



PANDUAN MIGRASI KE *POST-QUANTUM CRYPTOGRAPHY* VERSI 1.0

Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi
Badan Siber dan Sandi Negara

2025

PANDUAN MIGRASI KE *POST-QUANTUM CRYPTOGRAPHY* VERSI 1.0



Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi
Badan Siber dan Sandi Negara (BSSN)
Jl. Cijayanti No. 70, Kec. Babakan Madang, Kabupaten Bogor
Website : <https://www.bssn.go.id>
Email : humas@bssn.go.id

TIM PERUMUS PANDUAN

Pengarah : Tjahjo Khurniawan

Penanggung Jawab : Soetedjo Joewono

Tim Pereviu :

1. Martianus Frederic Ezerman, Ph.D.
(Nanyang Technological University, Singapura)
2. Dr. Pratama Dahlian Persadha
(Communication & Information System Security Research Center)
3. Christian Riesaputra
(Thales Indonesia)

Tim Penyusun :

1. Sari Agustini Hafman
2. Ratih Mumpuni Arti
3. Adang Rochiyat
4. Anjariah Dwi Astuti
5. Theresia Natalia
6. Novita Anggraini
7. Mohamad Rahmadi
8. Oky Jati Permana
9. Yhufi Swastantri Gustiviana
10. Siti Hikmatul Khasanah
11. Dian Yuda Paripurna
12. Andreas Lugas
13. Dandi Agus Ferdianto
14. Dewa Ari Baihaqi
15. I Ketut Yudi Sucipta
16. Rohiqi Maghtum Imama

Penyunting :

1. Sari Agustini Hafman
2. Ratih Mumpuni Arti
3. Mohamad Rahmadi
4. Oky Jati Permana
5. Siti Hikmatul Khasanah
6. Andreas Lugas

PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga buku *Panduan Migrasi ke Post-Quantum Cryptography Versi 1.0* ini dapat diselesaikan. Panduan ini lahir pada momentum yang sangat penting, ketika perkembangan komputasi kuantum global menghadirkan peluang besar sekaligus risiko serius terhadap ketahanan keamanan informasi nasional.

Kemampuan komputasi kuantum dalam memecahkan persoalan matematis kompleks secara eksponensial membuka untuk potensi melemahkan berbagai mekanisme kriptografi klasik yang selama ini menjadi fondasi perlindungan data nasional. Situasi ini menegaskan bahwa ancaman terhadap keamanan informasi tidak lagi bersifat jangka panjang, tetapi sudah mulai berdampak pada keamanan data strategis saat ini, termasuk risiko *harvest-now-decrypt-later*.

Menghadapi dinamika tersebut, komunitas internasional telah bergerak melalui standarisasi algoritma tahan-kuantum dan penyusunan model transisi oleh berbagai lembaga dunia. Indonesia harus mengambil langkah proaktif untuk memastikan kedaulatan digital dan keamanan siber nasional tetap terjaga di era pasca-kuantum. BSSN berkomitmen memimpin proses ini melalui kebijakan, koordinasi nasional, serta pembangunan kapasitas keamanan siber yang menyeluruh.



Panduan ini disusun sebagai acuan strategis dan operasional bagi seluruh Penyelenggara Sistem Elektronik, instansi pemerintah, dan pemangku kepentingan lainnya dalam melaksanakan migrasi menuju PQC secara aman, terukur, dan selaras dengan perkembangan standar internasional. Dokumen ini berisi kerangka dasar, tahapan migrasi, pendekatan penilaian risiko kuantum, serta prinsip *cryptographic agility* sebagai bagian dari strategi pertahanan siber nasional.

Selain itu, panduan ini disusun selaras dengan berbagai kebijakan nasional seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, dan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Keselarasan tersebut menjadikan panduan ini instrumen pendukung kebijakan yang memperkuat kesiapan Indonesia dalam menghadapi ancaman kuantum dan memastikan keberlanjutan transformasi digital yang aman dan berdaulat.

Saya menyampaikan apresiasi kepada seluruh jajaran BSSN, khususnya Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi, serta para pakar dan mitra yang telah berkontribusi dalam penyusunan panduan ini. Saya juga mengajak seluruh pemangku kepentingan baik dari pemerintah, pelaku usaha, akademisi, dan masyarakat/komunitas, untuk memperkuat kolaborasi dalam mengimplementasikan migrasi menuju PQC sesuai prioritas sektor masing-masing.

Kami berharap panduan ini dapat menjadi rujukan nasional dalam menjaga keamanan data strategis, memperkuat ketahanan siber nasional, dan meningkatkan kepercayaan publik terhadap ruang digital kita. Semoga panduan ini memberikan manfaat yang nyata dalam membangun ekosistem keamanan informasi yang tangguh, aman, dan berdaulat di era komputasi kuantum.

Drs. Nugroho Sulistyo Budi, M.M., M.Han.

Kepala Badan Siber dan Sandi Negara

Desember 2025



PENGANTAR DEPUTI I



Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa atas tersusunnya *Panduan Migrasi ke Post-Quantum Cryptography Versi 1.0* ini sebagai salah satu wujud nyata komitmen Badan Siber dan Sandi Negara (BSSN) dalam memperkuat keamanan informasi nasional.

Perkembangan teknologi informasi yang semakin pesat telah membawa kemudahan dan efisiensi dalam berbagai aspek kehidupan, namun sekaligus menghadirkan tantangan baru di bidang keamanan siber. Salah satu tantangan terbesar yang kini dihadapi dunia adalah kemajuan komputasi kuantum, yang berpotensi melemahkan sistem kriptografi klasik yang selama ini menjadi fondasi keamanan data dan komunikasi elektronik.

Sebagai lembaga yang memiliki tugas pemerintahan di bidang keamanan siber dan sandi, BSSN memandang perlu adanya langkah antisipatif yang terencana dan terukur untuk memastikan kesiapan bangsa dalam menghadapi era pasca-kuantum. Panduan ini hadir untuk memberikan acuan bagi instansi pemerintah, penyelenggara sistem elektronik, serta seluruh pemangku kepentingan dalam melakukan migrasi menuju PQC secara sistematis, efisien, dan sesuai dengan standar internasional.

Panduan ini tidak hanya memuat aspek teknis mengenai algoritma dan mekanisme transisi, tetapi juga menekankan pentingnya koordinasi lintas sektor, penguatan kapasitas sumber daya manusia, serta penerapan prinsip *cryptographic agility* sebagai bagian dari strategi pertahanan siber nasional.

Kami berharap panduan ini dapat menjadi referensi strategis dan operasional bagi seluruh pihak yang berperan dalam ekosistem keamanan informasi nasional. Melalui kolaborasi, inovasi, dan komitmen bersama, Indonesia dapat memastikan ketahanan siber yang tangguh dan berdaulat di era komputasi kuantum.

Akhir kata, kami mengucapkan terima kasih kepada seluruh pihak yang telah berkontribusi dalam penyusunan panduan ini. Semoga panduan ini memberikan manfaat nyata dalam mendukung upaya bangsa mewujudkan ruang siber yang aman, andal, dan berdaulat.

Tjahjo Khurniawan

Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi

Desember 2025



RINGKASAN EKSEKUTIF

Perkembangan teknologi komputasi kuantum membawa dampak besar terhadap keamanan siber global. Kemampuannya dalam menyelesaikan persoalan matematis kompleks mengancam keberlanjutan algoritma kriptografi klasik seperti Rivest–Shamir–Adleman (RSA), *Elliptic Curve Cryptography* (ECC), dan Diffie–Hellman yang selama ini digunakan untuk melindungi data dan komunikasi elektronik. Ancaman ini menuntut langkah antisipatif yang terencana melalui penerapan *Post-Quantum Cryptography* (PQC) guna memastikan ketahanan dan keamanan informasi nasional.

Panduan Migrasi ke PQC disusun sebagai acuan strategis, teknis, dan operasional bagi penyelenggara sistem elektronik, instansi pemerintah, dan pemangku kepentingan lainnya dalam melaksanakan proses transisi menuju sistem kriptografi tahan-kuantum. Panduan ini menguraikan prinsip tata kelola migrasi, penilaian risiko serangan berbasis komputasi kuantum, pemilihan algoritma PQC yang sesuai standar internasional, serta penerapan prinsip *cryptographic agility* untuk menjamin fleksibilitas dan keberlanjutan keamanan sistem.

Proses migrasi diarahkan melalui tahapan yang sistematis, meliputi:

1. Tahap persiapan, mencakup penentuan profil organisasi, identifikasi aset kriptografi, serta penetapan penanggung jawab dan strategi komunikasi.
2. Tahap pemahaman dasar, yang menekankan inventarisasi aset dan penilaian risiko sebagai dasar penyusunan prioritas migrasi.
3. Tahap perencanaan, berisi pedoman penyusunan rencana aksi, waktu pelaksanaan, serta estimasi kebutuhan sumber daya dan biaya.
4. Tahap pelaksanaan migrasi, yang memuat rekomendasi algoritma, strategi implementasi, dan integrasi protokol sesuai kebijakan nasional dan standar internasional.
5. Tahap pemantauan dan evaluasi, untuk memastikan kepatuhan terhadap standar, pengukuran keberhasilan, serta pembaruan berkelanjutan seiring perkembangan teknologi.

Melalui panduan ini, diharapkan seluruh instansi dan penyelenggara sistem elektronik dapat melaksanakan migrasi menuju PQC secara aman, efisien, terukur, dan terintegrasi lintas sektor. Langkah ini merupakan bagian dari strategi nasional dalam memperkuat ketahanan siber dan menjaga kedaulatan digital Indonesia di era komputasi kuantum.



DAFTAR ISI

TIM PERUMUS PANDUAN	ii
PENGANTAR	iii
PENGANTAR DEPUTI I	vi
RINGKASAN EKSEKUTIF	viii
DAFTAR ISI	x
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	2
1.2 Urgensi Migrasi Menuju <i>Post-Quantum Cryptography</i>	4
1.3 Manfaat Panduan	6
1.4 Ruang Lingkup	6
1.5 Cakupan dan Batasan	13
1.6 Hasil yang Diharapkan	13
1.7 Keterkaitan dengan Inisiatif Internasional	13
BAB II PRINSIP DAN PENDEKATAN MIGRASI PQC	15
2.1 Prinsip Umum Migrasi PQC	16
2.2 <i>Three-Phase Model</i> (Model Tiga fase)	28
2.3 Integrasi dengan model empat fase	31
2.4 Tahap Implementasi	31
BAB III TAHAP PERSIAPAN	33
3.1 Tujuan	34
3.2 Landasan Ilmiah/Teknis	34
3.3 Langkah-langkah	35
3.3.1 Penentuan profil organisasi	35
3.3.2 Menetapkan Strategi Penemuan Aset Kriptografi Dan Penanggung Jawab	38
3.3.3 Mengidentifikasi Pemangku Kepentingan dan Menyusun Strategi Komunikasi	41
BAB IV TAHAP PEMAHAMAN DASAR	44
4.1 Tujuan	45
4.2 Landasan Ilmiah/Teknis	45
4.3 Langkah-langkah	46

4.3.1 Inventarisasi Aset Kriptografi.....	46
4.3.2 Penilaian Risiko Kuantum	59
BAB V TAHAP PERENCANAAN.....	84
5.1 Tujuan	85
5.2 Landasan Ilmiah/Teknis	85
5.3 Langkah-langkah	85
5.3.1 Waktu memulai migrasi.....	85
5.3.2 Rekomendasi dalam perencanaan migrasi	90
5.3.3 Perkiraan Biaya Migrasi.....	103
BAB VI TAHAP PELAKSANAAN MIGRASI.....	106
6.1 Tujuan	107
6.2 Landasan ilmiah	107
6.3 Langkah-langkah	108
6.3.1 Strategi Umum	108
6.3.2 Rekomendasi <i>Primitives</i> Kriptografi.....	117
6.3.3 Pertukaran Kunci/ <i>Encapsulation</i> dan Tanda Tangan Digital	120
6.3.4 Migrasi Protokol.....	123
6.3.5 Ketangkasan Kriptografi (<i>Cryptographic Agility</i>)	138
BAB VII TAHAP PEMANTAUAN DAN EVALUASI.....	156
7.1 Tujuan	157
7.2 Landasan Ilmiah/Teknis	157
7.3 Langkah-langkah	158
7.3.1 Memverifikasi penerapan PQC dan memastikan kepatuhan terhadap standar yang berlaku.....	158
7.3.2 Menilai kebutuhan dan menyiapkan tenaga kerja yang dapat menerapkan PQC	159
7.3.3 Membuat ukuran untuk memantau keberhasilan migrasi ke PQC.	159
7.3.4 Melakukan pemantauan dan pembaruan secara berkelanjutan	160
BAB VIII PENUTUP	161
LAMPIRAN A DAFTAR PERIKSA LOKASI KRIPTOGRAFI.....	164
LAMPIRAN B ALGORITMA KRIPTOGRAFI PRIMITIF	171
DAFTAR REFERENSI.....	189

DAFTAR TABEL

Tabel 4.1	Struktur tabel inventarisasi sistem.....	47
Tabel 4.2	Inventarisasi komponen perangkat lunak	50
Tabel 4.3	Dokumentasi atribut teknis	55
Tabel 4.4	Contoh Struktur tabel CBOM	58
Tabel 4.5	Referensi Skor Kelemahan Kuantum	64
Tabel 4.6	Matriks asesmen upaya migrasi.....	75
Tabel 4.7	Skor risiko individu menjadi skor risiko akhir per aplikasi.	82
Tabel 5.1	Pemetaan dari Upaya Migrasi ke Jumlah Tahun.....	87
Tabel 5.2	Matriks Penilaian Model Maturitas	95
Tabel 6.1	Rekomendasi primitif kriptografi.....	118
Tabel 6.2	Rekomendasi parameter instansiasi dari primitif kriptografi ...	119



DAFTAR GAMBAR

Gambar 3.1	Diagram alur untuk menentukan profil PQC suatu organisasi digambar ulang dari [3].....	37
Gambar 4.1	Diagram alur untuk menentukan kelemahan kuantum digambar ulang dari [3].....	64
Gambar 4 2	Diagram alur untuk mengidentifikasi perkiraan dampak digambar ulang dari [1].....	70
Gambar 5.1	Linimasa berbagai skenario migrasi	87



BAB I

PENDAHULUAN



BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi komputasi kuantum menandai era baru dalam perhitungan dan pemrosesan data yang jauh melampaui kemampuan komputer klasik. Teknologi ini berpotensi merevolusi berbagai bidang, mulai dari penelitian ilmiah, keuangan, kesehatan, hingga pertahanan nasional dengan menawarkan percepatan eksponensial dalam komputasi. Namun, di balik potensi tersebut, tersimpan ancaman signifikan terhadap sistem keamanan informasi modern, yang sebagian besar bergantung pada skema kriptografi klasik seperti Rivest–Shamir–Adleman (RSA), *Elliptic Curve Cryptography* (ECC), dan Diffie–Hellman.

Keamanan skema-skema kriptografi klasik tersebut dirancang berdasarkan permasalahan matematis yang sulit dipecahkan oleh komputer konvensional, tetapi dapat diselesaikan secara efisien oleh komputer kuantum, misalnya dengan algoritma Shor. Hal ini berarti ketika *Cryptographically Relevant Quantum Computer* (CRQC) berhasil dibangun, seluruh skema keamanan digital berbasis infrastruktur kunci publik yang saat ini digunakan berpotensi usang dan tidak lagi menjamin keamanan. Konsekuensinya dapat sangat merugikan, meliputi kompromi data sensitif, pemalsuan tanda tangan digital, dan hilangnya kepercayaan publik terhadap sistem digital.

Ancaman ini bersifat lintas sektor dan strategis. Bagi Indonesia, sistem pemerintahan digital, layanan keuangan, energi, kesehatan, pendidikan hingga pertahanan negara sangat bergantung pada mekanisme kriptografi klasik untuk menjaga konfidensialitas (*confidentiality*), integritas (*integrity*), dan autentikasi (*authenticity*) data pihak-pihak yang terautentikasi. Keterlambatan dalam melakukan transisi ke kriptografi tahan-kuantum berpotensi mengancam kedaulatan digital dan keamanan nasional.

Dalam konteks mitigasi ancaman ini, komunitas global mengembangkan dua teknologi keamanan tahan-kuantum (*quantum-safe security technologies*), yaitu:

1. *Post Quantum Cryptography* (PQC) adalah koleksi skema dan protokol kriptografi utakhir yang dirancang untuk tetap aman terhadap serangan komputer kuantum. Algoritma PQC bekerja dalam kerangka sistem komputasi digital, sehingga dapat diimplementasikan pada perangkat keras dan perangkat lunak yang sudah ada tanpa memerlukan infrastruktur kuantum sehingga menjadi solusi praktis bagi mayoritas aplikasi digital.
2. *Quantum Key Distribution* (QKD), yaitu pendekatan berbasis fisika kuantum yang memungkinkan distribusi kunci enkripsi secara aman melalui prinsip ketidakpastian Heisenberg. QKD memanfaatkan partikel kuantum (*photon*) untuk mendeteksi penyadapan secara langsung selama proses distribusi kunci, karena setiap intervensi eksternal akan mengubah keadaan kuantum partikel tersebut. Teknologi ini menjanjikan keamanan fisik tanpa syarat (*information-theoretic security*), dan telah diuji coba di berbagai negara dalam konteks komunikasi antarbank, jaringan pemerintah, serta satelit komunikasi kuantum.

Kedua pendekatan ini tidak bersifat saling menggantikan, melainkan komplementer. PQC dipandang sebagai solusi utama jangka menengah yang dapat diterapkan secara luas, sedangkan QKD berpotensi menjadi lapisan keamanan tambahan jangka panjang untuk aplikasi dengan tingkat kerahasiaan sangat tinggi, seperti diplomasi, pertahanan, dan keuangan nasional.

Ancaman terhadap kriptografi publik tidak bersifat teoretis semata. Studi oleh Gidney dan Ekerå [1] menunjukkan bahwa kunci RSA 2048-bit dapat dipecahkan dalam delapan jam oleh komputer kuantum dengan 20 juta qubit, dan studi lanjutan oleh Gidney [2] memperkirakan

hal yang sama dapat dicapai dalam 4,63 hari dengan 900.000 qubit. Walau kapasitas ini masih di luar jangkauan teknologi saat ini, kemajuan pesat dalam riset kuantum menandakan bahwa waktu untuk mempersiapkan migrasi semakin sempit.

Salah satu bentuk ancaman yang paling relevan adalah serangan *Harvest-Now-Decrypt-Later* (HNDL), di mana penyerang dapat merekam komunikasi terenkripsi saat ini dan mendekripsinya di masa depan menggunakan komputer kuantum. Ancaman ini menunjukkan bahwa bahkan jika CRQC baru hadir satu atau dua dekade lagi, risiko kompromi data bersifat langsung dan jangka panjang.

Oleh karena itu, negara dan lembaga di seluruh dunia, termasuk Indonesia, perlu bertindak secara proaktif untuk membangun strategi dan roadmap migrasi ke sistem kriptografi tahan-kuantum — dengan mengadopsi kombinasi solusi PQC dan QKD yang sesuai dengan konteks nasional, kesiapan infrastruktur, dan tingkat risiko sektoral.

1.2 Urgensi Migrasi Menuju *Post-Quantum Cryptography*

Komunitas internasional, melalui lembaga seperti *National Institute of Standards and Technology* (NIST), telah menginisiasi proses standardisasi PQC sebagai solusi utama untuk menghadapi ancaman komputasi kuantum. Pada tahun 2024, NIST telah menstandarkan tiga algoritma utama, yaitu: (i) ML-KEM (berbasis *lattice*) untuk pertukaran kunci, (ii) ML-DSA (berbasis *lattice*) untuk tanda tangan digital, dan (iii) SLH-DSA (berbasis *hash*).

Migrasi ke PQC bukan sekadar pembaruan teknis, tetapi merupakan transformasi sistemik nasional yang mencakup aspek kebijakan, operasional, dan tata kelola. Berdasarkan pengalaman migrasi algoritma sebelumnya (misalnya transisi dari DES ke AES, SHA-1 ke SHA-256 atau dari RSA-1024 ke RSA-2048), perubahan kriptografi skala nasional memerlukan waktu lebih dari lima tahun. Oleh karena itu, langkah-

langkah awal migrasi harus segera dimulai melalui inventarisasi aset kriptografi, penilaian risiko, dan penguatan tata kelola keamanan informasi sebelum ancaman komputer kuantum terwujud nyata.

Panduan ini bertujuan untuk memberikan arah strategis, teknis, dan operasional dalam proses transisi dari kriptografi klasik menuju PQC bagi Penyelenggara Sistem Elektronik (PSE). Secara khusus, tujuan penyusunan panduan ini adalah sebagai berikut:

1. Menyediakan langkah-langkah praktis dan sistematis untuk migrasi PQC bagi PSE.

Panduan ini memberikan pedoman tahapan yang dapat langsung diimplementasikan mulai dari inventarisasi aset kriptografi, penilaian risiko kuantum, perencanaan, implementasi, hingga evaluasi. Struktur langkah-langkah ini diadaptasi dari pendekatan *three-phase model* yaitu *diagnosis, planning, execution* dari *Algemene Inlichtingen- en Veiligheidsdienst* (AIVD) – Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO) – *Centrum Wiskunde & Informatica* (CWI) [3] serta *Post-Quantum Cryptography Coalition* (PQCC) *migration categories* yaitu *preparation, understanding, execution, monitoring* [4].

2. Menjadi acuan untuk koordinasi lintas sektor dalam menghadapi ancaman kuantum.

Mengingat dampak ancaman komputer kuantum bersifat lintas sektor, panduan ini dapat menjadi dasar koordinasi antar pemerintah, akademisi/pakar, praktisi, pelaku usaha, dan pengguna akhir. Panduan ini diharapkan dapat mendorong terbentuknya koordinasi nasional PQC lintas sektor yang diinisiasi Badan Siber dan Sandi Negara (BSSN).

3. Mendorong penerapan prinsip *cryptographic agility* dan manajemen risiko berbasis keamanan kuantum.

Panduan ini menekankan pentingnya fleksibilitas sistem keamanan informasi untuk menyesuaikan algoritma kriptografi sesuai perkembangan teknologi. Melalui prinsip *cryptographic agility*,

instansi dapat melakukan pembaruan algoritma dengan disrupsi minimal terhadap jalannya layanan operasional. Selain itu, panduan ini memperkenalkan kerangka metodologi risiko kuantum [5] untuk membantu pengambil keputusan menilai dan memprioritaskan aset berdasarkan tingkat kerentanan, dampak, dan kompleksitas migrasi.

4. Meningkatkan kesiapan nasional menghadapi era pasca-kuantum. Panduan ini mendukung penyusunan strategi nasional keamanan siber yang berorientasi pada perlindungan jangka panjang data publik, aset digital strategis, serta sistem elektronik agar tetap aman terhadap ancaman serangan kuantum di masa depan.

1.3 Manfaat Panduan

Melalui penerapan panduan ini, setiap PSE diharapkan dapat:

1. Membangun kesadaran dan kesiapan menghadapi ancaman kuantum;
2. Melakukan perencanaan migrasi yang efisien, terukur, dan sesuai prioritas risiko;
3. Menjamin keberlangsungan keamanan data strategis;
4. Mendukung terciptanya ekosistem keamanan digital nasional yang tangguh dan berdaulat.

1.4 Ruang Lingkup

Panduan ini mencakup aspek manajerial, teknis, dan kebijakan yang diperlukan untuk melaksanakan migrasi ke PQC secara efektif dan berkelanjutan dengan ruang lingkup meliputi:

1. Proses Manajerial Migrasi PQC.

Proses manajerial terdiri atas menentukan profil organisasi dalam migrasi ke PQC, menetapkan strategi penemuan aset dan penanggung jawab migrasi, mengidentifikasi pemangku kepentingan serta menyusun strategi komunikasi dengan pemangku kepentingan.

2. Aspek Teknis dan Operasional Migrasi PQC.

Menyediakan panduan untuk pelaksanaan kegiatan teknis meliputi:

1. Inventarisasi aset kriptografi melalui deteksi dan klasifikasi penggunaan kriptografi, dokumentasi dan pengumpulan atribut teknis serta pembuatan format standar untuk pengelolaan inventarisasi aset kriptografi.
2. Penilaian risiko kuantum yang terdiri atas bagaimana mengidentifikasi penyerang yang realistis, kelemahan terhadap kuantum, analisis dampak, upaya migrasi dan skor risiko kuantum.
3. Perencanaan implementasi teknis yang terukur dan melaksanakan migrasi PQC secara bertahap serta terkontrol, mulai dari perencanaan proses bisnis, penilaian maturitas PQC, perencanaan teknis terkait aspek-aspek kriptografi yang perlu dimigrasikan, dan perkiraan biaya migrasi.
4. Pelaksanaan migrasi, mulai dari pemilihan algoritma PQC sesuai rekomendasi standar internasional. Misalnya FIPS 203 [6], FIPS 204 [7] dan FIPS 205 [8], implementasi mode hibrida antara algoritma klasik dengan PQC selama masa transisi hingga beralih sepenuhnya ke PQC serta langkah pemenuhan *cryptographic agility*.
5. Pemantauan dan evaluasi migrasi ke PQC untuk memastikan kepatuhan terhadap standar yang berlaku, pengukuran keberhasilan, serta pembaruan berkelanjutan seiring perkembangan teknologi.

3. Penilaian Risiko dan Prioritas Aset Digital.

Melalui penggunaan model kuantitatif berdasarkan metode *quantum risk framework* milik AIVD, CWI, dan TNO [3], panduan ini membantu PSE menentukan prioritas migrasi dengan mempertimbangkan tiga dimensi utama:

1. Kelemahan kuantum dari kriptografi yang digunakan pada tingkat sistem atau aplikasi.;

2. Dampak yang diharapkan dari serangan kuantum terhadap sistem;
3. Perkiraan waktu dan upaya yang diperlukan untuk melakukan migrasi ke PQC.
4. Pemantauan dan Evaluasi PQC.

Panduan ini menguraikan empat langkah yang dapat dilakukan dalam rangka pemantauan dan evaluasi migrasi ke PQC yaitu memverifikasi penerapan PQC dan memastikan tingkat kepatuhan terhadap standar yang berlaku, menilai kebutuhan dan menyiapkan tenaga kerja yang dapat menerapkan PQC, membuat ukuran untuk memantau keberhasilan migrasi ke PQC dan membuat ukuran untuk memantau keberhasilan migrasi ke PQC.
5. Penerapan Lintas Sektor dan Skalabilitas Nasional.

Panduan ini bersifat umum dan dapat diterapkan pada Penyelenggara Sistem Elektronik (PSE), baik PSE lingkup publik maupun lingkup privat sebagaimana diatur pada Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Selain itu, panduan ini juga dapat diterapkan oleh PSE yang memiliki kewajiban menjaga keamanan dan konfidensialitas data pengguna sesuai dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) serta kebijakan keamanan siber nasional yang dikoordinasikan oleh BSSN.

Sesuai dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 4, PSE wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum berikut:

1. dapat menampilkan kembali Informasi Elektronik dan/ atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan;

2. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam penyelenggaraan Sistem Elektronik tersebut;
3. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan Sistem Elektronik tersebut;
4. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan Sistem Elektronik tersebut; dan
5. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Dalam kaitannya dengan amanat tersebut, PSE dapat menerapkan algoritma kriptografi di dalam Sistem Elektronik guna memenuhi persyaratan yang terdapat pada huruf b, khususnya pelindungan terhadap keutuhan, keotentikan, dan kerahasiaan informasi elektronik.

Salah satu sektor yang memiliki risiko yang cukup tinggi terhadap ancaman serangan kuantum yaitu sektor Infrastruktur Informasi Vital (IIV). Berdasarkan Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan IIV, Penyelenggara IIV harus menyelenggarakan pelindungan IIV secara andal dan aman serta bertanggung jawab terhadap beroperasinya IIV sebagaimana mestinya dengan menerapkan standar keamanan informasi dan/atau standar keamanan lain yang ditetapkan oleh Kementerian atau Lembaga dan/atau Badan. Hal ini sejalan dengan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, di mana salah satu fokus area yang diatur di dalamnya yaitu penguatan pelindungan IIV. Selain itu, setiap Penyelenggara IIV wajib menerapkan manajemen risiko Keamanan Siber secara efektif. Penerapan manajemen risiko Keamanan Siber ini harus memenuhi

persyaratan kepatuhan terhadap peraturan perundang undangan dan kesesuaian dengan standar yang berlaku pada masing-masing sektor IIV.

Berdasarkan Peraturan BSSN Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan IIV, terdapat 4 domain pada kerangka kerja Penyelenggara IIV, salah satunya domain proteksi. Domain proteksi merupakan fungsi yang bertujuan untuk mendukung kemampuan Penyelenggara IIV dalam mencegah, membatasi, atau menahan dampak dari Insiden Siber. Di dalam domain proteksi, terdapat beberapa kegiatan yang harus dilakukan oleh Penyelenggara IIV, antara lain mengelola identitas, autentikasi, dan kendali akses, melindungi data, melindungi aplikasi, dan melindungi jaringan. Sesuai dengan kegiatan yang ada pada domain proteksi ini, Penyelenggara IIV dapat menerapkan algoritma kriptografi di dalam sistem elektronik mereka.

Sektor infrastruktur informasi vital (IIV) sebagaimana terdapat dalam Peraturan Presiden Nomor 82 Tahun 2022, yaitu:

- a. Sektor administrasi pemerintahan, yang menyelenggarakan sistem pemerintahan berbasis elektronik, termasuk layanan publik digital, sistem kepegawaian, arsip digital, serta layanan administrasi kependudukan dan keamanan nasional berbasis data.
- b. Sektor energi dan sumber daya alam, yang menyelenggarakan sistem kendali dan distribusi tenaga listrik, jaringan transmisi dan distribusi energi, sistem produksi dan distribusi minyak dan gas bumi, serta sistem monitoring sumber daya alam strategis yang mendukung keberlanjutan energi nasional.
- c. Sektor transportasi, yang menyelenggarakan sistem pengelolaan lalu lintas udara, laut, dan darat, sistem tiket dan logistik digital, pengendalian transportasi publik, serta infrastruktur digital yang menghubungkan jaringan

transportasi antarwilayah untuk menjamin mobilitas nasional yang aman dan efisien.

- d. Sektor keuangan, yang menyelenggarakan transaksi elektronik, sistem pembayaran, pertukaran data keuangan, serta layanan keuangan digital yang memproses data nasabah dan transaksi publik dalam jumlah besar.
- e. Sektor kesehatan, yang menyelenggarakan sistem rekam medis elektronik, data pasien, sistem manajemen rumah sakit, laboratorium digital, serta platform pertukaran data kesehatan nasional untuk mendukung pelayanan publik yang cepat dan aman.
- f. Sektor TIK, yang menyelenggarakan infrastruktur telekomunikasi, pusat data, layanan *cloud computing*, penyedia layanan internet, dan sistem penyiaran publik yang menjadi tulang punggung konektivitas dan interoperabilitas layanan digital nasional
- g. Sektor Pangan, yang menyelenggarakan sistem rantai pasok digital, sistem distribusi logistik bahan pokok, data ketahanan pangan nasional, serta sistem pengawasan mutu dan keamanan pangan untuk menjamin ketersediaan dan stabilitas bahan pangan nasional.
- h. Sektor Pertahanan yang mendukung sistem komando, kontrol, komunikasi, komputer, intelijen, pengawasan, dan pengintaian, serta sistem sensor, radar, dan jaringan kriptografi militer yang digunakan untuk menjaga keamanan dan kedaulatan negara.

Pada sektor keuangan, Bank Indonesia mengeluarkan kebijakan keamanan siber di dalam Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber Bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia. Di dalam peraturan tersebut, sistem informasi

kritikal yang berdampak luas dikategorikan sebagai infrastruktur informasi vital. Selain itu di dalam peraturan ini juga mengamanatkan untuk menyelenggarakan kegiatan proteksi yang memuat pengamanan dan perlindungan data dan/atau informasi berdasarkan klasifikasi data dan/atau informasi yang ditetapkan oleh Penyelenggara, serta memastikan kepatuhan perlindungan data pribadi.

Selain Bank Indonesia, Otoritas Jasa Keuangan (OJK) mengeluarkan Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum yang salah satunya mengatur tentang Ketahanan dan Keamanan Siber yang diselenggarakan oleh Bank Umum. Pada pasal 21 disebutkan bahwa Bank wajib menjaga ketahanan siber dengan melakukan proses yaitu identifikasi aset, ancaman, dan kerentanan, perlindungan aset, deteksi insiden siber, dan penanggulangan dan pemulihan insiden siber. Penjelasan untuk setiap proses tersebut lebih lanjut dijabarkan dalam Surat Edaran Otoritas Jasa Keuangan Republik Indonesia Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber Bagi Bank Umum.

Sejalan dengan hal tersebut, migrasi menuju PQC perlu dilakukan oleh PSE lintas sektor. Migrasi PQC ini bukan sekadar mengganti algoritma, tetapi mensyaratkan sinkronisasi dengan arsitektur keamanan siber nasional, termasuk kebijakan keamanan, tata kelola keamanan informasi, manajemen risiko, standardisasi teknis, dan interoperabilitas antar-sistem. Transformasi ini perlu diatur secara terarah, terukur, dan sistematis agar tidak menimbulkan gangguan terhadap operasional layanan vital. Dengan migrasi ini diharapkan operasional Sistem Elektronik dapat berjalan dengan aman dan tahan terhadap serangan kuantum.

1.5 Cakupan dan Batasan

Panduan ini tidak menggantikan regulasi teknis kriptografi nasional yang ditetapkan oleh BSSN, namun berfungsi sebagai kerangka pendukung implementasi yang melengkapi peraturan teknis dan pedoman keamanan siber lainnya. Panduan ini juga tidak menetapkan algoritma spesifik di luar standar internasional yang dipublikasikan oleh NIST, ETSI, atau ISO, tetapi memberikan fleksibilitas bagi instansi untuk memilih algoritma PQC yang sesuai dengan kebutuhannya, selama tetap memenuhi prinsip keamanan, interoperabilitas, dan efisiensi.

1.6 Hasil yang Diharapkan

Dengan penerapan panduan ini, diharapkan setiap PSE dapat:

1. Memiliki rencana migrasi PQC yang terukur dan terintegrasi dengan strategi keamanan siber dan sandi nasional;
2. Menyusun peta risiko kuantum untuk setiap aset kritikal;
3. Menyediakan mekanisme audit dan pelaporan berkala tentang kemajuan migrasi;
4. Meningkatkan resiliensi nasional terhadap ancaman pasca-kuantum melalui kolaborasi antar lembaga dan sektor industri.

1.7 Keterkaitan dengan Inisiatif Internasional

Panduan ini diselaraskan dengan berbagai inisiatif dan referensi internasional, antara lain:

1. *The PQC Migration Handbook Guidelines for Migrating to Post-Quantum Cryptography Revised and Extended Second Edition* [3] sebagai referensi utama model tiga tahap migrasi yaitu diagnosis, perencanaan, dan eksekusi;
2. *Post-Quantum Cryptography Migration Roadmap* [4] sebagai referensi struktur empat kategori implementasi yaitu persiapan, *baseline understanding*, eksekusi, dan pemantauan;

3. TNO 2024 R10707 *Quantum risicomethologie voor cryptografie* [5] sebagai acuan penilaian risiko kuantum berbasis skor kerentanan, dampak, dan upaya migrasi.

Panduan ini juga selaras dengan kebijakan standar internasional yang dikeluarkan oleh NIST, ISO/IEC, dan ETSI.



BAB II

PRINSIP & PENDEKATAN MIGRASI PQC



BAB II

PRINSIP DAN PENDEKATAN MIGRASI PQC

2.1 Prinsip Umum Migrasi PQC

Migrasi ke PQC bukan hanya persoalan teknis mengganti algoritma kriptografi, melainkan juga transformasi sistemik yang melibatkan manajemen risiko, tata kelola organisasi, interoperabilitas, serta kesiapan sumber daya manusia. Oleh karena itu, keberhasilan proses migrasi memerlukan prinsip-prinsip umum yang dapat diterapkan secara lintas sektor dan konsisten dengan standar internasional. Lima prinsip utama berikut dirumuskan berdasarkan rekomendasi dari AIVD, CWI, dan TNO [3], yang telah disesuaikan dengan konteks ekosistem digital Indonesia.

1. Serangan HNDL

HNDL merupakan strategi serangan di mana pihak penyerang mengumpulkan dan menyimpan data yang terenkripsi dengan harapan bahwa kemajuan teknologi kuantum di masa depan akan memungkinkan data tersebut untuk didekripsi. Strategi HNDL ini menimbulkan risiko kompromi terhadap kerahasiaan informasi yang bersifat jangka panjang dan sensitif, termasuk komunikasi pemerintah, catatan keuangan, data kesehatan, dan kekayaan intelektual [9]. Strategi HNDL semakin sering dibahas dalam konteks komputasi kuantum, karena kemunculan CRQC berpotensi memecahkan skema kriptografi kunci-publik yang digunakan secara luas saat ini, sehingga ciphertext yang diarsipkan hari ini dimungkinkan untuk dibuka di masa depan [10]. NIST menjelaskan bahwa meski penyerang saat ini belum mampu memecahkan enkripsi, mereka tetap dapat memperoleh keuntungan dengan mengumpulkan dan menyimpan data yang terenkripsi, dengan harapan bahwa di masa mendatang teknologi komputer kuantum akan mampu mendekripsinya. Praktik tersebut menjadi salah satu alasan untuk segera mulai menerapkan PQC

untuk memastikan perlindungan kerahasiaan data sensitif yang bersifat jangka panjang [11].

Bahaya utama HNDL muncul karena banyak jenis data memiliki masa sensitifitas yang panjang, sehingga tetap bernilai tinggi meskipun didekripsi bertahun-tahun setelah dikumpulkan HNDL secara khusus dikaitkan dengan data yang harus dijaga kerahasiaannya lebih dari 10 tahun, seperti data keuangan, rahasia dagang perusahaan, rahasia negara, (dokumen pemerintah yang berklasifikasi rahasia dan rahasia militer), rekam medis, kekayaan intelektual, dan data pribadi [12]. Berbagai kajian tentang kesiapan kuantum juga menekankan bahwa data yang dilindungi oleh protokol seperti TLS, SSH, dan IPsec merupakan target HNDL, terlebih karena protokol tersebut umum digunakan oleh berbagai perusahaan serta data yang ditransmisikan dalam protokol tersebut memungkinkan memiliki masa kerahasiaan yang panjang [10]. Selain itu, karena biaya penyimpanan data semakin murah dan praktik pencurian data seperti insiden *data breach* dan ransomware terus meningkat, maka penyerang dapat mengumpulkan dan mengarsipkan data terenkripsi dalam jumlah besar, yang kemudian menjadi aset intelijen atau ekonomi ketika teknologi dekripsi dari CRQC di masa depan telah tersedia [13].

Konsep HNDL sendiri bukan merupakan sesuatu yang sepenuhnya baru. Praktik mengumpulkan lalu mendekripsi komunikasi terenkripsi di kemudian hari, telah lama menjadi inti dari operasi intelijen sinyal (*signals intelligence*) [13]. Whitfield Diffie menjelaskan bahwa NSA dan organisasi serupa memiliki perpustakaan pita (*tape libraries*) yang sangat besar, berisi rekaman komunikasi yang disimpan selama beberapa dekade untuk kemudian dianalisis dan didekripsi ketika teknik kriptanalisis atau kapasitas komputasi meningkat. Whitfield Diffie menjelaskan bahwa pendekatan tersebut merupakan inti dari intelijen sinyal dan

menegaskan adanya arsip besar di NSA yang telah ada beberapa dekade yang lalu [14].

