



Pengenalan Standar Internasional tentang Distribusi Kunci Kuantum (*Quantum Key Distribution*) Versi 1.0

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

2025

PENGENALAN STANDAR INTERNASIONAL TENTANG DISTRIBUSI KUNCI KUANTUM (*QUANTUM KEY DISTRIBUTION*) 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

Pereviu : Assoc. Prof. Dr.Eng Khoirul Anwar, S.T.,
M.Eng (Telkom *University*)

Tim Penyusun :

1. Sari Agustini Hafman
2. Theresia Natalia
3. Mohamad Rahmadi
4. Yhufi Swastantri Gustiviana
5. Andreas Lugas

Tim Penyunting :

1. Yhufi Swastantri Gustiviana
2. Mohamad Rahmadi



PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya dokumen *Pengenalan Standar Internasional tentang Distribusi Kunci Kuantum (Quantum Key Distribution) Versi 1.0* ini dapat diselesaikan. Penyusunan dokumen ini merupakan langkah strategis untuk merespons kemajuan teknologi komputasi kuantum global yang berpotensi menimbulkan risiko signifikan terhadap ketahanan kriptografi klasik yang selama ini menjadi fondasi utama keamanan informasi nasional.



Dalam satu dekade terakhir, perkembangan teknologi kuantum menunjukkan percepatan yang sangat signifikan di berbagai aspek. Dalam lingkup keamanan informasi, *Quantum Key Distribution (QKD)* merupakan salah satu teknologi strategis yang menawarkan tingkat perlindungan tinggi melalui pemanfaatan prinsip kuantum. Dengan karakteristik tersebut, QKD berkembang menjadi salah satu pendekatan penting dalam peningkatan perlindungan komunikasi strategis di berbagai sektor.

Sejalan dengan perkembangan tersebut, berbagai organisasi standardisasi internasional seperti *International Organization for Standardization/International Electrotechnical Commission (ISO/IEC)*, *European Telecommunications Standards Institute (ETSI)*, dan *International Telecommunications Union – Telecommunication Sector (ITU-T)* telah mengembangkan beragam standar teknis untuk memastikan keamanan,

interoperabilitas, dan keandalan implementasi QKD di berbagai skenario operasional.

Dokumen ini disusun untuk memberikan gambaran yang sistematis mengenai standar internasional tersebut sebagai referensi awal bagi regulator, pengembang teknologi, akademisi, dan penyelenggara sistem elektronik. Pemahaman terhadap standar internasional QKD merupakan langkah strategis dalam mempersiapkan Indonesia menghadapi era teknologi kuantum, sekaligus memastikan bahwa pengembangan ekosistem keamanan siber nasional tetap selaras dengan praktik terbaik global.

BSSN berkomitmen untuk terus memperkuat kriptografi nasional melalui penyusunan kebijakan, pengembangan kapasitas, dan peningkatan keselarasan terhadap standar internasional. Kami berharap dokumen ini dapat menjadi pijakan awal untuk memperkaya kajian teknis dan kebijakan terkait teknologi kuantum, serta mendorong terciptanya infrastruktur keamanan informasi yang lebih tangguh, adaptif, dan berdaulat.

Saya menyampaikan apresiasi dan terima kasih kepada seluruh pihak yang telah berkontribusi dalam penyusunan dokumen ini. Semoga dokumen ini dapat menjadi kontribusi nyata dalam mendukung upaya kolektif menjaga kedaulatan dan keamanan ruang siber Indonesia di masa depan.

Drs. Nugroho Sulistyو 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 rahmat dan karunia-Nya, dokumen *Pengenalan Standar Internasional Tentang Distribusi Kunci Kuantum (Quantum Key Distribution) Versi 1.0* ini dapat disusun dan diterbitkan. Dokumen ini merupakan langkah penting dalam memperkuat keamanan informasi nasional di tengah munculnya

ancaman komputasi kuantum terhadap kriptografi klasik, yang menuntut solusi keamanan baru berbasis mekanika kuantum dengan jaminan keamanan yang tidak bergantung pada kekuatan komputasi penyerang.

Dokumen ini menyajikan gambaran komprehensif mengenai standar internasional *Quantum Key Distribution* (QKD) yang diterbitkan oleh *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC), *European Telecommunications Standards Institute* (ETSI), dan *International Telecommunications Union – Telecommunication Sector* (ITU-T), mencakup aspek keamanan, interoperabilitas, arsitektur sistem, serta metode evaluasi yang menjadi acuan global. Dokumen ini diharapkan menjadi referensi awal bagi regulator, peneliti, dan pengembang teknologi dalam memahami dan mengadopsi standar QKD sesuai dengan praktik terbaik internasional.

