability during transition periods between different cryptographic algorithms ahead of them becoming disallowed, and separately also for key migration."

Comment Number	Section / Line Number	Comment Type	Comment	Proposed Resolution
			valid for up to 30 years) this could involve encrypting these in an existing HSM that exclusively supports legacy algorithms for these keys to them be imported into a new module that supports the latest algorithms but also legacy encryption options for import. The problem with the current definition of 'legacy' is the different readings of 'already protected information'. In our case, we want to read this as it being OK to decrypt key objects passed in to a current HSM from an older HSM being retired. As mentioned above, CMVPs first read of above is to tie 'already protected' to a timeline linked to the when the algorithm transitioned to legacy. This doesn't work for support crypto estate migration to newer equipment where encryption using the legacy algorithm would need to occur today (or in the future) but where the current generation module would exclusively support decryption using the legacy algorithm.	
Thales_4	2.1.2.	Editorial	Section 2.1.1 on Digital signature algorithms includes the following statement: "These algorithms are vulnerable to Shor's Algorithm on a cryptographically relevant quantum computer." The same statement however is not included in section 2.1.2. on Key Establishment which could lead a reader to understand that the attacks linked to Shor's algorithm weren't applicable to Key Establishment and listed algorithms such as Diffie Hellman and Menezes-Qu-Vanstone. This is not the case.	Add: "*These algorithms are vulnerable to Shor's Algorithm on a cryptographically relevant quantum computer.*" on line 186 between the list of existing algorithms and the paragraph listing FIPS 203.

Comment Number	Section / Line Number	Comment Type	Comment	Proposed Resolution
Thales_5	Table 5.	Editorial	ML DSA 768 and ML DSA 1024 should be ML-KEM-768 and ML-KEM 1024	Correct DSA to KEM as proposed.
Thales_6	Section 1.1, line 121.	Editorial	The following sentence from section 1.1, suggests that 'legacy use' of quantum vulnerable algorithms will be permitted but where there are currently no instances of this present in chapter 5 on NISTS PQC transition timeline: *"This transition will involve the adoption of new PQC algorithms as well as the careful deprecation, **controlled legacy use**, and eventual removal of quantum vulnerable algorithms"*	Update sentence to be consistent with section 4. i.e. IF no algorithms are identified for 'legacy use' then this sentence should be updated to: *"This transition will involve the adoption of new PQC algorithms as well as the careful deprecation, and eventual removal of quantum vulnerable algorithms."*

Comments on NIST IR 8547

From Kaiduan Xie [redacted]
Date Sat 11/16/2024 11:26 AM
To pqc-transition <pqc-transition@nist.gov>
Cc Michele Mosca [redacted]

Hi,

I am a research associate at Institue of Quantum Computing, University of Waterloo under Professor Michele Mosca.

I read through the report of *Transition to Post-Quantum Cryptography Standards*, and have some comments below.

1. In Section 2.1.2 Key Establishment, it does not say if the algorithms specified in SP 800-56A/SP 800-56B are vulnerable to attack by quantum computer. However, Section 2.1.1 said clearly that algorithms in the SP 800-186 and SP800-208 are vulnerable to attack by quantum computer. Could you add to Section 2.1.2 please?

2. In Section 2.2.1, at line 236,

"other cases, more significant changes will be required to accommodate the larger sizes of the"

I think it should be the larger key sizes of the, key is missing here.

3. In Section 4.1.2 Table 5 at line 517,

ML-DSA-768 192 bits 3
ML-DSA-1024 256 bits 5

Should them be ML-KEM-768/ML-KEM-1024?

Many thanks for drafting this wonderful report!

Best regards,

/Kaiduan

Pqc-forum comments
https://groups.google.com/u/1/a/list.nist.gov/g/pqc-forum/c/uHMw8RNGkC8/m/BKI_b69gBAAJ

>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Michael Gardiner

Do you anticipate deprecating more options before 2035? Using something as if it was acceptable a few months before it transitions to disallowed seems odd. I would almost wonder why not mark them all deprecated in 2030 or 2033
perhaps.

Best Regards,
Michael

Nov 12, 2024

>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Can you please clarify whether the timeline for discouraging/disallowing ECC is also a timeline for discouraging/disallowing ECC+PQ?

For reasons explained in my pqc-forum posting dated 16 Oct 2024 21:14:23 +0200, I was hoping to see a document with (1) a much faster timeline for discouraging/disallowing ECC but (2) a clear statement that this isn't discouraging/disallowing ECC+PQ.