Salah satu contoh nyata dari HNDL adalah Proyek Venona yakni sebuah program kontra-intelijen Amerika Serikat yang dimulai pada 1943 untuk menganalisis dan mendekripsi pesan-pesan terenkripsi yang dikirim oleh badan intelijen Uni Soviet [15]. Dalam proyek ini, ratusan ribu pesan diplomatik dan intelijen Soviet disadap selama Perang Dunia II dan awal Perang Dingin, kemudian secara bertahap berhasil didekripsi selama puluhan tahun berikutnya, menghasilkan sekitar 2.000–3.000 pesan yang dapat dibaca dan memberikan informasi penting mengenai jaringan spionase Soviet, termasuk kebocoran terkait Proyek Manhattan dan pengembangan bom atom Soviet [16]. Meskipun nilai ekonomi langsungnya sulit diukur secara pasti, hasil Proyek Venona memiliki dampak strategis yang signifikan terhadap kebijakan keamanan nasional dan penanganan kasus spionase yang berdampak besar seperti Klaus Fuchs dan jaringan *Cambridge Five* [17].

Contoh lain yang serupa dengan konsep HNDL adalah pemecahan pesan terenkripsi yang dihasilkan oleh Enigma. Berdasarkan [18], pada 17 Januari 1940 pihak Polandia berhasil pertama kali mendekripsi pesan Enigma, dimana pesan tersebut merupakan pesan yang telah ditransmisikan tiga bulan sebelumnya. Pada paruh kedua tahun 1941, sekitar 30.000 pesan Enigma per bulan berhasil didekripsi, dan jumlah tersebut meningkat menjadi sekitar 90.000 pesan per bulan untuk gabungan dekripsi Enigma dan Fish pada periode akhir Perang Dunia II, dengan pemecahan Enigma dibantu oleh mesin bombe yang dikembangkan berdasarkan metode Alan Turing dan dibangun secara teknis oleh Harold Keen dari *British Tabulating Machine Company*. Keberhasilan Sekutu dalam mendekripsi pesan-pesan Enigma juga menunjukkan

besarnya dampak strategis dari kemampuan membaca komunikasi musuh, bahkan ketika dekripsi tidak selalu dilakukan secara instan. Berdasarkan [19], dekripsi terhadap pesan Enigma memberikan kontribusi yang sangat menentukan bagi kemenangan Sekutu dan disebut dapat memperpendek perang sebanyak dua hingga empat tahun. Meski pemecahan Enigma tidak terjadi dalam jangka waktu panjang karena dekripsinya umumnya terjadi dalam skala waktu harian, peristiwa tersebut menunjukkan bahwa akses terhadap isi pesan terenkripsi kapan pun waktunya dapat memberikan keuntungan intelijen yang signifikan. Dalam keterkaitannya dengan HNDL, hal tersebut menunjukkan bahwa keterlambatan dekripsi sekalipun masih dapat menghasilkan dampak strategis apabila data yang disadap merupakan data sensitif yang memiliki nilai jangka panjang.

Dalam konteks komputasi kuantum, HNDL menjadi lebih berbahaya karena munculnya CRQC dimasa depan berpotensi memecahkan skema kriptografi kunci-publik berbasis faktorisasi bilangan bulat dan logaritma diskret, seperti RSA dan elliptic-curve cryptography (ECC), yang saat ini menjadi dasar berbagai protokol keamanan internet. NIST SP 1800-38 menekankan bahwa penyerang yang menyimpan data terenkripsi hari ini secara teoritis dapat mendekripsi data tersebut di masa depan ketika CRQC tersedia sehingga skenario tersebut menimbulkan risiko signifikan terhadap kerahasiaan data jangka panjang [10]. *Canadian National Quantum-Readiness Best Practices and Guidelines* menegaskan bahwa data yang perlu dijaga kerahasiaannya lebih dari satu dekade mungkin sudah berisiko menjadi target HNDL [12]. Berbagai organisasi dan forum di sektor finansial memperingatkan bahwa pelaku kejahatan mungkin sudah menyimpan data sensitif terenkripsi saat ini dengan harapan mampu mendekripsinya di masa depan sehingga hal tersebut menambah urgensi bagi institusi keuangan untuk segera bermigrasi ke PQC [20].

Berbagai studi mencoba memperkirakan dampak ekonomi apabila serangan kuantum berhasil memecahkan sistem keuangan dan infrastruktur yang bergantung pada kriptografi asimetrik yang sudah digunakan saat ini. Berdasarkan [21], laporan dari *Quantum Alliance Initiative* di Hudson Institute memperkirakan bahwa serangan kuantum terhadap jaringan *distributed ledger* (DLT) dapat menimbulkan kerugian langsung sekitar 1,8 triliun dolar AS dan kerugian tidak langsung sekitar 1,4 triliun dolar AS. Berdasarkan [22], jika serangan kuantum berhasil dilakukan terhadap salah satu dari lima bank terbesar di Amerika agar bank tersebut kehilangan akses ke Fedwire yang merupakan sistem pembayaran antar bank atau RTGS di Amerika, maka dapat memicu kegagalan berantai di sektor keuangan seperti merusak hingga 62% aset perbankan dan menimbulkan kerugian antara \$2 hingga \$3,3 triliun secara tidak langsung. Serangan tersebut juga diperkirakan menyebabkan penurunan Produk Domestik Bruto (GDP) antara 10% hingga 17% yang cukup untuk mendorong Amerika Serikat ke dalam resesi selama setidaknya enam bulan. Pembahasan di World Economic Forum juga menegaskan bahwa aset bernilai triliunan dolar saat ini dilindungi oleh skema kriptografi yang rentan terhadap serangan kuantum di masa depan sehingga kegagalan untuk bertransisi ke PQC tepat waktu berpotensi menimbulkan gangguan ekonomi global yang sangat besar [23]. Berbagai pembahasan tersebut menunjukkan bahwa proyeksi nominal dari risiko serangan kuantum yang juga tidak terlepas dari HNDL memiliki skala risiko yang besar

2. Ancaman Komputasi Kuantum terhadap Pemalsuan Tanda Tangan Digital dan Verifikasi Identitas

Perkembangan komputer kuantum berskala besar membawa dampak langsung terhadap keamanan tanda tangan digital yang menjadi tulang punggung infrastruktur identitas modern. Sistem

seperti *Public Key Infrastructure* (PKI) mengandalkan kekuatan matematis RSA dan ECDSA, yang selama beberapa dekade dianggap aman karena pemfaktoran bilangan besar maupun penyelesaian *discrete logarithm* tidak dapat diselesaikan secara efisien oleh komputer klasik [24]. Namun, lanskap ini berubah secara fundamental dengan munculnya CRQC. Melalui algoritma Shor, penurunan kunci privat dari kunci publik RSA atau ECDSA dapat dilakukan dalam waktu polinomial, sebuah kemampuan yang secara teoretis telah ditunjukkan sejak publikasi awal pada 1999 [25].

Dalam konteks ancaman kuantum tersebut, kini muncul pula sebuah risiko strategis jangka panjang yang semakin sering dibahas, yaitu *Trust-Now-Forge-Later* (TNFL) [26]. Istilah ini merujuk pada situasi ketika tanda tangan digital yang saat ini dianggap valid dan tepercaya dapat dipalsukan pada masa depan ketika komputer kuantum cukup kuat untuk memecahkan algoritma klasik. Dengan demikian, serangan tidak harus terjadi hari ini, namun penyerang dapat “menyimpan” artefak digital sekarang dan memalsukannya di masa depan setelah kriptografi klasik runtuh.

Dampak perubahan ini dapat dipahami lebih jelas melalui skenario praktis. Misalkan sebuah *root Certificate Authority* (CA) milik pemerintah menggunakan RSA-2048 untuk menandatangani sertifikat layanan identitas nasional, mencakup portal administrasi publik, layanan tanda tangan elektronik warga negara, serta sistem otentikasi dokumen hukum. Sertifikat root semacam ini umumnya memiliki masa berlaku yang panjang dan menjadi dasar kepercayaan (*trust anchor*) bagi seluruh transaksi digital pemerintah. Selama kunci privat CA tetap terlindungi, mekanisme ini bekerja sebagaimana mestinya. Namun, dengan hadirnya CRQC, kunci privat tersebut berpotensi dihitung hanya dari kunci

publik yang tersedia secara terbuka. Berbagai perkiraan teknis modern mengindikasikan bahwa RSA-2048 dapat diretas menggunakan puluhan juta qubit dalam beberapa jam, dengan tren penelitian yang terus mengurangi kebutuhan sumber daya kuantum dari tahun ke tahun [27] [28]. Dengan kata lain, saat CRQC mencapai skala praktiknya, kunci privat yang selama ini dianggap aman dapat direkonstruksi tanpa kompromi internal maupun akses fisik.

Konsep TNFL menambah lapisan risiko tambahan pada skenario ini. Bahkan jika tanda tangan digital dianggap aman pada saat ini, penyerang dapat menyimpan sertifikat, *firmware*, atau dokumen digital sekarang, lalu memalsukannya di masa depan ketika kemampuan komputasi kuantum telah memadai. Hal ini sangat relevan di domain yang memiliki siklus hidup perangkat panjang, seperti industri otomasi (termasuk *operational technology*), infrastruktur kritis, perangkat IoT, maupun sistem PKI jangka panjang, karena pembaruan kriptografi kerap sulit atau tidak selalu dapat dilakukan secara cepat.

Berbagai perkiraan teknis modern mengindikasikan bahwa RSA-2048 dapat diretas menggunakan puluhan juta *qubit* dalam beberapa jam, dengan tren penelitian yang terus mengurangi kebutuhan sumber daya kuantum dari tahun ke tahun. Dengan kata lain, saat CRQC mencapai skala praktiknya, kunci privat yang selama ini dianggap aman dapat direkonstruksi tanpa kompromi internal maupun akses fisik. Pada titik inilah fenomena TNFL menjadi sangat berbahaya, penyerang tidak perlu mengeksploitasi sistem sekarang, namun hanya cukup menunggu sampai kemampuan kuantum memadai.

Ketika kunci privat CA berhasil dihitung, konsekuensinya menjadi sangat serius. Penyerang tidak hanya mampu memalsukan sertifikat server pemerintah, tetapi juga dapat bertindak sebagai

penerbit sertifikat yang sah. Penyerang dapat menghasilkan sertifikat TLS palsu untuk portal identitas digital nasional, menerbitkan sertifikat baru bagi entitas yang tidak pernah diverifikasi, atau bahkan meniru layanan tanda tangan elektronik resmi. Karena sertifikat tersebut secara kriptografis valid, ditandatangani menggunakan kunci privat *root* CA seluruh perangkat pengguna akan mempercayainya tanpa keraguan.

Dampaknya tidak berhenti pada pencurian identitas. Pengambilalihan kunci privat CA memungkinkan penyerang menyisipkan dokumen digital yang tampak legal, menandatangani kontrak atas nama individu tertentu, atau mengirimkan instruksi administratif palsu yang kemudian dianggap autentik oleh sistem pemerintah. Pada titik ini, sistem identitas nasional yang menjadi fondasi layanan publik digital, dapat mengalami keruntuhan total karena tidak ada lagi pemisahan yang dapat dibuktikan secara kriptografis antara entitas asli dan entitas palsu, yaitu penyerang. Ketika *trust anchor* itu sendiri telah dikompromikan, seluruh proses verifikasi tidak lagi memiliki dasar kriptografis yang dapat dipercaya.

Ancaman TNFL memperkuat urgensi tersebut karena ia mengungkap bahwa masalah tidak hanya muncul setelah serangan kuantum terjadi, melainkan dapat berasal dari artefak digital masa lalu yang sebelumnya dianggap aman. *Firmware programmable logic controller* (PLC), sertifikat CA, arsip dokumen legal, dan update perangkat yang ditandatangani secara klasik berpotensi dipalsukan di masa depan tanpa mekanisme deteksi. Dengan demikian, TNFL tidak hanya berimplikasi sebagai ancaman siber, tetapi juga sebagai risiko yang dapat berdampak pada kontinuitas layanan dan keselamatan fisik, terutama pada sektor infrastruktur kritis seperti pembangkit listrik, sistem energi, dan fasilitas manufaktur kimia.

Situasi tersebut menunjukkan bahwa kerentanan algoritma tanda tangan digital konvensional seperti RSA dan ECDSA terhadap CRQC bukan sekadar isu teknis, tetapi ancaman langsung terhadap keberlangsungan kepercayaan pada sistem identitas digital dan integritas infrastruktur kritis. Oleh karena itu, transisi menuju skema tanda tangan *post-quantum* menjadi kebutuhan yang tidak dapat ditunda. Keamanan tanda tangan digital harus dirancang agar tetap bertahan bahkan ketika komputer kuantum mencapai kapasitas operasional penuhnya [29].

3. *No-regret moves*

Prinsip *no-regret moves* menekankan bahwa langkah-langkah awal seperti inventarisasi kriptografi, penilaian risiko kuantum, dan pembentukan tata kelola tidak akan pernah menjadi upaya sia-sia, meskipun komputer kuantum yang mampu memecahkan kriptografi modern belum tersedia atau tidak bisa mencapai skala besar. Langkah-langkah ini memberikan keuntungan strategis jangka panjang, yaitu:

- a. Mengetahui secara menyeluruh posisi dan ketergantungan kriptografi dalam sistem organisasi;
- b. Mengidentifikasi aset yang membutuhkan konfidensialitas jangka panjang (*long-term confidentiality*);
- c. Menyiapkan struktur organisasi dan sumber daya untuk proses migrasi di masa depan.

Menurut PQCC [4], organisasi yang menunda langkah awal akan menghadapi risiko *cryptographic obsolescence*, yaitu kondisi di mana sistem menjadi tidak dapat diperbarui dengan aman karena kompleksitas dan keterbatasan dokumentasi kriptografi yang sudah kadaluarsa. Oleh sebab itu, inventarisasi kriptografi dan pemetaan risiko kuantum harus segera dilakukan tanpa perlu menunggu standar PQC diadopsi secara global.

4. *Cryptographic agility*

Prinsip *cryptographic agility* berarti bahwa sistem keamanan harus dirancang agar dapat beradaptasi dengan cepat terhadap perubahan algoritma, parameter, dan kebijakan kriptografi tanpa memerlukan rekonstruksi sistem secara menyeluruh. *Cryptographic agility* merupakan karakteristik penting dari infrastruktur digital masa depan. Berdasarkan AIVD, CWI, dan TNO [3], kemampuan ini menjadi penentu keberhasilan migrasi jangka panjang karena memungkinkan organisasi untuk:

- a. Mengganti algoritma yang rentan tanpa mengganggu layanan;
- b. Menggunakan beberapa algoritma secara paralel (misalnya, *hybrid cryptography*);
- c. Menerapkan kebijakan pembaruan berkala terhadap pustaka kriptografi (*cryptographic libraries*) dan manajemen kunci.

Dalam konteks nasional, prinsip ini sejalan dengan kebijakan BSSN yaitu Keputusan Kepala BSSN Nomor 443 Tahun 2025 tentang Algoritma Kriptografi Indonesia. Peraturan tersebut menetapkan paling sedikit dua algoritma untuk setiap jenis algoritma kriptografi sehingga PSE dapat menggunakan beberapa algoritma kriptografi pada sistem elektroniknya untuk menerapkan prinsip *cryptographic agility*.

5. Solusi Hibrida (*hybrid solution*)

Prinsip *hybrid solution* merujuk pada strategi penggunaan kombinasi algoritma klasik yang masih rentan terhadap serangan kuantum (seperti RSA atau ECC) dengan algoritma pasca-kuantum (misalnya ML-KEM atau ML-DSA) dalam satu skema keamanan selama masa transisi. Pendekatan ini, sebagaimana direkomendasikan oleh AIVD, CWI, dan TNO [3], memberikan dua manfaat utama, yaitu:

- a. memungkinkan uji coba interoperabilitas algoritma baru tanpa mengganggu operasi yang sedang berjalan;

- b. menyediakan lapisan keamanan ganda sehingga apabila salah satu algoritma mengalami kelemahan, perlindungan kriptografis tetap terjaga.

Konsisten dengan arah tersebut, NIST dalam NIST IR 8547.ipd [30] juga menyatakan bahwa migrasi menuju PQC kemungkinan akan dimulai dengan protokol hibrida yang mengombinasikan algoritma PQC dan algoritma rentan-kuantum, dengan prinsip bahwa keamanan tetap terjamin selama minimal satu algoritma komponen berada dalam kondisi aman. Namun, NIST menekankan bahwa solusi hibrida bersifat sementara karena menambah kompleksitas arsitektur, risiko keamanan, dan biaya implementasi, sehingga pada akhirnya diperlukan transisi kedua menuju sistem yang sepenuhnya berbasis PQC. Dalam konteks *key establishment*, teknik hibrida dapat menggabungkan dua atau lebih skema pembentukan kunci menjadi struktur komposit, seperti dijelaskan dalam SP 800-56C [31], termasuk penggunaan dua *shared secret* (Z dan T) yang dikonkatenasi untuk derivasi kunci. Standar NIST juga mengakomodasi penggunaan kunci FIPS 203 [6] sebagai komponen dalam mode komposit, dengan panduan tambahan yang akan disediakan melalui SP 800-227 [32]. Sementara itu, untuk tanda tangan digital, teknik hibrida umumnya diwujudkan melalui *dual signatures*, yakni dua atau lebih tanda tangan pada pesan yang sama, yang dapat diterapkan baik pada data maupun sertifikat dalam PKI, selama salah satu algoritmanya merupakan algoritma yang disetujui NIST. Meskipun demikian, penggunaan teknik ini harus mempertimbangkan implikasi biaya, penurunan kinerja, serta kompleksitas rekayasa. Penerapan *hybrid solution* direkomendasikan khususnya bagi sektor dengan keterhubungan sistem dan kompleksitas teknologi tinggi seperti pemerintahan berbasis elektronik, keuangan, dan telekomunikasi.

6. *Risk-based approach*

Prinsip *risk-based approach* menekankan bahwa setiap langkah migrasi harus didasarkan pada analisis risiko terhadap aset, algoritma, dan dampak bisnis. Berdasarkan hasil analisis risiko, organisasi harus memprioritaskan migrasi untuk sistem elektronik yang memiliki nilai risiko lebih tinggi atau data yang membutuhkan konfidensialitas jangka panjang, seperti:

- a. Data rahasia instansi/organisasi;
- b. Data elektronik tertutup;
- c. Informasi keuangan [33];
- d. Rekam medis elektronik dan data pribadi jangka panjang;
- e. Data pertanahan.

AIVD, CWI, dan TNO [3] serta TNO [5] menyarankan pendekatan penilaian risiko berbasis tiga dimensi yaitu kerentanan, dampak dan upaya migrasi. Dengan menghitung skor risiko kuantum, instansi dapat menentukan prioritas migrasi secara objektif dan efisien.

7. Kolaborasi dan Interoperabilitas

Migrasi PQC adalah upaya kolektif yang memerlukan kolaborasi antara pemerintah, akademisi, pelaku usaha dan konsumen. AIVD, CWI, dan TNO [3] menekankan pentingnya *ecosystem readiness*, yaitu kesiapan seluruh rantai ekosistem mulai dari pembuat kebijakan, developer perangkat lunak/perangkat keras/perangkat tegar, vendor keamanan, hingga pengguna akhir. Dalam konteks Indonesia, kolaborasi ini dapat diwujudkan melalui:

- a. Koordinasi nasional PQC lintas sektor yang diinisiasi BSSN;
- b. Kerja sama dengan instansi pengawas dan pengatur sektor (IPPS), seperti OJK, BI, Komdigi, Kemenhan, Kemenkes, dll.
- c. Kolaborasi riset dengan universitas dan lembaga penelitian untuk pengujian algoritma dan pengembangan *quantum-safe libraries*;

- d. Partisipasi dalam forum internasional, diantaranya ISO/IEC JTC1/SC27, ETSI *Industry Specification Group on Quantum Safe Cryptography* (ISG QSC), *Post-Quantum Cryptography Coalition* (PQCC), *Post-Quantum Cryptography Alliance* (PQCA), *GSMA Post-Quantum Telco Network Task Force*.
- e. Pemetaan vendor dan kesiapan/rencana/langkah vendor untuk migrasi ke PQC.

Selain kolaborasi, interoperabilitas juga menjadi kunci. Sistem PQC harus kompatibel lintas vendor, *platform*, dan protokol agar tidak menimbulkan fragmentasi keamanan di tingkat nasional.

2.2 Three-Phase Model (Model Tiga fase)

Pendekatan model tiga fase yang dikembangkan oleh AIVD, CWI, dan TNO [3] merupakan salah satu metodologi yang paling banyak diadopsi secara internasional dalam perencanaan migrasi PQC. Pendekatan ini terbukti efektif karena memberikan kerangka kerja progresif yang menggabungkan penilaian risiko, perencanaan teknis, dan implementasi bertahap.

Ketiga fase tersebut adalah:

1. *Quantum-vulnerability diagnosis* (diagnosis kerentanan kuantum)
Fase ini bertujuan untuk mengidentifikasi, memetakan, dan mengevaluasi semua penggunaan kriptografi yang ada dalam organisasi. Kegiatannya terdiri atas:
 - a. Melakukan inventarisasi:
 - 1) aset kriptografi pada seluruh sistem, perangkat, dan aplikasi;
 - 2) seluruh data yang dikelola oleh organisasi; dan
 - 3) pemasok aset kriptografi.
 - b. Menyusun format standar untuk mendokumentasikan semua elemen kriptografi;
 - c. Menilai risiko tingkat kerentanan kuantum menggunakan kerangka kerentanan, dampak dan upaya migrasi

- d. Menentukan prioritas sistem yang harus dimigrasikan lebih dulu.
2. *Migration planning* (perencanaan migrasi)
- Setelah diagnosis selesai, instansi memasuki tahap perencanaan strategis dan teknis. Langkahnya terdiri atas:
- a. Menyusun rencana migrasi organisasi (*migration roadmap*) mencakup penetapan prioritas, identifikasi ketergantungan, serta antisipasi konsekuensi migrasi;
 - b. Mengintegrasikan rencana migrasi dengan proses bisnis melalui penunjukan manajer migrasi yang kompeten, penyediaan anggaran yang memadai, pengelolaan waktu henti (*down time*) secara cermat, serta koordinasi dengan organisasi sejenis untuk menjaga interoperabilitas dan efisiensi;
 - c. Mengidentifikasi dan mengatasi tantangan migrasi secara kolaboratif menggunakan model maturitas berbasis delapan aspek prioritas [3] untuk menilai kemajuan dan merumuskan langkah perbaikan ;
 - d. Menetapkan urutan dan metode penggantian aset kriptografi berdasarkan ketergantungan antar aset, menjaga perlindungan melalui isolasi bila diperlukan, mempersiapkan penggantian perangkat keras, serta merencanakan dan melaksanakan pengujian menyeluruh terhadap solusi baru sebelum diterapkan pada sistem aktif atau lingkungan berskala luas (*production/enterprise environment*);
 - e. Melakukan estimasi biaya serta alokasi sumber daya berdasarkan inventaris dan hasil penilaian risiko, dengan memperhitungkan kebutuhan perangkat keras, layanan, dan tenaga ahli, menyiapkan mekanisme pemulihan untuk mengantisipasi *downtime*, serta berinvestasi pada kemampuan *cryptographic agility* agar sistem dapat beradaptasi terhadap perkembangan standar dan ancaman kriptografi di masa depan.

3. *Execution* (pelaksanaan migrasi)

Tahap terakhir berfokus pada implementasi bertahap dan pengujian sistem PQC-*ready*. Kegiatannya mencakup:

- a. Melaksanakan rencana migrasi berdasarkan *roadmap* yang telah disusun, dimulai dari aset prioritas tinggi, dengan memastikan inventaris aset kriptografi selalu diperbarui secara berkelanjutan.
- b. Menjalankan migrasi dengan cermat, memastikan pemilihan algoritma pengganti, konfigurasi, dan implementasi dilakukan dengan benar untuk menghindari munculnya kerentanan baru atau perluasan permukaan serangan.
- c. Memastikan pemahaman internal terhadap PQC meskipun pelaksanaan migrasi dilakukan oleh pihak ketiga, agar organisasi mampu menilai keamanan dan kesesuaian solusi yang digunakan.
- d. Memigrasikan primitif atau protokol kriptografi sesuai kebutuhan, dengan memprioritaskan pembaruan protokol (misalnya peningkatan versi TLS ke versi 1.3) bagi organisasi yang tidak mengembangkan algoritma sendiri.
- e. Memprioritaskan migrasi kriptografi asimetris, terutama pada sistem dengan masa pakai panjang atau berisiko tinggi terhadap serangan HNDL, sementara kriptografi simetris umumnya tetap aman.
- f. Menerapkan pendekatan *hybrid* AND yang menggabungkan algoritma klasik dan PQC secara bersamaan untuk memastikan keamanan transisi dan menjaga interoperabilitas.
- g. Menghindari pendekatan *hybrid* OR karena berpotensi menyebabkan *downgrade attacks*. Namun jika harus digunakan, harus dipastikan ada kebijakan dan kontrol keamanan yang jelas serta mekanisme “*fallback/rollback*”.
- h. Mempertimbangkan penggunaan *pre-shared keys* (PSK) hanya untuk sistem tertutup dan sangat terkendali, dengan

distribusi kunci rahasia yang aman serta komunikasi terbatas antar sistem terpercaya.

- i. Melakukan pengujian dan validasi menyeluruh terhadap seluruh komponen migrasi, termasuk kompatibilitas algoritma PQC, performa sistem, serta efektivitas solusi hibrida.
- j. Memonitor dan mengevaluasi hasil migrasi untuk memastikan semua aset telah terlindungi dengan algoritma yang tahan kuantum dan siap untuk dilakukan pembaruan atau penyesuaian di masa mendatang.

2.3 Integrasi dengan model empat fase

Untuk melengkapi model tiga fase dari AIVD, CWI, dan TNO [3], panduan ini juga mengadopsi kerangka yang diajukan PQCC [4] yang membagi kegiatan ke dalam empat fase, yaitu:

1. *Preparation* (persiapan), organisasi menetapkan tujuan migrasi, menunjuk pemimpin, dan menyelaraskan pemangku kepentingan melalui komunikasi strategis;
2. *Baseline Understanding* (pemahaman dasar), organisasi menetapkan inventaris data, menetapkan aset prioritas, serta menilai kebutuhan sumber daya dan anggaran;
3. *Execution* (eksekusi), organisasi berkolaborasi dengan vendor dan pemilik sistem untuk mengembangkan atau mengimplementasikan solusi PQC secara efektif.;
4. *Monitoring and Evaluation* (pemantauan dan evaluasi), organisasi memantau kemajuan migrasi dan meninjau ulang keamanan kriptografi seiring perkembangan kemampuan kuantum.

Kombinasi kedua model ini memastikan proses migrasi PQC berjalan komprehensif, terukur, dan berkelanjutan, serta dapat diterapkan pada berbagai skala instansi di Indonesia.

2.4 Tahap Implementasi

Migrasi ke PQC merupakan proses jangka panjang yang memerlukan koordinasi lintas fungsi, pembiayaan strategis, serta kesiapan organisasi

baik dari sisi teknis maupun tata kelola. Berdasarkan pendekatan AIVD, TNO, dan CWI [3] serta PQCC [4] proses ini dapat dibagi menjadi lima tahap, yaitu:

1. Tahap Persiapan
2. Tahap *Baseline understanding* (pemahaman dasar)
3. Tahap Perencanaan
4. Tahap Pelaksanaan Migrasi
5. Tahap Pemantauan dan Evaluasi

Keempat tahap ini membentuk siklus migrasi berkelanjutan yang memungkinkan PSE beradaptasi terhadap dinamika perkembangan standar PQC dan ancaman komputer kuantum.



BAB III

TAHAP PERSIAPAN



BAB III

TAHAP PERSIAPAN

Bab ini menjelaskan langkah-langkah awal yang perlu dilakukan organisasi untuk mempersiapkan migrasi ke PQC. Tahap persiapan mencakup pembangunan dasar kesiapan organisasi melalui penetapan tujuan, pemahaman risiko dan urgensi, pembentukan kepemimpinan yang jelas, pemetaan inventaris kriptografi, penyelarasan pemangku kepentingan, serta kolaborasi awal dengan vendor yang menyediakan solusi PQC. Hasil dari tahap ini menjadi fondasi penting bagi penyusunan strategi migrasi yang efektif, terukur, dan berkelanjutan.

3.1 Tujuan

Membangun dasar kesiapan organisasi untuk migrasi PQC melalui pemahaman risiko dan urgensi, penetapan jadwal migrasi, pembentukan kepemimpinan yang jelas, pemetaan inventaris dan kesadaran akan PQC, penyelarasan pemangku kepentingan, serta inisiasi kolaborasi dengan penyedia vendor solusi PQC [4].

3.2 Landasan Ilmiah/Teknis

Tahap persiapan menjadi fondasi penting dalam migrasi ke PQC karena memastikan kesiapan strategis organisasi. Pemahaman atas kerentanan dan urgensi memungkinkan penentuan prioritas aset dan jadwal migrasi yang tepat. Penunjukan pemimpin migrasi menjamin koordinasi yang efektif. Identifikasi inventaris serta kesadaran akan PQC membantu memetakan kondisi awal dan kapasitas sumber daya. Penyelarasan pemangku kepentingan melalui komunikasi strategis membangun komitmen bersama. Keterlibatan awal dengan vendor solusi PQC juga memastikan strategi migrasi disusun berdasarkan informasi teknis yang akurat dan selaras dengan praktik terbaik.

3.3 Langkah-langkah

3.3.1 Penentuan profil organisasi

Untuk menentukan tingkat keterlibatan dalam migrasi PQC, organisasi perlu menetapkan tujuan migrasi dengan memahami tingkat risiko yang dapat diterima dalam melindungi data dan aset. Tahapan ini meliputi identifikasi kerentanan dan urgensi, penetapan jadwal migrasi, penunjukan pemimpin migrasi, pemetaan inventaris dan kesadaran akan PQC, penyelarasan pemangku kepentingan melalui komunikasi strategis, serta keterlibatan awal dengan vendor solusi PQC. Berdasarkan hasil analisis tersebut, organisasi diklasifikasikan ke dalam kategori profil PQC untuk menetapkan waktu, prioritas, dan strategi migrasi yang paling tepat.

Terdapat tiga profil PQC [3], yaitu:

1. *Urgent adopters* (adopter mendesak)

Organisasi yang harus segera memulai migrasi PQC karena memiliki risiko tinggi terhadap serangan kuantum. Organisasi yang termasuk dalam profil ini, yaitu:

- a. Pengelola data pribadi, terutama yang bersifat jangka panjang;
- b. Pengelola data sensitif organisasi;
- c. Penyedia infrastruktur kritis;
- d. Penyedia infrastruktur jangka panjang.

2. *Regular adopters* (adopter reguler)

Organisasi yang tidak termasuk dalam profil adopter mendesak, dengan risiko rendah terhadap serangan kuantum sehingga dapat menunda migrasi PQC. Namun demikian, organisasi tersebut perlu memastikan bahwa mereka berada dalam kondisi terbaik untuk melakukan migrasi di kemudian hari.

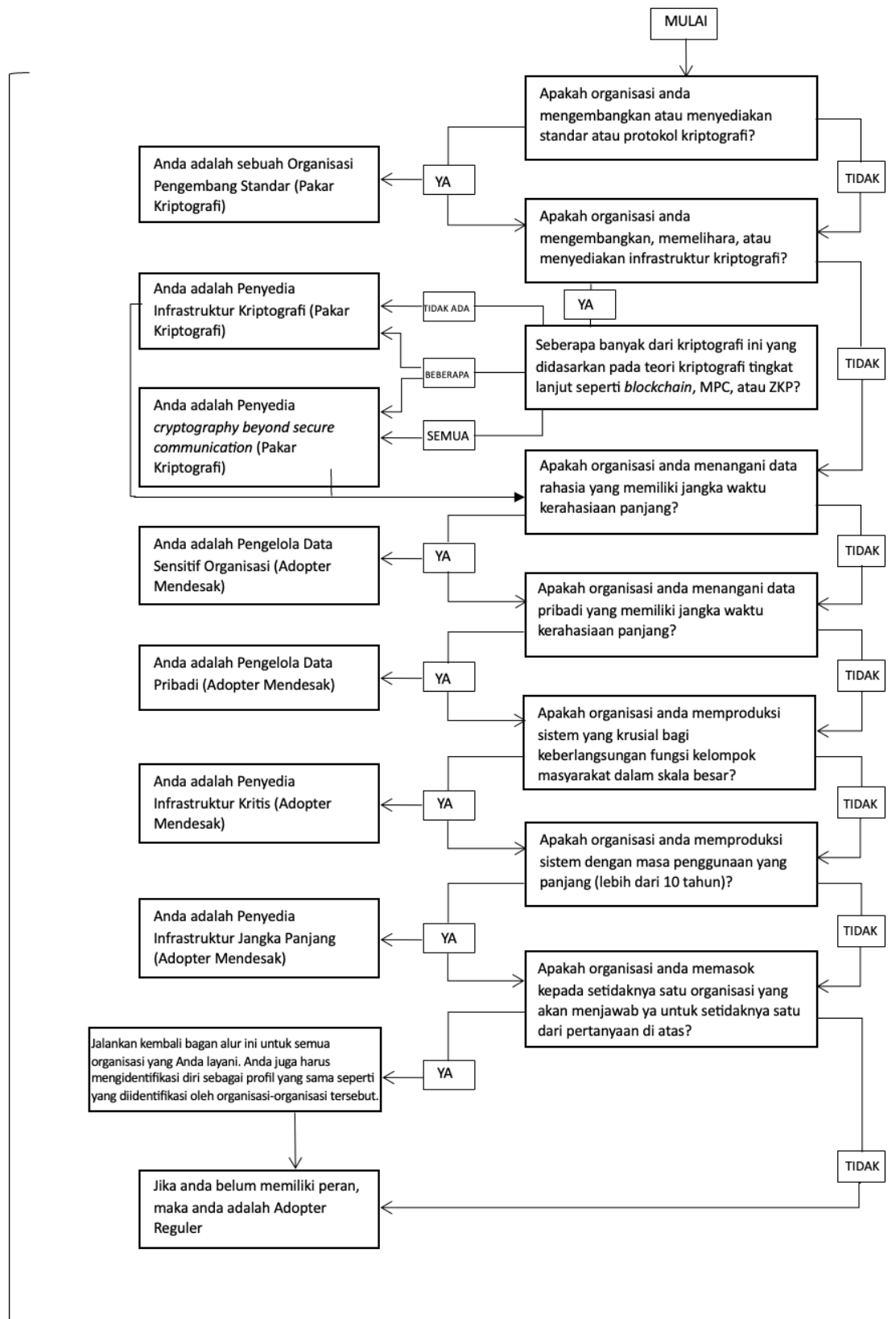
3. *Cryptography experts* (pakar kriptografi)

Organisasi yang memiliki keahlian internal untuk migrasi PQC dan bertanggung jawab atas keamanan aset kriptografi organisasi lain. Organisasi yang termasuk dalam profil ini, yaitu:

- a. Organisasi pengembang standar;
- b. Penyedia infrastruktur kriptografi;
- c. Penyedia *cryptography beyond secure communication*.

Organisasi yang termasuk dalam kategori pakar kriptografi perlu segera menerapkan rekomendasi migrasi pada infrastruktur internal serta bersiap mengimplementasikan algoritma *quantum-safe* setelah standar tersedia, mengingat perannya yang penting sebagai penyedia aset kriptografi dalam rantai pasok.

Untuk menentukan profil PQC yang paling sesuai, baik bagi organisasi sendiri maupun bagi organisasi lain yang menerima layanannya, disarankan agar dilakukan pencocokan kondisi aktual organisasi dengan seluruh deskripsi profil yang telah dijelaskan pada bagian sebelumnya. Selain itu, diagram alur pada Gambar 3.1 dapat digunakan sebagai alat bantu visual untuk memudahkan proses identifikasi dan penetapan profil PQC yang tepat.



Gambar 3.1 Diagram alur untuk menentukan profil PQC suatu organisasi digambar ulang dari [3].

3.3.2 Menetapkan Strategi Penemuan Aset Kriptografi Dan Penanggung Jawab

Langkah ini bertujuan memastikan proses inventarisasi kriptografi dan aset data terlaksana secara sistematis, mencakup seluruh komponen relevan dalam organisasi, serta memiliki penanggung jawab yang jelas.

Tahapnya adalah sebagai berikut:

1. Menunjuk Penanggung Jawab dan Tim Pelaksana
 - a. Menunjuk penanggung jawab utama, seperti *chief information security officer* (CISO), atau tim keamanan informasi, yang memiliki kewenangan secara menyeluruh terhadap pelaksanaan, koordinasi, dan pemantauan kemajuan kegiatan migrasi. Penanggung jawab utama berperan sebagai koordinator strategis antara tim teknis, manajemen, dan penyedia solusi, sekaligus memastikan seluruh kegiatan selaras dengan tujuan organisasi. Posisi ini sebaiknya berada pada tingkat strategis agar dapat mengambil keputusan lintas unit dan menjaga konsistensi arah kebijakan migrasi PQC.
 - b. Membentuk tim teknis pendukung yang terdiri atas perwakilan unit TI, pengelola sistem, dan pemilik aplikasi untuk mendukung proses identifikasi aset. Tim ini bertugas mendukung proses identifikasi aset, pengumpulan data, serta analisis kebutuhan migrasi. Untuk memastikan efisiensi, perlu ditetapkan mekanisme koordinasi antar-unit agar proses berjalan terintegrasi dan tidak terjadi tumpang tindih pekerjaan.
2. Menetapkan Tujuan

Menentukan maksud dari pelaksanaan penemuan aset kriptografi. Tujuan dapat mencakup pemenuhan

kepatuhan, pemeliharaan sistem keamanan, atau pembaruan mekanisme perlindungan kriptografi.

3. Menetapkan Ruang Lingkup

Menentukan jenis aset yang akan diidentifikasi dan prioritasnya. Informasi yang perlu diidentifikasi dapat berupa informasi dasar tentang algoritma dan sistem, serta informasi tambahan untuk inventaris dan otomatisasi inventaris. Informasi terkait jenis aset yang diidentifikasi paling sedikit dapat berupa:

- a. Nama yang dapat diidentifikasi secara unik untuk sistem, kode atau aplikasi yang menggunakan kriptografi
- b. Tujuan keamanan: konfidensialitas, integritas, autentikasi, non-repudiasi atau kontrol akses
- c. Nama Algoritma kriptografi
- d. Panjang kunci kriptografi (jika relevan)
- e. Jumlah bit keluaran fungsi *hash* (jika relevan)
- f. Menerapkan skema hibrida (menerapkan algoritma kriptografi klasik yang rentan terhadap kuantum dan algoritma PQC secara bersamaan dalam satu protokol tunggal) atau tidak
- g. Jika menerapkan skema hibrida, maka menyebutkan:
 - 1) nama algoritma kriptografi pada skema hibrida
 - 2) panjang kunci dari masing-masing algoritma kriptografi pada skema hibrida (jika relevan)
 - 3) panjang bit keluaran fungsi *hash* dari masing-masing algoritma kriptografi pada skema hibrida (jika relevan)
 - 4) mekanisme pencampuran kunci (*key mixing*).

4. Menetapkan Metodologi Penemuan

Menentukan alat, teknik, dan prosedur yang akan digunakan. Langkah ini mencakup pemilihan perangkat pendeteksi (*scanning tools*) untuk mendeteksi algoritma

kriptografi, penentuan sistem yang dianalisis, serta pembagian peran dan tanggung jawab antar anggota tim.

5. Menetapkan Analisis Data

Menentukan jenis dan kedalaman informasi yang diperlukan untuk setiap aset, termasuk metrik evaluasi efektivitas, kepatuhan, serta tingkat risiko yang terkait dengan masing-masing aset kriptografi.