Kami berharap panduan ini dapat mendorong harmonisasi kebijakan nasional, memperkuat ekosistem teknologi keamanan kuantum, dan meningkatkan ketahanan keamanan informasi Indonesia di masa depan. Semoga dokumen ini menjadi fondasi strategis bagi pengembangan keamanan informasi nasional menuju era teknologi kuantum yang aman, andal, dan berdaulat.

Tjahjo Khurniawan

Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi

Desember 2025



RINGKASAN EKSEKUTIF

Munculnya ancaman komputasi kuantum terhadap kriptografi klasik mendorong perlunya solusi keamanan informasi yang lebih tangguh dan berkelanjutan. Salah satu pendekatan yang saat ini berkembang secara global adalah kriptografi berbasis *Quantum Key Distribution* (QKD), yaitu metode kriptografi berbasis kunci yang didasarkan pada prinsip-prinsip mekanika kuantum dan menawarkan jaminan keamanan yang tidak lagi bergantung pada kekuatan komputasi penyerang.

Dokumen ini disusun sebagai pengantar untuk sejumlah standar internasional yang relevan dengan potensi implementasi dan evaluasi sistem QKD di Indonesia. Tiga organisasi utama untuk standardisasi adalah *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC), *European Telecommunications Standards Institute* (ETSI), dan *International Telecommunications Union – Telecommunication Sector* (ITU-T), yang masing-masing telah menerbitkan dokumen-dokumen teknis dengan fokus pada aspek keamanan, interoperabilitas, arsitektur sistem, parameter teknis, dan metode evaluasi QKD.

Secara struktural, dokumen ini terdiri atas lima bab yang menguraikan dua standar ISO/IEC 23837 (mengatur persyaratan keamanan dan metode evaluasi sistem QKD dengan pendekatan berbasis ISO/IEC 15408 dan ISO/IEC 18045). Bab III membahas tujuh standar ETSI, mencakup terminologi, *use cases*, pembuktian keamanan, spesifikasi teknis, dan antarmuka sistem QKD, termasuk *Common Criteria Protection Profile*. Sedangkan, Bab IV menyampaikan terkait standar ITU-T Y.3800 yang memberikan kerangka umum bagi penerapan QKD dalam infrastruktur jaringan global. Kemudian, Bab V menyampaikan simpulan terkait pentingnya pemahaman dan adopsi standar sebagai langkah awal menuju penerapan sistem QKD yang selaras dengan praktik terbaik internasional.

Dokumen ini diharapkan menjadi referensi awal yang berguna bagi para pemangku kepentingan, termasuk regulator, pengembang teknologi, peneliti,

dan perancang sistem keamanan siber, dalam memahami dan mengadopsi standar internasional QKD. Lebih jauh, pemanfaatan dokumen ini dapat mendukung harmonisasi kebijakan nasional dan mendorong penguatan ekosistem teknologi keamanan kuantum, serta meningkatkan ketahanan keamanan informasi Indonesia di masa depan.

Apabila pengguna menemukan keraguan dalam panduan ini, maka disarankan untuk melihat referensi asli yang terdapat pada daftar referensi.