D. J. Bernstein

Nov 12, 2024

bruno writes:
> I read it as ECC is disallowed in hybrid or single use after 2035

With the current text, I expect a problematic split between readers interpreting it that way (disallowing ECC includes disallowing ECC+PQ hybrids), readers interpreting it the other way (the critical point is to include PQ, so of course disallowing ECC doesn't disallow ECC+PQ), and readers who aren't sure. So clarification is needed.

> and it make sense IMHO anyway starting to when a CRQC is available.

See https://blog.cr.yp.to/20240102-hybrid.html for comments on this.

Anyway, the goal of the White House directive at hand is "moving the maximum number of systems off quantum-vulnerable cryptography within a decade of the publication of the initial set of standards". ECC+PQ isn't

any more quantum-vulnerable than PQ is. A clear recommendation of ECC+PQ does a better job of encouraging a prompt move than recommending PQ.

---D. J. Bernstein

Nove 13, 2024

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

John Mattsson

Good with a clear date, 2035, for disallowment of RSA and ECC.

The first implication of this new very though requirement from US government is that Ericsson, telecom, and most other industries will very likely go for 100% hybrids aligning with e.g., ANSSI's requirement that "Post-quantum algorithms must be hybridized" [1]. When SIKE was presented at the first PQC workshop, Shamir said: "I don't think this should be deployed in the next 20 years". The same is true for early implementations, many of them have severe implementation bugs and the vast majority of them have horrible side-channels. We have previous had a lot of discussions internally about using non-hybrids, but I think this new requirement from US government puts an abrupt end to such discussions. The 2035 end date means that we need to pick the very first available implementations and use them in production systems.

As NIST correctly states, the journey from algorithm standardization (2024) to full integration into information systems can take 20 years. In retrospect, there should probably not have been such a long competition, but instead the most promising candidates should have been picked much earlier.

Dan Bernstein wrote:

>Can you please clarify whether the timeline for discouraging/disallowing

>ECC is also a timeline for discouraging/disallowing ECC+PQ?

My understanding of the definition "*disallowed - The algorithm or key length is no longer allowed for applying cryptographic protection*" is that a ML-KEM-512+P-521 hybrid would have a NIST security strength of 256 bit until 2035 when it drops to 128 bits (or category 1).

Cheers,
John

[1] https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_jerome-plut_anssi_anssi-plan-for-post-quantum-transition.pdf

Nov 12, 2024

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Paulo Barreto

The document states (section 4.1.3) that symmetric cryptography standards at the 112-bit level will be *disallowed* in 2030.

Presumably this includes SHA-224 and same-sized hashes, but aren't these required for ECDSA at the same security level? And yet, for the 112-bit level ECDSA will only be *deprecated* at that time, but not disallowed until 2035, so something is a bit off.

Maybe the text in section 4.1.3 is a typo and should read *deprecated* instead?

Paulo Barreto.

Nov 13, 2024

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Loganaden Velvindron

Dear Dustin,

Please kindly note that I would also suggest identifying and fixing
servers/middleboxes that don't read large TLS client hello messages
properly and instead downgrade to
classic TLS client hello messages.
(https://tldr.fail/).

This could be added to section 3.1.3. Network Security Protocols where
TLS migration strategy is discussed.

Nov 15, 2024

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

I wonder if there isn’t an error in Table 5, on page 15 of this document:

https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

The table appears to erroneously refer to ML-DSA-768 and ML-DSA-1024, whereas these should be (unless I’m mistaken) ML-KEM-768 and ML-KEM-1024.

Nadim Kobeissi
Symbolic Software • https://symbolic.software

Nov 19, 2024

>>

Arne Padmos

Another error appears to be present in table 7, 'Hash functions and XOFs', where SHAKE256 is noted to have 512 bits preimage security strength. Whereas table 4, 'Security strengths of the SHA-1, SHA-2, and SHA-3 function', from FIPS 202 highlights the maximum preimage and 2nd preimage strengths as 256 bits provided sufficiently long XOF output is used.

Regards,
Arne

Nov 19, 2024

>>

Dustin,

Substantive feedback:

I would add a glossary. It would be great for NIST to provide an authoritative definition to a bunch of terms that have lead to great deals of hallway arguments -- “post quantum” vs “quantum resistant” vs “quantum secure” vs “quantum safe”. Personally, I like the interpretation that “Post-Quantum” is simply a name for the set of algorithms that arose from the NIST Post-Quantum “Competition”, and that PQ algs can be used to build a “quantum-secure” or “quantum-safe” or “quantum-resistant” solution. Once you define these terms, you can straighten out your usage of them because I think you’re using a few of these interchangeably throughout. Also “classical” vs “traditional” vs “quantum-vulnerable” vs “quantum-cryptography (QKD and friends)”.