6. Pelaporan

Menetapkan mekanisme dokumentasi dan pelaporan hasil penemuan. Format dan struktur laporan perlu disusun secara jelas, mencakup data hasil identifikasi, analisis, serta rekomendasi tindak lanjut, sehingga informasi yang disajikan mudah dipahami dan dapat ditindaklanjuti oleh pihak terkait secara tepat.

7. Reviu

Menentukan frekuensi dan mekanisme pembaruan inventaris untuk memastikan data tetap mutakhir, akurat, dan relevan dengan perubahan aset maupun kebijakan organisasi.

Sebagai bagian dari strategi ini, penanggung jawab utama bersama timnya juga perlu melakukan identifikasi inventaris dan penilaian kesiapan organisasi. Kegiatan ini bertujuan memperoleh gambaran menyeluruh tentang kondisi aktual penggunaan kriptografi, tingkat kesadaran organisasi terhadap ancaman kuantum, serta kesiapan sumber daya untuk melaksanakan migrasi PQC.

Tahapan ini mencakup penelaahan terhadap inventaris aset, *Software Bill of Materials* (SBOM), *Cryptographic Bill of Materials* (CBOM) dan penilaian risiko terhadap komputasi kuantum yang dimiliki organisasi. Dokumen-dokumen ini sering kali dibuat untuk tujuan berbeda pada waktu yang berbeda, sehingga perlu

diperbarui dan diseragamkan. Dalam proses peninjauan, setiap aset harus didokumentasikan dengan jelas, mencakup lokasi data, penanggung jawab, tujuan penggunaan, serta cara pengelolaannya. Pendokumentasian ini membantu mengidentifikasi kesenjangan sejak awal dan mencegah pemborosan sumber daya, sekaligus memastikan migrasi PQC dapat dilakukan secara efisien dan terarah [4].

Setelah strategi dirumuskan, organisasi dapat segera melaksanakan proses inventarisasi aset kriptografi pada seluruh sistem, aplikasi, dan infrastruktur yang digunakan sebagai dasar dalam penyusunan inventaris kriptografi.

3.3.3 Mengidentifikasi Pemangku Kepentingan dan Menyusun Strategi Komunikasi

Tahap ini bertujuan untuk memastikan penyelarasan antara pimpinan organisasi dan pemangku kepentingan utama terhadap nilai strategis serta tujuan migrasi PQC. Penanggung jawab utama perlu menyusun rencana komunikasi strategis yang mencakup identifikasi pemangku kepentingan, penyelarasan peran dan tanggung jawab, serta strategi komunikasi yang menjelaskan proses dan kebutuhan migrasi PQC.

Aktivitas ini dapat mencakup keterlibatan awal dengan operator sistem dan vendor guna menilai kesiapan migrasi, mengidentifikasi ketersediaan solusi PQC, serta memahami konteks operasional organisasi. Dalam penyusunan strategi komunikasi, organisasi perlu mempertimbangkan aspek nilai investasi (*return on investment*), urgensi migrasi, metode pengukuran dampak, dan kebutuhan sumber daya finansial serta operasional.

Pemangku kepentingan mencakup pihak-pihak yang memiliki ketergantungan terhadap sistem kriptografi organisasi atau berperan dalam mendukung keberhasilan migrasi PQC. Pemahaman terhadap kepentingan, ekspektasi, dan pengaruh setiap pihak menjadi dasar untuk membangun komunikasi yang efektif dan memperoleh dukungan berkelanjutan.

Organisasi disarankan untuk menyusun pernyataan posisi (*positioning statement*) yang menjelaskan tujuan, ruang lingkup, dan urgensi migrasi PQC, serta menyiapkan pesan tanggapan terhadap potensi resistensi. Selain itu, penyusunan *elevator pitch* (penjelasan singkat mengenai nilai migrasi PQC) yang ringkas dan terarah dapat digunakan untuk menjelaskan nilai strategis migrasi kepada pemangku kepentingan internal dan eksternal. Karena komunikasi dan keterlibatan pemangku kepentingan merupakan proses berkelanjutan, organisasi perlu menetapkan mekanisme untuk memantau efektivitas pesan dan tingkat dukungan terhadap kegiatan migrasi PQC.

Keterlibatan dengan vendor dan operator sistem juga menjadi bagian penting dari tahap ini, mencakup evaluasi kesiapan teknis, rencana implementasi, serta dampak bisnis dari penerapan PQC. Pertanyaan teknis utama yang perlu dikaji meliputi [4]:

1. Ketersediaan dan jadwal rilis solusi PQC dari vendor, termasuk solusi untuk sistem internal;
2. Kebutuhan pembaruan perangkat keras maupun perangkat lunak;
3. Estimasi biaya implementasi dan pemeliharaan;
4. Dampak bisnis yang diperkirakan;
5. Ketersediaan SBOM dan CBOM; serta
6. Dukungan terhadap *cryptographic agility*.

Pendekatan ini membantu organisasi memperoleh pemahaman menyeluruh mengenai kesiapan ekosistemnya, sekaligus memastikan bahwa strategi migrasi PQC dirancang secara terukur, efisien, dan berkelanjutan.



BAB IV

TAHAP PEMAHAMAN

DASAR



BAB IV

TAHAP PEMAHAMAN DASAR

Bab ini memberikan informasi mengenai tujuan dan landasan ilmiah dari tahap pemahaman dasar, serta langkah – langkah yang dilakukan dalam melakukan inventarisasi aset kriptografi dan penilaian risiko kuantum yang dapat dijadikan sebagai panduan oleh organisasi

4.1 Tujuan

Tujuan dari tahap ini adalah untuk memperoleh pemahaman yang komprehensif mengenai seluruh aset data dan aset kriptografi yang digunakan dalam organisasi sebagai dasar perencanaan migrasi ke PQC. Tahap ini dimaksudkan untuk memastikan tidak terdapat algoritma kriptografi yang rentan dalam sistem serta untuk mendukung upaya mitigasi risiko terhadap ancaman kuantum maupun non-kuantum. Selain itu, inventaris kriptografi yang tersusun secara lengkap dapat dimanfaatkan sebagai bagian dari kebijakan kriptografi organisasi guna mengidentifikasi penggunaan yang tidak sesuai serta memperkuat tata kelola keamanan informasi secara menyeluruh.

4.2 Landasan Ilmiah/Teknis

Pemahaman dasar merupakan fase fundamental dalam proses migrasi PQC karena membentuk dasar pengetahuan tentang kondisi sistem kriptografi dalam organisasi. Pada tahap ini dilakukan-inventarisasi aset kriptografi dan penilaian risiko kuantum. Inventarisasi aset kriptografi terdiri dari kegiatan deteksi dan klasifikasi penggunaan kriptografi, dokumentasi dan pengumpulan atribut teknis, dan pembuatan CBOM. Penilaian risiko kuantum terdiri dari kegiatan identifikasi penyerang yang realistis, kelemahan terhadap kuantum, analisis dampak, upaya migrasi, dan skor risiko kuantum.

Secara ilmiah, tahap ini diperlukan untuk memastikan bahwa organisasi memiliki pemahaman dasar yang terukur dan

terdokumentasi mengenai ekosistem kriptografinya yaitu algoritma, protokol, kunci, sertifikat, serta integrasi antarsistem. Tanpa adanya pemahaman dasar tersebut, risiko *blind spot* terhadap algoritma lama, ketergantungan pihak ketiga, atau aset yang belum terinventarisasi dapat meningkat, yang dapat berdampak pada terhambatnya efektivitas dan keamanan proses migrasi.

Tahap Pemahaman Dasar juga memungkinkan organisasi untuk melakukan klasifikasi aset berdasarkan risiko dan masa hidup data (*data lifespan*). Pendekatan ini penting untuk prioritas migrasi, karena aset dengan nilai risiko lebih tinggi atau data yang membutuhkan konfidensialitas jangka panjang harus diprioritaskan untuk migrasi terlebih dahulu.

Dengan demikian, tahapan ini bukan sekadar administrasi teknis, melainkan merupakan dasar ilmiah dan strategis bagi perumusan kebijakan, alokasi sumber daya, dan penentuan prioritas migrasi. Hasil dari tahap ini akan meningkatkan efektivitas pengambilan keputusan dan menjamin bahwa setiap langkah transisi menuju PQC dilakukan secara terarah dan berbasis risiko.

4.3 Langkah-langkah

4.3.1 Inventarisasi Aset Kriptografi

Inventarisasi aset kriptografi merupakan langkah awal dalam proses migrasi yang bertujuan untuk mengidentifikasi seluruh area dan sistem yang menggunakan fungsi kriptografi. Lampiran A memberikan gambaran umum mengenai kemungkinan keberadaan komponen kriptografi, serta petunjuk lokasi atau sumber informasi tempat elemen-elemen kriptografi dapat ditemukan. Inventarisasi aset kriptografi dilakukan terhadap aset-aset yang berpotensi mengandung algoritma kriptografi, meliputi:

1. Sistem inti organisasi (*core systems*), seperti Sistem Pemerintahan Berbasis Elektronik (SPBE), layanan publik, dan sistem identitas;
2. Infrastruktur jaringan, seperti gateway, VPN, *firewall*, dan *router*;
3. Aplikasi bisnis dan publik (*mobile apps, web services, database, cloud*);
4. Perangkat keras dan perangkat tegar (*firmware*) yang mengandung fungsi enkripsi (IoT, *hardware security module* (HSM), *key management system*, sensor, *endpoint, smartcard*).

Untuk tujuan efisiensi, kegiatan inventarisasi aset kriptografi dapat dilakukan dengan memprioritaskan sistem berisiko tinggi atau bersifat strategis nasional sesuai metodologi TNO. Inventarisasi aset kriptografi dilakukan dalam beberapa tahap, yaitu:

1. Inventarisasi Sistem

Inventarisasi sistem merupakan tahap pertama dalam proses migrasi ke PQC. Tujuan inventarisasi sistem adalah untuk mengidentifikasi seluruh aset yang terkait dengan penggunaan kriptografi, seperti perangkat keras, firmware, sistem operasi, aplikasi dan layanan yang menjadi dasar analisis lebih lanjut, termasuk untuk pembuatan SBOM dan CBOM, serta penentuan prioritas migrasi PQC. Tabel 4.1 menggambarkan struktur tabel inventarisasi sistem.

Tabel 4.1 Struktur tabel inventarisasi sistem

Atribut	Deskripsi	Contoh pengisian
Nama Aset / Sistem	Nama sistem, aplikasi, perangkat atau komponen	Reverse Proxy Gateway (NGINX 1.22)

Atribut	Deskripsi	Contoh pengisian
	teknologi yang diinventarisasi.	
Lokasi / pemilik	Menunjukkan siapa yang bertanggung jawab serta lokasi dimana aset berada.	Pusat Data/ Tim Infrastruktur Layanan
Apakah memiliki fungsi kriptografi? (ya/tidak)	Untuk mengetahui apakah aset menggunakan kriptografi dalam bentuk apapun.	Ya
Contoh Algoritma yang digunakan	Menjelaskan jenis algoritma yang digunakan pada aset tersebut	AES-GCM RSA
SBOM/CBOM tersedia	Untuk menyatakan ketersediaan SBOM/CBOM sehingga dapat membantu identifikasi <i>library</i> dan komponen kriptografi yang tersembunyi atau tidak terdokumentasi.	SBOM: Tidak CBOM: Tidak
Tingkat kesiapan migrasi	Menilai kesiapan aset untuk bermigrasi ke	Rendah

Atribut	Deskripsi	Contoh pengisian
	algoritma PQC. Dikategorikan menjadi : • Tinggi: siap, vendor dan platform sudah menyediakan <i>roadmap</i> migrasi • Sedang: perlu reviu dan update, namun vendor dan platform sudah menyediakan <i>roadmap</i> migrasi • Rendah: tidak siap; ketergantungan algoritma atau <i>hardware legacy</i>	
Tindakan	Dapat diisi dengan informasi tindak lanjut yang harus dilakukan.	Periksa dukungan algoritma PQC pada modul TLS.

2. SBOM

Setelah inventarisasi sistem, langkah selanjutnya adalah inventarisasi komponen perangkat lunak yang digunakan oleh sistem-sistem tersebut atau SBOM. SBOM adalah

daftar yang menggambarkan komponen-komponen yang membentuk suatu perangkat lunak serta hubungan antar komponen tersebut. Inventarisasi SBOM ini bertujuan mengidentifikasi ketergantungan kriptografi di dalam perangkat lunak sehingga organisasi dapat:

- a. Menilai potensi dampak migrasi PQC terhadap sistem.
- b. Menentukan sistem mana yang paling membutuhkan pembaruan *library* atau modul kriptografis.
- c. Merencanakan prioritas mitigasi dan tindakan migrasi

Salah satu aspek penting dari daftar ini adalah strukturnya yang terstandardisasi dan dapat dibaca oleh mesin, sehingga memungkinkan proses otomatisasi. Tabel 4.2 berikut menggambarkan struktur tabel inventarisasi komponen perangkat lunak.

Tabel 4.2 Inventarisasi komponen perangkat lunak

Atribut	Deskripsi	Contoh pengisian
Nama sistem/ aplikasi	Nama sistem, aplikasi, layanan, atau komponen perangkat lunak yang diinventarisasi	Sistem Registrasi Online
Tujuan penggunaan	Fungsi atau kegunaan utama sistem dalam organisasi. Biasanya menjelaskan aktivitas bisnis yang didukung.	Registrasi akun layanan publik

Atribut	Deskripsi	Contoh pengisian
URL	Alamat akses sistem, baik publik maupun internal. Jika tidak berbasis web, bisa diisi “N/A”.	https://reg.gov.id
Mode layanan	Cara layanan disampaikan: <i>Online / Offline, API-based, Batch, Web Application, Mobile.</i>	<i>Online</i>
Sasaran pengguna	Pihak yang menggunakan sistem: masyarakat, ASN, mitra, internal, atau kombinasi.	Masyarakat
Komponen perangkat lunak	Daftar <i>library, framework, runtime, dependencies</i>	Node.js 18 LTS, OpenSSL 3.0.2, ReactJS
Modul pihak ketiga yang digunakan	Modul pihak ketiga yang digunakan dalam sistem	JWT Auth Module, Passport.js

Atribut	Deskripsi	Contoh pengisian
API atau layanan eksternal yang terhubung	Integrasi dengan sistem atau API eksternal yang digunakan untuk operasional.	MyIdentity (SSO), SMS Gateway API
Tingkat kritikalitas	Dampak pada keamanan dan operasional jika komponen perangkat lunak mengalami kerentanan, kegagalan, atau kompromi (rendah/ sedang/ tinggi/ sangat tinggi)	Tinggi
Kategori data yang diproses	klasifikasi data : publik, internal, terbatas, rahasia, atau sangat rahasia	Rahasia
Data Lifespan	Jangka waktu data disimpan dan digunakan dalam sistem sebelum dihapus	10 tahun
Status penggunaan sistem / aplikasi	Apakah sistem aktif digunakan,	Aktif digunakan

Atribut	Deskripsi	Contoh pengisian
	sedang dalam pemeliharaan, <i>deprecated</i> , atau akan dinonaktifkan	
Pengembang sistem/aplikasi	Pihak pengembang sistem, misalnya vendor eksternal, tim pengembang internal, atau <i>hybrid</i>	Vendor: PT. Digital Nusantara
Apakah memiliki mandat khusus (misal secara nasional) terkait sistem tersebut	Menjelaskan apakah sistem diatur oleh mandat hukum, kebijakan nasional, atau standar tertentu	Ya, PP 80 Tahun 2021
Ketersediaan kompetensi teknis di internal	Apakah organisasi memiliki SDM dengan kemampuan teknis mengelola, memelihara, atau memodifikasi sistem / aplikasi	Tidak
Rujukan ke dokumen CBOM	Referensi untuk inventarisasi	CBOM#1

Atribut	Deskripsi	Contoh pengisian
	komponen kriptografi	

3. Inventarisasi Komponen Kriptografi

Inventarisasi komponen kriptografi bertujuan untuk mengidentifikasi penggunaan algoritma dalam sistem. Tahap ini merupakan proses *discovery* untuk dapat menemukan bagaimana kriptografi diimplementasikan. Prosesnya dapat dilakukan dengan metode otomatis maupun manual. Metode yang direkomendasikan meliputi:

- Static analysis* terhadap kode sumber, file konfigurasi, atau skrip enkripsi;
- Dynamic analysis* dengan memantau lalu lintas jaringan, TLS *handshake*, dan aktivitas API;
- Dependency scanning* terhadap *library* eksternal (misalnya OpenSSL, OpenQuantumSafe, BouncyCastle, Libsodium);
- Hardware* audit untuk perangkat dengan enkripsi terpasang (misalnya *smartcard*, TPM, HSM).

Hasil inventarisasi tersebut kemudian diklasifikasikan konteks penggunaannya ke dalam kategori: *data at rest encryption*, *data in transit encryption*, *authentication/signature mechanisms* dan *key management* atau *key exchange*. Tahap ini memberikan gambaran menyeluruh mengenai penggunaan kriptografi dalam sistem sebelum dilakukan pemetaan lebih lanjut menggunakan format standar.

Untuk setiap komponen yang terdeteksi, dilakukan pendokumentasian secara detail seperti ditunjukkan pada Tabel 4.3.

Tabel 4.3 Dokumentasi atribut teknis

Parameter	Deskripsi	Contoh
Nama sistem/aplikasi	Identifikasi sistem atau layanan yang menggunakan kriptografi	e-Procurement Portal
Jenis algoritma	RSA, ECC, AES, SHA-256, HMAC, dll.	RSA
Panjang kunci (bit)	Ukuran kekuatan kriptografi	2048-bit untuk RSA
Fungsi utama	Enkripsi data, tanda tangan digital, autentikasi, dll.	Tanda tangan digital
Lokasi penyimpanan kunci	File lokal, HSM, KMS, <i>cloud key store</i>	HSM lokal
<i>Library</i> / modul	<i>Library</i> atau modul kriptografi yang digunakan	OpenSSL 1.1.1
Protokol terkait	TLS, IPSec, SSH, S/MIME, dll.	TLS 1.2
Status dukungan PQC	Sudah mendukung/ belum mendukung algoritma PQC	Belum mendukung

Setelah seluruh komponen kriptografi teridentifikasi dan diklasifikasikan, organisasi perlu memerlukan cara pendokumentasian yang terstruktur dan konsisten agar setiap algoritma, *library*, kunci dan protokol kriptografi dapat dilacak dan dianalisis. Untuk memastikan interoperabilitas, efisiensi dan kemampuan analisis otomatis, diperlukan format baku yang dapat dibaca mesin.

Pada tahap inilah CBOM mulai digunakan untuk menyusun inventarisasi kriptografi secara sistematis.

CBOM adalah format standar yang dapat dibaca mesin yang didasarkan pada CycloneDX SBOM yang sudah ada untuk keamanan rantai pasokan dan manajemen masa pakai aset perangkat lunak. CBOM bertujuan untuk meng-*capture* kriptografi yang digunakan, termasuk metadata, dan untuk melacak ketergantungan antara algoritma kriptografi, sekaligus menyediakan sarana untuk menggabungkan skor kerentanan keamanan klasik dan kuantum dengan aset yang ditemukan.

CBOM dikembangkan oleh IBM dengan tujuan menciptakan inventaris khusus aset kriptografi, dan per April 2024, CBOM didukung penuh dalam CycloneDX SBOM versi 1.6. CBOM dapat mengakomodasi inventaris kriptografi yang sangat detail dan menyeluruh, yang mencantumkan semua jenis protokol keamanan aset kriptografi, algoritma kriptografi, kunci kriptografi, materi kriptografi seperti ciphertext, tanda tangan, digest, initialization vector, token, nonce, dan artefak seperti sertifikat digital, kredensial, kata sandi, dan lainnya.

Format standar dalam membuat CBOM mencakup:

- a. Identitas sistem dan modul;
- b. Komponen kriptografi yang digunakan;
- c. Atribut teknis (kunci, algoritma, versi library);
- d. Status risiko kuantum;
- e. Rencana mitigasi/migrasi.

Format tersebut direkomendasikan oleh NIST SP 1800-38B [10] dan TNO PQC *Migration Framework* [3] untuk

memastikan interoperabilitas antar organisasi dan mempermudah audit. Contoh struktur tabel CBOM ditunjukkan pada Tabel 4.4.

Setelah CBOM dibuat, unit TI, keamanan, dan vendor akan melakukan validasi silang untuk memastikan keakuratan data. Kemudian, hasil CBOM diintegrasikan ke dalam:

- a. Sistem manajemen keamanan informasi;
- b. *Enterprise Architecture Repository*; dan
- c. *PQC Risk Register* untuk memantau progres migrasi.

Ada berbagai cara untuk membuat dan mengelola inventarisasi aset kriptografi. Namun, penggunaan format standar sangat diperlukan agar proses pembuatan, pengelolaan, dan analisis inventarisasi aset kriptografi dapat dilakukan secara lebih efisien dan konsisten. Dengan format yang seragam, inventarisasi aset kriptografi tidak hanya dapat dikelola oleh organisasi itu sendiri, tetapi juga dapat digunakan secara bersama oleh pemasok dan klien. Pendekatan ini meningkatkan transparansi, mempermudah koordinasi antar pihak, serta mencegah terjadinya masalah interoperabilitas antara pengguna dan penyedia layanan.

Tabel 4.4 Contoh Struktur tabel CBOM

ID	Nama sistem/ aplikasi	Algoritma	Panjang Kunci/ Output Hash (bit)	Mode Operasi/ Parameter	Fungsi	Library/ modul	Dukungan <i>Cryptographic Agility</i>	Strategi Migrasi
CBOM #1	<i>e-Procurement</i>	RSA	2048	PSS	Tanda tangan digital	OpenSSL	Ya	Ganti ke ML-DSA
CBOM #2	<i>E-Health API</i>	ECDH	256	<i>secp256r1</i>	<i>Key exchange</i>	Bouncy Castle	Ya	Hybrid ML- KEM + ECC
CBOM #3	<i>SecureMail</i>	AES	256	GCM	Enkripsi data	Libsodium	Tidak	Tetap digunakan

Kegiatan inventarisasi aset kriptografi seharusnya bersifat dinamis dan harus diperbarui apabila terdapat hal berikut:

1. Pembaruan sistem, patch keamanan, atau pergantian vendor;
2. Perubahan konfigurasi kriptografi;
3. Integrasi layanan baru yang menggunakan enkripsi.

Kemudian, untuk memastikan proses inventarisasi berjalan efektif dan berulang secara sistematis, disarankan agar organisasi untuk:

1. Menggunakan alat bantu otomatis (*crypto discovery tools*);
2. Menetapkan template CBOM standar nasional agar seragam lintas instansi;
3. Menyimpan hasil inventarisasi dalam repositori aman dan terenkripsi, dengan kontrol akses terbatas;
4. Melakukan revaluasi tahunan CBOM sebagai bagian dari audit keamanan dan program *cryptographic agility readiness*.

4.3.2 Penilaian Risiko Kuantum

Dalam bagian ini diasumsikan bahwa organisasi telah menyusun inventaris aset kriptografi, atau setidaknya memiliki informasi yang memadai mengenai algoritma kriptografi yang digunakan, sehingga data tersebut dapat diakses dengan mudah untuk mendukung pelaksanaan penilaian risiko kuantum.

Secara konkret, risiko kuantum terdiri atas tiga komponen berikut:

1. Kelemahan kuantum dari kriptografi yang digunakan pada tingkat sistem atau aplikasi. Penilaian ini dilakukan berdasarkan kekuatan serangan kuantum yang sudah diketahui.

2. Dampak yang diharapkan dari serangan kuantum terhadap sistem. Penilaian ini dilakukan berdasarkan pemahaman atas konsekuensi apabila kriptografi berhasil ditembus, dengan mempertimbangkan tujuan penggunaan kriptografi tersebut.
3. Perkiraan waktu dan upaya yang diperlukan untuk melakukan migrasi ke PQC. Perkiraan ini disusun berdasarkan tantangan migrasi yang telah diketahui serta pengalaman dari proses migrasi kriptografi sebelumnya.

Pada bagian selanjutnya, akan dijelaskan panduan penilaian risiko kuantum, terdiri atas bagaimana mengidentifikasi penyerang yang realistis, kelemahan terhadap kuantum, analisis dampak, upaya migrasi dan skor risiko kuantum. Pada pembahasan skor risiko kuantum, akan digabungkan komponen penilaian kelemahan terhadap kuantum, analisis dampak dan upaya migrasi, dengan rentang nilai antara 0 hingga 4 yang dapat digunakan sebagai acuan dalam rencana migrasi PQC maupun dalam proses manajemen risiko secara umum.

1. Penyerang Realistis dengan Komputer Kuantum

Sebelum melakukan penilaian risiko, suatu organisasi perlu mengidentifikasi penyerang yang secara realistis akan menyerang mereka. Dalam konteks penilaian risiko kuantum, diasumsikan bahwa penyerang memiliki ketertarikan untuk menyerang organisasi secara keseluruhan, bukan hanya sistem tertentu di dalam organisasi tersebut.

Saat ini, para ahli memprediksi bahwa ancaman nyata dari komputer kuantum akan muncul dalam kurun waktu 10 hingga 20 tahun mendatang, dengan kemungkinan terjadinya meningkat dari 25% dalam sepuluh tahun menjadi lebih dari 60% dalam dua puluh tahun [34].

Mengingat bahwa komputer kuantum pada awalnya akan sangat mahal dan membutuhkan SDM dengan keahlian khusus, wajar untuk memperkirakan bahwa aktor negara atau penyerang yang sangat termotivasi dan memiliki kemampuan tinggi akan menjadi pihak pertama yang menggunakannya untuk menyerang infrastruktur kriptografi.

Motivasi mereka umumnya bersifat politik, militer, dan ekonomi, misalnya untuk menyebabkan gangguan atau mengumpulkan informasi intelijen dari negara lain. Ancaman ini sangat relevan bagi organisasi yang memang sudah menjadi target dari aktor negara, khususnya dari negara dengan kapabilitas siber tinggi. Selain itu, organisasi yang mengelola infrastruktur kritis atau menyimpan informasi rahasia yang harus dijaga keamanannya, termasuk dalam ruang lingkup yang perlu waspada.

Dalam laporan tahunan tahun 2023 dari dinas intelijen Belanda (AIVD), disebutkan beberapa contoh target dari negara-negara lain [35]. Di antaranya, AIVD secara eksplisit memperingatkan pemerintah, industri pertahanan, dan perusahaan teknologi terkemuka terhadap ancaman spionase yang terus berlangsung. Secara khusus mengenai ancaman dari aktor negara, dokumen lain juga diterbitkan pada tahun 2022 oleh AIVD, Dinas Intelijen Militer (MIVD), dan Koordinator Nasional Keamanan dan Kontra-Terrorisme (NCTV) [36].

Seiring dengan adanya isu bahwa komputasi kuantum akan tersedia melalui layanan *cloud*, transisi dari penggunaan oleh aktor negara (*state actor*) ke penyerang yang termotivasi (*motivated attackers*) diperkirakan akan berlangsung

dengan cepat. Dalam skenario ini, penyerang dengan motif keuntungan finansial dapat menjalankan serangan kuantum, misalnya untuk mencuri uang atau memperoleh informasi komersial yang sensitif. Meskipun serangan berbasis *cloud* kuantum diperkirakan masih memerlukan beberapa tahun lagi untuk benar-benar terwujud karena memerlukan sumber daya yang tinggi, pada akhirnya setiap organisasi yang berhadapan dengan *motivated attackers* ini diperkirakan akan menghadapi ancaman ini dalam jangka waktu yang tidak jauh berbeda dari organisasi yang saat ini telah menjadi target aktor negara. Dengan demikian, jika suatu organisasi saat ini sudah memiliki profil ancaman dari penyerang, maka hanya tinggal menunggu waktu hingga organisasi menghadapi risiko eksploitasi kerentanan tersebut. Karena biaya eksploitasi yang tinggi, maka yang paling berisiko adalah perusahaan multinasional besar, organisasi yang bergerak di bidang teknologi tinggi atau solusi inovatif, serta target-target bernilai tinggi lainnya.

2. Kelemahan terhadap Kuantum

Tingkat kelemahan algoritma kriptografi yang digunakan dalam suatu aplikasi dibagi ke dalam tiga kategori skor kelemahan kuantum, yaitu:

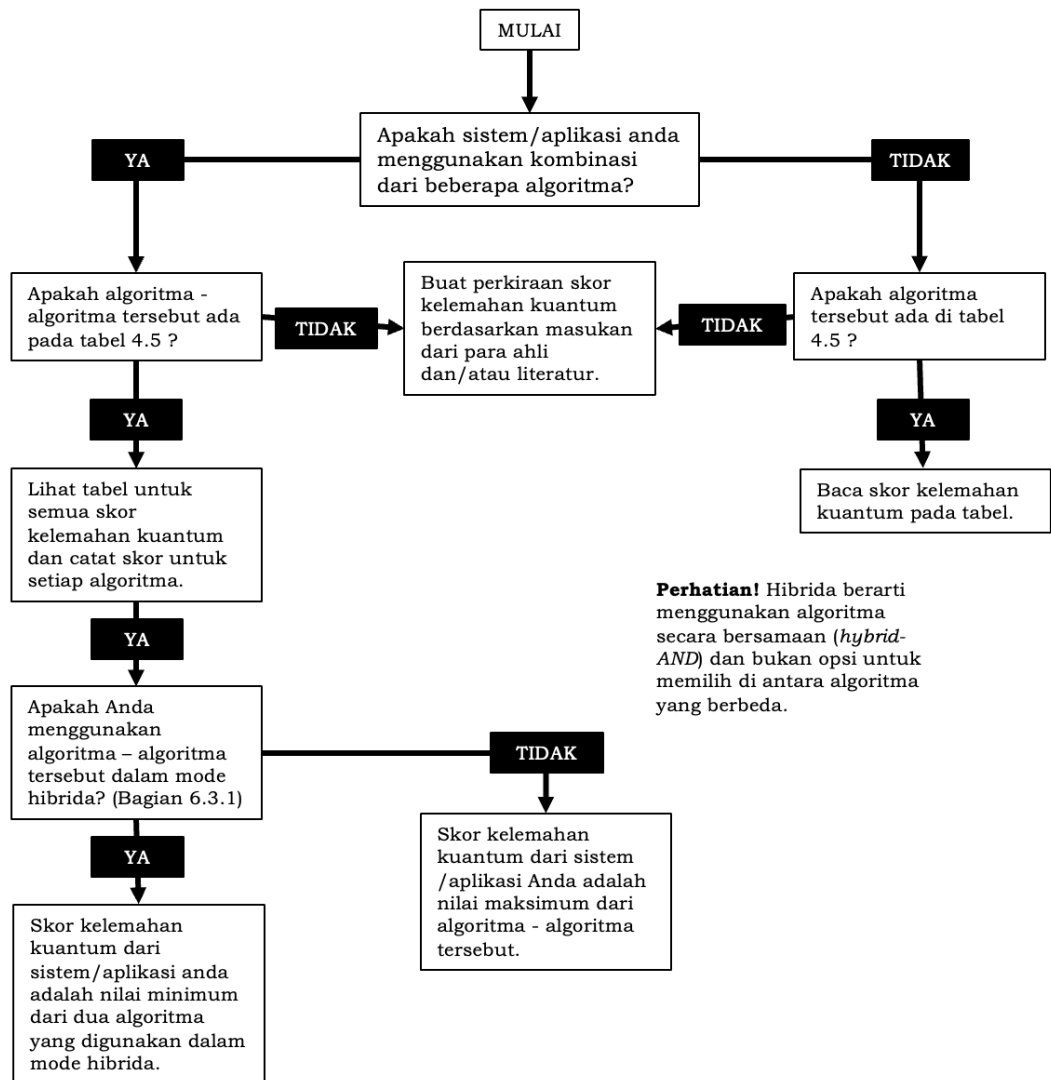
- a. Skor 0: Algoritma yang digunakan dianggap aman terhadap serangan kuantum dan, berdasarkan pengetahuan saat ini, tidak memerlukan migrasi.
- b. Skor 1: Algoritma belum (atau belum diperkirakan dalam waktu dekat) dapat ditembus oleh komputer kuantum, tetapi tetap memerlukan perhatian di masa mendatang. Contoh kategori ini adalah algoritma kunci simetris dan fungsi *hash*. Meskipun terdapat serangan kuantum secara teoretis terhadap beberapa algoritma

tersebut, serangan tersebut tidak dianggap layak dilakukan dalam waktu dekat.

- c. Skor 2: Algoritma tidak aman terhadap komputer kuantum dan karena itu harus segera digantikan dengan alternatif yang aman terhadap serangan kuantum (*quantum-safe*).

Daftar berbagai algoritma kriptografi yang umum digunakan dapat dilihat pada Lampiran B.

Dalam berbagai aplikasi yang ada saat ini, algoritma kriptografi sering kali dikombinasikan untuk membentuk satu solusi kriptografi. Sebagai contoh, protokol TLS memungkinkan pemilihan dari berbagai algoritma kriptografi untuk melindungi suatu sesi tertentu, dan menggunakan enkripsi kunci publik untuk menetapkan kunci bagi algoritma kunci simetris. Dalam contoh tersebut, kelemahan kuantum pada tingkat aplikasi ditentukan oleh skor kelemahan tertinggi dari seluruh algoritma yang digunakan. Secara intuitif, hal ini dapat dijelaskan dengan logika bahwa penyerang akan selalu memilih algoritma yang paling lemah untuk menyerang sistem. Namun, dalam kasus di mana digunakan konstruksi *hybrid-AND* yaitu ketika beberapa algoritma kriptografi digunakan secara berlapis maka skor kelemahan pada tingkat sistem ditentukan oleh skor kelemahan terendah dari masing-masing algoritma yang digunakan. Diagram alur untuk membantu organisasi dalam menentukan kelemahan kuantum suatu sistem dapat dilihat pada Gambar 4.1.



Gambar 4.1 Diagram alur untuk menentukan kelemahan kuantum digambar ulang dari [3].

Tabel 4.5 Referensi Skor Kelemahan Kuantum

Algoritma	Panjang Kunci	Output Hash	Skor Kelemahan Kuantum	Masalah Keamanan Klasik
RSA	Tidak relevan	N/A	2	
ElGamal	Tidak relevan	N/A	2	
Paillier	Tidak relevan	N/A	2	

Algoritma	Panjang Kunci	Output Hash	Skor Kelemahan Kuantum	Masalah Keamanan Klasik
ECDH	Tidak relevan	N/A	2	
ECDSA	Tidak relevan	N/A	2	
EdDSA	Tidak relevan	N/A	2	
ECIES	Tidak relevan	N/A	2	
CRYSTALS-Kyber / ML-KEM	Tidak relevan	N/A	0	
CRYSTALS-Dilithium / ML-DSS	Tidak relevan	N/A	0	
XMSS	Tidak relevan	N/A	0	
LMS	Tidak relevan	N/A	0	
HSS	Tidak relevan	N/A	0	
FrodoKEM	Tidak relevan	N/A	0	
Falcon	Tidak relevan	N/A	0	
SPHINCS+	Tidak relevan	N/A	0	
Classic McEliece	Tidak relevan	N/A	0	
AES (128 bit)	128	N/A	1	
AES (192 bit)	192	N/A	0	
AES (256 bit)	256	N/A	0	
DES	56	N/A	–	!

Algoritma	Panjang Kunci	Output Hash	Skor Kelemahan Kuantum	Masalah Keamanan Klasik
3DES	168	N/A	–	!
Camellia (128-bit)	128	N/A	1	
Camellia (192-bit)	192	N/A	0	
Camellia (256-bit)	256	N/A	0	
Blowfish	variabel	N/A	1	
Twofish	128	N/A	1	
Twofish	192	N/A	0	
Twofish	256	N/A	0	
IDEA	128	N/A	1	
RC5	Variabel	N/A	1	
ChaCha20	256	N/A	0	
RC4	Variabel	N/A	–	!
Trivium	80	N/A	–	
Salsa20	128	N/A	1	
Salsa20	256	N/A	0	
A5/1	64	N/A	–	!
A5/2	64	N/A	–	!
MD5	Tidak relevan	N/A	–	!
SHA-1	N/A	Tidak relevan	1	!
SHA-2	N/A	224	1	
SHA-2	N/A	256–512	0	
SHA-3	N/A	224	1	

Algoritma	Panjang Kunci	Output Hash	Skor Kelemahan Kuantum	Masalah Keamanan Klasik
SHA-3	N/A	256–512	0	
Whirlpool	N/A	512	0	
BLAKE2	N/A	224	1	
BLAKE2	N/A	256–512	0	
BLAKE3	N/A	224	1	
BLAKE3	N/A	256–512	0	
PBKDF2	N/A	N/A	0	
HKDF	N/A	N/A	0	
Argon2id	N/A	N/A	0	
scrypt	N/A	Variabel	0	
bcrypt	N/A	192	0	

Keterangan : *! (tanda seru): Mengindikasikan adanya masalah keamanan klasik yang serius (contoh: RC4, A5/1, A5/2, MD5, SHA-1).

Perlu diperhatikan bahwa diagram alur ini menilai kombinasi algoritma yang digunakan untuk melindungi satu koneksi jaringan. Apabila suatu aplikasi menggunakan kriptografi untuk melindungi dua titik akhir (*endpoints*), maka diagram alur tersebut perlu diikuti secara terpisah untuk masing-masing titik akhir.

3. Analisis Dampak

Analisis dampak dilakukan untuk mengidentifikasi apakah secara realistis terdapat kemungkinan bahwa penyerang akan menargetkan organisasi tersebut. Melalui analisis ini,

organisasi dapat memperkirakan tingkat kerugian potensial yang mungkin timbul apabila terserang. Hasil penilaian ini kemudian dinyatakan dalam bentuk skor dampak, yang bertujuan untuk mengukur seberapa besar konsekuensi yang dapat dialami oleh organisasi apabila kriptografi dalam suatu sistem berhasil ditembus.

Skor dampak dibagi ke dalam tiga tingkat (1, 2, dan 3). Penilaian skor dimulai dari 1, bukan dari 0, karena setiap sistem yang berhasil ditembus pasti akan menimbulkan dampak, sekecil apa pun itu. Gambar 4.2 dapat digunakan sebagai panduan dalam menilai perkiraan dampak apabila kriptografi pada suatu sistem berhasil ditembus. Jika diperlukan pemahaman tambahan mengenai masing-masing tingkat atau jika diagram alur tidak sesuai untuk sistem tertentu, berikut adalah penjelasan intuitif untuk setiap tingkat:

- a. Tingkat 1: Tidak terdapat dampak signifikan yang memerlukan perhatian khusus.

Contohnya adalah ketika kriptografi tidak digunakan untuk melindungi sistem sensitif, ancaman masih diperkirakan akan terjadi lebih dari sepuluh tahun ke depan, tidak ada penyerang yang secara realistis ditargetkan ke sistem tersebut, atau terdapat langkah pengamanan lain yang memadai.

- b. Tingkat 2: Terdapat penyerang yang secara realistis dapat menimbulkan dampak, meskipun tidak dalam jangka pendek.