DAFTAR ISI

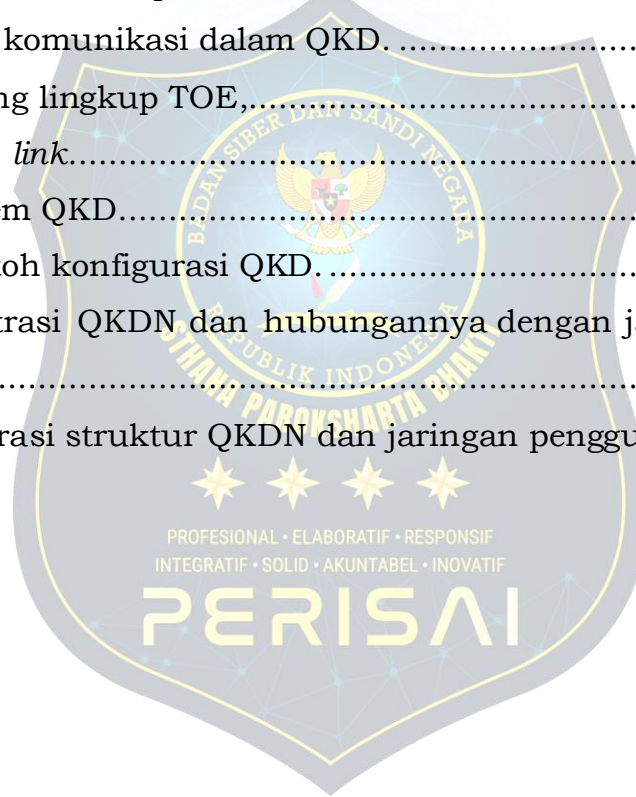
PENGANTAR	iii
PENGANTAR DEPUTI I	v
RINGKASAN EKSEKUTIF	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	xi
DAFTAR TABEL	xii
BAB I PENDAHULUAN	1
A. LATAR BELAKANG	2
B. TUJUAN DAN MANFAAT	3
C. RUANG LINGKUP	4
D. SISTEMATIKA PENYUSUNAN DOKUMEN	5
BAB II STANDAR ISO/IEC	7
A. ISO/IEC 23837-1:2023 <i>Information security — Security requirements, test and evaluation methods for quantum key distribution Part 1: Requirements</i>	8
B. ISO/IEC 23837-2:2023 <i>Information security — Security requirements, test and evaluation methods for quantum key distribution Part 2: Evaluation and testing methods</i>	52
BAB III STANDAR ETSI	98
A. ETSI GR QKD 007 V.1.1.1 <i>Quantum Key Distribution (QKD): Vocabulary</i>	99
B. ETSI GS QKD 002 V.1.1.1 <i>Quantum Key Distribution (QKD): Use Cases</i>	109
C. ETSI GS QKD 005 V1.1.1 <i>Quantum Key Distribution (QKD): Security Proofs</i>	122
D. ETSI GS QKD 008 V1.1.1 <i>Quantum Key Distribution (QKD): QKD Module Security Specification</i>	141
E. ETSI GS QKD 012 V1.1.1 <i>Quantum Key Distribution (QKD): Device and Communication Channel Parameters for QKD Deployment</i>	181
F. ETSI GK QKD 016 V.1.1.1 <i>Quantum Key Distribution (QKD): Common Criteria Protection Profile – Pair of Prepare and Measure Quantum Key Distribution Modules</i>	188
G. ETSI GR QKD 003 V2.1.1 <i>Quantum Key Distribution (QKD): Components and Internal Interfaces</i>	210
H. ETSI GS QKD 015 V2.1.1 <i>Quantum Key Distribution (QKD): Control Interface for Software Defined Networks</i>	221
BAB IV STANDAR ITU-T	228

A.	RUANG LINGKUP.....	229
B.	GAMBARAN UMUM TEKNOLOGI QKD	229
C.	KAPABILITAS JARINGAN UNTUK MENDUKUNG QKD.....	233
D.	STRUKTUR KONSEPTUAL DAN FUNGSI DASAR.....	235
BAB V PENUTUP		242
DAFTAR REFERENSI		244



DAFTAR GAMBAR

Gambar 2.1 Protokol PM-QKD	18
Gambar 2.2 Protokol MDI-QKD	19
Gambar 2.3 Protokol EB-QKD	20
Gambar 2.4 Antarmuka eksternal modul QKD generik	22
Gambar 2.5 Struktur internal generik dari implementasi protokol PM-QKD	24
Gambar 2.6 FTP_QKD <i>quantum key distribution</i>	43
Gambar 2.7 Struktur EM spesifik untuk modul QKD.....	54
Gambar 3.1 Alur komunikasi dalam QKD.	127
Gambar 3.2 Ruang lingkup TOE,.....	190
Gambar 3.3 QKD <i>link</i>	191
Gambar 3.4 Sistem QKD.....	191
Gambar 4.1 Contoh konfigurasi QKD.....	230
Gambar 4.2 Ilustrasi QKDN dan hubungannya dengan jaringan pengguna.	231
Gambar 4.3 Ilustrasi struktur QKDN dan jaringan pengguna.	236