Are you brave enough (and is this document the right place) to take a stab at defining “cryptography agility”? This is a term in need of a robust definition, and I think some of the sections would benefit from it.

4.1

I notice that you have not given yourself the ability to move these timelines forward if quantum computer research progresses faster than expected.

Referring to EC / RSA by bit strength seems like it might be a bit of a moving goalpost over time if, for example, we see a big advancement in number field sieve that significantly drops all RSA variants’ security. Is this intentional? If so, it’s probably worth stating that explicitly.

Nitpicky feedback:

1. Introduction

“In response, NIST has released three PQC standards…” Why no mention of SP 800-208 here? It is mentioned further down in the document.

The framing of “harvest now, decrypt later” makes it seem like only encryption has urgency. Of course, there are also signature usecases with similar levels of urgency and criticality, let’s not downplay that.

1. Scope and Purpose

It might be worth expanding, even for one sentence, on why the PQC migration has an unprecedented scale -- you have to touch *everything*. And also unprecedented complexity – bigger size, KEMs don't fit cleanly into protocols designed for RSA or DH, etc.

2.1.2 Key Establishment

It might be worth a sentence describing that the three key establishment types described here (RSA, ECDH, ML-KEM) all have different APIs that cause them to behave differently, and therefore ML-KEM can not always be used as a direct drop-in-replacement to existing protocols and applications. You allude to this in 2.2.1, but I would bring it up here more explicitly. Another source of refactoring is the inordinate amount of RSA stuff that "cheats" and uses an encryption key to sign something like a CSR. You just won't be able to do this with PQC algs. A lot of registration flows are going to need serious re-thinking.

2.1.3 Symmetric Cryptography

I find your definition a bit wonky because hash functions, KDFs, and random bit generators don't have "keys", nor do they have "an operation and its inverse". Perhaps this would present cleaner if you split this section into "keyed" and "non-keyed" symmetric primitives?

2.2.1

You are using here the term "classical" for the first time. This probably deserves a proper definition up above.

Note: within the IETF, we prefer "traditional" – "quantum-vulnerable" is also popular -- because in physics "classical" is the opposite of "quantum", so you would assume that "classical cryptography" is anything that runs on my laptop, which includes both RSA and ML-KEM, and that the opposite is "quantum cryptography" which requires quantum hardware, such a QKD. In the end, you're probably good to use whatever terms you want, just define it clearly at the top.

2.2.2

Nit: JCA is not a library, it's just an interface (set of APIs) that any java-compatible crypto library has to implement. The java runtime ships with the Oracle SUN Provider as its default crypto library [1].

3 Migration Considerations

This wording really emphasizes that encryption is the only use-case with urgency, and not signatures. I would change "avoid having their encrypted data exposed" to "avoid having their cryptographically-protected data compromised". Similarly, the reference to "harvest now, decrypt later" should be accompanied by the signature equivalent, which unfortunately doesn't have a flashy name, but might be something like "eventual forgery of long-lived signed data".

3.1.1 Code Signing

Another case is that there's a lot of old software in the world. Go have a poke around your C:\Program Files and I bet you'll find some DLLs that were built in 2008 and are still happily running. Giving signed software packages the longest possible shelf-life is a good thing.

3.1.4

I find it a little odd that you're mentioning S/MIME here, but not OpenPGP, PDF signing, etc. And that you don't mention specific technologies / protocols in other subsections of 3.1.

3.2 Hybrids

You expected me to have lots to say here. No, this is well-written, I have no objections.

Table 1

Thank you for including this. This was actually fairly hard to find and reference before.

Table 5 has a typo: it lists ML-DSA parameter sets.

Table 7 is interesting. Am I supposed to infer that SHA-1 is still allowed in contexts where only preimage security is required? Is that actual NIST guidance? Am I allowed to take that to my lab and start using HMAC-SHA1 again?

[1]: https://docs.oracle.com/javase/6/docs/technotes/guides/security/SunProviders.html

---

Mike Ounsworth

Nov 19, 2024

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Hello all,

Regarding Tables 1 and 7, I noticed the following:

- In Table 1, only security categories 2 and 4 are defined in terms of collision searches. However, in Table 7, the column for collision security categories also contains values <1 and 5.
- Furthermore, Table 7 contains a column for "Preimage Security Category". However, the document does not explain what a "Preimage Security Category" is, in particular not in Table 1.

I know what it means, but I think some additional explanations to Table 1 would be good to make it easier for readers to interpret the terminology and information in Table 7 about security categories correctly.
The way it is written now, Table 7 seems to not match the definitions from Table 1 very well.

Best Regards | Viele Grüße
Mario Schiener
Nov 22, 2024
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>