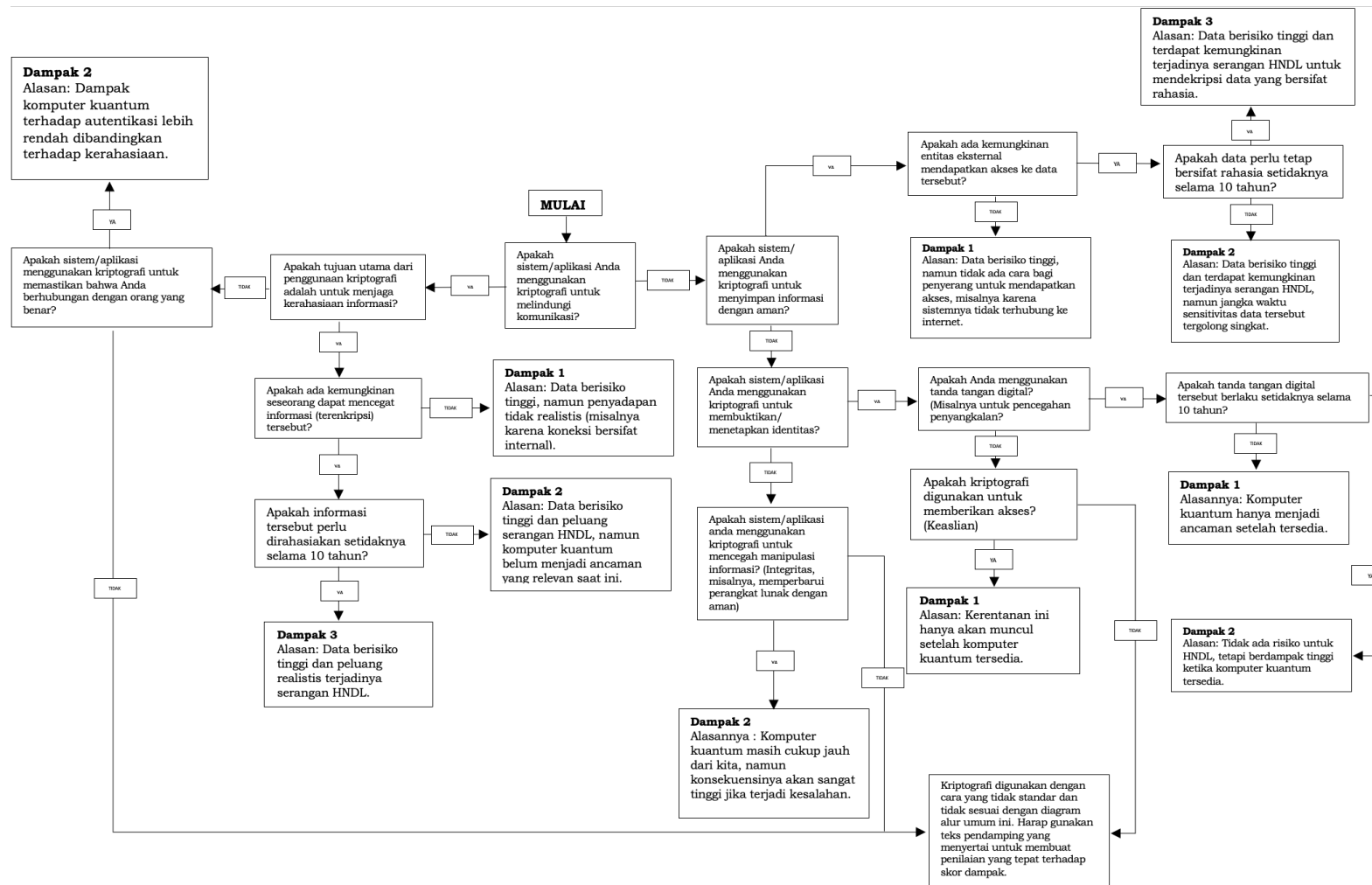
Contohnya adalah data sensitif yang dapat disadap namun tidak lagi relevan ketika dapat didekripsi di masa depan. Contoh lainnya adalah sistem yang memiliki dampak tinggi terhadap bisnis, seperti sistem untuk verifikasi identitas atau pengamanan

pembaruan perangkat lunak. Dalam kasus seperti ini, terdapat risiko dan kemungkinan serangan yang tinggi ketika komputer kuantum tersedia. Oleh karena itu, sangat penting untuk melakukan migrasi ke PQC tepat waktu.

- c. Tingkat 3: Skor dampak tertinggi diberikan apabila dampaknya sudah sedemikian besar sehingga perlu segera ditangani.

Hal ini terjadi ketika terdapat penyerang yang secara realistis dapat menyadap pesan saat ini dan pesan tersebut masih bersifat sensitif ketika komputer kuantum yang relevan telah tersedia. Data yang dalam kasus ini dapat dikompromikan akan tetap berdampak besar terhadap organisasi atau individu dalam jangka waktu 10–20 tahun ke depan. Contohnya meliputi rahasia negara, kekayaan intelektual, kontrak rahasia, atau data pribadi khusus.

Skor dampak ini merupakan gambaran situasi saat ini sehingga dampak dari suatu kelemahan dapat berubah jika sensitivitas aplikasi atau perkiraan waktu ketersediaan komputer kuantum berubah. Selain itu, skor dampak juga dapat berubah apabila sistem mengalami pembaruan. Oleh karena itu, disarankan agar penilaian risiko ini dilakukan secara berkala sebagai bagian dari proses penilaian risiko yang rutin. Diagram alur untuk mengidentifikasi perkiraan dampak apabila kriptografi dalam suatu sistem berhasil ditembus ditunjukkan pada Gambar 4.2.



Gambar 4 2 Diagram alur untuk mengidentifikasi perkiraan dampak digambar ulang dari [1].

4. Upaya Migrasi

Di dalam melakukan migrasi ke PQC, perlu memperkirakan seberapa besar upaya dan waktu yang dibutuhkan, serta sejauh mana tantangan tak terduga yang mungkin dihadapi. Perlu dicatat bahwa bagian ini hanya berfokus pada estimasi waktu yang diperlukan untuk bermigrasi ke PQC. Dalam praktiknya, sumber daya lain seperti tenaga manusia dan dana juga sangat penting untuk keberhasilan migrasi PQC. Skor upaya migrasi dibagi ke dalam tiga tingkat:

- a. Skor 1: Tidak ada tantangan besar yang diantisipasi dan waktu yang dibutuhkan untuk migrasi penuh suatu sistem ke PQC diperkirakan tidak lebih dari dua tahun.
- b. Skor 2: Migrasi tidak bersifat sepele namun tidak ada hambatan besar yang diantisipasi; waktu yang diperlukan diperkirakan hingga delapan tahun.
- c. Skor 3: Migrasi akan sulit dilakukan dan sulit diprediksi tantangan apa yang akan muncul. Ini contohnya jika terdapat banyak ketergantungan pada pihak lain, rendahnya prioritas, sistem yang sulit dijangkau secara fisik, atau faktor penunda lainnya. Dalam kasus ini, migrasi ke PQC akan memakan waktu lebih dari delapan tahun.

Upaya untuk bermigrasi ke PQC bergantung pada banyak faktor yang sangat bervariasi antar organisasi. Oleh karena itu, tidak ada cara umum untuk menentukan skor upaya migrasi dan hal ini perlu dinilai sendiri oleh organisasi yang bersangkutan. Pada bagian selanjutnya, akan dijelaskan beberapa faktor umum yang dapat membantu organisasi dalam menilai upaya migrasi.

Faktor-faktor tersebut meliputi:

a. Kematangan manajemen organisasi

Organisasi yang memiliki manajemen siklus hidup aset yang baik seperti inventaris perangkat lunak, kriptografi, dan sertifikat yang mutakhir, akan lebih mudah dalam menemukan dan memigrasikan instansi kriptografi yang perlu diperbarui.

b. Ketergantungan eksternal pada standardisasi dan regulasi

Terkadang, organisasi tidak dapat melakukan migrasi secara mandiri karena terikat oleh regulasi tertentu atau diharuskan menggunakan algoritma yang telah distandardisasi. Proses ini bisa memakan waktu lama dan berada di luar kendali organisasi. Di sisi lain, regulasi juga dapat mempercepat adopsi PQC.

c. Ketergantungan eksternal pada penyedia

Banyak organisasi yang menggunakan perangkat lunak atau perangkat keras dari penyedia eksternal. Ini dapat mempercepat migrasi jika penyedia tersebut sudah mengembangkan solusi PQC, sehingga organisasi dapat fokus pada proses pembaruan secara mulus. Sebaliknya, jika penyedia tidak memprioritaskan PQC, perangkat lunaknya tidak lagi dipelihara, atau penyedia sudah tidak ada, hal ini bisa menghambat. Selain itu, kompatibilitas antara sistem yang dikelola oleh organisasi berbeda juga menjadi faktor besar yang memperlambat migrasi PQC.

d. Ketergantungan pada perangkat keras eksternal

Perangkat keras sering digunakan untuk mempercepat atau mengelola proses kriptografi.

Contohnya, HSM sering digunakan untuk membuat dan mengelola kunci kriptografi. HSM harus mendukung algoritma PQC terlebih dahulu sebelum aplikasi lain dapat menggunakannya. Selain itu, akselerator perangkat keras sering dipakai untuk mempercepat operasi kriptografi. Jika akselerator tersebut tidak mendukung algoritma PQC, maka kinerja sistem dapat menurun signifikan. Dalam kasus ini, diperlukan pemasangan perangkat keras baru yang memerlukan waktu, biaya, dan bahkan mungkin tidak memungkinkan di lingkungan teknologi operasional (*Operational Technology* (OT)).

- e. Keterbatasan kapabilitas perangkat keras
Sejalan dengan ketergantungan perangkat keras, keterbatasan pada *bandwidth*, penyimpanan, kecepatan, dan jenis operasi yang didukung dapat meningkatkan upaya migrasi ke PQC. Algoritma PQC memiliki kebutuhan yang berbeda dibandingkan algoritma yang saat ini digunakan. Perangkat dengan spesifikasi rendah mungkin mengalami kesulitan menyesuaikan kebutuhan tersebut. Contoh penting termasuk smartcard, perangkat IoT, sistem OT, serta sistem kelas atas yang menjalankan banyak operasi kriptografi seperti perangkat jaringan korporat.
- f. Perangkat lunak/kode yang dikelola sendiri
Jika suatu aplikasi atau sistem dikelola sendiri, maka keahlian yang dibutuhkan untuk melakukan migrasi ke PQC juga harus tersedia secara internal. Jika keahlian tersebut tersedia, waktu migrasi bisa jauh lebih singkat. Namun sebaliknya, jika

organisasi tidak memiliki keahlian tersebut, hal ini dapat menjadi hambatan besar.

Dengan mengidentifikasi kesiapan organisasi berdasarkan faktor tersebut, organisasi dapat memperoleh pemahaman yang lebih jelas mengenai kondisi aktual serta kerangka asesmen yang terstruktur untuk mengevaluasi kesiapan upaya migrasi. Matriks asesmen penentuan upaya migrasi disajikan pada Tabel 4.6.



Tabel 4.6 Matriks asesmen upaya migrasi

Faktor	Pertanyaan	Jawaban Pertanyaan	
		Ya	Tidak
Kematangan manajemen organisasi	Apakah organisasi Anda memiliki kebijakan formal atau roadmap migrasi kriptografi?	Organisasi telah memiliki kebijakan formal atau roadmap migrasi kriptografi yang telah diformalkan	Organisasi belum memiliki kebijakan formal atau roadmap migrasi kriptografi dan/atau belum diformalkan
	Apakah organisasi Anda memiliki inventaris aset kriptografi yang lengkap, akurat dan termutakhir atas semua penggunaan algoritma/protokol kriptografi dalam sistem Anda?	Organisasi telah memiliki inventaris aset kriptografi yang lengkap, akurat dan termutakhir untuk semua penggunaan algoritma atau protokol kriptografi dalam sistem. Organisasi telah menetapkan periode pemutakhiran inventaris aset kriptografi tersebut	Organisasi belum memiliki dan/atau hanya memiliki sebagian inventaris aset kriptografi yang lengkap, akurat dan termutakhir untuk semua penggunaan algoritma atau protokol kriptografi dalam sistem. Organisasi belum menetapkan periode

Faktor	Pertanyaan	Jawaban Pertanyaan	
		Ya	Tidak
			pemutakhiran inventaris aset kriptografi tersebut
	Apakah organisasi Anda memiliki dokumentasi teknis aset kriptografi sesuai dengan inventaris aset kriptografi yang lengkap, akurat dan termutakhir untuk semua penggunaan algoritma atau protokol kriptografi dalam sistem Anda?	Organisasi telah memiliki dokumentasi teknis aset kriptografi yang lengkap, akurat dan termutakhir untuk semua penggunaan algoritma atau protokol kriptografi dalam sistem. Organisasi telah menetapkan periode pemutakhiran dokumentasi teknis aset kriptografi tersebut.	Organisasi belum memiliki dan/atau hanya memiliki sebagian dokumentasi teknis aset kriptografi yang lengkap, akurat dan termutakhir untuk semua penggunaan algoritma atau protokol kriptografi dalam sistem. Organisasi belum menetapkan periode pemutakhiran dokumentasi teknis aset kriptografi tersebut

Faktor	Pertanyaan	Jawaban Pertanyaan	
		Ya	Tidak
	Apakah sistem Anda memungkinkan penggantian algoritma secara modular (<i>Crypto-agile</i>)?	Sistem mendukung penggantian algoritma secara modular	Sistem tidak mendukung penggantian algoritma secara modular
	Apakah sistem Anda memungkinkan penggunaan algoritma kriptografi yang dapat dikonfigurasi atau diganti tanpa perubahan kode sumber (tidak <i>hardcoded</i>)?	Sistem memungkinkan penggunaan algoritma kriptografi dikonfigurasi tanpa perubahan kode sumber (tidak <i>hardcoded</i>)	Sistem tidak dapat dikonfigurasi secara langsung karena tertanam langsung (<i>hardcoded</i>)
	Apakah Organisasi Anda hanya memiliki 1 (satu) sistem atau aplikasi yang perlu dimigrasikan ke PQC?	Organisasi hanya memiliki satu aplikasi yang perlu dimigrasikan ke PQC	Organisasi memiliki beberapa sistem atau aplikasi yang perlu dimigrasikan ke PQC
Ketergantungan eksternal pada	Apakah organisasi Anda memiliki regulasi, standar teknis, dan	Organisasi telah memiliki dan/atau menerapkan regulasi/standar teknis/	Organisasi belum memiliki regulasi/standar teknis/persyaratan kepatuhan

Faktor	Pertanyaan	Jawaban Pertanyaan	
		Ya	Tidak
standardisasi dan regulasi	persyaratan kepatuhan untuk melakukan migrasi PQC?	persyaratan kepatuhan yang mendorong untuk melakukan migrasi PQC	yang mendorong untuk melakukan migrasi PQC, dan/atau sudah memiliki regulasi/ standar teknis/ persyaratan kepatuhan namun terdapat klausul dalam regulasi/standar teknis/ persyaratan kepatuhan tersebut yang dapat menghambat organisasi untuk melakukan migrasi PQC
	Apakah organisasi Anda dapat memulai migrasi PQC tanpa menunggu panduan/ regulasi resmi?	Organisasi dapat memulai migrasi PQC tanpa menunggu panduan/ regulasi resmi	Organisasi tetap memerlukan panduan/regulasi resmi sebelum memulai migrasi ke PQC.

Faktor	Pertanyaan	Jawaban Pertanyaan	
		Ya	Tidak
Ketergantungan eksternal pada penyedia	Apakah organisasi Anda menggunakan library terbuka dari pihak ketiga/ vendor, sehingga dapat dan/atau mudah untuk dimodifikasi?	Organisasi menggunakan library terbuka pihak ketiga atau vendor, sehingga dapat/atau mudah untuk dimodifikasi.	Organisasi menggunakan library tertutup dari pihak ketiga atau vendor sehingga sulit dimodifikasi.
Ketergantungan pada perangkat keras eksternal	Apakah perangkat keras kriptografi pada organisasi Anda (misalnya HSM) telah menggunakan algoritma PQC yang dikeluarkan oleh BSSN?	Organisasi telah menggunakan perangkat keras kriptografi yang sesuai dengan algoritma PQC yang dikeluarkan oleh BSSN.	Organisasi belum menggunakan perangkat keras kriptografi yang sesuai dengan algoritma PQC yang dikeluarkan oleh BSSN.
Keterbatasan kapabilitas perangkat keras	Apakah perangkat keras Anda telah diuji atau disimulasikan untuk menjalankan algoritma PQC tanpa hambatan performa (RAM/CPU/latensi)?	Organisasi telah melakukan pengujian dan/atau simulasi perangkat keras untuk dapat menjalankan	Organisasi belum melakukan pengujian dan/atau simulasi perangkat keras untuk dapat menjalankan

Faktor	Pertanyaan	Jawaban Pertanyaan	
		Ya	Tidak
		algoritma PQC tanpa hambatan performa.	algoritma PQC dan/atau hasil uji dan simulasi masih ditemukan hambatan performa.
Perangkat lunak/kode yang dikelola sendiri	Apakah sistem Anda mendukung penggunaan PQC dalam mode hybrid (bersama algoritma klasik)?	Sistem sudah mendukung penggunaan PQC dalam mode <i>hybrid</i> .	Sistem belum mendukung penggunaan PQC dalam mode <i>hybrid</i> .
	Apakah organisasi Anda memiliki tim teknis yang memahami PQC?	Organisasi memiliki tim teknis yang memahami PQC sehingga dapat mempermudah proses migrasi PQC	Organisasi belum memiliki tim teknis yang memahami PQC dan/atau belum memiliki keahlian yang diperlukan sehingga proses migrasi PQC terhambat.

5. Skor Risiko Kuantum

Sebagai langkah akhir, ketiga skor individu perlu dikombinasikan menjadi satu skor risiko kuantum dengan rentang nilai antara 0 hingga 4. Skor risiko kuantum ini merujuk pada sistem-sistem dalam suatu organisasi. Skor tersebut dapat dilihat pada Tabel 4.3. Jika sebuah sistem memiliki skor kelemahan kuantum sebesar 0, maka skor risiko kuantumnya juga akan otomatis menjadi 0 karena sistem tersebut telah terlindungi secara memadai. Interpretasi dari keempat tingkat risiko tersebut adalah sebagai berikut:

- a. Skor Risiko 0 (Tidak ada risiko): Seluruh ancaman kuantum telah ditangani dengan memadai.
- b. Skor Risiko 1 (Risiko rendah): Terdapat risiko dalam jangka panjang, namun saat ini belum memerlukan prioritas.
- c. Skor Risiko 2 (Risiko sedang): Tindakan diperlukan, tetapi kriptografi yang digunakan saat ini masih aman dalam jangka pendek atau proses migrasinya diperkirakan cukup sederhana.
- d. Skor Risiko 3 (Risiko tinggi): Diperlukan prioritas dalam jangka pendek karena dampak yang diharapkan cukup besar dan/atau proses migrasi ke PQC diperkirakan akan memakan waktu lama.
- e. Skor Risiko 4 (Risiko akut): Sistem sudah berada dalam kondisi berisiko, misalnya karena kombinasi antara upaya migrasi yang berat dan lamanya waktu data harus tetap aman melebihi perkiraan waktu saat komputer kuantum dapat memecahkan kriptografi yang ada. Dalam hal ini, terdapat ancaman yang realistis dan membutuhkan

perhatian segera, termasuk dari manajemen jika berdampak signifikan terhadap bisnis.

Bergantung pada profil PQC suatu organisasi, beberapa risiko mungkin dapat ditoleransi, sementara yang lain tidak. Sebagai contoh, organisasi dengan profil adopter reguler mungkin masih dapat menunda migrasi untuk sistem dengan skor risiko kuantum 1 atau 2. Sebaliknya, adopter mendesak kemungkinan perlu mulai memprioritaskan sistem dengan skor risiko kuantum mulai dari 1 atau 2, karena potensi kerugian yang dihadapi jauh lebih besar apabila sistem tersebut disusupi. Pada akhirnya, cara organisasi memprioritaskan sistem dengan berbagai skor risiko kuantum sangat bergantung pada proses manajemen risikonya secara keseluruhan, sumber daya yang tersedia, serta tingkat toleransi risiko yang dimiliki oleh organisasi tersebut.

Tabel 4.7 Skor risiko individu menjadi skor risiko akhir per aplikasi.

Kelemahan	Dampak			Upaya Migrasi			Risiko
0	1	2	3	1	2	3	0
1	1			1			1
1	1			2			1
1	1			3			1
1	2			1			1
1	2			2			1
1	2			3			1
1	3			1			1
1	3			2			2

Kelemahan	Dampak	Upaya Migrasi	Risiko
1	3	3	2
2	1	1	1
2	1	2	1
2	1	3	2
2	2	1	2
2	2	2	2
2	2	3	3
2	3	1	3
2	3	2	4
2	3	3	4

Keterangan:

	Skor Risiko 0
	Skor Risiko 1
	Skor Risiko 2
	Skor Risiko 3
	Skor Risiko 4

BAB V

TAHAP PERENCANAAN



BAB V

TAHAP PERENCANAAN

Bab ini memberikan informasi mengenai tujuan dan landasan ilmiah dari tahap perencanaan migrasi PQC. Selain itu, bab ini menguraikan kegiatan yang dilakukan pada fase awal migrasi PQC, meliputi penentuan waktu untuk memulai pelaksanaan migrasi, rekomendasi dalam perencanaan migrasi yang mencakup perencanaan proses bisnis, penilaian maturitas PQC, dan perencanaan teknis. Pada bab ini juga menyajikan perkiraan kebutuhan biaya yang diperlukan untuk mendukung pelaksanaan migrasi secara menyeluruh.

5.1 Tujuan

Menyusun rencana implementasi teknis yang terukur dan melaksanakan migrasi PQC secara bertahap serta terkontrol.

5.2 Landasan Ilmiah/Teknis

Menurut [3], fase ini adalah inti dari proses migrasi PQC. Pada tahap ini, organisasi mengubah hasil penilaian risiko menjadi rencana konkret, kemudian mengimplementasikan dan menguji solusi PQC di lingkungan produksi atau *pilot project*. Keberhasilan tahap ini sangat dipengaruhi oleh kemampuan organisasi dalam mengelola interoperabilitas, *cryptographic agility*, serta integrasi antara sistem klasik dan PQC.

5.3 Langkah-langkah

5.3.1 Waktu memulai migrasi

Penentuan waktu pelaksanaan migrasi didasarkan pada tiga variabel, yaitu:

1. Waktu X , merupakan periode waktu yang menunjukkan berapa lama suatu aset harus tetap aman;

2. Waktu Y , merupakan waktu yang dibutuhkan untuk menyelesaikan proses migrasi; dan
3. Waktu Z , merupakan waktu yang tersisa sebelum komputer kuantum mampu memecahkan kriptografi kunci-publik.

Migrasi dikatakan dapat dilaksanakan tepat waktu apabila memenuhi kondisi sesuai pertidaksamaan (1).

$$X + Y < Z \quad (1)$$

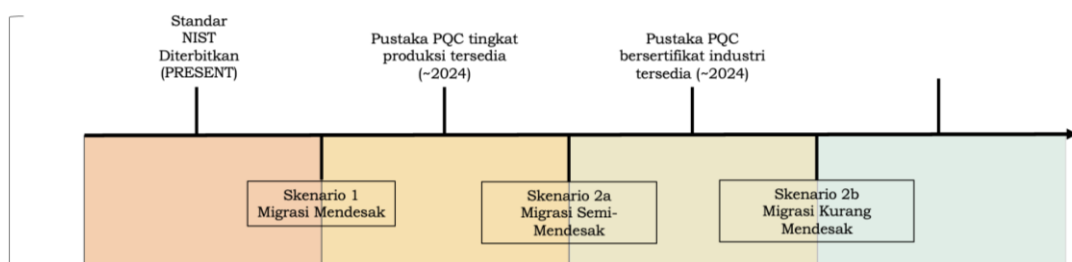
Pertidaksamaan (1) dikenal sebagai pertidaksamaan Mosca (*Mosca's inequality*), dinamai berdasarkan peneliti yang memperkenalkannya. Berdasarkan pertidaksamaan tersebut, semakin nilai $X + Y$ mendekati Z , maka semakin mendesak migrasi untuk dilakukan. Perlu dicatat bahwa organisasi sudah dapat memulai untuk mempersiapkan proses migrasi melalui langkah yang menerapkan prinsip *no-regret moves*.

Dalam penilaian risiko kuantum, terdapat beberapa kasus bahwa skor dampak secara langsung dipengaruhi oleh lamanya suatu aset harus tetap aman. Hal ini berlaku, apabila skor dampak berada pada level 3 akibat adanya kemungkinan serangan jenis HNLD. Dalam kasus seperti ini, disarankan untuk segera memulai proses migrasi. Selain itu, skor upaya migrasi secara langsung berkaitan dengan variabel Y , yaitu waktu yang dibutuhkan untuk menyelesaikan proses migrasi. Dalam hal ini, skor upaya migrasi secara umum dapat dipetakan ke dalam parameter Y seperti yang ditunjukkan pada Tabel 5.1.

Tabel 5.1 Pemetaan dari Upaya Migrasi ke Jumlah Tahun.

Skor Upaya Migrasi	Y
1	0-2 tahun
2	5-8 tahun
3	>8 tahun

Berdasarkan hal tersebut, perlu dipertimbangkan tahapan menuju implementasi bersertifikasi industri dari standar PQC yang ditetapkan oleh lembaga standardisasi, beserta *milestone* pencapaiannya. Berdasarkan Gambar 5.1, terdapat tiga *milestone* dalam linimasa skenario migrasi PQC. Adapun *milestone* yang pertama yaitu publikasi standar NIST yang telah tercapai pada bulan Agustus 2024. Bagian ini bertujuan untuk membantu pengambilan keputusan mengenai waktu yang tepat untuk melakukan migrasi setiap aset kriptografi. Setiap aset sebaiknya dimigrasikan dalam skenario yang sesuai dengan *milestone* M , sebagaimana ditunjukkan dalam Gambar 5.1, sehingga waktu migrasi $X + Y + M$ masih berada dalam rentang waktu sebelum Z .



Gambar 5.1 Linimasa berbagai skenario migrasi
Digambar ulang dari [3].

1. Perkiraan Nilai M

Pada dasarnya, sulit untuk menentukan kapan *library* PQC pada tingkat produksi dan/atau bersertifikasi industri akan tersedia secara umum.

Hal ini semakin kompleks mengingat bahwa *library* PQC yang berbeda akan dioptimalkan untuk berbagai kasus penggunaan, seperti kartu pintar (*smartcard*) atau perangkat IoT. Oleh karena itu, pengalaman dari situasi serupa merupakan pendekatan yang berguna dalam menentukan rentang waktu ini. Selain itu, pengguna akhir (*end-user*) dapat mempengaruhi linimasa ini. Periode ini merupakan waktu bagi para penyedia (*vendor*) untuk mulai mengembangkan *library* PQC tingkat produksi. Menghubungi *vendor* atau menyampaikan kebutuhan akan *library* ini melalui umpan balik komunitas atau forum daring dapat mempengaruhi kecepatan proses publikasinya.

2. Perkiraan Nilai Z

Menentukan kapan komputer kuantum akan memiliki kapabilitas untuk memecahkan kriptografi kunci-publik merupakan hal yang kompleks dan masih menjadi perdebatan di antara para pakar. Untuk memberikan perkiraan yang akurat, Michele Mosca setiap tahun melakukan survei terhadap sejumlah pakar dalam bidang komputasi kuantum, untuk mengetahui probabilitas komputer kuantum akan mampu memecahkan RSA-2048 dalam kurun waktu 5, 10, 15, 20, dan 30 tahun ke depan. Berdasarkan hasil tersebut, perkiraan konservatif menyatakan bahwa kriptografi kunci-publik akan diretas pada tahun 2040, sementara perkiraan yang lebih agresif, memperkirakan kemungkinan tersebut sudah terjadi pada tahun 2030.

Perlu diperhatikan bahwa waktu yang dibutuhkan untuk melaksanakan migrasi akan bervariasi di tiap organisasi atau bahkan antar aset. Hal ini bisa

disebabkan oleh ketersediaan dokumentasi *library*, dukungan komersial, serta tingkat pengetahuan umum mengenai PQC, yang kemungkinan besar akan lebih lengkap jika migrasi dilakukan pada waktu yang lebih lambat. Oleh karena itu, sangat penting bahwa setiap sistem pada akhirnya bermigrasi ke implementasi yang telah mencapai tingkat produksi atau telah tersertifikasi dari standar PQC NIST. Perlu ditekankan kembali bahwa waktu pasti untuk melakukan migrasi akan sangat bergantung pada tingkat toleransi risiko organisasi.

3. Catatan mengenai *Library* yang Tersertifikasi

Bagi sebagian organisasi, sangat penting untuk melakukan migrasi pada Skenario 1 Migrasi Mendesak (ditunjukkan pada Gambar 5.1), yang berarti bermigrasi ke standar PQC meskipun *library* yang tersertifikasi belum tersedia. Perlu dicatat bahwa langkah ini membawa kerugian tambahan karena penggunaan *library* yang belum tersertifikasi dapat menimbulkan kendala dalam proses sertifikasi, serta penggunaan kode yang belum mencapai tingkat produksi dapat menimbulkan berbagai masalah keamanan. Kerugian ini perlu dipertimbangkan secara cermat saat menentukan skenario migrasi yang akan diambil. Penting juga untuk dicatat bahwa standar kriptografi yang saat ini paling banyak digunakan, yaitu FIPS 140-3 dan *Common Criteria*, sudah memungkinkan penerapan skema hibrida. Artinya, sertifikasi setidaknya masih dapat diperoleh dengan pendekatan hibrida.

4. Menentukan Skenario Migrasi

Sebagai bagian dari penilaian risiko kuantum, telah ditetapkan skor risiko keseluruhan untuk setiap sistem. Prioritas migrasi bergantung pada tingkat risiko yang dihadapi sistem dan tingkat toleransi risiko organisasi terhadap sistem tersebut. Selanjutnya, organisasi dapat memilih untuk langsung melaksanakan migrasi dengan menerapkan salah satu dari tiga skenario, yaitu migrasi mendesak, semi-mendesak, atau kurang mendesak; atau menunggu hingga seluruh *milestone* tercapai dengan mempertimbangkan kesenjangan antara risiko yang dihadapi dan kesiapan organisasi dalam menerima risiko tersebut.

5. Strategi umum

Karena tidak mungkin untuk melakukan migrasi secara menyeluruh sekaligus, maka diperlukan suatu strategi umum. Oleh karena itu, disarankan agar organisasi terlebih dahulu memigrasikan protokol-protokol yang sudah usang ke protokol yang saat ini direkomendasikan oleh NCSC-NL. Langkah ini berguna untuk menguji manajemen aset serta *cryptographic agility* maupun organisasi secara keseluruhan. Setelah langkah ini dilaksanakan, disarankan untuk memulai proses migrasi menuju PQC. Dengan cara ini, organisasi dapat mulai memodernisasi proses migrasinya guna memperlancar transisi di masa mendatang.

5.3.2 Rekomendasi dalam perencanaan migrasi

Tujuan utama dari langkah ini adalah:

1. Menentukan untuk setiap aset kriptografi apakah perlu diganti, dan jika ya, menetapkan dengan apa aset tersebut seharusnya diganti;
2. Menentukan urutan migrasi dari masing-masing aset kriptografi.

Bagian ini menyediakan sumber daya yang berguna untuk membantu dalam menentukan elemen kriptografi mana yang perlu diganti serta memberikan usulan solusi penggantinya. Prioritas migrasi bergantung pada hasil penilaian risiko yang telah ditetapkan pada bab sebelumnya, namun juga harus mempertimbangkan ketergantungan antar sistem dan konsekuensi migrasi terhadap bisnis tertentu. Berikut ini merupakan tahapan dalam perencanaan migrasi, yaitu:

1. Perencanaan Proses Bisnis

Karena sebagian besar proses migrasi berkaitan erat dengan proses bisnis, maka tahap perencanaan perlu difokuskan pada aspek tersebut. Langkah-langkah utama yang perlu diperhatikan dalam perencanaan migrasi meliputi:

- a. Organisasi perlu menunjuk seorang manajer migrasi yang bertanggung jawab atas pelaksanaan proses migrasi. Manajer ini harus memiliki pemahaman mendalam mengenai struktur dan proses organisasi serta memiliki akses ke seluruh unit kerja untuk membimbing para pegawai dalam menjalankan langkah-langkah dan jadwal migrasi.
- b. Alokasi anggaran yang memadai harus disiapkan untuk mendukung tahapan migrasi, termasuk kebutuhan waktu, pendanaan, dan fasilitas.

- c. Selama proses migrasi berlangsung, akan terdapat keadaan di mana sebagian layanan atau bagian dari organisasi harus diisolasi atau dihentikan sementara. Pengelolaan *down time* ini perlu direncanakan dengan cermat sebelumnya untuk meminimalkan dampaknya terhadap kelangsungan operasional organisasi.

Perencanaan yang baik juga mempertimbangkan jalur migrasi dari organisasi lain guna menjaga interoperabilitas. Oleh karena itu, perencanaan migrasi secara bersama dengan komunitas organisasi sejenis patut dipertimbangkan. Dalam beberapa kasus, hal ini bahkan mungkin menjadi keharusan karena keterkaitan sistem dan aset kriptografi antarorganisasi. Meskipun tidak ada keterkaitan langsung, perencanaan migrasi secara kolektif tetap dapat memberikan manfaat, seperti pembagian beban kerja dalam menyusun perencanaan tersebut.

2. Penilaian Maturitas PQC

Agar proses migrasi dapat berhasil, penting untuk mengidentifikasi permasalahan utama yang menghambat transisi di dalam suatu organisasi. Model maturitas yang dijabarkan dalam [37] dapat membantu memahami aspek utama dari proses migrasi yang perlu menjadi fokus, serta memahami tantangan teknis maupun non-teknis yang muncul. Dalam laporan tersebut, terdapat 13 tantangan utama migrasi yang dijelaskan secara lebih rinci sebagai berikut:

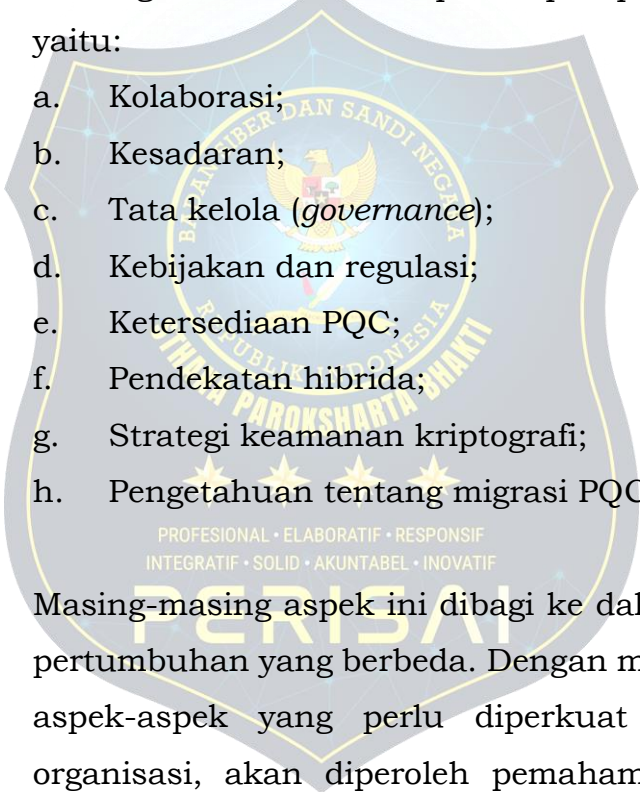
- a. Migrasi sistem warisan (*legacy systems*);
- b. Ketiadaan standar PQC;

- c. Ketiadaan sertifikasi perangkat lunak dan perangkat keras PQC serta implementasi tingkat tinggi;
- d. Kurangnya pemahaman terhadap dampak komputasi kuantum, serta risiko dan kerentanannya;
- e. Tidak adanya rasa urgensi dalam satu organisasi;
- f. Tidak adanya visi jangka panjang terhadap manfaat organisasi;
- g. Keterbatasan tenaga ahli yang memiliki pengetahuan tentang PQC;
- h. Ketiadaan perencanaan dan kesadaran organisasi terkait urgensi migrasi;
- i. Tidak adanya urgensi dari para pemangku kepentingan;
- j. Ketiadaan kepemimpinan di antara para pemangku kepentingan;
- k. Ketiadaan kolaborasi di antara para pemangku kepentingan;
- l. Ketiadaan kebijakan dan kejelasan implikasi hukum;
- m. Kompleksitas teknis dari proses migrasi.

Tantangan tersebut tidak berdiri sendiri, melainkan saling memengaruhi. Penanganan terhadap satu tantangan dapat menimbulkan efek domino yang positif, yaitu semakin cepat sebuah organisasi mulai mengambil tindakan di dalam ekosistemnya, maka akan semakin mudah untuk mengatasi tantangan lanjutan. Sebaliknya, bila mencoba mengatasi tantangan secara terpisah, proses migrasi akan menjadi jauh lebih sulit. Berdasarkan analisis dalam laporan tersebut, tindakan kolektif dan kolaborasi

yang kuat sangat disarankan sebagai langkah awal dalam proses migrasi.

Untuk membantu menangani tantangan tersebut, model maturitas yang ditawarkan dalam laporan dapat dijadikan acuan untuk memperoleh gambaran menyeluruh terhadap langkah awal migrasi. Model maturitas ini disajikan dalam bentuk matriks asesmen yang mengelompokkan kelima belas tantangan ke dalam delapan aspek prioritas utama, yaitu:

- 
- a. Kolaborasi;
 - b. Kesadaran;
 - c. Tata kelola (*governance*);
 - d. Kebijakan dan regulasi;
 - e. Ketersediaan PQC;
 - f. Pendekatan hibrida;
 - g. Strategi keamanan kriptografi;
 - h. Pengetahuan tentang migrasi PQC.

Masing-masing aspek ini dibagi ke dalam lima tahap pertumbuhan yang berbeda. Dengan mengidentifikasi aspek-aspek yang perlu diperkuat dalam suatu organisasi, akan diperoleh pemahaman yang jelas mengenai kemajuan yang telah dicapai dan tindakan spesifik yang perlu dilakukan. Kerangka kerja yang terstruktur ini berfungsi sebagai alat asesmen yang bernilai, memungkinkan organisasi untuk mengevaluasi status terkini pada tiap aspek. Matriks asesmen tersebut disajikan dalam Tabel 5.2.