DAFTAR TABEL

Tabel 2.1	Klasifikasi protokol QKD berdasarkan metode pengodean balik (decoding) keadaan kuantum.....	15
Tabel 2.2	Klasifikasi protokol QKD berdasarkan arsitektur protokol.	17
Tabel 2.3	Overview baseline kumpulan SFR untuk modul QKD.....	45
Tabel 2.4	EA untuk mengevaluasi FTP_QKD.....	54
Tabel 2.5	EA untuk mengevaluasi keamanan komponen quantum optic pada modul TX.....	56
Tabel 2.6	EA untuk mengevaluasi keamanan komponen quantum optic pada modul RX.....	59
Tabel 2.7	EA yang terkait dengan prosedur parameter adjustment.....	63
Tabel 2.8	EA tambahan untuk kelas APE.....	66
Tabel 2.9	EA tambahan untuk kelas ASE.	71
Tabel 2.10	EA tambahan untuk kelas ADV.	74
Tabel 2.11	EA tambahan pada kelas AGD.....	81
Tabel 2.12	EA tambahan untuk kelas ATE.....	83
Tabel 2.13	EA tambahan untuk kelas AVA.	90
Tabel 3.1	Istilah.....	100
Tabel 3.2	Singkatan	104
Tabel 3.3	Dasar Keamanan dari primitive kriptografi.....	111
Tabel 3.4	Korespondensi antara permasalahan dan tujuan keamanan... ..	200
Tabel 3.5	Korespondensi antara tujuan keamanan TOE dengan SFR....	201
Tabel 3.6	Parameter untuk menentukan detektor photon-tunggal.....	212
Tabel 3.7	Parameter untuk menentukan receiver CV_QKD dan kanal receiver.	214
Tabel 3.8	Parameter untuk menentukan kinerja dari pemancar Single-photon.	217
Tabel 3.9	Parameter untuk menentukan kinerja dari pemancar CV-QKD.	219
Tabel 3.10	Parameter untuk menentukan modulator.	220
Tabel 3.11	SD-QKD node.	223

BAB I

PENDAHULUAN



BAB I

PENDAHULUAN

Bab ini memberikan landasan awal untuk memahami konteks penyusunan dokumen Pengenalan Standar Internasional terkait *Quantum Key Distribution* (QKD). Potensi ancaman dari komputasi kuantum terhadap kriptografi klasik mendorong pengembangan QKD sebagai metode distribusi kunci yang aman berdasarkan prinsip mekanika kuantum. Untuk memastikan keamanan, interoperabilitas, dan keandalan operasional QKD, berbagai organisasi internasional seperti *International Organization for Standardization/ International Electrotechnical Commission* (ISO/IEC), *European Telecommunications Standards Institute* (ETSI), dan *International Telecommunications Union – Telecommunication Sector* (ITU-T) telah menetapkan sejumlah standar teknis yang relevan. Bab ini terdiri atas 4 (empat) subbagian yang secara berurutan membahas mengenai latar belakang penyusunan panduan, tujuan dan manfaat yang ingin dicapai, ruang lingkup materi, serta sistematika penulisan. Hal ini dimaksudkan sebagai kerangka awal sebelum memasuki pembahasan teknis pada bab berikutnya.

A. LATAR BELAKANG

Kemajuan teknologi informasi dan komunikasi telah mendorong perlunya sistem keamanan siber yang lebih kuat, khususnya dalam melindungi kerahasiaan dan integritas data. Munculnya teknologi kuantum membawa potensi ancaman serius terhadap algoritma kriptografi klasik. Untuk merespons tantangan tersebut, QKD dikembangkan sebagai salah satu solusi yang menawarkan distribusi kunci kriptografi dengan tingkat keamanan tinggi berdasarkan prinsip-prinsip mekanika kuantum.

Sebagai teknologi yang masih berkembang, implementasi QKD memerlukan acuan teknis dan kebijakan yang jelas untuk menjamin

keamanan, interoperabilitas, dan keandalan operasional dan berbagai skenario penggunaan. Menanggapi kebutuhan tersebut, sejumlah organisasi internasional seperti ISO/IEC, ETSI, dan ITU-T telah mengembangkan berbagai standar teknis terkait terminologi, arsitektur, antarmuka, spesifikasi keamanan, parameter komunikasi, hingga metode pengujian dan evaluasi sistem QKD.

Dokumen ini disusun untuk memberikan gambaran komprehensif terhadap standar-standar internasional, sebagai acuan bagi para pemangku kepentingan, termasuk pengembang teknologi, perancang sistem, pembuat kebijakan dan kalangan akademisi dalam memahami serta mengadopsi QKD sesuai dengan praktik terbaik yang telah disepakati secara global. Dengan demikian, penerapan QKD di tingkat nasional diharapkan dapat selaras dengan perkembangan standar internasional.

B. TUJUAN DAN MANFAAT

Dokumen ini disusun untuk memberikan gambaran umum terhadap beberapa standar internasional penting yang dikeluarkan oleh ISO/IEC, ETSI, dan ITU-T yang berkaitan langsung dengan teknologi QKD. Dengan memahami isi dan cakupan dari standar-standar tersebut, para pemangku kepentingan, termasuk perancang sistem, pengembang teknologi, regulator, dan akademisi diharapkan mampu mengimplementasikan sistem QKD yang sesuai dengan praktik terbaik global.