Tabel 5.2 Matriks Penilaian Model Maturitas

	Kolaborasi	Kesadaran	Tata Kelola	Kebijakan & Regulasi	Ketersediaan PQC	Pendekatan Hibrida	Strategi Keamanan Kriptografi	Pengetahuan tentang Migrasi PQC
PERTANYAAN								
	Bagaimana tingkat kolaborasi organisasi Anda dengan ekosistem (instansi pemerintah, industri, akademisi, komunitas, dan pemangku kepentingan lainnya) dalam mendukung migrasi menuju PQC?	Sejauh mana tingkat kesadaran organisasi Anda terhadap kebutuhan migrasi menuju PQC dan dampaknya terhadap keamanan sistem yang ada?	Bagaimana tingkat penerapan tata kelola (governance) dalam organisasi Anda untuk mendukung migrasi menuju PQC?	Sejauh mana kebijakan dan regulasi terkait PQC telah dikembangkan dan diterapkan dalam organisasi Anda maupun dalam ekosistem yang relevan?	Sejauh mana organisasi Anda telah mempersiapkan, menilai, dan mengimplementasikan teknologi PQC dalam sistem yang ada?	Sejauh mana organisasi Anda telah menerapkan atau mempersiapkan pendekatan hibrida (penggunaan kombinasi algoritma klasik dan PQC) dalam proses migrasi menuju PQC?	Sejauh mana organisasi Anda telah mengembangkan dan menerapkan strategi keamanan kriptografi untuk memastikan ketahanan terhadap ancaman saat ini dan masa depan?	Sejauh mana tingkat pengetahuan organisasi Anda mengenai langkah, kebutuhan, dan pendekatan dalam migrasi menuju PQC?
JAWABAN								
Level 0	1.0 Ketidakterlibatan Organisasi tidak terlibat dalam	2.0 Ketidaksadaran Organisasi tidak memiliki kesadaran	3.0 Ketidaksadaran Organisasi belum memahami	4.0 Tidak Ada Kebijakan & Regulasi Formal Tidak terdapat proses	5.0 Pengetahuan Terbatas tentang PQC Organisasi tidak memiliki	6.0 Pengetahuan Terbatas tentang PQC Organisasi tidak	7.0 Praktik Reaktif & Ad Hoc Organisasi bersikap reaktif terhadap	8.0 Pengetahuan Terbatas tentang Migrasi PQC

	Kolaborasi	Kesadaran	Tata Kelola	Kebijakan & Regulasi	Ketersediaan PQC	Pendekatan Hibrida	Strategi Keamanan Kriptografi	Pengetahuan tentang Migrasi PQC
	ekosistem. Organisasi terputus dan tidak berpartisipasi aktif.	akan migrasi PQC, belum siap, dan belum mengenali relevansi serta manfaat PQC.	urgensi tata kelola dalam migrasi PQC dan tidak mengidentifikasi peran strategisnya.	sertifikasi resmi untuk PQC. Regulasi dan kebijakan terkait migrasi PQC juga belum tersedia.	pemahaman dasar mengenai konsep utama migrasi PQC dan tidak menyadari urgensinya.	memahami konsep inti migrasi PQC serta tidak menyadari kebutuhan implementasinya.	keamanan dan manajemen risiko. Algoritma kriptografi diimplementasikan secara tidak terencana.	Organisasi tidak tahu langkah yang harus dilakukan dan tidak menyadari ancaman kuantum maupun manfaat PQC.
Level 1	1.1 Komunikasi & Pemantauan Organisasi mulai menyadari pentingnya kolaborasi dalam ekosistem dan membangun saluran komunikasi serta pemantauan terkait migrasi PQC.	2.1 Kesadaran yang Diakui Muncul diskusi tentang migrasi PQC. Organisasi mulai menyadari perlunya perubahan dan memahami dampak ancaman kuantum terhadap sistem yang ada.	3.1 Pengakuan terhadap Penilaian & Perencanaan Organisasi mulai memahami perlunya tata kelola migrasi dalam ekosistem dan mengidentifikasi tujuan bersama.	4.1 Wawasan & Pertimbangan Awal Organisasi menyadari perlunya kebijakan dan regulasi dasar untuk mendukung implementasi PQC.	5.1 Pemahaman Dasar tentang PQC Organisasi memiliki pemahaman awal tentang migrasi PQC, tetapi belum melakukan penilaian teknis terhadap sistem yang ada.	6.1 Pemahaman Dasar tentang PQC Organisasi memahami konsep dasar PQC, namun belum melakukan penilaian teknis sistem saat ini.	7.1 Kebijakan & Prosedur yang Ditetapkan Organisasi mulai memiliki panduan dan kebijakan kriptografi formal mengenai algoritma yang dapat digunakan dan praktik manajemen kunci.	8.1 Pengetahuan tentang Infrastruktur yang Ada Organisasi telah melakukan inventarisasi kriptografi dan memahami area rentan serta lokasi di mana PQC perlu diterapkan.

	Kolaborasi	Kesadaran	Tata Kelola	Kebijakan & Regulasi	Ketersediaan PQC	Pendekatan Hibrida	Strategi Keamanan Kriptografi	Pengetahuan tentang Migrasi PQC
Level 2	1.2 Identifikasi Pemangku Kepentingan Organisasi mengidentifikasi arah potensial migrasi PQC dan mulai menyusun rencana komunikasi dengan para pemangku kepentingan.	2.2 Kesadaran yang Berkembang Organisasi mulai mencari informasi tentang PQC dan memahami konsep dasarnya, meski belum sepenuhnya menguasai ruang lingkupnya.	3.2 Prinsip Tata Kelola Bersama Organisasi mulai berpartisipasi dalam diskusi untuk menyusun prinsip tata kelola bersama terkait migrasi PQC.	4.2 Wawasan & Diskusi Bersama Organisasi aktif dalam berbagi pandangan mengenai pedoman dan standar informal PQC di lingkup industri.	5.2 Penilaian Inventaris Teknis Organisasi menilai infrastruktur yang ada dan mengidentifikasi area potensial untuk penerapan PQC, meski belum memahami keseluruhan cakupannya.	6.2 Penilaian Inventaris Teknis Organisasi menilai sistem yang ada dan mengidentifikasi area potensial implementasi PQC.	7.2 Pendekatan Berbasis Risiko Organisasi menerapkan pendekatan berbasis risiko untuk keamanan kriptografi. Penilaian risiko dilakukan untuk mengidentifikasi kerentanan dan ancaman.	8.2 Pengetahuan tentang PQC Organisasi memahami keterbatasan dan tantangan dari berbagai algoritma PQC, serta mengetahui di mana pendekatan hibrida dapat diterapkan.
Level 3	1.3 Upaya Terkoordinasi Organisasi berkolaborasi dengan ekosistem untuk mengoordinasikan langkah migrasi PQC	2.3 Kesadaran yang Terinformasi Organisasi mengeksplorasi berbagai kemungkinan terkait migrasi PQC dan mulai mengidentifikasi	3.3 Struktur Tata Kelola Organisasi membentuk struktur formal, seperti komite tata kelola untuk mengatur migrasi PQC, dengan peran dan tanggung	4.3 Analisis Kesenjangan & Persiapan Organisasi mengidentifikasi celah kebijakan dan regulasi terkait PQC serta mengevaluasi risiko dan	5.3 Spesifikasi Pengujian & Kasus Uji Organisasi melakukan pengujian PQC dan mengembangkan skenario serta use-case untuk	6.3 Spesifikasi Pengujian & Kasus Uji Organisasi menguji PQC dan mengembangkan kasus uji untuk menilai performa dan ketahanan.	7.3 Pendekatan Proaktif Organisasi mulai menerapkan pendekatan proaktif dalam keamanan kriptografi dan menanamkan kelincahan kriptografi (cryptographic	8.3 Pengetahuan tentang Seleksi PQC Organisasi memahami berbagai algoritma PQC dan menentukan algoritma yang sesuai, serta menyusun

	Kolaborasi	Kesadaran	Tata Kelola	Kebijakan & Regulasi	Ketersediaan PQC	Pendekatan Hibrida	Strategi Keamanan Kriptografi	Pengetahuan tentang Migrasi PQC
	dan memanfaatkan sumber daya bersama.	si area sistem yang memerlukan PQC.	jawab yang jelas.	dampak potensialnya.	memastikan interoperabilitas dan ketahanan.		agility) dalam strateginya.	roadmap dan sumber daya implementasi.
Level 4	1.4 Aksi Kolaboratif Organisasi bekerja sama dalam proyek dan inisiatif bersama untuk mendukung migrasi PQC dan memperkuat ekosistem secara kolektif.	2.4 Kesadaran Strategis Organisasi menyelaraskan kesadarannya terhadap tujuan strategis migrasi PQC dan menyusun rencana untuk transisi yang mulus.	3.4 Implementasi & Penegakan Struktur tata kelola yang telah dibentuk mulai diimplementasikan secara aktif untuk memastikan kepatuhan dan akuntabilitas.	4.4 Pedoman Sukarela Pedoman dan standar informal mulai diperkenalkan sebagai rekomendasi menuju sistem yang tahan terhadap ancaman kuantum.	5.4 Uji Coba & Validasi Organisasi melakukan implementasi skala kecil (<i>pilot project</i>) untuk menguji efektivitas PQC bersama para pemangku kepentingan.	6.4 Uji Coba & Validasi (Pendekatan Hibrida) Organisasi mengimplementasikan PQC dalam skala kecil dengan pendekatan hibrida, melakukan pemantauan dan evaluasi kinerja.	7.4 Peningkatan Berkelanjutan terhadap Keamanan Kriptografi Organisasi terus memperbarui langkah-langkah keamanan kriptografi dengan fokus pada kelincahan algoritma.	8.4 Pengetahuan tentang Implementasi PQC Organisasi memiliki rencana strategis untuk implementasi PQC secara menyeluruh dalam sistem yang ada.
Level 5	1.5 Aksi Kolaboratif & Dialog Berkelanjutan Organisasi menjaga komunikasi dan kerja	2.5 Kesadaran Visioner Organisasi selalu memperbarui diri terhadap perkembangan terbaru PQC	3.5 Evaluasi & Adaptasi Berkelanjutan Organisasi menilai efektivitas kerangka tata kelola dan melakukan	4.5 Kebijakan & Regulasi Wajib Kebijakan dan regulasi PQC menjadi wajib secara hukum, dengan badan regulasi yang	5.5 Penerapan Skala Penuh Organisasi memilih dan mengimplementasikan algoritma PQC dalam sistem	6.5 Penerapan Skala Penuh (Pendekatan Hibrida) Organisasi mengimplementasikan algoritma PQC menggunakan	7.5 Keamanan Kriptografi yang Matang & Tangguh Organisasi sangat responsif terhadap ancaman kriptografi baru	8.5 Pengetahuan tentang Pemanfaatan PQC Organisasi memantau performa PQC, mengumpulkan

	Kolaborasi	Kesadaran	Tata Kelola	Kebijakan & Regulasi	Ketersediaan PQC	Pendekatan Hibrida	Strategi Keamanan Kriptografi	Pengetahuan tentang Migrasi PQC
	sama berkelanjutan dalam ekosistem melalui pelaporan, umpan balik, dan koordinasi antara pimpinan.	dan secara strategis mempersiapkan diri menghadapi tantangan masa depan.	penyesuaian untuk menghadapi kebutuhan yang terus berkembang.	memberlakukan mandat legal bagi organisasi terkait.	yang ada, kemudian memperluas penerapannya secara bertahap.	pendekatan hibrida dan memperluas penerapannya ke seluruh sistem.	dan mengintegrasikan kelincahan kriptografi di seluruh unit bisnis.	data, dan berbagi pengalaman penerapan sesuai praktik terbaik industri.



3. Perencanaan Teknis

Bagian teknis dari tahap perencanaan harus difokuskan pada aspek-aspek seperti prioritisasi kriptografi yang perlu dimigrasikan, kapan migrasi tersebut harus dilakukan, serta metode apa yang akan digunakan.

a. Ketergantungan Aset

Salah satu tujuan penting dari perencanaan ini adalah mengidentifikasi ketergantungan antar aset kriptografi dan menentukan urutan migrasi. Apabila suatu aset A bergantung pada aset B, maka perlu ditentukan apakah A atau B yang harus dimigrasikan terlebih dahulu. Ketergantungan semacam ini seharusnya telah tercatat dalam inventaris. Untuk menjaga interoperabilitas antar aset selama proses migrasi, protokol pasca-kuantum dapat diterapkan secara opsional terlebih dahulu hingga seluruh aset terkait telah selesai dimigrasikan.

b. Penggantian Kriptografi

Dengan telah ditetapkannya inventaris kriptografi dan ketergantungan antar aset kriptografi, perencanaan aktual penggantian aset kriptografi dapat dimulai. Untuk setiap aset kriptografi, harus ditentukan terlebih dahulu apakah aset tersebut perlu diganti, dirancang ulang, dihentikan, atau dilakukan tindakan lainnya. Keputusan ini bergantung pada berbagai faktor seperti pentingnya aset bagi organisasi, konsekuensi dari kegagalan fungsi aset, risiko serangan terhadap aset tersebut,

serta sumber daya yang tersedia. Setelah diputuskan bahwa suatu aset perlu diganti atau dirancang ulang, langkah selanjutnya adalah menentukan solusi pasca-kuantum yang akan digunakan. Disarankan untuk menggunakan solusi *cryptographic agility* agar implementasinya dapat diperbarui dengan cepat ketika standar atau ketentuan baru diterbitkan.

Penting untuk memastikan bahwa aset kriptografi tetap terlindungi selama masa migrasi. Hal ini dapat dilakukan dengan beberapa cara. Cara paling sederhana adalah dengan mempertahankan perlindungan kriptografi tradisional terhadap aset tersebut hingga perlindungan pasca-kuantum baru telah diterapkan. Jika hal ini tidak memungkinkan, maka isolasi aset menjadi alternatif.

c. **Isolasi Aset**

Dalam beberapa kasus, isolasi data/sistem merupakan satu-satunya cara untuk melindungi suatu aset. Hal ini berlaku untuk data pribadi serta pengelola data sensitif organisasi. Terdapat beberapa situasi di mana isolasi aset dianjurkan, atau bahkan diperlukan. Pertama, isolasi data memberikan perlindungan terhadap serangan HNDL. Dengan memisahkan data ini secara fisik dari jaringan, risiko serangan semacam itu dapat dihilangkan. Hal ini terutama berlaku untuk data dalam transmisi (*data in transit*), karena jenis serangan ini dilakukan dengan menyadap saluran komunikasi. Data yang disimpan (*data at*

rest) cenderung kurang rentan terhadap serangan tersebut.

Situasi lain yang memerlukan isolasi aset adalah ketika tidak memungkinkan untuk menjaga perlindungan aset selama masa migrasi seperti disebutkan sebelumnya. Karena proses migrasi melibatkan banyak langkah, mungkin tidak memungkinkan untuk memperbarui semua sistem secara bersamaan. Oleh karena itu, mungkin diperlukan untuk mencabut perlindungan kriptografi yang lama sebelum perlindungan pasca-kuantum baru diterapkan. Atau, mungkin saat ini biaya migrasi untuk aset tertentu terlalu tinggi, meskipun ada keinginan untuk tetap menjaga perlindungan terhadap aset tersebut. Dalam kedua kasus ini, mengisolasi aset selama masa kerentanannya akan memastikan bahwa perlindungan terhadap aset tetap terjaga. Setelah tahapan migrasi yang diperlukan selesai dilakukan, aset tersebut dapat dikeluarkan kembali dari kondisi isolasi.

Namun demikian, perlu dicatat bahwa isolasi aset berdampak besar terhadap fungsionalitas dan availabilitas data. Selama aset diisolasi, aset tersebut tidak dapat digunakan sama sekali. Hal ini merupakan aspek penting yang harus dipertimbangkan sebelum memutuskan untuk melakukan isolasi aset. Dalam beberapa skenario, isolasi aset bahkan tidak memungkinkan karena pembatasan ini.

d. Penggantian Perangkat Keras

Migrasi mungkin akan memerlukan penggantian perangkat keras. Dalam kasus penggantian perangkat keras berskala besar, availabilitas produk baru serta waktu penerapan harus dipertimbangkan dalam perencanaan migrasi.

e. Pengujian

Solusi baru baik di tingkat perangkat keras maupun perangkat lunak akan memerlukan tahapan pengujian. Bagian pengujian ini sangat penting dan harus dipersiapkan sebelumnya. Pengujian perlu memastikan bahwa algoritma baru kompatibel dengan infrastruktur lainnya dan benar-benar memberikan tingkat keamanan yang dijanjikan.

5.3.3 Perkiraan Biaya Migrasi

Komponen penting dalam perencanaan migrasi PQC adalah estimasi biaya dan alokasi sumber daya. Perkiraan biaya yang komprehensif harus diperhitungkan dalam pengambilan keputusan strategis terkait PQC serta dalam menentukan prioritas tindakan. Sebagai contoh, pemerintah federal Amerika Serikat telah memperkirakan total biaya migrasi PQC di seluruh instansi pemerintah antara tahun 2025 hingga 2035 sebesar 7,1 miliar dolar AS [38]. Estimasi biaya ini disediakan sebagai bagian dari persiapan migrasi PQC, dan pemerintah federal mewajibkan setiap instansi untuk memperbarui estimasi biaya mereka setiap tahun.

Berdasarkan inventaris aset kriptografi, cakupan dan kompleksitas migrasi PQC dapat ditentukan. Kompleksitas

ini juga dipengaruhi oleh persyaratan regulasi organisasi serta hasil penilaian risiko PQC. Setelah itu, organisasi harus memperkirakan jumlah tenaga kerja dan keahlian yang dibutuhkan untuk melaksanakan migrasi PQC, dengan mempertimbangkan bagian infrastruktur kriptografi mana yang berada langsung di bawah kendali organisasi dan bagian mana yang dikelola oleh pihak vendor.

Selain itu, berbagai perangkat bantu dan layanan telah tersedia untuk membantu proses migrasi PQC. Dengan melakukan estimasi terhadap biaya alat dan layanan tersebut, organisasi dapat mengambil keputusan yang tepat mengenai alat dan layanan mana yang perlu diakuisisi.

Perangkat keras juga mungkin perlu diganti apabila tidak mendukung PQC atau jika vendornya tidak berencana untuk menyertakan dukungan PQC. Algoritma PQC juga umumnya memerlukan lebih banyak langkah komputasi, sehingga perangkat keras kriptografi yang saat ini digunakan bisa jadi tidak mencukupi. Jika ternyata perangkat keras yang ada tidak lagi memadai, maka penggantian juga harus dilakukan.

Pertimbangan tambahan terkait biaya migrasi PQC adalah potensi *downtime*. Idealnya, organisasi meminimalkan *downtime* dan dampaknya terhadap operasional bisnis, namun komplikasi yang tidak terduga mungkin terjadi. Oleh karena itu, sistem cadangan harus tersedia, disertai prosedur pemulihan infrastruktur komunikasi organisasi yang tangguh.

Akhirnya, proses migrasi PQC memberikan peluang besar untuk meningkatkan kebijakan dan proses kriptografi organisasi ke tingkat yang lebih tinggi. Hal ini sangat diharapkan, mengingat kemungkinan bahwa migrasi kriptografi ini bukanlah yang terakhir. Primitif kriptografi baru terus dikembangkan dan distandarkan, sehingga berpotensi memberikan peningkatan lebih lanjut di masa depan. Di sisi lain, kemajuan dalam kriptanalisis juga dapat menyebabkan perlunya penyesuaian atau migrasi kriptografi berikutnya. Biaya yang terkait dengan kemungkinan ini perlu diperhitungkan, namun dapat dikurangi melalui investasi saat ini dalam kemampuan *cryptographic agility*.



BAB VI

TAHAP PELAKSANAAN MIGRASI



BAB VI

TAHAP PELAKSANAAN MIGRASI

Bab ini memberikan informasi mengenai tujuan dan landasan ilmiah dari tahap pelaksanaan migrasi, serta panduan teknis mengenai pelaksanaan proses migrasi ke PQC yang aman terhadap ancaman komputasi kuantum yang dapat dijadikan sebagai panduan oleh organisasi.

6.1 Tujuan

Tujuan dari tahap ini adalah melaksanakan proses migrasi ke PQC yang aman terhadap ancaman komputasi kuantum. Di dalamnya disajikan pedoman untuk memigrasikan algoritma kriptografi dan protokol yang sudah tidak lagi aman, melalui tahapan yang mencakup langkah strategis maupun tindakan operasional yang lebih rinci. Panduan ini diharapkan dapat membantu memastikan transisi berjalan terencana, terukur dan efektif menuju lingkungan kriptografi yang tahan terhadap ancaman komputasi kuantum.

6.2 Landasan ilmiah

Pelaksanaan migrasi ke PQC mencakup langkah strategis maupun tindakan operasional yang lebih rinci. Beberapa langkah pada tahap ini bersifat kondisional dan bergantung pada waktu pelaksanaan migrasi oleh masing-masing organisasi, sehingga sangat penting untuk terlebih dahulu menentukan skenario migrasi (Tahap Perencanaan). Selain itu, organisasi perlu segera meningkatkan *cryptographic agility* pada seluruh aset yang dimiliki untuk mempermudah penyesuaian terhadap perubahan algoritma kriptografi di masa depan. Secara umum, rekomendasi untuk sebagian besar protokol kriptografi adalah menggunakan pendekatan hibrida, yaitu mengombinasikan algoritma kriptografi klasik dengan algoritma PQC selama masa transisi.

6.3 Langkah-langkah

6.3.1 Strategi Umum

Tahapan akhir dalam proses migrasi adalah pelaksanaan rencana yang telah disusun pada bab sebelumnya. Idealnya, pada titik ini organisasi telah memiliki gambaran lengkap mengenai seluruh aset kriptografi yang dimiliki, serta rencana yang memetakan alternatif algoritma PQC yang akan digunakan untuk menggantikan aset yang rentan. Sebagai alternatif, organisasi dapat memilih untuk terlebih dahulu memigrasikan aset-aset berprioritas tinggi sebelum keseluruhan rencana rampung, dan melaksanakan tahap akhir secara paralel dengan tahapan lainnya. Perlu diingat bahwa lingkungan teknologi informasi terus mengalami perubahan. Inventarisasi aset yang disusun dua tahun lalu kemungkinan besar tidak lagi merepresentasikan kondisi kriptografi terkini dalam organisasi. Oleh karena itu, penting untuk memastikan bahwa inventarisasi aset tersebut selalu diperbarui secara berkelanjutan.

Bagian pertama dalam bab ini menyajikan strategi umum yang dapat diterapkan dalam proses migrasi menuju PQC. Dua bagian berikutnya akan membahas secara lebih rinci mengenai cara memigrasikan primitif kriptografi dan protokol yang digunakan.

Peringatan:

Pelaksanaan rencana migrasi harus dilakukan dengan sangat hati-hati. Penggantian suatu aset kriptografi dengan aset lain yang baru berpotensi menimbulkan kerentanan baru. Kesalahan dalam memilih algoritma pengganti atau konfigurasi yang keliru dapat menurunkan tingkat keamanan. Selain itu, fase migrasi itu sendiri dapat memperluas permukaan serangan (*attack surface*). Bahkan jika suatu organisasi menyerahkan proses ini kepada pihak ketiga, tetap diperlukan pemahaman internal mengenai PQC agar organisasi dapat memahami berbagai pertimbangan yang menyertai setiap solusi pengganti. Perlu pula disadari bahwa kriptografi asimetris *post-quantum* masih belum sematang algoritma asimetris yang rentan terhadap kuantum dan masih memerlukan waktu bertahun-tahun untuk pengujian kriptanalitik mendalam guna mencapai tingkat kepercayaan yang setara. Namun demikian, hal ini tidak seharusnya menjadi alasan untuk menunda migrasi. Skema hibrida memungkinkan tingkat keamanan setidaknya setara dengan algoritma lama yang digunakan, sehingga secara signifikan mengurangi ancaman dari keberadaan komputer kuantum.

1. Migrasi Primitif vs. Protokol

Sebelum membahas lebih lanjut mengenai migrasi primitif maupun protokol, penting untuk memahami perbedaannya secara mendasar. Primitif kriptografi umumnya tidak digunakan secara terpisah, melainkan merupakan bagian dari protokol yang lebih besar. Artinya, sebagian besar organisasi sebenarnya tidak secara langsung berinteraksi dengan detail teknis dari algoritma kriptografi itu sendiri.

Sebaliknya, mereka menggunakan *library* perangkat lunak yang mengimplementasikan protokol kriptografi yang umum digunakan, seperti TLS. Melalui *library* tersebut, berbagai pilihan kriptografi dapat disesuaikan, seperti jenis primitif yang digunakan atau ukuran kunci, namun pada umumnya bukan menjadi tanggung jawab organisasi untuk membangun algoritma kriptografi mereka sendiri dari awal.

Secara umum, migrasi langsung terhadap primitif hanya relevan dalam kasus-kasus tertentu, yakni ketika organisasi memang berinteraksi langsung dengan *library* kriptografi murni dan bahkan mungkin mengembangkan protokolnya sendiri. Sebaliknya, bagi banyak organisasi, memperbarui protokol yang tidak mereka kembangkan sendiri biasanya cukup dilakukan dengan memperbarui versi protokol tersebut, misalnya dari TLS 1.2 ke TLS 1.3. Daftar primitif kriptografi, karakteristik utamanya, serta status keamanan terhadap ancaman kuantum dapat dilihat pada Lampiran A.

2. Migrasi Kriptografi Simetris

Secara teoritis, komputer kuantum dapat menyerang kriptografi kunci simetris, termasuk fungsi *hash*, dengan efisiensi yang lebih tinggi dibandingkan komputer klasik. Namun secara umum, keunggulan kuantum yang bersifat teoritis tersebut tidak berarti bahwa kriptografi kunci simetris akan sepenuhnya dapat ditembus. Meski demikian, kondisi ini mungkin menuntut penggunaan kunci kriptografi yang lebih panjang. Namun, analisis yang lebih mendalam

menunjukkan bahwa kecil kemungkinannya keunggulan kuantum tersebut akan dimanfaatkan secara efektif untuk menembus kriptografi kunci simetris. Oleh sebab itu, primitif kriptografi simetris diperkirakan tetap aman terhadap serangan berbasis kuantum, bahkan tanpa perlu menambah panjang kunci. Atas dasar ini, penekanan utama diarahkan pada pentingnya memprioritaskan migrasi kriptografi kunci asimetris.

3. Migrasi Kriptografi Asimetris dengan Menggunakan Solusi Hibrida

Komputer kuantum yang relevan secara kriptografis akan mampu membobol algoritma kriptografi kunci asimetris tertentu, sehingga seluruh jaminan keamanan yang terkait dengannya menjadi terancam. Skema enkripsi dan mekanisme pertukaran atau enkapsulasi kunci, yang bertugas melindungi konfidensialitas data, sangat rentan terhadap serangan bertipe HNDL. Untuk mengurangi risiko ini, migrasi algoritma kriptografi kunci asimetris tepat waktu ke PQC menjadi hal yang sangat penting.

Serangan HNDL dapat berkembang menjadi risiko lain, yaitu Trust-Now-Forge-Later (TNFL) [26]. TNFL menggambarkan kondisi saat artefak digital, misalnya dokumen bertanda tangan elektronik, kontrak digital, atau sertifikat keamananyang saat ini dianggap sah dan tepercaya dapat dipalsukan setelah komputer kuantum cukup kuat untuk mematahkan algoritma kriptografi klasik.

Risiko ini semakin signifikan bagi sistem dengan masa pakai panjang, seperti infrastruktur kritis, satelit, sistem telekomunikasi, serta teknologi operasional, karena pembaruan perangkat lunak maupun perangkat keras sering kali rumit, mahal, atau bahkan tidak dimungkinkan. Jika sistem tersebut tidak sejak awal dibangun dengan mekanisme tanda tangan digital yang tahan terhadap serangan kuantum, maka integritas, autentikasi, dan kontinuitas kepercayaan jangka panjang dapat terganggu. Oleh karena itu, migrasi ke skema PQC bukan sekadar upaya peningkatan teknologi, tetapi langkah strategis untuk memastikan keberlanjutan kepercayaan terhadap identitas digital dan sistem keamanan informasi di era pasca-kuantum.

4. Solusi Hibrida

Solusi hibrida mengacu pada penggunaan kriptografi yang rentan terhadap kuantum dan PQC secara bersamaan dalam satu protokol tunggal. Untuk membobol skema ini, seorang penyerang harus berhasil menembus kedua algoritma tersebut sekaligus. Dengan demikian, tingkat keamanan keseluruhan dari skema hibrida setidaknya setara dengan algoritma terlemah di dalamnya.

Tujuan utama dari pendekatan ini adalah untuk mengurangi risiko keamanan yang ditimbulkan oleh belum matangnya algoritma PQC yang baru, sambil tetap memanfaatkan keamanan tambahan dari algoritma PQC. Selain aspek keamanan matematis tersebut, penerapan algoritma PQC dan algoritma yang rentan terhadap komputasi kuantum secara

paralel dalam skema hibrida juga dapat menghindari kesalahan implementasi dalam penerapan PQC yang masih baru.

Lebih lanjut, solusi hibrida sangat relevan diterapkan dalam lingkungan yang belum sepenuhnya memperbolehkan atau mempercayai PQC. Dengan menggabungkan PQC dan algoritma klasik yang telah dipercaya, organisasi tetap dapat menggunakan PQC tanpa melanggar regulasi yang berlaku.

Pendekatan hibrida sangat direkomendasikan bagi organisasi yang perlu menerapkan kriptografi tahan-kuantum sebelum tersedia implementasi standar algoritma PQC yang telah diakui. Contohnya, jika data organisasi saat ini sudah berisiko terhadap serangan HNDL, maka migrasi segera menjadi hal yang krusial.

Kelemahan utama dari pendekatan ini adalah kemungkinan terjadinya beban tambahan, baik dari sisi waktu pemrosesan maupun penggunaan memori, karena dua algoritma harus dijalankan dalam satu proses enkripsi atau penandatanganan. Namun demikian, karena kebanyakan skema PQC memang sudah membutuhkan sumber daya lebih besar dibandingkan algoritma klasik, beban tambahan ini umumnya masih dapat diterima.

Dalam skenario umum, solusi hibrida biasanya hanya digunakan satu kali pada tahap awal untuk menetapkan pasangan kunci simetris yang kemudian digunakan untuk mengenkripsi komunikasi berikutnya. Dalam kasus seperti ini, biaya tambahan

dari solusi hibrida relatif kecil jika dibandingkan dengan keseluruhan koneksi.

Peringatan:

Apabila suatu produk mengklaim menggunakan enkripsi atau tanda tangan hibrida, organisasi perlu memastikan bahwa penerapannya sesuai dengan pengertian yang dijelaskan sebelumnya, yaitu penggunaan algoritma rentan-kuantum dan algoritma PQC secara bersamaan dalam satu proses enkripsi atau penandatanganan (dikenal dengan pendekatan *hybrid* AND). Hal ini tidak boleh disalahartikan sebagai pemberian pilihan antara menggunakan algoritma rentan-kuantum atau algoritma PQC (dikenal dengan pendekatan *hybrid* OR). Selain itu, istilah enkripsi hibrida juga sering digunakan untuk menggambarkan kombinasi antara kriptografi simetris dan asimetris, dimana kriptografi asimetris digunakan untuk membentuk kunci bagi algoritma simetris. Namun, ini bukanlah pendekatan hibrida seperti yang dijelaskan di atas.

5. Serangan Penurunan Tingkat (*Downgrade Attacks*)
Beberapa pendekatan hibrida menghadapi risiko terjadinya *downgrade attacks*. Hal ini terjadi ketika suatu sistem menerapkan pendekatan *hybrid* OR dari pada *hybrid* AND sebagaimana telah dijelaskan sebelumnya.

Pendekatan *hybrid* OR, atau yang dikenal juga sebagai *optional* PQC, menggambarkan situasi yang melibatkan algoritma yang rentan terhadap komputasi kuantum dan algoritma PQC keduanya

diimplementasikan pada sisi server. Namun, dalam proses komunikasi dengan server, klien dapat memilih untuk menggunakan salah satu di antara kedua algoritma tersebut, tanpa kewajiban untuk menggunakan keduanya sekaligus. Konfigurasi seperti ini memberikan keuntungan dalam hal kompatibilitas ke belakang (*backward compatibility*), yang sangat berguna pada tahap pengujian maupun pengembangan awal guna memastikan interoperabilitas. Namun, pendekatan ini juga membawa risiko yang signifikan. Seorang penyerang dapat berpura-pura tidak mendukung protokol pasca-kuantum dan dengan demikian memaksa server untuk berkomunikasi menggunakan algoritma yang rentan terhadap komputasi kuantum. Serangan semacam ini dikenal sebagai *downgrade attack*. Bahkan apabila pelaku tidak dapat secara langsung membobol algoritma klasik yang digunakan, ia tetap dapat melakukan serangan HNDL.

Oleh karena itu, secara umum disarankan agar sistem internal menggunakan pendekatan *hybrid AND* sebagaimana telah dijelaskan atau menggunakan mekanisme *key mixing* yang aman sesuai [30]. Namun demikian, untuk sistem yang berinteraksi langsung dengan pihak luar, pendekatan ini mungkin lebih sulit diterapkan, dan *hybrid OR* dapat menjadi satu-satunya pilihan. Untuk itu, perlu dirumuskan kebijakan dan strategi yang jelas mengenai waktu dan mekanisme skema hibrida semacam ini dapat digunakan secara tepat.

6. Migrasi Kriptografi Asimetris Menggunakan Kunci yang Telah Dibagi Sebelumnya (*Pre-shared Keys*)

Cara lain untuk menjadikan kriptografi asimetris tahan terhadap ancaman komputasi kuantum adalah dengan memanfaatkan kriptografi simetris menggunakan *pre-shared keys*. Metode ini bertujuan untuk membangun komunikasi tanpa melibatkan bentuk kriptografi kunci publik. Untuk menerapkannya, kunci yang telah dibagi sebelumnya harus didistribusikan melalui cara fisik, misalnya dengan perangkat USB. Karena hal ini, proses pembentukan kunci menjadi cukup merepotkan, terutama dalam infrastruktur yang melibatkan banyak pihak (*many-to-many*), sehingga metode ini sulit untuk dilaksanakan.

Selain itu, karena pendekatan ini menghindari penggunaan kriptografi kunci publik, maka proses validasi sertifikat tidak dapat dilakukan. Namun, setelah kunci-kunci tersebut berhasil dibagikan, metode ini dapat memberikan tingkat keamanan yang sangat tinggi dan efisiensi yang baik. Dengan pertimbangan tersebut, pendekatan hibrida tetap direkomendasikan. Penggunaan *pre-shared keys* direkomendasikan apabila sistem memenuhi seluruh persyaratan berikut:

- a. Sistem tersebut merupakan bagian dari skenario 1 (migrasi mendesak) sebagaimana dijelaskan pada Tahap Perencanaan.
- b. Sistem berada sepenuhnya di bawah kendali organisasi dan dapat dipercaya secara menyeluruh.

- c. Sistem hanya akan berkomunikasi dengan sistem lain yang sama-sama tepercaya dan dikendalikan secara penuh.
- d. Terdapat cara praktis untuk mendistribusikan kunci rahasia di antara sistem komunikasi tersebut.
- e. Jaringan tempat sistem-sistem ini berada bersifat sangat tertutup dan tidak mengalami perubahan struktur secara rutin.
- f. Jarang dilakukan penambahan atau penghapusan *node* dalam jaringan.

Contoh protokol yang memungkinkan penggunaan *pre-shared keys* antara lain adalah TLS dan IPSec.

6.3.2 Rekomendasi *Primitives* Kriptografi

Pelaksanaan migrasi ke PQC memerlukan pengambilan keputusan yang sangat spesifik, salah satunya adalah pemilihan primitif pasca-kuantum yang akan digunakan dalam praktik. Keputusan ini dapat menjadi tugas yang menantang dan memerlukan keahlian serta pengetahuan yang mendalam. Bagian ini menyajikan tabel primitif kriptografi yang direkomendasikan (Tabel 6.1) serta tabel himpunan parameter yang direkomendasikan untuk masing-masing primitif tersebut (Tabel 6.2). Selain itu, disertakan pula penjelasan teknis dan alasan di balik rekomendasi tersebut. Penting untuk dicatat bahwa tabel-tabel ini tidak bersifat menyeluruh. Sebagai contoh, meskipun SHA-2 dan SHA-3 direkomendasikan sebagai keluarga fungsi *hash*, keduanya mungkin tidak sesuai untuk semua skenario penerapan. Misalnya, *password hashing* umumnya memerlukan fungsi *hash* khusus seperti Argon2 [39]. Secara umum, terdapat beragam skenario penggunaan yang dapat memerlukan primitif

kriptografi di luar pembahasan pada bagian ini. Bagian ini ditujukan sebagai panduan bagi pengembang perangkat lunak dan arsitek keamanan, dengan asumsi bahwa pembaca memiliki tingkat pemahaman tertentu mengenai kriptografi.

Untuk pembahasan yang lebih komprehensif mengenai primitif kriptografi yang direkomendasikan, dapat melihat Lampiran A.

Tabel 6.1 Rekomendasi primitif kriptografi

Fungsionalitas	Tipe	Disarankan	Diterima	Usang
Pertukaran Kunci/ Enkapsulasi Kunci	Asimetris	ML-KEM ¹	FrodoKEM ¹ Classic McEliece ¹	ECDH ³ RSA ³
Tanda Tangan Digital - <i>Stateless</i>	Asimetris	ML-DSA ² SLH-DSA	FN-DSA ²	ECDSA ³ EdDSA ³ RSA ³
Tanda Tangan Digital - <i>Stateful</i>	Asimetris	XMSS LMS HSS		
Fungsi Hash	Hash	SHA-2 SHA-3	BLAKE2	MD5 SHA-1
<i>Block cipher</i>	Simetris	AES	Camellia	(T)DES IDEA Blowfish
<i>Stream cipher</i>	Simetris	AES-CTR ChaCha20		RC4
Enkripsi	Simetris	AES-CTR ChaCha20		
<i>Authenticated Encryption (with</i>	Simetris	AES-GCM (-SIV)		

Fungsionalitas	Tipe	Disarankan	Diterima	Usang
<i>Associated Data</i>)		AES-OCB ChaCha20- Poly1305		
<i>Message Authentication Code</i>	Simetris	CMAC-AES HMAC-SHA-2 KMAC	CMAC- Camellia BLAKE2- MAC	CBC- MAC

¹Direkomendasikan untuk diterapkan dalam kombinasi hibrida dengan ECDH.

²Direkomendasikan untuk diterapkan dalam kombinasi hibrida dengan ECDSA atau EdDSA.

³Aman terhadap serangan klasik dan dapat menjadi bagian dari skema hibrida

Tabel 6.2 Rekomendasi parameter instansiasi dari primitif kriptografi

Primitif	Direkomendasikan	Akseptabel
ML-KEM ³	ML-KEM-1024 ¹	ML-KEM-768 ¹
ML-DSA ³	ML-DSA-87 ²	ML-DSA-65 ²
SLH-DSA	SLH-DSA- (SHA2/SHAKE)-256(s/f) SLH-DSA- (SHA2/SHAKE)-192(s/f)	SLH-DSA-(SHA2/SHAKE)- 128(s/f)
AES	AES-256	AES-128
SHA-3	SHA-3-256 SHA-3-384 SHA-3-512 (c)SHAKE256	SHA-3-224(c)SHAKE128
SHA-2	SHA-256 SHA-384 SHA-512	SHA-224

¹Direkomendasikan untuk diterapkan dalam kombinasi hibrida dengan ECDH.

²Direkomendasikan untuk diterapkan dalam kombinasi hibrida dengan ECDSA atau EdDSA.

³BSI, ANSSI, dan NLNCSA merekomendasikan penggunaan set parameter NIST level 5 atau 3. NSA CNSA 2.0 mewajibkan level 5

6.3.3 Pertukaran Kunci/*Encapsulation* dan Tanda Tangan Digital

Baru-baru ini, NIST telah menetapkan standar untuk primitif kriptografi asimetris berbasis *lattice*, yaitu mekanisme enkapsulasi kunci ML-KEM [6] dan algoritma tanda tangan digital ML-DSA [7]. Selain ML-KEM, pada tanggal 11 Maret 2025 NIST melalui NIST IR 8545 [40] mengumumkan bahwa *Hamming Quasi-Cyclic* (HQC) telah dipilih untuk proses standardisasi dan diharapkan dapat ditetapkan pada tahun 2027. Primitif ini telah melalui proses peninjauan mendalam selama proses standardisasi PQC oleh NIST, sehingga dianggap siap untuk diimplementasikan secara praktis.

Primitif ini direkomendasikan untuk diimplementasikan dalam mode hibrida, dikombinasikan dengan primitif berbasis kurva eliptik, untuk memastikan bahwa kerentanan implementasi PQC dan potensi kemajuan dalam kriptanalisis berbasis *lattice* tidak langsung menjadikan sistem kriptografi tersebut tidak aman. Kedua standar ini menetapkan tiga set parameter, yang masing-masing berkaitan dengan tingkat keamanan 1 (atau 2 dalam kasus ML-DSA), 3, dan 5. Jika memungkinkan, direkomendasikan untuk menginisialisasi primitif-primitif ini dengan set parameter terkuat, yaitu tingkat keamanan 5, dan menganggap tingkat keamanan 3 sebagai alternatif yang dapat diterima (lihat Tabel 6.2). Standar ML-KEM menetapkan tingkat keamanan 3 sebagai opsi *default*.

Standar PQC ketiga yang diterbitkan oleh NIST adalah algoritma tanda tangan digital berbasis *hash* SLH-DSA. Karena keamanannya hanya bergantung pada keamanan

hash yang mendasarinya, SLH-DSA dianggap sebagai pilihan yang sedikit lebih konservatif dibandingkan ML-DSA berbasis *lattice*. Oleh karena itu, tidak dianggap perlu untuk mengimplementasikan skema ini dalam kombinasi hibrida dengan primitif berbasis kurva eliptis. Dengan alasan yang sama, dapat digunakan tingkat keamanan 1 sebagai instansiasi SLH-DSA.

FN-DSA, yang sebelumnya dikenal sebagai Falcon, merupakan algoritma tanda tangan digital berbasis *lattice* tambahan. Bersama dengan ML-KEM, ML-DSA, dan SLH-DSA, algoritma ini telah dipilih untuk proses standardisasi. Namun, berbeda dengan ketiga primitif lainnya, standar FN-DSA belum difinalisasi. Oleh karena itu, dalam panduan ini direkomendasikan penggunaan ML-DSA dan SLH-DSA dibandingkan FN-DSA.

Untuk skenario yang membutuhkan tingkat kehati-hatian lebih tinggi, FrodoKEM dan Classic McEliece¹ menyediakan fungsi enkapsulasi kunci. Dengan mengorbankan efisiensi secara keseluruhan, primitif-primitif ini dibangun berdasarkan asumsi yang lebih konservatif dan disertai dengan analisis keamanan yang juga lebih konservatif. Oleh karena itu, kemungkinan asumsi-asumsi dasarnya akan terbukti tidak valid dan serangan kriptanalisis yang layak dilakukan menjadi lebih kecil. Namun, FrodoKEM dan Classic McEliece belum distandardisasi. Sampai hal tersebut tercapai, primitif-primitif tersebut tetap dianggap sebagai solusi yang dapat diterima dengan mengikuti set parameter terbaru yang ditujukan untuk tingkat keamanan 5 atau 3.

¹ Catatan: NIST telah memutuskan bahwa Classic McEliece tidak akan dilanjutkan ke proses standardisasi

1. Algoritma Tanda Tangan Digital *Stateful*

Selain SLH-DSA, primitif XMSS, LMS, dan HSS juga menyediakan algoritma tanda tangan digital berbasis *hash* yang telah distandardisasi. Primitif-primitif ini lebih efisien dan lebih disukai dibandingkan algoritma tanda tangan digital yang telah disebutkan sebelumnya. Namun demikian, terdapat satu kelemahan utama, yaitu primitif-primitif ini bersifat *stateful*. Skema tanda tangan yang bersifat *stateful* hanya dapat menghasilkan sejumlah tanda tangan yang terbatas dan memerlukan manajemen status (*state*) yang sangat cermat. Secara lebih spesifik, setelah setiap penggunaan kunci privat, status tersebut harus diperbarui. Apabila status ini hilang, maka skema menjadi tidak aman. Karena alasan tersebut, skema tanda tangan *stateful* hanya cocok digunakan dalam skenario tertentu yang memungkinkan pengelolaan status secara hati-hati. Namun, jika diimplementasikan dengan benar, skema tanda tangan *stateful* dapat memberikan fungsi tanda tangan digital yang efisien dan konservatif. NIST telah menerbitkan seperangkat pedoman komprehensif untuk penerapan skema tanda tangan *stateful* [41].

2. Kriptografi Kunci Simetris

Secara teoretis, primitif kunci simetris dapat diserang menggunakan algoritma kuantum Grover dengan jumlah langkah yang secara kuadratik lebih sedikit dibandingkan serangan *brute-force* klasik. Hal ini menunjukkan adanya pengurangan tingkat keamanan menjadi setengahnya, yang dapat dikompensasi dengan menggandakan panjang kunci.

Secara lebih konkret, hal ini berarti bahwa panjang kunci 128 bit sebaiknya dihindari, dan kunci 256 bit lebih dianjurkan.

Namun, analisis yang lebih mendalam terhadap serangan kuantum Grover menunjukkan bahwa biaya serangan tersebut setidaknya sebanding dengan biaya serangan klasik [42]. Alasan utamanya adalah bahwa tidak seperti serangan kuantum, serangan klasik dapat dilakukan secara paralel. Oleh karena itu, besar kemungkinan bahwa primitif kunci simetris 128 bit akan tetap aman jauh melampaui kemunculan komputer kuantum yang mampu memecahkan primitif kunci asimetris. Jika memungkinkan, direkomendasikan penggunaan kunci 256 bit, dan menganggap kunci 128 bit sebagai alternatif yang masih dapat diterima.

Hal yang perlu diperhatikan adalah bahwa organisasi seharusnya memprioritaskan migrasi primitif kunci asimetris, sehingga disarankan agar organisasi hanya mengalokasikan sumber daya untuk meningkatkan panjang kunci simetris setelah seluruh primitif asimetris telah dimigrasikan ke alternatif pasca-kuantum.

6.3.4 Migrasi Protokol

Bagian ini membahas cara melakukan migrasi protokol ke versi yang tahan terhadap ancaman kuantum. Beberapa protokol yang umum digunakan akan dibahas, dan untuk setiap protokol disajikan setidaknya satu solusi migrasi ke PQC. Untuk masing-masing solusi tersebut, dijelaskan langkah-langkah yang perlu dilakukan oleh administrator sistem, *library developers*, serta personel yang bertanggung

jawab terhadap kebijakan keamanan dalam organisasi. Perlu dicatat bahwa pembahasan ini masih berada pada tingkat yang cukup umum, namun sudah memberikan panduan bagi pihak-pihak terkait.

Perlu juga diketahui bahwa hanya protokol yang sangat umum digunakan yang disertakan dalam bagian ini, yaitu TLS, SSH, S/MIME, PGP, IPSec, dan X.509. Sebagian besar protokol tersebut didefinisikan dalam jenis dokumen yang disebut (*Request for Comments*). RFC merupakan dokumen standardisasi yang diterbitkan oleh *Internet Engineering Task Force* (IETF). Versi rancangan standar disebut sebagai *Internet-Draft*.

1. TLS

- Deskripsi: Menjamin konfidensialitas, autentisitas, dan integritas komunikasi melalui Internet.
- Versi Saat Ini: TLS 1.3
- Dokumen Standardisasi: RFC 8446 [43].
- Penggunaan Umum: TLS digunakan dalam berbagai domain seperti HTTPS dan surat elektronik yang aman. Untuk melakukan migrasi TLS ke PQC, terdapat dua opsi yang dapat dipilih, yaitu menggunakan *pre-shared keys* (Opsi 1) dan pendekatan hibrida (Opsi 2).
- Catatan untuk Administrator Sistem: Untuk setiap skenario atau opsi, disarankan untuk menggunakan TLS 1.3 selama perangkat keras mendukungnya. Selain itu, pastikan bahwa *cipher suites* yang dipilih untuk *Authenticated Encryption with Associated Data* yaitu AES-256-GCM atau ChaCha20-Poly1305.

a. TLS Opsi 1: *Pre-shared Keys*

- Kebijakan yang Diperlukan: Meskipun kebijakan dapat bervariasi bergantung pada kasus penggunaan, suatu kebijakan yang ketat terkait mekanisme berbagi kunci simetris ini harus ditetapkan untuk mencegah aktor jahat memperoleh kunci tersebut, serta untuk mencegah kesalahan distribusi kunci ke sistem yang tidak semestinya. Selain itu, perlu ditetapkan pula kebijakan yang secara jelas mendefinisikan sistem mana yang menggunakan TLS dengan *pre-shared keys*. Terakhir, kebijakan manajemen kunci juga harus diperbarui untuk mencerminkan penggunaan *pre-shared keys* ini.

Pre-shared keys sebaiknya memiliki panjang minimal 256 bit guna mencegah serangan HNDL. Namun, penggunaan kunci dengan ukuran lebih pendek dapat diterima apabila mempertimbangkan jangka waktu informasi tersebut perlu dijaga konfidensialitasnya, sebagaimana telah dijelaskan sebelumnya.

Terakhir, kebijakan yang jelas perlu disusun untuk menentukan waktu dan mekanisme peralihan dari *pre-shared keys* menjadi pendekatan hibrida atau sepenuhnya pasca-kuantum.

- *Administrator System* (Administrator Sistem): Administrator sistem harus mengkonfigurasi TLS agar menggunakan *pre-shared keys*. Selain itu, kunci tersebut harus dikelola dengan baik, mencakup proses pembangkitan, distribusi, penyimpanan, dan

pencabutannya secara aman. Informasi ini dapat ditemukan dalam dokumentasi vendor TLS. Jika implementasi TLS yang digunakan tidak mendukung *pre-shared keys*, maka hubungi vendor TLS terkait.

- Pengembang Pustaka (*Library Developers*): Penjelasan teknis secara rinci mengenai implementasi *pre-shared keys* dalam TLS telah ditetapkan dalam RFC 4279 [44] dan RFC 5487 [45]. *Library Developers* harus memastikan bahwa implementasi TLS yang dikembangkan sesuai dengan standar-standar tersebut.

b. TLS Opsi 2: Pendekatan Hibrida

Internet-draft yang menjelaskan cara melakukan *hybrid key exchange* merupakan referensi yang berguna untuk memahami implementasi solusi hibrida terdapat dalam TLS [46] [47].

- Kebijakan yang Diperlukan: Perlu dilakukan diskusi antara administrator sistem dan pakar kriptografi (jika diperlukan), mengenai *cipher suite* yang diperbolehkan untuk memastikan keamanan terhadap ancaman kuantum. Tidak semua sistem harus dipastikan tahan terhadap ancaman kuantum, sebagaimana dijelaskan sebelumnya mengenai serangan HNDL, sehingga penting untuk menetapkan sistem mana saja yang akan menggunakan versi TLS yang telah dimodifikasi ini.

Hal ini menjadi sangat penting karena RFC terkait masih berada dalam bentuk draf dan kemungkinan akan mengalami pembaruan,

sehingga kebijakan yang ditetapkan harus dapat menyesuaikan dengan perubahan tersebut. Selain itu, perlu ada kebijakan jelas yang menetapkan waktu dan mekanisme peralihan dari pendekatan hibrida menjadi penggunaan algoritma yang sepenuhnya pasca-kuantum.

- **Administrator Sistem:** Administrator sistem harus mengonfigurasi TLS agar menggunakan pendekatan hibrida ini. Informasi mengenai hal ini dapat ditemukan pada dokumentasi vendor TLS. Apabila implementasi TLS yang digunakan belum mendukung RFC ini, maka disarankan untuk mempertimbangkan penggantian vendor TLS atau menghubungi vendor terkait.
- **Library Developers:** *Library developers* dapat mengimplementasikan fitur eksperimental ini berdasarkan RFC yang tersedia. Mengingat draf ini masih dalam tahap pengembangan, maka diperkirakan akan ada revisi lanjutan, sehingga implementasinya pun dapat berubah seiring waktu.

2. SSH

- **Deskripsi:** *Secure Shell* (SSH) merupakan protokol jaringan yang dirancang untuk menyediakan komunikasi jarak jauh secara aman melalui kanal terenkripsi. SSH memungkinkan autentikasi, eksekusi perintah, dan pengelolaan sistem jarak jauh melalui mekanisme enkripsi simetris, pertukaran kunci asimetris, serta autentikasi host dan pengguna.

- Versi Saat Ini: Protokol yang digunakan secara luas adalah SSH-2.0, sebagaimana didefinisikan dalam rangkaian dokumen RFC 4251 s.d. RFC 4254
- Dokumen Standardisasi: RFC 4251 [48], RFC 4252 [49], RFC 4253 [50], RFC 4254 [51], RFC 5656 [52], RFC 8332 [53], RFC 8308 [54].
- Penggunaan Umum: SSH digunakan secara luas untuk akses jarak jauh ke server, menjalankan perintah secara aman, melakukan transfer berkas (SCP/SFTP), dan sebagai komponen dasar berbagai sistem otomasi serta orkestrasi server.
- Tidak seperti TLS 1.3 yang menyediakan mekanisme *pre-shared keys* (PSK) sebagai bagian dari protokol, SSH tidak dirancang untuk menggunakan PSK sebagai mekanisme pertukaran kunci sesi. SSH menggunakan kombinasi:
 - *Key Exchange* (KEX) berbasis algoritma publik (mis. ECDH),
 - autentikasi host melalui *host key*, dan
 - autentikasi pengguna (password, public key, GSSAPI, dll.).

Walaupun file *known_hosts* menyimpan kunci publik host yang telah dikenal sebelumnya, mekanisme ini bukan PSK formal, melainkan bagian dari model autentikasi host SSH. Dengan demikian, dalam konteks migrasi PQC, SSH memerlukan pendekatan hibrida yang menggabungkan algoritma klasik dengan algoritma pasca-kuantum untuk

mempertahankan kompatibilitas dan ketahanan jangka panjang.

- Saat ini, standar PQC untuk SSH masih dalam tahap pengembangan melalui Internet-Draft IETF/CFRG mengenai *Post-Quantum Hybrid Key Exchange for SSH*. Sejumlah implementasi, seperti OpenSSH versi terbaru, telah mengadopsi KEX hibrida (misalnya x25519-sha256 dikombinasikan dengan ML-KEM/Kyber [55]) dan sntrup761x25519-sha512 [56]

Pendekatan hibrida diperlukan untuk:

- menjaga kompatibilitas dengan perangkat lama yang hanya mendukung algoritma klasik,
 - menghindari penurunan keamanan apabila algoritma PQC direvisi atau ditemukan kelemahan baru,
 - memberikan perlindungan terhadap serangan kuantum dengan tetap mempertahankan keamanan klasik
- Kebijakan yang Diperlukan: Perlu dilakukan diskusi antara administrator sistem dan, jika diperlukan, pakar kriptografi, mengenai *cipher* yang diizinkan guna memastikan ketahanan terhadap ancaman kuantum. Tidak semua sistem harus dipastikan aman dari ancaman kuantum, sehingga penting untuk menentukan sistem yang akan menggunakan versi SSH yang telah dimodifikasi. Hal ini sangat penting mengingat RFC terkait masih dalam bentuk draf dan kemungkinan akan mengalami pembaruan, sehingga kebijakan yang ditetapkan harus mencerminkan perubahan tersebut.

Selain itu, perlu ditetapkan kebijakan yang jelas mengenai waktu dan mekanisme peralihan dari pendekatan hibrida ke algoritma yang sepenuhnya pasca-kuantum.

- Administrator Sistem: Administrator sistem harus mengonfigurasi server dan klien SSH untuk mendukung algoritma KEX hibrida yang sesuai dengan kebijakan organisasi. Langkah-langkah tersebut meliputi:
 - memastikan versi perangkat lunak SSH mendukung algoritma PQC yang direkomendasikan vendor,
 - memverifikasi kompatibilitas antarversi (misalnya OpenSSH klien dan server),
 - mengaktifkan algoritma KEX hibrida dalam konfigurasi, dan
 - melakukan pengujian handshake lintas versi untuk memastikan tidak terjadi *downgrade attack* atau kegagalan negosiasi.
- *Library Developers*: *Library developer* dapat mengimplementasikan fitur ini berdasarkan RFC yang tersedia. Mengingat draf ini masih dalam tahap pengembangan, maka diperkirakan akan ada revisi tambahan, sehingga implementasinya pun kemungkinan akan mengalami perubahan dari waktu ke waktu.

3. S/MIME

- Deskripsi: *Secure/Multipurpose Internet Mail Extensions* (S/MIME) merupakan mekanisme standar untuk menyediakan *confidentiality*, *integrity*, *authentication*, dan *non-repudiation* pada data berbasis MIME, seperti email dan

lampiran multimedia. S/MIME memanfaatkan PKI berbasis sertifikat X.509 untuk melakukan enkripsi serta *digital signing*..

- Versi Saat Ini: S/MIMEv4 [57], [58], [59].
- Dokumen Standardisasi: RFC 8551 [60] dan RFC 5652 [57].
- Penggunaan Umum: S/MIME banyak digunakan dalam sistem email korporat dan pemerintahan untuk melakukan enkripsi pesan end-to-end serta verifikasi tanda tangan digital. Dalam lingkungan enterprise, S/MIME terintegrasi dengan PKI organisasi untuk manajemen sertifikat pengguna.
- Saat ini, masih sangat sedikit penelitian mengenai penerapan algoritma pasca-kuantum pada S/MIME. OpenQuantumSafe menyediakan cabang (*fork*) dari OpenSSL yang mencakup versi S/MIME yang tahan terhadap serangan kuantum dengan menggunakan pendekatan hibrida maupun murni algoritma PQC [61]. Namun demikian, *library* tersebut dinyatakan tidak diperuntukkan bagi lingkungan produksi, sehingga penerapannya di dunia nyata masih terbatas.
- Karena protokol ini tidak mendukung penggunaan *pre-shared keys*, maka seluruh skenario sebaiknya mempertimbangkan pendekatan hibrida.
- Kebijakan yang diperlukan: Kebijakan ideal yang dapat diterapkan adalah tidak menggunakan email untuk bertukar informasi yang perlu dirahasiakan dalam jangka waktu yang lebih lama dari dimulainya serangan HNDL. Setiap

pertukaran informasi seperti itu sebaiknya dikategorikan sebagai insiden keamanan. Jika vendor telah mengimplementasikan versi S/MIME yang aman secara pasca-kuantum dan siap digunakan dalam produksi, maka harus dibuat kebijakan yang mengatur penggunaan yang tepat serta proses transisi menuju versi tersebut.

Selain itu, penting untuk memiliki kebijakan yang jelas mengenai waktu dan mekanisme transisi dari pendekatan hibrida ke solusi yang sepenuhnya pasca-kuantum harus dilakukan.

- **Administrator Sistem:** Jika vendor telah menyediakan versi S/MIME yang aman secara pasca-kuantum dan siap digunakan di lingkungan produksi, maka administrator sistem harus mengonfigurasi versi tersebut sesuai kebijakan yang telah ditetapkan. Menghubungi vendor S/MIME yang sedang digunakan untuk menanyakan kesiapan terhadap ancaman kuantum juga merupakan langkah yang dapat dilakukan.
- **Library Developers:** *OpenQuantumSafe* library yang disebutkan sebelumnya dapat digunakan sebagai dasar untuk memodifikasi library S/MIME agar mendukung algoritma pasca-kuantum. Fitur ini harus secara eksplisit diberi label sebagai fitur eksperimental dan pengembang harus terus memantau perkembangan terbaru di bidang ini.

4. PGP

- Deskripsi: PGP menyediakan konfidensialitas dan autentikasi terhadap data serta layanan untuk manajemen kunci dan sertifikat.
- Versi Saat Ini: OpenPGP [62] dan GnuPGP [63].
- Dokumen Standardisasi: RFC 9580 [62].
- Penggunaan Umum: PGP sering digunakan dalam komunikasi email yang aman.
- Administrator Sistem: Setiap pertukaran informasi yang memerlukan konfidensialitas jangka panjang sebaiknya dikategorikan sebagai insiden keamanan. Menghubungi vendor PGP yang digunakan saat ini untuk menanyakan kesiapan terhadap ancaman kuantum juga merupakan langkah yang dapat dipertimbangkan, dan organisasi harus terus memantau perkembangan terbaru di bidang ini.
- *Library Developers*: Memantau draf RFC dan literatur ilmiah yang berkaitan dengan area ini sangat penting agar PGP dapat mulai dimigrasikan ke versi yang aman terhadap ancaman kuantum.

5. IPSec

- Deskripsi: IPSec mengenkripsi dan mengautentikasi paket IP antara pihak-pihak yang berkomunikasi.
- Versi Saat Ini: IPSec-v3 [64].
- Dokumen Standardisasi: RFC 6071 [64].
- Penggunaan Umum: IPSec sering digunakan dalam *Virtual Private Network* (VPN). Untuk memigrasikan IPSec agar aman terhadap ancaman kuantum, terdapat dua opsi yang dapat

dipertimbangkan: menggunakan kunci yang telah dibagikan sebelumnya (*pre-shared keys*, Opsi 1) dan pendekatan hibrida (Opsi 2).

a. IPSec Opsi 1: *Pre-shared Keys*

- Kebijakan yang Diperlukan: Meskipun kebijakan dapat berbeda-beda bergantung pada kasus penggunaan, suatu kebijakan yang ketat mengenai pembagian kunci simetris harus ditetapkan. Selain itu, kebijakan yang secara jelas mendefinisikan sistem mana saja yang menggunakan IPSec dengan *pre-shared keys* juga perlu disusun. Terakhir, kebijakan manajemen kunci harus diperbarui untuk mencerminkan pengenalan penggunaan *pre-shared keys* ini.

Penting bagi para pihak yang memegang kunci simetris tersebut untuk mematuhi persyaratan bahwa panjang kunci harus minimal 256 bit guna menghindari serangan HNDL. Namun, penggunaan kunci dengan panjang bit yang lebih pendek juga dapat diterima dengan mempertimbangkan jangka waktu informasi tersebut harus tetap dijaga konfidensialitasnya, sebagaimana telah dibahas sebelumnya. Terakhir, perlu ditetapkan kebijakan yang jelas mengenai waktu dan mekanisme transisi dari penggunaan *pre-shared keys* ke pendekatan hibrida atau sepenuhnya pasca-kuantum.

- Administrator Sistem: Secara alami, administrator sistem harus mengonfigurasi

IPSec agar menggunakan *pre-shared keys*. Informasi teknis mengenai konfigurasi ini dapat ditemukan dalam dokumentasi dari penyedia IPSec. Jika implementasi IPSec tidak mendukung *pre-shared keys*, maka perlu dipertimbangkan untuk mengganti penyedia IPSec (setidaknya untuk sistem yang memerlukan *pre-shared keys*, atau menghubungi penyedia IPSec tersebut.

- *Library Developers*: Penjelasan teknis mendetail tentang proses ini dapat ditemukan dalam RFC 7296 [65].
- *Library developers* harus memastikan bahwa implementasi IPSec mereka sesuai dengan standar tersebut. Selain itu, terdapat juga sebuah *Internet-Draft* yang dapat digunakan oleh pengembang untuk menerapkan *pre-shared keys* dalam rangka mencapai keamanan pasca-kuantum [66].

b. *IPSec Option 2 Hybrid Approach*

Salah satu sumber teknis yang bermanfaat untuk mencapai keamanan pasca-kuantum dalam IPSec adalah ETSI TR 103 617 [67].

- *Kebijakan yang Diperlukan*: Perlu dilakukan diskusi antara administrator sistem dan, bila diperlukan, para pakar kriptografi mengenai *cipher suites* yang diizinkan untuk memastikan keamanan terhadap ancaman kuantum. Tidak semua sistem mungkin perlu segera dimutakhirkan menjadi aman terhadap kuantum, sebagaimana telah dijelaskan sebelumnya terkait serangan HNDL, sehingga penting untuk

mendefinisikan sistem mana saja yang akan menggunakan IPSec dengan pendekatan yang telah dimodifikasi. Hal ini sangat penting karena dokumen RFC saat ini masih dalam bentuk draf dan kemungkinan akan diperbarui, yang berarti kebijakan organisasi harus disesuaikan dengan perkembangan tersebut. Selain itu, penting untuk menetapkan kebijakan yang jelas mengenai waktu dan mekanisme peralihan dari pendekatan hibrida ke sistem yang sepenuhnya menggunakan kriptografi pasca-kuantum.

- **Administrator Sistem:** Administrator sistem harus mengonfigurasi IPSec agar dapat menggunakan pendekatan hibrida ini. Informasi teknis mengenai konfigurasi tersebut dapat ditemukan dalam dokumentasi dari penyedia IPSec. Jika implementasi IPSec tidak mendukung pendekatan hibrida ini, maka disarankan untuk mempertimbangkan penggantian penyedia IPSec (setidaknya untuk sistem yang memerlukan pendekatan hibrida) atau menghubungi penyedia IPSec tersebut.
- **Library Developers:** Library developers dapat mengimplementasikan fitur ini berdasarkan laporan teknis dari ETSI [67]. Tentu saja, seiring waktu akan diterbitkan revisi-revisi tambahan dari draf ini, sehingga diharapkan implementasi akan terus berkembang menyesuaikan perubahan tersebut.

6. X.509

- Deskripsi: X.509 digunakan untuk membuktikan kepemilikan atas sebuah kunci publik.
- Versi Saat Ini: X.509v3 [68].
- Dokumen Standardisasi: RFC 5280 [69] dan ITU-T X.509 [70], [71].
- Penggunaan Umum: X.509 secara luas digunakan untuk mengautentikasi situs web dalam komunikasi HTTPS.
- Karena protokol X.509 tidak mendukung penggunaan *pre-shared keys*, maka semua skenario harus mempertimbangkan pendekatan hibrida. ITU-T telah menetapkan varian sertifikat hibrida (dengan beberapa algoritma) dalam Bagian 9.8 dari [70]. Standar ini merujuk pada Internet-Draft yang telah kedaluwarsa oleh Truskovsky et al. [72], dan dalam literatur, sertifikat tersebut sering disebut sebagai *catalyst certificates*. Selain itu, IETF sedang mengembangkan *Internet-Drafts* baru [73], [74] yang menawarkan bentuk alternatif dari sertifikat hibrida, yang disebut *composite certificates*. Seiring waktu, semakin banyak *root CA* dan *CA* yang akan mulai menyediakan sertifikat post-kuantum, sehingga penting untuk senantiasa mengikuti perkembangan pasar.
- Kebijakan yang diperlukan: Tidak semua sertifikat harus kompatibel dengan solusi hibrida, sebagaimana dijelaskan sebelumnya terkait serangan HNDL. Oleh karena itu, perlu ditentukan sistem-sistem yang akan menggunakan sertifikat X.509 dan yang telah dimodifikasi. Selain itu, perlu dicatat bahwa

library kriptografi dan protokol yang digunakan harus kompatibel dengan jenis sertifikat baru ini. Akhirnya, sangat penting untuk menetapkan kebijakan yang jelas mengenai waktu dan mekanisme peralihan dari pendekatan hibrida ke pendekatan yang sepenuhnya berbasis post-kuantum. Untuk mewujudkan hal ini, komunikasi dan perencanaan dengan CA atau *root CA* menjadi hal yang sangat krusial.

- **Administrator Sistem:** Administrator sistem harus mengkonfigurasi sertifikat X.509 agar kompatibel dengan pendekatan hibrida.
- **Library Developers:** *Library developers* dapat mengimplementasikan fitur eksperimental ini berdasarkan dokumen RFC dan standar dari ITU-T. Tentu saja, seiring dengan diterbitkannya revisi baru dari draf, diharapkan bahwa implementasi juga akan mengalami penyesuaian dari waktu ke waktu.

6.3.5 Ketangkasan Kriptografi (*Cryptographic Agility*)

Cryptographic agility merupakan bentuk *agility* yang memungkinkan organisasi untuk beradaptasi terhadap risiko penggunaan kriptografi dengan upaya seminimal mungkin. Secara konkret, *cryptographic agility* merujuk pada praktik penataan teknologi, proses, dan kebijakan agar kriptografi yang digunakan dalam suatu organisasi dapat dikonfigurasi secara efisien. Artinya, kriptografi tersebut dapat diperbarui, diubah, atau diganti sepenuhnya dengan upaya dan konsekuensi minimal, seperti waktu henti sistem yang rendah bagi organisasi.

Cryptographic agility dapat diterapkan pada berbagai tingkatan, misalnya dalam mempermudah pencabutan kunci kriptografi, pembaruan parameter, penggantian satu algoritma kriptografi dengan algoritma lainnya, atau penggantian implementasi dari suatu algoritma kriptografi. *Cryptographic agility* bukanlah sesuatu yang dapat dibeli, melainkan memerlukan keselarasan pada berbagai tingkatan dalam organisasi. Solusi teknis memang tersedia, misalnya untuk mendeteksi secara otomatis permasalahan pada kriptografi atau mengonfigurasi atau mengganti implementasi algoritma kriptografi. Namun demikian, *cryptographic agility* juga perlu terintegrasi dalam proses bisnis dan kebijakan organisasi agar solusi teknis tersebut dapat digunakan secara efektif. Misalnya, *cryptographic agility* dapat dimasukkan ke dalam proses manajemen perubahan (*change management*), proses pengadaan, dan kebijakan kriptografi untuk mewajibkan penerapan langkah-langkah tertentu secara menyeluruh di seluruh organisasi.

Algoritma PQC yang saat ini telah atau sedang distandardisasi masih relatif belum banyak diuji di lingkungan nyata. Oleh karena itu, sangat mungkin bahwa pengaturan, parameter, atau bahkan keseluruhan algoritma tersebut perlu diperbarui di masa depan. Dengan *cryptographic agility* yang telah diterapkan, pembaruan ini dapat dilakukan dengan sumber daya dan gangguan yang minimal. Terutama jika organisasi memutuskan untuk melakukan migrasi sebagian terhadap aset kriptografi sebelum tersedia standar dan implementasi yang divalidasi, maka organisasi tersebut harus siap untuk dengan mudah mengganti algoritma kriptografi ketika standar tersebut diterbitkan atau implementasi baru

direkomendasikan. Hal ini berbeda dengan algoritma kriptografi rentan-kuantum yang saat ini digunakan, yang standar dan parameter sudah mapan, serta perubahan jarang terjadi.

Selain mendukung proses migrasi ke PQC, *cryptographic agility* juga membantu dalam pengelolaan kriptografi secara umum. Oleh karena itu, membangun organisasi yang lebih tangkas secara kriptografi dianggap sebagai langkah tanpa penyesalan (*no-regret move*), karena sudah memberikan manfaat saat ini, misalnya dengan membantu mengidentifikasi potensi kerentanan lebih awal dan mempercepat respons terhadap insiden.

Namun demikian, *cryptographic agility* masih merupakan konsep yang agak abstrak dalam praktiknya. Pembahasan mengenai bentuk atau metode penerapan *cryptographic agility* secara spesifik dapat membantu memperjelas tujuan yang ingin dicapai. Dalam bab ini disampaikan panduan mengenai integrasi *cryptographic agility* dalam teknologi, proses, dan kebijakan serta penjelasan mengenai berbagai bentuk *cryptographic agility* dan tantangan umum untuk mencapainya. Terakhir, disampaikan pertimbangan-pertimbangan dalam memilih strategi *cryptographic agility* yang tepat.

1. Langkah Teknis untuk Mewujudkan *Cryptographic agility*

Pada tingkat teknis, berbagai langkah dapat diterapkan untuk memastikan transisi antar algoritma kriptografi, parameter, atau implementasi. Titik awal untuk mencapai *cryptographic agility* adalah dengan mengetahui jenis dan lokasi

penggunaan kriptografi dalam organisasi. Memelihara inventarisasi kriptografi yang selalu diperbarui sangat membantu dalam memantau, mengidentifikasi, dan memperbarui kriptografi yang rentan secara cepat.

Selain itu, tantangan utama dalam pengelolaan *cryptographic agility* adalah permasalahan kompatibilitas. Misalnya, situasi ketika algoritma baru telah diadopsi oleh satu pihak, tetapi belum oleh pihak lainnya. Dengan adanya inventarisasi kriptografi yang terpusat, proses pemantauan agar pembaruan dilakukan secara serentak di seluruh organisasi menjadi lebih mudah. Pengelolaan kriptografi juga mencakup manajemen kunci dan sertifikat. Saat ini tersedia alat bantu yang memungkinkan proses pembuatan, distribusi, dan penghentian penggunaan kunci serta sertifikat kriptografi dilakukan secara otomatis (atau sebagian otomatis).

Tahap selanjutnya yang penting untuk *cryptographic agility* adalah dalam proses pengembangan sistem yang menggunakan kriptografi. Untuk memudahkan penggantian suatu algoritma dengan algoritma lain, maka pemanggilan fungsi-fungsi kriptografi dalam kode sumber sebaiknya dibuat seabstrak mungkin. Selain itu, *Continuous Integration/Continuous Deployment* (CI/CD) dapat dimanfaatkan untuk menguji fungsi-fungsi kriptografi, sehingga kesalahan penggunaan atau masalah kompatibilitas dapat dideteksi lebih awal. Informasi ini juga dapat meningkatkan kinerja alat bantu lainnya, seperti dalam proses penemuan aset.

Sistem yang menggunakan kriptografi juga dapat dirancang untuk mendukung beberapa algoritma secara bersamaan, memungkinkan sistem lain untuk memilih algoritma mana yang akan digunakan dalam setiap koneksi. Hal ini dapat membantu meningkatkan *system agility* secara keseluruhan serta kompatibilitas (termasuk kompatibilitas mundur). Namun, pendekatan ini juga dapat membuka potensi kerentanan baru, seperti serangan *downgrade* [75].

Cryptographic agility juga dapat ditingkatkan dengan mempertimbangkan kebutuhan perangkat keras dari algoritma kriptografi di masa depan. Algoritma PQC umumnya membutuhkan kapasitas lebih besar dalam hal penyimpanan, bandwidth, dan lainnya. Oleh karena itu, penting untuk mengevaluasi kecukupan perangkat keras saat ini untuk menjalankan PQC di masa mendatang. Jika tidak, maka perlu mulai dipertimbangkan alternatif untuk meningkatkan atau mengganti perangkat keras tersebut.

2. *Cryptographic agility* dalam Proses

Selain solusi teknis, *cryptographic agility* juga dapat dilakukan melalui integrasi ke dalam proses-proses organisasi yang telah ada. Bergantung pada tingkat kematangan sistem, langkah-langkah organisasi dapat lebih mudah diadopsi dibandingkan solusi teknis, terutama bagi sistem yang sudah digunakan. Dengan mendokumentasikan secara eksplisit *cryptographic agility* dalam proses, titik-titik lemah dan hambatan dalam pembaruan kriptografi dapat

diidentifikasi dengan lebih mudah. Selain itu, proses yang terdokumentasi membantu menyelaraskan pemahaman di antara para pemangku kepentingan yang terlibat (baik internal maupun eksternal), dan tetap dapat diterapkan meskipun terjadi pergantian personel. Pada akhirnya, hal ini akan mengurangi kesalahan dalam pembaruan kriptografi serta menekan kebutuhan sumber daya seperti waktu dan biaya. Terlebih lagi, dokumentasi yang jelas atas langkah-langkah dalam menerapkan *cryptographic agility* menciptakan bentuk auditabilitas yang sangat dibutuhkan dalam konteks ini.

Untuk mengintegrasikan *cryptographic agility* ke dalam suatu proses, pertama-tama perlu ditentukan ruang lingkupnya. Misalnya, bentuk *cryptographic agility* yang ingin dicapai serta waktu mulai dan berakhirnya proses. Hal ini juga akan membantu dalam mengidentifikasi keterkaitan dengan proses lain.

Beberapa proses umum yang dapat dimasukkan unsur *cryptographic agility* di dalamnya antara lain proses pengadaan, manajemen perubahan, pengembangan dan peluncuran perangkat lunak, serta manajemen respons insiden.

Cryptographic agility perlu diperhitungkan dalam proses pengadaan yang berkaitan dengan pembelian komponen perangkat lunak dan perangkat keras baru. Hal ini penting agar komponen tersebut dapat diperbarui di masa depan. Tinjauan dan pengujian secara cermat terhadap klaim kemampuan *agility* dari

suatu produk juga merupakan langkah penting. Untuk perangkat keras, produk sebaiknya telah mendukung berbagai algoritma atau parameter sejak awal, atau setidaknya mudah untuk diperbarui. Perlu dicatat bahwa penerapan *cryptographic agility* sejak awal siklus hidup sistem umumnya lebih mudah dibandingkan menambahkan kemampuan tersebut ke dalam sistem yang sudah berjalan. Oleh karena itu, proses-proses ini sangat penting untuk memasukkan pertimbangan *cryptographic agility*. Hal ini juga berkaitan erat dengan kebijakan kriptografi, yang dapat mewajibkan tingkat *agility* tertentu pada produk-produk baru.

Selanjutnya, proses yang berkaitan dengan pengembangan dan peluncuran perangkat lunak dapat meningkatkan *cryptographic agility* melalui mekanisme pengujian. Misalnya, proses tersebut dapat menjelaskan mekanisme dan waktu pengujian kriptografi untuk mencegah masalah kompatibilitas atau kerentanan lainnya. Apabila perlu dilakukan pembaruan pada kriptografi, maka proses tersebut juga harus mencakup tata cara pelaksanaan pembaruan tersebut sebagai bagian dari siklus rilis perangkat lunak.

Proses manajemen perubahan menggambarkan cara organisasi mengimplementasikan perubahan secara efisien. Proses ini dapat mencakup alasan di balik suatu perubahan, cara pelaksanaannya, serta langkah-langkah organisasi untuk dapat beradaptasi terhadap perubahan tersebut. Dalam konteks *cryptographic agility*, proses ini harus menjelaskan

mekanisme pengaturan pembaruan atau penggantian kriptografi. Misalnya, penentuan pihak yang bertanggung jawab atas kriptografi tertentu, serta mekanisme untuk memastikan bahwa seluruh organisasi melakukan perubahan yang sama secara serempak. Pihak-pihak yang biasanya terlibat dalam proses ini antara lain manajemen atau pembuat kebijakan yang harus menyetujui perubahan kriptografi, serta pengembang perangkat lunak atau arsitek keamanan yang harus melaksanakan pembaruan tersebut.

Terakhir, proses respons insiden menjelaskan mekanisme tindakan organisasi ketika terjadi insiden. Misalnya, proses dapat menjabarkan langkah-langkah yang harus diambil apabila terjadi kompromi terhadap kunci kriptografi. Karena waktu respons biasanya menjadi pertimbangan utama, maka dokumentasi langkah-langkah yang berkaitan dengan *cryptographic agility* dapat membantu memperlancar keseluruhan proses. Sebagai contoh, pemantauan terus-menerus terhadap seluruh kriptografi yang digunakan sebagai bagian dari prosedur penilaian risiko akan membantu mengidentifikasi potensi ancaman sejak dini. Selain itu, dalam situasi insiden, proses ini dapat membantu menentukan pihak yang bertanggung jawab dalam pengambilan keputusan dan menetapkan langkah penghentian penggunaan kunci kriptografi yang terdampak.

3. *Cryptographic agility* dalam Kebijakan

Cryptographic agility juga harus diintegrasikan dalam kebijakan yang mengatur pengelolaan kriptografi.

Cara logis untuk memasukkan *cryptographic agility* dalam kebijakan adalah dengan mewajibkan penerapan langkah teknis maupun prosedural yang mendukung *cryptographic agility*, terutama untuk sistem-sistem baru.

Selain itu, kebijakan kriptografi juga dapat mewajibkan pemutakhiran inventaris kriptografi secara berkala, serta menetapkan individu atau unit yang bertanggung jawab atas pengelolaan kriptografi. Misalnya, kebijakan dapat menentukan pihak yang bertanggung jawab dalam memantau keamanan dari kriptografi yang digunakan, atau pihak yang berwenang menyetujui maupun melakukan pembaruan jika diperlukan. Kebijakan kriptografi juga dapat mengatur mekanisme dan waktu pengujian proses yang telah mencakup *cryptographic agility* untuk memastikan proses tersebut berjalan sebagaimana mestinya.

Dalam kebijakan pengadaan pun, *cryptographic agility* sebaiknya turut diperhatikan. Misalnya, vendor dapat diwajibkan untuk mengadopsi algoritma PQC baru dalam jangka waktu tertentu setelah algoritma tersebut distandardisasi.

Namun demikian, hambatan umum dalam proses pembaruan atau penggantian kriptografi adalah ketika kebijakan hanya mengizinkan satu algoritma atau satu set parameter tertentu. Dengan demikian, ketika migrasi ke algoritma atau parameter baru diperlukan, maka kebijakan harus diperbarui terlebih dahulu. Oleh sebab itu, kebijakan kriptografi

sebaiknya disusun agar mengakomodasi lebih banyak opsi. Di sisi lain, organisasi juga harus berhati-hati agar kebijakan kriptografinya tidak mencantumkan algoritma atau parameter yang sudah usang dan tidak lagi aman.

Terdapat dua hal yang harus diperhatikan dalam *cryptographic agility*, yaitu:

1. Bentuk *cryptographic agility*

Alasan organisasi menginginkan *cryptographic agility* bergantung pada konteks masing-masing. Penelaahan dengan saksama terhadap kebutuhan dalam konteks tertentu membantu memahami dengan lebih baik hal-hal yang benar-benar perlu disiapkan untuk mencapai tingkat *cryptographic agility* yang memadai sesuai dengan tujuan yang diharapkan. Berikut adalah penjelasan berbagai bentuk *cryptographic agility* beserta tantangan umum yang harus diatasi untuk mencapainya [76]:

- a. Ketangkasan Migrasi (*Migration Agility*)

Agility ini dapat dikatakan sebagai bentuk *cryptographic agility* yang paling dikenal. Tujuannya adalah untuk dapat mengganti satu algoritma kriptografi dengan algoritma lainnya. Oleh karena itu, *agility* ini akan menjadi bentuk utama *cryptographic agility* yang dibutuhkan untuk bermigrasi dari kriptografi yang rentan terhadap kuantum ke PQC. Memiliki bentuk *cryptographic agility* ini penting sebelum, selama, dan setelah migrasi ke PQC dilakukan karena algoritma saat ini dan yang baru akan selalu perlu diperbarui seiring waktu.

Penting untuk memastikan bahwa *migration agility* diterapkan pada setiap penggunaan algoritma untuk layanan atau aplikasi. Tidak memperbarui algoritma atau parameternya di semua tempat dapat menyebabkan masalah ketidakcocokan ketika satu sisi komunikasi menggunakan konfigurasi baru sementara sisi lainnya masih menggunakan konfigurasi lama. Hal ini sangat sulit jika berbagai instansi algoritma dikelola oleh entitas (eksternal) yang berbeda. Selain itu, tidak memverifikasi bahwa algoritma telah diperbarui di seluruh organisasi dapat memperkenalkan kerentanan karena penyerang akan dengan mudah menyerang bagian yang masih menggunakan konfigurasi lama.

Terakhir, kompatibilitas perangkat keras dapat menjadi hambatan bagi *migration agility*, karena perangkat keras misalnya perlu mampu mendukung kunci atau ciphertext yang lebih besar. Lebih lanjut, akselerasi perangkat keras saat ini bisa jadi tidak kompatibel dengan algoritma baru, sehingga membuatnya jauh lebih lambat.

Langkah-langkah untuk meningkatkan bentuk *cryptographic agility* ini dan mengurangi risiko terkait dilakukan melalui manajemen aset kriptografi, pengabstraksian kode yang bertanggung jawab atas operasi kriptografi sehingga hanya perlu diubah di satu lokasi, dan memiliki pandangan yang tepat serta jalur

komunikasi dengan ketergantungan internal dan eksternal. Selain itu, mendukung beberapa algoritma atau set parameter dalam cara “ATAU” dapat membantu mengatasi masalah ketidakcocokan (sementara) ini. Namun, hal ini juga dapat menimbulkan risiko serangan penurunan (*downgrade attack*), ketika penyerang secara sengaja memilih algoritma yang lebih lemah untuk diserang [75]. Oleh karena itu, algoritma yang didukung harus dimonitor dan dihapus setelah tidak lagi diperlukan untuk kompatibilitas atau tidak lagi aman.

b. Ketangkasan Kepatuhan (*Compliance Agility*)

Bentuk *agility* ini merujuk pada infrastruktur kriptografi yang dapat dengan mudah dikonfigurasi ulang untuk memenuhi berbagai regulasi (*regional*) secara bersamaan. Dalam hal ini, akan ada beberapa “versi” dari sistem yang sama, masing-masing dengan konfigurasi kriptografi yang berbeda. Sangat penting untuk memiliki inventaris yang baik mengenai konfigurasi sistem dan area penerapannya. Jika bentuk *agility* ini diinginkan untuk menyesuaikan kriptografi dengan perubahan regulasi, maka sifatnya mirip dengan *migration agility* dengan tambahan persyaratan adanya bentuk pemantauan untuk dengan cepat mengenali ketika terjadi perubahan regulasi yang berlaku pada bagian tertentu dari kriptografi. Sebagai contoh, suatu negara dapat mewajibkan penggunaan set parameter baru untuk informasi yang bersifat rahasia. Selain itu, jika *migration*

agility hanya memperbarui suatu sistem, maka dengan *compliance agility*, versi berbeda dari sistem yang sama yang mematuhi regulasi berbeda harus dapat berfungsi secara bersamaan.

c. Ketangkasan Implementasi (*Implementation Agility*)

Pada tingkat aplikasi, dari pada memperbarui algoritma kriptografi, tujuannya adalah untuk dapat mengganti seluruh implementasi dari sebuah algoritma. Hal ini dapat terjadi, misalnya, jika versi baru dari implementasi dirilis. Risiko yang serupa dengan *migration agility* juga berlaku untuk *implementation agility*. Sebagai contoh, masalah kompatibilitas dan ketergantungan juga menjadi tantangan untuk bentuk *agility* ini. Selain itu, mengganti implementasi biasanya memerlukan proses yang lebih kompleks dalam organisasi. Misalnya, sebuah perusahaan dapat memiliki kebijakan dan/atau solusi CI/CD untuk menguji perangkat lunak sebelum dapat dirilis. Penting untuk menyadari proses-proses ini dan mempertimbangkan durasinya dalam waktu migrasi. Di sisi lain, solusi CI/CD juga dapat menjadi peluang besar untuk mengintegrasikan pengujian otomatis terhadap implementasi kriptografi terhadap kerentanan atau kesalahan yang diketahui.

d. Ketangkasan Platform (*Platform Agility*)

Bentuk *agility* ini merujuk pada algoritma kriptografi yang dapat diintegrasikan secara mulus dengan berbagai jenis platform. Bentuk *agility* ini terutama menarik bagi organisasi yang menyediakan implementasi kriptografi kepada pelanggan. Hal ini berarti bahwa algoritma kriptografi yang sama harus dapat dijalankan pada berbagai perangkat yang berbeda, terlepas dari perangkat keras dan perangkat lunak yang digunakan. Terutama ketika menjalankan kriptografi pada perangkat tertentu, masalah dapat muncul ketika algoritma kriptografi baru tidak dapat diterapkan pada perangkat keras yang ada, dan perangkat keras tersebut sulit untuk diganti. Selain itu, beberapa algoritma yang aman terhadap kuantum memerlukan operasi yang lebih kompleks yang dapat sulit untuk diimplementasikan dan dijalankan pada perangkat tersebut. Disarankan untuk mempertimbangkan hal-hal ini.

e. Bentuk-Bentuk *Agility* Lainnya

Empat bentuk *cryptographic agility* lainnya telah diidentifikasi dalam [77], tetapi kemungkinan besar tidak relevan bagi sebagian besar organisasi. Hal ini dapat disebabkan karena bentuk-bentuk tersebut terlalu maju, terlalu spesifik, atau terlalu berisiko.

Bentuk-bentuk *cryptographic agility* ini direkomendasikan untuk diterapkan apabila suatu organisasi benar-benar memahami sistem

kriptografi yang sedang mereka bangun dan benar-benar membutuhkan bentuk *agility* tersebut. Bentuk-bentuk tersebut meliputi: *security strength agility*, *retirement agility*, *composability agility*, dan *context agility*.

1) *Security strength agility* merujuk pada sistem yang secara dinamis mengubah parameter keamanan dari kriptografi berdasarkan konfigurasi sistem secara keseluruhan. Ini dapat menghemat banyak usaha bagi organisasi yang secara terus-menerus menerapkan sistem mereka dalam berbagai konteks yang memiliki kebutuhan berbeda. Di sisi lain, bagi (mayoritas) organisasi yang tidak berada dalam kondisi demikian, bentuk *agility* ini mungkin tidak layak untuk dikejar.

2) *Composability agility* merujuk pada pembangunan kriptografi sedemikian rupa sehingga dapat dengan mudah dikomposisikan dengan blok bangunan kriptografi lainnya. Bentuk *agility* ini sangat berguna dalam konteks migrasi PQC, karena komposisi kriptografi berbasis *hybrid-AND* diperkirakan akan digunakan sebagai solusi sementara. Namun, kami memperkirakan bahwa bentuk *agility* ini terutama akan digunakan oleh para ahli kriptografi yang benar-benar membangun sistem kriptografi tersebut.

3) *Retirement agility* merujuk pada sistem yang secara otomatis menghentikan penggunaan

algoritma kriptografi yang sudah usang atau tidak aman.

- 4) *Context agility* merujuk pada sistem kriptografi yang secara otomatis menentukan algoritma dan kekuatan keamanan yang harus digunakan berdasarkan konteks. Sebagai contoh, memilih versi algoritma yang lebih kuat berdasarkan klasifikasi data yang akan dienkripsi. Meskipun ini merupakan bentuk *agility* yang berguna, terdapat risiko dalam memilih parameter yang kurang aman secara tidak sengaja dan, oleh karena itu, perlindungan menjadi tidak memadai. Bagi sebagian besar organisasi yang tidak perlu sering memperbarui tingkat keamanan, lebih aman jika keputusan ini dibuat secara manual oleh manusia.

2. Pemilihan Strategi *Cryptographic Agility* yang Tepat
Meskipun solusi teknis, proses, dan kebijakan semuanya penting untuk membantu menjadikan suatu sistem lebih tangkas secara kriptografi, mengintegrasikan *cryptographic agility* ke dalam proses lain diperkirakan akan lebih mudah dilakukan oleh banyak organisasi dibandingkan dengan solusi teknis dan kebijakan. Di sisi lain, solusi teknis dapat menjadi cara yang sangat efektif untuk meningkatkan kecepatan perubahan kriptografi, sementara kebijakan dapat menjadi katalis yang baik untuk menegakkan *cryptographic agility*.

Menentukan langkah yang tepat dan tingkat *cryptographic agility* yang dibutuhkan untuk suatu sistem atau rantai pasok tertentu dapat menjadi tugas yang menantang. Meskipun demikian, memungkinkan untuk mempertimbangkan kecepatan perubahan kriptografi yang dibutuhkan berdasarkan permukaan risiko dari suatu aplikasi, persona organisasi, dan bentuk *cryptographic agility* yang diinginkan.

Untuk sistem lama yang sudah digunakan, solusi teknis seperti mengabstraksikan pemanggilan kriptografi dalam kode sulit untuk diterapkan secara retrospektif. Untuk aplikasi atau produk yang belum digunakan dalam produksi, sangat disarankan untuk menyelidiki kemungkinan memasukkan solusi *cryptographic agility* ke dalam desain produk atau aplikasi. Hal ini juga dapat didorong dengan memasukkan aspek-aspek ini ke dalam proses pengadaan sistem baru. Perlu dicatat bahwa kemungkinan untuk memasukkan solusi *cryptographic agility* secara teknis juga dibatasi oleh tingkat kematangan organisasi secara keseluruhan. Sebagai contoh, memperbarui parameter suatu algoritma kriptografi secara otomatis hanya dapat dilakukan jika organisasi memiliki inventaris kriptografi yang baik dan terkini.

Namun, untuk banyak bentuk *cryptographic agility* dan banyak organisasi, adanya sedikit penundaan dalam mengubah atau memperbarui kriptografi masih dapat diterima, selama durasinya dapat dijamin dalam batas yang besar. Sebagai contoh,

organisasi yang membutuhkan *compliance agility* dalam produk mereka untuk dirilis di negara lain tidak perlu dapat mengganti kriptografi dalam hitungan menit. Faktanya, peluncuran produk dapat memakan waktu berminggu-minggu, sehingga kemampuan untuk mengganti kriptografi baru dalam waktu beberapa minggu dapat dianggap cukup selama organisasi tersebut yakin tidak akan ada penundaan signifikan.

Di sisi lain, organisasi yang menginginkan *migration agility* untuk merespons kerentanan baru yang ditemukan dalam kriptografi mereka guna melindungi data pribadi yang mereka kelola perlu dapat merespons dengan jauh lebih cepat dan memiliki kepastian yang lebih tinggi terhadap potensi penundaan.

Secara keseluruhan, mengevaluasi aspek teknis, proses, dan kebijakan dari *cryptographic agility* serta mengujinya akan membantu dalam memperkirakan kelayakan durasi yang dibutuhkan. Jika penundaan dalam perubahan kriptografi tidak dapat diterima dengan mempertimbangkan toleransi risiko dan bentuk *agility* yang diinginkan, maka organisasi perlu menyelidiki lebih lanjut kemungkinan untuk meningkatkan efisiensi proses tersebut.

BAB VII

TAHAP PEMANTAUAN DAN EVALUASI



BAB VII

TAHAP PEMANTAUAN DAN EVALUASI

Bab ini memberikan informasi mengenai tujuan, landasan ilmiah serta langkah-langkah pemantauan dan evaluasi untuk memastikan migrasi ke PQC terimplementasi dengan baik sesuai rencana dan terkendali secara berkelanjutan

7.1 Tujuan

Tahap ini bertujuan untuk memastikan bahwa proses migrasi ke PQC berjalan dengan baik dan terdokumentasi secara lengkap, serta menilai kembali keamanan kriptografi yang digunakan agar tetap relevan dengan perkembangan kemampuan komputasi kuantum.

7.2 Landasan Ilmiah/Teknis

Tahap ini perlu dilakukan karena migrasi ke PQC bukan hanya sekadar mengganti algoritma lama, melainkan melibatkan perubahan besar yang memengaruhi sistem, data, infrastruktur, dan kebijakan keamanan organisasi. Tanpa pemantauan dan evaluasi yang sistematis, risiko kesalahan implementasi, ketidaksesuaian terhadap standar, serta munculnya celah keamanan baru dapat meningkat dan justru melemahkan perlindungan data. Selain itu, kemampuan komputer kuantum yang terus berkembang berpotensi membuat algoritma kriptografi yang saat ini aman menjadi tidak lagi efektif di masa depan. Oleh karena itu, evaluasi berkala diperlukan agar organisasi dapat memastikan sistemnya tetap tangguh terhadap ancaman baru, selalu menggunakan algoritma kriptografi yang relevan, serta mengikuti perkembangan standar dan teknologi keamanan terbaru.

7.3 Langkah-langkah

Berdasarkan [2], terdapat empat langkah yang dapat dilakukan pada tahap pemantauan dan evaluasi. Keempat langkah tersebut, yaitu:

7.3.1 Memverifikasi penerapan PQC dan memastikan kepatuhan terhadap standar yang berlaku.

Verifikasi penerapan PQC bertujuan untuk memastikan bahwa implementasi PQC telah dijalankan secara tepat. Hal-hal yang dapat dilakukan pada proses ini adalah sebagai berikut:

1. Melakukan penilaian mengenai seberapa efektif PQC yang sudah diterapkan dalam melindungi aset-aset prioritas. Penilaian ini dapat dilakukan oleh *migration lead* (pemimpin migrasi) bersama dengan *system implementor* (tim pelaksana sistem).
2. Melakukan pemeriksaan kebutuhan interoperabilitas dan operasional sistem dan mendokumentasikannya, agar dapat diketahui apakah kebutuhan tersebut telah dipenuhi oleh PQC yang diimplementasikan. Pemeriksaan ini dapat dilakukan oleh *system operator* (operator sistem), misalnya dengan memeriksa apakah sistem tetap bisa berfungsi dengan versi sebelumnya maupun dengan versi yang baru.
3. Melakukan pembaruan daftar inventori agar menggambarkan status/kondisi sistem yang baru. Daftar inventori yang telah diperbarui tersebut dipastikan kembali oleh pemimpin migrasi.

Dalam memastikan kepatuhan terhadap standar industri ataupun peraturan yang berlaku, maka organisasi perlu memperhatikan jenis data yang dikelola. Sebagai contoh sebagaimana disebutkan dalam [4], organisasi di sektor kesehatan dapat menilai migrasi ke PQC-nya berdasarkan standar HIPAA, sedangkan organisasi yang beroperasi di

Uni Eropa perlu memastikan kepatuhan terhadap NIS2. Beberapa standar tersebut mungkin sudah mencakup kegiatan yang berkaitan dengan PQC, misalnya seperti langkah-langkah antisipasi masa depan dan penilaian risiko secara berkala, yang menjadi alasan kuat untuk mulai merencanakan migrasi ke PQC. Selain memastikan kepatuhan terhadap standar, organisasi juga harus mendokumentasikan bagaimana proses migrasi ke PQC-nya mematuhi standar industri tersebut.

7.3.2 Menilai kebutuhan dan menyiapkan tenaga kerja yang dapat menerapkan PQC

Pada langkah ini, pemimpin migrasi menilai bagaimana cara mengoptimalkan tenaga kerja yang ada di organisasi untuk menerapkan dan memelihara PQC yang baru diperoleh atau dikembangkan. Proses penilaian ini mencakup koordinasi dengan *system owner* (pemilik sistem) atau operator sistem untuk mengidentifikasi kekurangan dalam alur kerja yang ada. Melalui penilaian tersebut, organisasi dapat menentukan apakah perlu untuk memberikan peningkatan pelatihan keamanan dalam rangka mendukung penerapan PQC yang baru, dan organisasi juga dapat menentukan apakah perlu dibutuhkan tenaga kerja tambahan untuk membantu pengoperasian atau proses migrasi ke PQC.

7.3.3 Membuat ukuran untuk memantau keberhasilan migrasi ke PQC.

Organisasi perlu menetapkan indikator atau ukuran kinerja yang jelas, terukur, dan berbasis data untuk memastikan keberhasilan migrasi ke PQC terpantau secara objektif. Melalui indikator tersebut, organisasi dapat mengetahui seberapa banyak informasi sensitif yang

telah terlindungi oleh PQC, sekaligus menilai efektivitas langkah-langkah yang telah dilakukan. Dalam memastikan tahap persiapan misalnya, indikator dapat difokuskan untuk memantau dampak komunikasi strategis terhadap keselarasan para pemangku kepentingan. Sedangkan dalam memastikan tahap perencanaan dan pelaksanaan migrasi, indikator dapat difokuskan untuk memantau jumlah sistem yang telah berhasil bermigrasi ke PQC.

7.3.4 Melakukan pemantauan dan pembaruan secara berkelanjutan

Pada langkah ini, pemimpin migrasi memiliki peran untuk terus memantau dan menilai perkembangan keamanan di organisasi, memperbarui daftar inventori, memantau kepatuhan terhadap standar baru, serta menilai lingkungan risiko organisasi. Setiap perubahan atau pembaruan yang terjadi dalam proses-proses tersebut penting untuk didokumentasikan. Dengan melakukan pemantauan dan pembaruan secara berkelanjutan, maka organisasi dapat terus memperbarui daftar inventori algoritma kriptografi agar seluruh perubahan sistem dan penggunaan algoritma tercatat dengan baik; organisasi dapat secara berkelanjutan mengukur kemajuan migrasi terhadap tujuan organisasi untuk memastikan setiap langkah yang diambil tetap sejalan dengan rencana strategis; serta organisasi dapat menjaga kesiapan dengan membuat proses untuk memantau perkembangan teknologi dan status risiko sehingga selalu siap menghadapi perubahan standar maupun potensi ancaman keamanan di masa mendatang.

BAB VIII

PENUTUP



BAB VIII

PENUTUP

Migrasi ke PQC merupakan investasi strategis jangka panjang untuk memastikan keamanan dan ketahanan siber nasional di tengah pesatnya perkembangan teknologi komputasi kuantum. Upaya ini membutuhkan komitmen lintas sektor, keselarasan kebijakan, serta dukungan berkelanjutan dari seluruh pemangku kepentingan, baik pemerintah, industri, akademisi, maupun penyedia layanan teknologi.

Panduan ini disusun sebagai titik awal untuk mendorong langkah kolaboratif yang terstruktur dan berkesinambungan dalam mempersiapkan infrastruktur digital nasional memasuki era pasca-kuantum. Dengan demikian, dokumen ini dapat menjadi rujukan awal dalam memandu perencanaan, pengambilan keputusan, dan penyusunan kebijakan yang lebih komprehensif guna memperkuat ekosistem keamanan siber nasional di masa depan.

Untuk memastikan keberlanjutan penyelenggaraan migrasi ke PQC tersebut, berikut beberapa rekomendasi strategis yang perlu dipertimbangkan sebagai tindak lanjut komprehensif dari panduan ini, yaitu:

1. Penyusunan dokumen Panduan *Quantum Incident Response* yang terintegrasi dengan rencana *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP) organisasi untuk memberikan tata laksana respons insiden yang terdokumentasi dan terstruktur. Hal ini karena migrasi PQC berpotensi menimbulkan risiko baru, seperti kesalahan konfigurasi yang menyebabkan *downtime* sistem, serangan yang memanfaatkan kelemahan implementasi, ataupun kelemahan baru dalam penerapan migrasi;
2. Melakukan analisis biaya terhadap manfaat terhadap perhitungan dampak ekonomi dari migrasi PQC untuk mendukung prioritas

kebijakan, efisiensi anggaran, serta pengambilan keputusan berbasis risiko;

3. Mengidentifikasi kompetensi kritis dan mengembangkan kapasitas SDM untuk menunjang proses migrasi PQC; dan
4. Membentuk koordinasi nasional migrasi PQC untuk menyelaraskan peta jalan dan praktik terbaik penyelenggaraan migrasi PQC.



LAMPIRAN A

DAFTAR PERIKSA LOKASI KRIPTOGRAFI

Tabel A.1 Sistem yang pada umumnya menggunakan kriptografi

Sistem	Deskripsi
Sistem Basis Data	Digunakan untuk penyimpanan kunci, dengan kriptografi digunakan di dalam enkripsi basis data.
Perangkat Lunak Virtualisasi	Kriptografi digunakan untuk melindungi mesin virtual. Contohnya adalah sistem dengan kunci yang dikelola oleh Vsphere Native Key Provider.
Infrastruktur internal untuk koneksi pengguna ke sistem	SSH (kunci SSH), VPN, koneksi Remote Desktop, SFTP (SSH <i>File Transfer Protocol</i>).
Infrastruktur internal antar sistem	Pengamanan koneksi antara server/aplikasi, workstation, dan sumber daya. Contohnya: jaringan internal, <i>SharePoint environment</i> , manajemen perangkat mobile, dan keamanan API.
Enkripsi Email	Misalnya S/MIME, atau startTLS dalam server surat elektronik.
Infrastruktur internal yang terhubung ke layanan eksternal	Koneksi antara server dan API eksternal. Koneksi ini hampir selalu menggunakan kriptografi untuk autentikasi dan enkripsi.
Infrastruktur internal yang terhubung ke pengguna eksternal	Koneksi server-client (misalnya TLS pada situs web).

Sistem	Deskripsi
Tanda tangan pada perangkat lunak	Aplikasi yang dikembangkan dan didistribusikan sering kali mencakup tanda tangan untuk membuktikan keaslian dan mencegah manipulasi.
PKI internal/eksternal (infrastruktur kunci publik)	PKI (sistem yang mengatur sertifikat). Kriptografi digunakan untuk keamanan tambahan (terutama pada rantai kunci dari <i>root</i> ke <i>intermediate</i> CA). Kunci tersebut terkadang memiliki masa berlaku tertentu. Dapat juga menjadi sumber yang baik untuk aplikasi yang menggunakan sertifikat.
Modul Keamanan Perangkat Keras (HSM)	Perangkat enkripsi di dalam sistem dan perangkat HSM menyimpan kunci utama (<i>master keys</i>). Dapat menjadi sumber yang baik untuk aplikasi yang memerlukan kunci.
Solusi Autentikasi	<i>Active Directory</i> (AD), sistem <i>two-factor authentication</i> (2FA), LDAP (<i>Lightweight Directory Access Protocol</i>).
Keamanan fisik dan kontrol akses	Pintu masuk, kartu akses, dll.
Kriptografi dalam aplikasi	Sebagian besar aplikasi menggunakan kriptografi. Contoh: manajemen kata sandi, enkripsi basis data, komunikasi

Sistem	Deskripsi
	terenkripsi, autentikasi pengguna.
IoT (Internet of Things)	Kamera pengawasan (CCTV), sistem alarm, kunci, kontrol akses (pintu dan gerbang).
ICS (Industrial Control System)	Sistem SCADA.
Sistem Cadangan (Backup System)	Baik cadangan kunci maupun kriptografi yang melindungi cadangan itu sendiri digunakan.
Penandatanganan PDF/Dokumen	Misalnya untuk tujuan hukum, seperti pada kontrak.
Produk Keamanan	Misalnya: tanda tangan yang digunakan dalam pemindai virus, kriptografi yang diterapkan pada sistem pencegahan/deteksi intrusi (IDS dan IPS).
Keamanan Jaringan	Misalnya WPA2 (WiFi).
Pembaruan Perangkat Lunak (<i>Software Updates</i>)	Misalnya pemeriksaan nilai <i>hash</i> untuk pembaruan otomatis.

Tabel A.2 Sumber Informasi tentang Sistem/Rincian Kriptografi

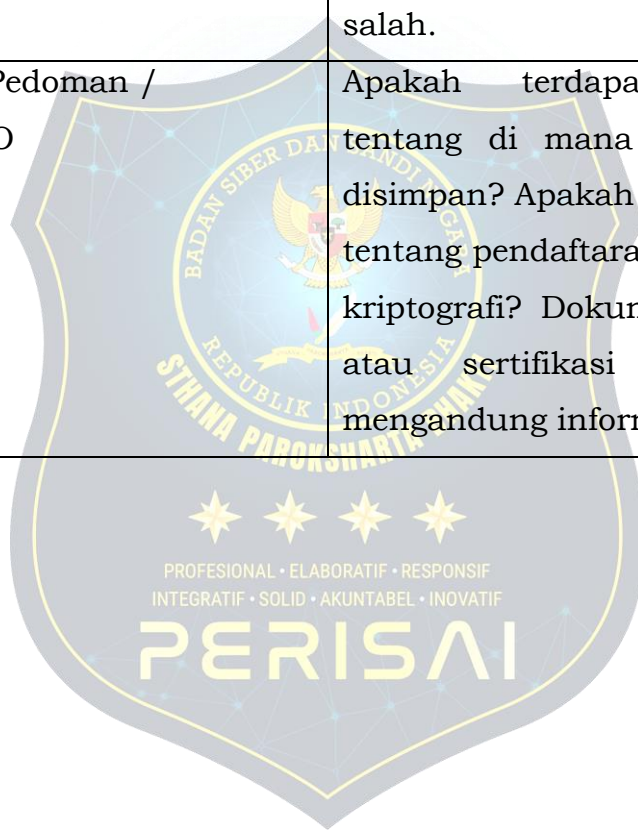
Sumber Sistem/Perangkat Lunak	Deskripsi
Perangkat lunak manajemen kunci (<i>Key management software</i>)	Keyvault, HSM terkelola Azure, AWS KMS, AWS Secrets Manager, <i>credential hub</i> . Pada beberapa produk, misalnya berbasis <i>cloud</i> , admin dapat memperoleh gambaran umum global tentang kunci yang digunakan dan disimpan.

Sumber Sistem/Perangkat Lunak	Deskripsi
Perangkat lunak HSM / tim kriptografi / tim PKI / perangkat lunak manajemen PKI	Sertifikat merupakan titik awal yang baik untuk mengetahui aplikasi mana yang menggunakan kriptografi, terutama kriptografi asimetris. Dapat juga digunakan untuk mengetahui di mana kunci disimpan atau dihasilkan — misalnya pada HSM, atau dikelola oleh tim PKI/HSM.
CMDB (<i>Configuration Management Database</i>)	Misalnya untuk Kubernetes (file konfigurasi). Konfigurasi untuk VPN, router, dan sebagainya sering kali mengandung informasi penting tentang algoritma atau kunci kriptografi yang digunakan.
Lingkungan pengembangan (<i>Development streets</i> / OTAP di NL), perangkat lunak CI/CD <i>pipeline</i>	Alat bantu untuk mendeteksi kerentanan dan menilai kualitas kode dapat digunakan untuk menilai penggunaan kriptografi yang tepat. Contohnya adalah SonarQube dan plugin kualitas GitLab.
Ikhtisar Arsitektur TI/Keamanan	Dokumen arsitektur keamanan dapat berisi informasi kriptografi, terutama untuk sistem terisolasi yang tidak mudah diakses oleh pemindai, seperti sistem di

Sumber Sistem/Perangkat Lunak	Deskripsi
	lingkungan offline atau sistem kontrol akses untuk gedung.
Pemindai jaringan (<i>Network scanners</i>)	Pemindai <i>port</i> dapat mengidentifikasi <i>port</i> yang digunakan serta memberikan informasi tentang kemungkinan penggunaan kriptografi. Contohnya, pemindai seperti Qualys SSL Test dapat memberikan informasi tentang konfigurasi TLS dari koneksi eksternal, misalnya untuk situs web HTTPS.
Pemindai kerentanan	Pemindai kerentanan dapat mengidentifikasi kriptografi yang tidak aman atau lemah. Beberapa pemindai juga dapat mengidentifikasi bentuk enkripsi yang digunakan oleh aplikasi. Contoh: pemindai dapat mengumpulkan informasi tentang versi TLS yang digunakan, cipher suite, dan algoritma tanda tangan. Contoh lainnya adalah Qualys, Nessus, atau Nexus.
Rencana Tanggapan Insiden	Prosedur pemulihan atau cadangan dapat memberikan wawasan tambahan tentang ketergantungan antar sistem,

Sumber Sistem/Perangkat Lunak	Deskripsi
	dan dalam beberapa kasus bahkan mencakup ketergantungan pada kunci kriptografi.
ITSM (<i>IT Service Management</i>)	Sebagian besar sistem <i>IT Service Management</i> (ITSM) tidak berisi informasi tentang kunci kriptografi. Namun, sering kali mengandung informasi berharga tentang tingkat sensitivitas komponen TI, seperti skor BIV/CIA (Keandalan, Integritas, Kerahasiaan).
Sistem ISMS (<i>Information Security Management System</i>)	<i>Information Security Management System</i> digunakan untuk mengidentifikasi dan mengelola risiko keamanan. Risiko terkait kriptografi, termasuk risiko kuantum, dapat menjadi bagian dari sistem ini.
(D)PIA (<i>Privacy Impact Assessment</i>)	Penilaian privasi dapat berisi informasi tentang tingkat sensitivitas data/aplikasi dan berapa lama data tersebut harus tetap terlindungi. Karena kriptografi merupakan langkah mitigasi terhadap risiko privasi, dokumen ini terkadang juga mencantumkan informasi

Sumber Sistem/Perangkat Lunak	Deskripsi
	mengenai penggunaan kriptografi.
Laporan Penilaian Keamanan / Pengujian Penetrasi (<i>Security Assessments / Pentest Reports</i>)	Pengujian penetrasi sering menemukan kerentanan yang berkaitan dengan algoritma kriptografi yang sudah usang atau konfigurasi kriptografi yang salah.
Kebijakan / Pedoman / Sertifikasi ISO	Apakah terdapat kebijakan tentang di mana kunci harus disimpan? Apakah ada kebijakan tentang pendaftaran penggunaan kriptografi? Dokumen kebijakan atau sertifikasi sering kali mengandung informasi tersebut.



LAMPIRAN B

ALGORITMA KRIPTOGRAFI PRIMITIF

Tujuan lampiran ini adalah untuk membantu *library developers* dalam memilih berbagai algoritma kriptografi primitif yang akan dimasukkan ke dalam *library*-nya serta membantu organisasi memahami primitif mana yang harus dipilih dan bagaimana mengonfigurasinya saat bermigrasi ke versi protokol yang aman terhadap kuantum. Lampiran ini juga dimaksudkan untuk membantu penemuan aset dan penilaian risiko. Karena audiens yang dituju dan informasi yang akan dibahas, diasumsikan bahwa pembaca memiliki pengetahuan dasar kriptografi yang memadai.

Tersedia daftar algoritma primitif kriptografi yang umum digunakan. Untuk setiap primitif, disajikan karakteristik utamanya dan apakah primitif tersebut menyediakan keamanan terhadap kuantum atau tidak. Tabel 1 menunjukkan daftar primitif kriptografi yang umum digunakan. Tabel ini bukan daftar yang lengkap, dan penting untuk mencatat semua algoritma kriptografi lain yang digunakan dalam organisasi.

Tabel 1 Algoritma kriptografi primitif yang umum digunakan

Simetrik	Asimetrik	Fungsi Hash	MAC	Stateful HBS
AES	RSA	SHA-2	HMAC	XMSS
ChaCha20	ECDH	SHA-3	CMAC	XMSS ^{MT}
	ECDSA	Blake	BLAKE2- MAC	LMS
	EdDSA		CBC-MAC	HSS

A. Algoritma Kriptografi Asimetris yang Rentan terhadap Serangan Kuantum

Pada bagian ini tercantum beberapa algoritma kriptografi asimetris yang umum digunakan tetapi rentan terhadap komputer kuantum.

1. ECDH

- Deskripsi: ECDH adalah varian kurva eliptik dari pertukaran kunci Diffie-Hellman [78].
- Ukuran Kunci Publik (bit): Bergantung pada kurva yang digunakan. Misalnya, menggunakan NIST P-256P menghasilkan kunci publik tidak terkompresi sepanjang 512 bit.
- Ukuran Kunci Privat (bit): Bergantung pada kurva yang digunakan. Misalnya, menggunakan NIST P-256P menghasilkan kunci privat sepanjang 256 bit.
- Ukuran *Ciphertext* (bit): Dua kali panjang kunci privat.
- Asumsi Kekuatan: *Decisional* Diffie-Hellman.
- Fungsi Kriptografi: ECDH digunakan untuk pertukaran kunci.
- Aplikasi: ECDH digunakan dalam protokol yang memerlukan pertukaran kunci.
- Komentar Lanjutan: ECDH digunakan dalam Protokol Signal.
- Dokumen Standardisasi: NIST SP 800-56A rev. 3 [78], ANSI X9.63 [79], SECG SEC-1 [80].
- Aman terhadap kuantum?: Tidak.

2. ECDSA

- Deskripsi: ECDSA adalah varian kurva eliptik dari Algoritma Tanda Tangan Digital yang distandardisasi oleh NIST [81].
- Ukuran Kunci Publik (bit): Bergantung pada kurva yang digunakan. Misalnya, menggunakan NIST P-256P

menghasilkan kunci publik tidak terkompresi sepanjang 512 bit.

- Ukuran Kunci Privat (bit): Bergantung pada kurva yang digunakan. Misalnya, menggunakan NIST P-256P menghasilkan kunci privat sepanjang 256 bit.
- Ukuran Tanda Tangan (bit): Dua kali panjang kunci privat.
- Asumsi Kekuatan: Logaritma Diskret.
- Fungsi Kriptografi: ECDSA digunakan untuk tanda tangan digital.
- Aplikasi: ECDSA digunakan di berbagai domain perangkat lunak maupun perangkat keras.
- Komentar Lanjutan: ECDSA adalah salah satu standar de facto untuk tanda tangan digital.
- Dokumen Standardisasi: FIPS 186-5 [81], ANSI X9.63 [82], ANSI X9.142 [83], ISO/IEC 14888-3:2018 [84], SECG SEC-1 [80].
- Aman terhadap kuantum?: Tidak.

3. EdDSA

- Deskripsi: EdDSA adalah varian kurva eliptik dari Algoritma Tanda Tangan Digital yang distandardisasi oleh NIST. Dalam EdDSA, digunakan kurva Edwards yang dipelintir (*twisted Edwards*), seperti Curve25519 [85].
- Ukuran Kunci Publik (bit): Bergantung pada kurva yang digunakan. Misalnya, menggunakan Curve25519 menghasilkan kunci publik tidak terkompresi sepanjang 512 bit.
- Ukuran Kunci Privat (bit): Bergantung pada kurva yang digunakan. Misalnya, menggunakan Curve25519 menghasilkan kunci privat sepanjang 256 bit.
- Ukuran Tanda Tangan (bit): Dua kali panjang kunci privat.
- Asumsi Kekuatan: Logaritma Diskret.

- Fungsi Kriptografi: EdDSA digunakan untuk tanda tangan digital.
- Aplikasi: EdDSA cocok untuk penggunaan umum.
- Komentar Lanjutan: EdDSA didasarkan pada tanda tangan Schnorr dan digunakan, misalnya, dalam GnuPG dan OpenSSH.
- Dokumen Standardisasi: FIPS 186-5 [81], RFC 8032 [85].
- Aman terhadap kuantum?: Tidak.

4. RSA

- Deskripsi: RSA adalah sandi asimetris yang sangat populer untuk penggunaan umum, berdasarkan kesulitan memfaktorkan sebuah bilangan menjadi dua bilangan prima [86].
- Ukuran Kunci Publik (bit): ≥ 2048 .
- Ukuran Kunci Privat (bit): Sekitar sebesar kunci publik.
- Ukuran *Ciphertext* (bit): Paling banyak sebesar kunci publik.
- Asumsi Kekuatan: Faktorisasi bilangan bulat.
- Fungsi Kriptografi: RSA digunakan untuk enkapsulasi kunci dan tanda tangan digital.
- Aplikasi: RSA digunakan di berbagai domain perangkat lunak maupun perangkat keras.
- Dokumen Standardisasi: FIPS 186-5 [81], NIST SP 800-56B rev.2 [87], RFC 8017 [86], ANSI X9.44 [88], PKCS #1 [86], ISO/IEC 14888-2:2008 [89], ISO/IEC 11770-3:2021 [90], SNI ISO/IEC 11770-3:2021 [91], ISO/IEC 9796-2:2010 [92], ISO/IEC 18033-2:2006 [93], SNI ISO/IEC 18033-2:2006 [94].
- Aman terhadap kuantum?: Tidak.

B. Algoritma Kriptografi Asimetris yang Aman terhadap Serangan Kuantum

Pada bagian ini tercantum beberapa algoritma kriptografi asimetris yang aman terhadap kuantum.

1. Pertukaran Kunci dan Mekanisme Enkapsulasi Kunci

Perlu diingat bahwa terdapat perbedaan dalam fungsi yang disediakan oleh pertukaran kunci dan mekanisme enkapsulasi kunci. Perbedaan ini berada di luar lingkup dokumen ini, sehingga primitif-primitif tersebut digabungkan bersama. Selain itu, perlu dicatat bahwa bagian ini tidak membahas kandidat NIST sebelumnya, SIKE, karena telah berhasil dikriptanalisis [95].

a. ML-KEM

- Deskripsi: ML-KEM, modifikasi atas CRYSTALS-Kyber, adalah KEM berbasis *lattice* dan merupakan KEM utama yang sekarang telah distandardisasi oleh NIST [6].
- Ukuran Parameter (dalam bit): Ukuran panjang kunci dan ukuran *ciphertext* ML-KEM:

Security category	Parameter set	Panjang Kunci Publik	Panjang Kunci Privat	Ukuran Ciphertext
1	ML-KEM-512	6.400	13.056	6.144
3	ML-KEM-768	9.472	19.200	8.704
5	ML-KEM-1024	12.544	25.344	12.544

- Asumsi Kekuatan: *Module Learning with Errors* (MLWE).
- Komentar Lanjutan: NIST merekomendasikan ML-KEM-768 (Kategori 3) sebagai *default*. Badan keamanan Eropa juga merekomendasikan setidaknya kategori 3.
- Dokumen Standardisasi: FIPS 203 [6].
- Aman terhadap kuantum?: Ya.

b. BIKE

- Deskripsi: BIKE [96] adalah KEM berbasis kode yang menjadi salah satu kandidat pada Putaran 4 kompetisi NIST. Namun, BIKE tetapi tidak terpilih pada putaran tersebut dan tidak distandardkan oleh NIST.
- Ukuran Parameter (dalam bit): Dinyatakan mampu mencapai kategori keamanan tertentu menurut NIST:

Security category	Parameter set	Panjang Kunci Publik	Panjang Kunci Privat	Ukuran Ciphertext
1	BIKE-L1	12.323	2.244	12.579
3	BIKE-L3	24.659	3.346	24.915
5	BIKE-L5	40.973	4.640	41.229

- Asumsi Kekuatan: Masalah *Quasi-Cyclic Syndrome Decoding*.
- Komentar Lanjutan: Kandidat Putaran 4 NIST.
- Dokumen Standardisasi: Situs web BIKE [96].
- Aman terhadap kuantum?: Ya.

c. Classic McEliece

- Deskripsi: Classic McEliece [97] adalah KEM berbasis kode yang konservatif dan didasarkan pada kriptosistem McEliece tahun 1978 [98]. Classic McEliece menjadi salah satu kandidat pada Putaran 4 kompetisi NIST. Namun, Classic McEliece tetapi tidak terpilih pada putaran tersebut dan tidak distandardkan oleh NIST. Meskipun demikian, algoritma ini sedang dipertimbangkan untuk distandardisasi oleh ISO.
- Ukuran Parameter (dalam bit): Dinyatakan mampu mencapai kategori keamanan tertentu menurut NIST:

Security category	Parameter set	Panjang Kunci Publik	Panjang Kunci Privat	Ukuran Ciphertext
1	Classic-McEliece-348864	2.088.960	51.936	768
3	Classic-McEliece-460896	4.193.280	108.864	1,248
5	Classic-McEliece-6688128	8.359.936	111.456	1.664
	Classic-McEliece-6960119	8.378.552	111.584	1.552
	Classic-McEliece-8192128	10.862.592	112.960	1.664

- Asumsi Kekuatan: Masalah *Syndrome Decoding* (keamanan pesan) dan pemulihan kode Goppa (keamanan kunci).
- Komentar Lanjutan: Classic McEliece membutuhkan ukuran kunci yang sangat besar tetapi *ciphertext* kecil, sehingga kemungkinan tidak dapat digunakan untuk sistem penyimpanan rendah seperti kartu pintar atau IoT. Namun demikian, algoritma ini telah bertahan dari kriptanalisis besar selama puluhan tahun dan badan keamanan Eropa yakin akan keamanannya.
- Dokumen Standardisasi: Situs Classic McEliece [97].
- Aman terhadap kuantum?: Ya.

d. FrodoKEM

- Deskripsi: FrodoKEM adalah KEM berbasis *lattice* yang mendukung konstruksi yang konservatif namun praktis. Algoritma ini tidak akan distandardisasi oleh NIST [99].
- Ukuran Parameter (dalam bit): Dinyatakan mampu mencapai kategori keamanan tertentu menurut NIST:

Security category	Parameter set	Panjang Kunci Publik	Panjang Kunci Privat	Ukuran Ciphertext
1	FrodoKEM-640-AES	76.928	159.104	78.016
3	FrodoKEM-976-AES	125.056	250.368	126.336
5	FrodoKEM-1344-AES	172.160	344.704	173.568

- Asumsi Kekuatan: *Plain Learning with Errors* (LWE).
- Komentar Lanjutan: Saat ini, FrodoKEM tidak akan distandardisasi oleh NIST, tetapi sedang dipertimbangkan untuk distandardisasi oleh ISO, dan direkomendasikan oleh badan keamanan Eropa.
- Dokumen Standardisasi: Situs FrodoKEM [99].
- Aman terhadap kuantum?: Ya.

e. HQC

- Deskripsi: HQC [100] adalah KEM berbasis kode yang merupakan salah satu kandidat pada Putaran 4 kompetisi NIST. Berdasarkan proses evaluasi yang melibatkan umpan balik publik dan kajian internal, HQC ditetapkan sebagai satu-satunya algoritma KEM pada putaran tersebut yang akan distandardkan oleh NIST

- Ukuran Parameter (dalam bit): Dinyatakan mampu mencapai kategori keamanan tertentu menurut NIST:

Security category	Parameter set	Panjang Kunci Publik	Panjang Kunci Privat	Ukuran Ciphertext
1	HQC-L1	17.992	448	35.976
3	HQC-L2	36.176	512	72.336
5	HQC-L3	57.960	576	115.880

- Asumsi Kekuatan: *Decisional Quasi-Cyclic Syndrome Decoding Problem*.
- Komentar Lanjutan: HQC adalah kandidat Putaran 4 NIST. Algoritma ini dapat dianggap sebagai analog berbasis kode dari ML-KEM.
- Dokumen Standardisasi: Situs HQC [100].
- Aman terhadap kuantum?: Ya.

2. Algoritma Tanda Tangan Digital *Stateful*

a. LMS and HSS

- Deskripsi: Leighton-Micali Signatures adalah skema tanda tangan berbasis *hash* dengan status yang menggunakan LM-OTS untuk tanda tangan satu kali dan didasarkan pada pohon *hash* Merkle. HSS adalah varian yang memiliki beberapa pohon *hash* [101].
- Ukuran Kunci Publik (bit): 384-448 (hanya untuk LMS, tidak ada parameter standar untuk jumlah pohon *hash* pada HSS).
- Ukuran Kunci Privat (bit): Beberapa kunci privat satu kali yang bergantung pada banyak variabel dan asumsi, sulit untuk diperkirakan.
- Ukuran Tanda Tangan (bit): 6240-74592 (hanya untuk LMS, tidak ada parameter standar untuk jumlah pohon *hash* pada HSS).

- Asumsi Kekuatan: Tahan terhadap tabrakan (*Collision Resistance*).
- Komentar Lanjutan: Manajemen status yang hati-hati sangat penting dan merupakan isu utama dari algoritma ini.
- Dokumen Standardisasi: SP800-208 [102], RFC 8554 [103].
- Aman terhadap kuantum?: Ya.

b. XMSS dan XMSS^{MT}

- Deskripsi: *eXtended Merkle Signature Scheme* (XMSS) adalah skema tanda tangan berbasis *hash* dengan status yang menggunakan WOTS+ untuk tanda tangan satu kali dan didasarkan pada pohon *hash* Merkle. XMSSMT adalah varian yang memiliki beberapa pohon *hash* [102].
- Ukuran Kunci Publik (bit): 384-1024.
- Ukuran Kunci Privat (bit): Beberapa kunci privat satu kali yang bergantung pada banyak variabel dan asumsi.
- Ukuran Tanda Tangan (bit): 11.936-221.504.
- Asumsi Kekuatan: Tahan terhadap tabrakan (*Collision Resistance*).
- Komentar Lanjutan: Manajemen status yang hati-hati sangat penting dan merupakan isu utama dari algoritma ini.
- Dokumen Standardisasi: SP800-208 [102], RFC 8391 [104].
- Aman terhadap kuantum?: Ya.

3. Algoritma Tanda Tangan Digital *Stateless*

a. ML-DSA

- Deskripsi: ML-DSA, modifikasi atas CRYSTAL-Dilithium, adalah skema tanda tangan berbasis *lattice*

dan merupakan skema tanda tangan utama yang sekarang telah distandardisasi oleh NIST [7].

- Ukuran Parameter (dalam bit): Ukuran kunci dan tanda tangan ML-DSA:

Security category	Parameter set	Panjang Kunci Publik	Panjang Kunci Privat	Ukuran Ciphertext
1	ML-DSA-44	10.496	20.480	19.360
3	ML-DSA-65	15.616	32.256	26.472
5	ML-DSA-87	20.736	39.168	37.016

- Asumsi Kekuatan: *Module Small Integer Problem* (MSIS) dan *Module Learning with Errors* (MLWE).
- Komentar Lanjutan: ML-DSA merupakan padanan tanda tangan digital dari ML-KEM kunci publik, yang juga distandardisasi oleh NIST. Badan keamanan Eropa merekomendasikan penggunaan parameter yang sesuai dengan kategori keamanan minimal 3.
- Dokumen Standardisasi: FIPS 204 [7].
- Aman terhadap kuantum?: Ya.

b. FN-DSA (Falcon)

- Deskripsi: FN-DSA, juga dikenal sebagai Falcon [105], adalah skema tanda tangan berbasis *lattice* yang dipilih oleh NIST untuk distandardisasi.
- Ukuran Parameter (dalam bit): Dinyatakan mampu mencapai kategori keamanan tertentu menurut NIST:

Security category	Parameter set	Panjang Kunci Publik	Panjang Kunci Privat	Ukuran Ciphertext
1	Falcon-padded-512	7.176	10.248	5.328
5	Falcon-padded-1024	14.344	18.440	10.240

- Asumsi Kekuatan: Masalah *Short Integer Solution* (SIS) pada *lattice* NTRU.
- Komentar Lanjutan: Skema tanda tangan utama NIST adalah ML-DSA. Falcon menggunakan aritmetika titik mengambang, yang tidak umum dalam kriptografi. Secara khusus, dianggap sulit untuk mengimplementasikannya secara aman agar tahan terhadap serangan side-channel dan tidak direkomendasikan oleh badan keamanan Eropa.
- Dokumen Standardisasi: Situs web Falcon [105].
- Aman terhadap kuantum?: Ya.

c. SLH-DSA

- Deskripsi: SLH-DSA, modifikasi atas SPHINCS+, adalah skema tanda tangan berbasis *hash* tanpa status yang sekarang telah distandardisasi oleh NIST [8].
- Ukuran Parameter (dalam bit): Ukuran kunci dan tanda tangan SLH-DSA:

Security category	Parameter set	Panjang Kunci Publik	Panjang Kunci Privat	Ukuran Ciphertext
1	SLH-DSA-SHA2-128s	256	512	62.848
3	SLH-DSA-SHA2-192s	384	768	129.792
5	SLH-DSA-SHA2-256s	512	1.024	238.336

- Asumsi Kekuatan: Tahan terhadap *second-preimage*.
- Komentar Lanjutan: Skema tanda tangan utama NIST adalah ML-DSA.
- Dokumen Standardisasi: FIPS 205 [8].
- Aman terhadap kuantum?: Ya.

C. Algoritma Kriptografi Simetris

Berikut adalah beberapa kriptografi algoritma simetris yang memiliki aman terhadap komputer kuantum.

1. Algoritma Simetrik

a. AES

- Deskripsi: AES adalah *block cipher* yang distandardisasi oleh NIST [106].
- Panjang Kunci yang Didukung (bit): 128, 192, 256.
- Aplikasi: AES digunakan di berbagai implementasi perangkat lunak maupun perangkat keras.
- Komentar Lanjutan: AES merupakan standar *de facto* untuk sandi simetris.
- Dokumen Standardisasi: FIPS 197 [106], ISO/IEC 18033-3:2010 [107], SNI ISO/IEC 18033-3:2010 [108].

- Aman terhadap kuantum?: Ya.

b. ChaCha20

- Deskripsi: ChaCha20 adalah *stream cipher* yang biasanya digabungkan dengan Poly1305 [109] ketika digunakan dalam TLS.
- Panjang Kunci yang Didukung (bit): 128, 256.
- Aplikasi: ChaCha20 digunakan dalam berbagai protokol seperti TLS dan S/MIME (umumnya di domain perangkat lunak).
- Komentar Lanjutan: ChaCha20 dikenal karena kecepatan dan kesederhanaan implementasinya.
- Dokumen Standardisasi: RFC 8439 [109].
- Aman terhadap kuantum?: Ya.

2. Fungsi Hash

a. SHA-3 (Keccak)

- Deskripsi: SHA-3, juga dikenal sebagai Keccak, adalah sekumpulan fungsi *hash* yang distandardisasi oleh NIST.
- Ukuran Output Hash (bit): 224, 256, 384, 512.
- Aplikasi: SHA-3 digunakan di berbagai domain perangkat lunak maupun perangkat keras.
- Komentar Lanjutan: SHA-3 merupakan standar *de facto* untuk algoritma fungsi *hash*. SHA-3 adalah penerus SHA-2 dan SHA-1. Baik SHA-3 maupun SHA-2 direkomendasikan, sementara SHA-1 tidak aman dan sudah tidak digunakan lagi.
- Dokumen Standardisasi: FIPS 180-4 [110], NIST SP 800-107 Rev. 1 [111], RFC 6234 [112], ISO/IEC 10118-3:2018 [113] (SHA2), FIPS 180-4 [110], FIPS 202 [114],

NIST SP 800-107 Rev. 1 [111], ISO/IEC 10118-3:2018 [113] (SHA3).

- Aman terhadap kuantum?: Ya.

b. SHA-2

- Deskripsi: SHA-2 adalah sekumpulan fungsi *hash* yang distandardisasi oleh NIST dan awalnya dirancang oleh NSA [NIST02], yang menggantikan SHA-1.
- Ukuran Output *Hash* (bit): 224, 256, 384, 512.
- Aplikasi: SHA-2 digunakan di berbagai domain perangkat lunak maupun perangkat keras.
- Komentar Lanjutan: SHA-3 adalah penerus SHA-2 dan SHA-1. Baik SHA-3 maupun SHA-2 direkomendasikan, sementara SHA-1 tidak aman dan sudah tidak digunakan lagi.
- Dokumen Standardisasi: FIPS 180-4 [110], NIST SP 800-107 Rev. 1 [111], RFC 6234 [112], ISO/IEC 10118-3:2018 [113] (SHA2), FIPS 180-4 [110], FIPS 202 [114], NIST SP 800-107 Rev. 1 [111], ISO/IEC 10118-3:2018 [113] (SHA3).
- Aman terhadap kuantum?: Ya.

c. BLAKE2

- Deskripsi: BLAKE2 adalah fungsi *hash* yang memiliki kinerja perangkat lunak lebih baik dibandingkan SHA-3 [115]. Fungsi ini tersedia dalam dua varian, BLAKE2b dan BLAKE2s.
- Ukuran Output *Hash* (bit): ≤ 512 (BLAKE2b), ≤ 256 (BLAKE2s).
- Aplikasi: BLAKE2 digunakan baik dalam konteks kriptografi maupun non-kriptografi.

- Komentar Lanjutan: SHA-3 dan SHA-2 direkomendasikan. BLAKE2 telah dianalisis jauh lebih sedikit dibandingkan SHA-3 dan SHA-2.
- Dokumen Standardisasi: RFC 7693 [116].
- Aman terhadap kuantum?: Ya, jika menggunakan BLAKE2b.

3. *Message Authentication Codes* (MAC)

a. CMAC

- Deskripsi: CMAC adalah cara lain untuk membangun MAC dari *block cipher* [117].
- Ukuran Kunci MAC (bit): Bergantung pada *block cipher* yang dipilih.
- Ukuran Output MAC (bit): Bergantung pada *block cipher* yang dipilih.
- Aplikasi: CMAC tidak digunakan seluas CBC-MAC.
- Komentar Lanjutan: Disarankan digunakan dengan AES. CMAC-AES direkomendasikan oleh NIST sebagai pengganti CBC-MAC.
- Dokumen Standardisasi: NIST SP 800-38B [118], RFC 4493 [117], ISO/IEC 9797-1:2011 [119], SNI ISO/IEC 9797-1:2011 [120].
- Aman terhadap kuantum?: Ya, jika fungsi *hash* yang mendasarinya aman terhadap kuantum.

b. HMAC

- Deskripsi: HMAC adalah cara untuk membangun MAC dari fungsi *hash* [121].
- Ukuran Kunci MAC (bit): Sesuai kebutuhan.
- Ukuran Output MAC (bit): Bergantung pada fungsi *hash* yang dipilih.

- Aplikasi: HMAC digunakan dalam protokol IPsec, SSH, dan TLS.
- Komentar Lanjutan: HMAC dapat mengalami masalah kinerja.
- Dokumen Standardisasi: FIPS 198-1 [122], RFC 2104 [121].
- Aman terhadap kuantum?: Ya, jika fungsi *hash* yang mendasarinya aman terhadap kuantum.

c. KMAC

- Deskripsi: KMAC adalah MAC dengan ukuran output yang dapat bervariasi berdasarkan SHA-3 [123].
- Ukuran Kunci MAC (bit): ≥ 128 .
- Ukuran Output MAC (bit): Bervariasi.
- Aplikasi: Autentikasi simetris.
- Komentar Lanjutan : -
- Dokumen Standardisasi: NIST SP 800-185 [123].
- Aman terhadap kuantum?: Ya.

d. BLAKE3-MAC

- Deskripsi: BLAKE2 tidak perlu menggunakan transformasi HMAC untuk digunakan sebagai MAC karena sudah termasuk mekanisme penguncian kunci [116].
- Ukuran Kunci MAC (bit): Sesuai kebutuhan.
- Ukuran Output MAC (bit): 512 (BLAKE2b), ≤ 256 (BLAKE2s).
- Aplikasi: BLAKE2-MAC digunakan di domain perangkat lunak.
- Komentar Lanjutan: HMAC-SHA-2 dan KMAC direkomendasikan. BLAKE2-MAC lebih cepat daripada

HMAC karena memiliki mekanisme penguncian kunci bawaan.

- Dokumen Standardisasi: RFC 7693 [116].
- Aman terhadap kuantum?: Ya, jika menggunakan BLAKE2b.

e. CBC-MAC

- Deskripsi: CBC-MAC adalah cara untuk membangun MAC dari *block cipher* [119], [120].
- Ukuran Kunci MAC (bit): Bergantung pada *block cipher* yang dipilih.
- Ukuran Output MAC (bit): Bergantung pada *block cipher* yang dipilih.
- Aplikasi: CBC-MAC biasanya digunakan untuk pesan dengan panjang tetap.
- Komentar Lanjutan: CBC-MAC telah digantikan oleh CMAC.
- Dokumen Standardisasi: ISO/IEC 9797-1 [119], SNI ISO/IEC 9797-1:2011 [120].
- Aman terhadap kuantum?: Ya, jika *block cipher* yang digunakan aman terhadap kuantum, tetapi disarankan menggunakan HMAC atau CMAC.

DAFTAR REFERENSI

- [1] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 443, 2021.
- [2] C. Gidney, "How to factor 2048 bit RSA integers with less than a million noisy qubits," *Quantum Physics*, 2025.
- [3] AIVD, CWI and TNO, The PQC Migration Handbook Guidelines for Migrating to Post-Quantum Cryptography Revised and Extended Second Edition, 2024.
- [4] PQCC, Post-Quantum Cryptography (PQC) Migration Radmap, The MITRE Corporation, 2025.
- [5] M. de Vries, S. E. Bootsma, V. A. Dunning and M. J. van Vliet, "TNO 2024 R10707- 19 Juli 2024 Quantum risicomethologie voor cryptografie," TNO Public, 2024.
- [6] NIST, FIPS 203 Federal Information Processing Standards Publications Module-Lattice-Based Key-Encapsulation Mechanism Standard, Gaithersburg, MD: NIST, 2024.
- [7] NIST, FIPS 204 Module-Lattice-Based Digital Signature Standard, Gaithersburg, MD: NIST, 2024.
- [8] NIST, FIPS 205 Stateless Hash-Based Digital Signature Standard, Gaithersburg, MD: NIST, 2024.
- [9] A. T. Olutimehin, S. A. Joseph, A. J. Ajayi, O. C. Metibemu, A. Y. Balogun and O. O. Olaniyi, "Future-Proofing Data: Assessing the Feasibility of Post Quantum Cryptographic Algorithms to Mitigate 'Harvest Now, Decrypt Later' Attacks," *Archives of Current Research International*, vol. 25, no. 3, pp. 60-80, 2025.
- [10] W. Newhouse , M. Souppaya, D. McGrew, D. Hook, W. Barker, A. Dames, R. Garcia, C. Brown, V. Soukharev, E. Gervis, P. Kampanakis, P. Lafrance, E. Kim, C. Lee, A. Hu and M. Manzano, NIST SP 1800-38B Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery Volume B: Approach, Architecture, and Security Characteristics of Public

Key Application Discovery Tools, Gaithersburg, MD: NCCoE NIST, 2023.

- [11] NIST, "What Is Post-Quantum Cryptography?," 11 June 2025. [Online]. Available: <https://www.nist.gov/cybersecurity/what-post-quantum-cryptography>.
- [12] Quantum-Readiness Working Group (QRWG), Canadian National Quantum-Readiness BEST PRACTICES AND GUIDELINES, 2024.
- [13] Marin, "Harvest Now, Decrypt Later (HNDL) Risk," 8 June 2023. [Online]. Available: <https://postquantum.com/post-quantum/harvest-now-decrypt-later-hndl/>.
- [14] A. Ipsen, "Think your sensitive data is safe until quantum arrives? It's not.," 16 June 2025. [Online]. Available: <https://www.pluralsight.com/resources/blog/cybersecurity/quantum-hndl-present-threat>.
- [15] "Venona: Soviet Espionage and The American Response 1939-1957," 1996.
- [16] R. L. Benson, "THE VENONA STORY," Center for Cryptologic History.
- [17] Wikipedia, "Venona project," [Online]. Available: https://en.wikipedia.org/wiki/Venona_project?utm_source=chatgpt.com#cite_note-FOOTNOTEBenson200134-4.
- [18] Wikipedia, "Ultra (cryptography)," [Online]. Available: [https://en.wikipedia.org/wiki/Ultra_\(cryptography\)](https://en.wikipedia.org/wiki/Ultra_(cryptography)).
- [19] D. Anderson, "The Influence of ULTRA in the Second World War," 26 November 1996. [Online]. Available: https://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.
- [20] Reuters, "Europol body: Banks should prepare for quantum computer risk now," 7 February 2025. [Online]. Available: <https://www.reuters.com/technology/cybersecurity/europol-body-banks-should-prepare-quantum-computer-risk-now-2025-02-07/>.

- [21] A. Herman, "Can Crypto Still Save the World," 27 June 2022. [Online]. Available: <https://www.hudson.org/economics/can-crypto-still-save-the-world>.
- [22] A. W. Butler, A. Herman and Q. A. Initiative, Prosperity at Risk: The Quantum Computer Threat to the US Financial System, Washington, D.C: Hudson Institute, 2023.
- [23] J. Jurgens, I. Kohn and C. Soutar, Transitioning to a Quantum-Secure Economy White Paper, World Economic Forum, 2022.
- [24] SSL.com, "Mengamankan PKI dengan Solusi Tahan Kuantum," [Online]. Available: <https://www.ssl.com/id/artikel/ancaman-kuantum-pki-security-pqc-solutions/>.
- [25] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, vol. 41, S. Review, Ed., 1999, p. 303–332.
- [26] Post-Quantum.com, "Trust Now, Forge Later (TNFL) – The Overlooked Quantum Threat," [Online]. Available: <https://postquantum.com/post-quantum/trust-now-forge-later/> PostQuantum.com.
- [27] R. Bavdekar, E. J. Chopde, A. Agrawal, A. Bhatia and K. Tiwari, Post quantum cryptography: A review of techniques, challenges and standardizations, Proc. 2023 Int. Conf. Information Networking (ICOIN), 2023, p. 146–151.
- [28] N. Kilber, D. Kaestle and S. Wagner, "Cybersecurity for quantum computing," 2021.
- [29] G. P. Panjaitan, "Sistem Kriptografi Kuantum".
- [30] D. Moody, R. Perlner, A. Regenscheid, A. Robinson and D. Cooper, NIST Internal Report NIST IR 8547.ipd Transition to Post-Quantum Cryptography Standards, Gaithersburg, MD: NIST, 2024.
- [31] NIST, SP 800-56Cr2 Recommendation for Key-Derivation Methods in Key-Establishment Schemes, Gaithersburg, MD: NIST, 2020.

- [32] NIST, SP 800-227 Recommendations for Key-Encapsulation Mechanisms, Gaithersburg, MD: NIST, 2025.
- [33] MasterCard, N. T. University and PQStation, Migration to Post-Quantum Cryptography, 2024.
- [34] M. Mosca and M. Piani, "Quantum Threat Timeline Report," 2023. [Online]. Available: <https://globalriskinstitute.org/publications/2023-quantum-threat-timeline-report/>.
- [35] AIVD, "AIVD-jaarverslag 2023," 2023. [Online]. Available: <https://www.aivd.nl/onderwerpen/jaarverslagen/documenten/jaarverslagen/2024/04/22/jaarverslag-2023>.
- [36] AIVD, MIVD and NCTV, "Dreigingsbeeld Statelijke Actoren 2," 2022. [Online]. Available: <https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2>.
- [37] I. Kong, M. Janssen and N. Bharosa, "Organizational Readiness Model for Quantum-safe Transition," [Online]. Available: <https://hapkido.tno.nl/deliverables/organizational-readiness-model-quantum/>. [Accessed 28 October 2025].
- [38] "Executive Office of the President of the United States. Report on Post-Quantum Cryptography as required by the Quantum Computing Cybersecurity Preparedness Act, Public Law No 117-260," 2024. [Online]. Available: [url: https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf](https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf).
- [39] A. Biryukov, D. Dinu, D. Khovratovich and S. Josefsson, "IRTF RFC 9106 Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications," 2021. [Online]. Available: <https://datatracker.ietf.org/doc/rfc9106/>.
- [40] G. Alagic, M. Bros, P. Ciadoux, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, H. Silberg, D. Smith-Tone and N. Waller, NIST IR 8545 Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process, Gaithersburg, MD: NIST, 2025.

- [41] NIST, SP 800-208 Recommendation for Stateful Hash-Based Signature Schemes, Gaithersburg, MD: NIST, 2020.
- [42] S. Jaques, M. Naehrig, M. Roetteler and F. Virdia, "Implementing Grover Oracles for Quantum Key Search on AES and LowMC," *Lecture Notes in Computer Science*, vol. 12106, pp. 280-310, 2020.
- [43] E. Rescorla, "RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3," 2018.
- [44] P. Eronen and H. Tschofenig, RFC 4279: Pre-Shared Key Ciphersuites for Transport Layer Security (TLS), 2005.
- [45] M. Badra, RFC 5487: Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode, 2009.
- [46] D. Stebila, S. Fluhrer and S. Gueron, Hybrid key exchange in TLS 1.3 draft-ietf-tls-hybrid-design-16, 2026.
- [47] T. Reddy and H. Tschofenig, PQ/T Hybrid KEM: HPKE with JOSE/COSE draft-reddy-cose-jose-pqc-hybrid-hpke-06, 2025.
- [48] M. C. Lonvick and T. Ylonen, RFC 4251 The Secure Shell (SSH) Protocol Architecture, 2006.
- [49] T. Ylonen and C. Lonvick, RFC 4252 The Secure Shell (SSH) Authentication Protocol, 2006.
- [50] T. Ylonen and C. Lonvick, RFC 4253 The Secure Shell (SSH) Transport Layer Protocol, 2006.
- [51] T. Ylonen and C. Lonvick, The Secure Shell (SSH) Connection Protocol, 2006.
- [52] D. Stebila and J. Green, RFC 5656 Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer, 2009.
- [53] D. Bider, RFC 8332 Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol, 2018.
- [54] D. Bider, RFC 8308 Extension Negotiation in the Secure Shell (SSH) Protocol, 2018.

- [55] P. Kampanakis, D. Stebila and T. Hansen, Internet-Draft PQ/T Hybrid Key Exchange with ML-KEM in SSH draft-ietf-sshm-mlkem-hybrid-kex-04, 2026.
- [56] M. Friedl, J. Mojzis and S. Josefsson, Internet-Draft Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512 draft-ietf-sshm-ntruprime-ssh-00, 2024.
- [57] R. Housley, IETF RFC 5652 Cryptographic Message Syntax (CMS), 2009.
- [58] R. Housley, IETF RFC 8933 Update to the Cryptographic Message Syntax (CMS) for Algorithm Identifier Protection, 2020.
- [59] R. Housley, J. Gray and T. Okubo, IETF RFC 9629 Using Key Encapsulation Mechanism (KEM) Algorithms in the Cryptographic Message Syntax (CMS), 2024.
- [60] K. D. Gillmor, B. Hoeneisen and A. Melnikov, IETF RFC 8551 Header Protection for Cryptographically Protected Email, 2025.
- [61] OQS S/MIME, "Open Quantum Safe CMS and S/MIME Fork," October 2024. [Online]. Available: <https://openquantumsafe.org/applications/>.
- [62] P. Wouters, D. Huigens, J. Winter and Y. Niibe, "RFC 9580 OpenPGP," Internet Engineering Task Force (IETF), 2024.
- [63] N. Mavrogiannopoulos and S. Josefsson, "The GNU Privacy Guard," [Online]. Available: <https://www.gnupg.org/index.html>.
- [64] S. Frankel and S. Krishnan, RFC 6071 IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, Internet Engineering Task Force (IETF), 2011.
- [65] C. Kaufman, E. P. Hoffman, Y. Nir, P. Eronen and T. Kivinen, RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2), 2014.
- [66] S. Fluhrer, P. Kampanakis, D. McGrew and V. Smyslov, RFC 8784 Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security, 2020.

- [67] ETSI, TR 103 617 Quantum-Safe Virtual Private Networks, Valbonne: FR ETSI, 2018.
- [68] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley and W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2008.
- [69] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley and W. Polk, RFC 5280 Internet X.509 Public Key Infrastructure Certificate, 2008.
- [70] ITU-T, ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and Interconnection – The Directory: Public-key and, ITU-T, 2019.
- [71] International Telecommunication Union (ITU), ITU-T X.509 (2019) Cor. 2 Information technology - Open Systems Interconnection - The Directory Public-key and attribute certificate frameworks Technical Corrigendum 2, ITU, 2023.
- [72] A. Truskovsk, D. v. Geest, S. Fluhrer, P. Kampanakis, M. Ounsworth and S. Mister, Multiple Public-Key Algorithm X.509 Certificates, 2023.
- [73] M. Ounsworth, J. Gray, M. Pala, J. Klaussner and S. Fluhrer, LAMPS Internet-Draft Composite ML-DSA for use in Internet PKI draft-ietf-lamps-pq-composite-sigs-02, 2025.
- [74] M. Ounsworth, J. Gray, M. Pala, J. Klaussner and S. Fluhrer, "Composite ML-KEM for use in X.509 Public Key Infrastructure draft-ietf-lamps-pq-composite-kem-10," 24 November 2025. [Online]. Available: <https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/>.
- [75] Dutch National Cyber Security Centre, "Het crypto-agilitymonster op een bierviltje," [Online]. Available: <https://www.ncsc.nl/actueel/weblog/weblog/2024/het-crypto-agilitymonster>.
- [76] N. Alnahawi, N. Schmitt, A. Wiesmaier, A. Heinemann and T. Grasmeyer, "On the State of Crypto-Agility".

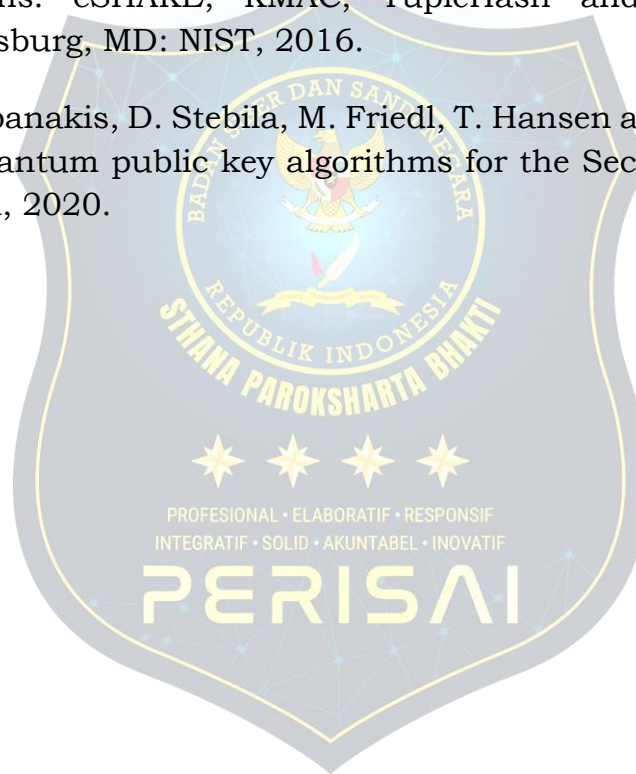
- [77] D. Ott and C. Peikert, "Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility," Computing Community Consortium, 2019.
- [78] E. Barker, L. Chen, A. Roginsky, A. Vassilev and R. Davis, SP 800-56A Revision 3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, Gaithersburg, MD:: NIST, 2018.
- [79] A. N. S. Institute., Key Agreement and Key Transport Using Elliptic Curve Cryptography., ANSI, 2017.
- [80] D. Brown, Elliptic Curve Cryptography, SEC 1. Standards for Efficient Cryptography, 2009.
- [81] NIST, FIPS 186-5: Digital Signature Standard (DSS)., Gaithersburg, MD:: NIST, 2023.
- [82] American National Standards Institute., Key Agreement and Key Transport Using Elliptic Curve, ANSI, 2007.
- [83] American National Standards Institute, Financial services - Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm - ECDSA., ANSI, 2020.
- [84] International Organization for Standardization, ISO/IEC 14888-3:2018 Information Technology – Security Techniques –Digital signatures with Appendix – Part 3 Discrete Logarithm Based Mechanisms, Geneva: ISO, 2018.
- [85] S. Josefsson and I. Liusvaara, RFC 8032 Edwards-Curve Digital Signature Algorithm (EdDSA), 2017.
- [86] K. Moriarty, B. Kaliski, J. Jonsson and A. Rusch, RFC 8017 PKCS #1: RSA Cryptography Specifications Version 2.2, 2016.
- [87] E. Barker, L. Chen, A. Roginsky, A. Vassilev, R. Davis and S. Simon, SP 800-56B Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography, Gaithersburg, MD:: NIST, 2019.
- [88] American National Standards Institute, Key Establishment Using Integer Factorization Cryptography, ANSI, 2017.

- [89] International Organization for Standardization, ISO/IEC 1488-2:2008 Information Technology – Security Techniques –Digital Signatures with Appendix – Part 2 Integer Factorization Based Mechanisms., 2008.
- [90] International Organization for Standardization, ISO/IEC 11770-3:2021 Information security — Key management Part 3: Mechanisms using asymmetric techniques, ISO, 2021.
- [91] BSN, SNI ISO/IEC 11770-3:2021. Keamanan informasi – Manajemen kunci – Bagian 3: Mekanisme menggunakan teknik asimetris, BSN, 2021.
- [92] I. O. f. Standardization, ISO/IEC 9796-2:2010 Information technology – Security techniques –Digital signature schemes giving message recovery – Part 2 Integer factorization based mechanisms, ISO, 2010.
- [93] I. O. f. Standardization., ISO/IEC 18033-2:2006 Information technology – Security techniques – Encryption algorithms – Part 2 Asymmetric ciphers, ISO, 2006.
- [94] BSN, SNI ISO IEC 18033-2:2006 - 2022 Teknologi informasi – Teknik keamanan – Algoritma enkripsi – Bagian 2: Penyandian asimetris (ISO/IEC 18033-2:2006 dan ISO/IEC 18033-2/Amd 1:2017, IDT, Eng), BSN, 2022.
- [95] W. Castryck and T. Decru, "An Efficient Key Recovery Attack on SIDH," in *In Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Lyon, France, 2023.
- [96] N. Aragon, P. Barreto, S. Bettaleb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Guneyasu, C. A. Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J.-P. Tillich, G. Zemor, V. V. S. Ghosh and J. R. Brokmann, "BIKE - Bit Flipping Key Encapsulation," [Online]. Available: <https://bikesuite.org/>.
- [97] M. Albrecht, D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram,, I. v. von, R. Misoczki, R. Niederhagen, K. G. Paterson, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C. . J. Tjhai, M. Tomlinson and W. Wang, "Classic

- McEliece Website," [Online]. Available: <https://classic.mceliece.org/>.
- [98] R. J. McEliece, "A Public-Key System Based on Algebraic Coding Theory," Jet Propulsion Lab, 1978.
- [99] E. Alkim, J. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. R. Raghunathan, D. Stebila, K. Easterbrook and B. La-Macchia., "FrodoKEM Website," [Online]. Available: <https://frodokem.org/>.
- [100] C. A. Melchor, N. Aragon, S. Bettaieb, B. Loïc., O. Blazy, J. C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, J. Bos, A. Dion, L. Jerome, R. Jean-Marc and P. Veron, "HQC Website," [Online]. Available: <http://pqc-hqc.org/>.
- [101] NIST, "NIST IR 8309 Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," Washington,DC, 2020.
- [102] D. A. Cooper, D. C. Apon, Q. H. Dang, M. S. Davidson, M. J. Dworkin and C. A. Miller, NIST SP 800-208 Recommendation for Stateful Hash-Based Signature Schemes, Gaithersburg, MD: NIST, 2020.
- [103] D. McGrew, M. Curcio and S. Fluhrer, IRTF RFC 8554 Leighton-Micali Hash-Based Signatures, IRTF, 2019.
- [104] A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld and A. Mohaisen, IRTF RFC 8391XMSS: eXtended Merkle Signature Scheme, 2018.
- [105] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte and Z. Zhang, "FALCON," [Online]. Available: <https://falcon-sign.info/>.
- [106] NIST, FIPS 197 Advanced encryption standard (AES), Gaithersburg, MD, 2001.
- [107] I. O. f. Standardization, ISO/IEC 18033-3:2010 Information technology – Security techniques –Encryption algorithms – Part 3 Block ciphers, Geneva, CH: ISO, 2010.

- [108] BSN, SNI ISO/IEC 18033-3:2010 Teknologi informasi – Teknik keamanan – Algoritma enkripsi – Bagian 3: Penyandian blok, Jakarta: BSN, 2010.
- [109] Y. Nir and A. Langley, RFC 8439 ChaCha20 and Poly1305 for IETF Protocols, 2018.
- [110] NIST, FIPS 180-4 Secure Hash Standard (SHS), Gaithersburg, MD: NIST, 2015.
- [111] Q. Dang, SP 800-107 Rev. 1 Recommendation for Applications Using Approved Hash Algorithms, Gaithersburg, MD: NIST, 2012.
- [112] T. Hansen and D. E. Eastlake 3rd, RFC 6234 US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF), 2011.
- [113] International Organization for Standardization, ISO/IEC 10118-3:2018 IT Security techniques – Hash-functions - Part 3:Dedicated hash-functions, Geneva, CH: ISO, 2018.
- [114] NIST, FIPS 202 SHA-3 Standard Permutation-Based Hash and Extendable-Output Functions, Gaithersburg, MD: NIST, 2015.
- [115] J.-P. Aumasson, S. Neves, Z. Wilcox-O’Hearn and C. Winnerlein, "BLAKE2 – fast secure hashing," 2017. [Online]. Available: <https://www.BLAKE2.net/>.
- [116] M.-J. O. Saarinen and J.-P. Aumasson, RFC 7693 The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC), 2015.
- [117] T. Iwata, J. Song, J. Lee and R. Poovendran, RFC 4493 The AES-CMAC Algorithm, 2006.
- [118] M. Dworkin, SP 800-38B Recommendation for Block Cipher Modes of Operation the CMAC Mode for Authentication, Gaithersburg, MD: NIST, 2016.
- [119] International Organization for Standardization, ISO/IEC 10118-3:2018 Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1 Mechanisms using a block cipher., Geneva, CH: ISO, 2018.

- [120] BSN, SNI ISO IEC 9797-1:2011 Teknologi informasi — Teknik keamanan — Message Authentication Codes (MACs) — Bagian 1: Mekanisme menggunakan penyandian blok (ISO/IEC 9797-1:2011 dan ISO/IEC 9797-1:2011/Amd 1:2023, IDT, Eng), Jakarta: BSN, 2011.
- [121] H. Krawczyk, M. Bellare and R. Canetti, RFC 2104 HMAC Keyed-Hashing for Message Authentication., 1997.
- [122] NIST, FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC), Gaithersburg, MD: NIST, 2008.
- [123] J. Kelsey, S.-j. Chang and R. Perlner, SP 800-185 SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash, Gaithersburg, MD: NIST, 2016.
- [124] P. Kampanakis, D. Stebila, M. Friedl, T. Hansen and D. Sikeridis, Post-quantum public key algorithms for the Secure Shell (SSH) protocol, 2020.





**BADAN SIBER
DAN SANDI
NEGARA**



**Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi
Badan Siber dan Sandi Negara**

Jl. Cijayanti No. 70, Kec. Babakan Madang, Kabupaten Bogor

2025

PUBLIK