Dokumen ini diharapkan dapat memberikan manfaat sebagai berikut:

1. menjadi referensi awal bagi pihak-pihak yang ingin memahami standar internasional QKD;
2. mendukung upaya harmonisasi implementasi QKD dengan standar global;

3. menjadi bahan acuan dalam pengembangan kebijakan nasional dan teknis terkait sistem kriptografi kuantum.

C. RUANG LINGKUP

Dokumen ini berisi pembahasan terhadap sejumlah dokumen standar internasional terkait QKD yaitu:

1. ISO/IEC 23837-1:2023 *Information Security — Security Requirements, Test and Evaluation Methods For Quantum Key Distribution Part 1: Requirements*

Dokumen ini menetapkan persyaratan keamanan serta metode pengujian dan evaluasi untuk sistem QKD.

2. ISO/IEC 23837-2:2023 *Information security — Security requirements, test and evaluation methods for quantum key distribution Part 2: Evaluation and testing methods*

Dokumen ini berisi informasi tentang metode pengujian dan evaluasi sistem QKD berdasarkan persyaratan ISO/IEC 23837

3. ETSI GR QKD 007 V.1.1.1 *Quantum Key Distribution (QKD): Vocabulary*

Dokumen ini menyediakan terminologi umum dan definisi yang digunakan dalam ekosistem QKD.

4. ETSI GK QKD 016 V.2.1.1 *Quantum Key Distribution (QKD): Common Criteria Protection Profile – Pair of Prepare and Measure Quantum Key Distribution Modules*

Dokumen ini berisi informasi tentang komponen-komponen dalam sistem QKD dan antarmuka internal antar modul.

5. ETSI GR QKD 003 V2.1.1 *Quantum Key Distribution (QKD): Components and Internal Interfaces*

Dokumen ini mendefinisikan antarmuka kontrol antara modul QKD dan infrastruktur *Software Defined Network* (SDN).

6. ETSI GS QKD 015 V2.1.1 *Quantum Key Distribution (QKD): Control Interface for Software Defined Networks;*

Dokumen ini mendefinisikan antarmuka manajemen untuk integrasi QKD dalam arsitektur bidang kontrol jaringan terdisagregasi, khususnya dengan *Software Defined Networks* (SDN).

7. ETSI GS QKD 012 V1.1.1 *Quantum Key Distribution* (QKD): *Device and Communication Channel Parameters for QKD Deployment*

Dokumen ini menyajikan parameter teknis perangkat dan kanal komunikasi untuk penerapan sistem QKD.

8. ETSI GS QKD 005 V1.1.1 *Quantum Key Distribution* (QKD): *Security Proofs*

Dokumen ini menguraikan spesifikasi keamanan untuk modul-modul QKD.

9. ETSI GS QKD 008 V1.1.1 *Quantum Key Distribution* (QKD): *QKD Module Security Specification*

Dokumen ini menyajikan *protection profile* berbasis Common Criteria untuk modul QKD jenis *prepare and measure*.

10. ITU-T Y.3800 *Overview on Supporting Quantum Key Distribution*

Dokumen ini memberikan tinjauan umum tentang dukungan terhadap QKD dalam infrastruktur komunikasi.

D. SISTEMATIKA PENYUSUNAN DOKUMEN

Untuk selanjutnya, dokumen ini disusun sebagai berikut:

BAB II. STANDAR ISO/IEC

Bab ini berisi informasi tentang 2 (dua) standar terkait QKD yang diterbitkan ISO/IEC yaitu ISO/IEC 23837-1 dan ISO/IEC 23837-2:2023.

BAB III. STANDAR ETSI

Bab ini berisi informasi tentang 7 (tujuh) standar terkait QKD yang diterbitkan ETSI yaitu ETSI GR QKD 007 V.1.1.1, ETSI GK QKD 016 V.2.1.1, ETSI GR QKD 003 V2.1.1, ETSI GS QKD 015 V2.1.1, ETSI GS

QKD 012 V1.1.1, ETSI GS QKD 005 V1.1.1 dan ETSI GS QKD 008 V1.1.1.

BAB IV. STANDAR ITU-T

Bab ini berisi informasi tentang 1 (satu) standar terkait QKD yang diterbitkan oleh ITU-T yaitu ITU-T Y.3800.

BAB IV. PENUTUP

Bab ini menyajikan kesimpulan atas seluruh isi dokumen.



BAB II

STANDAR ISO / IEC



BAB II

STANDAR ISO/IEC

Bab ini membahas dua standar internasional yang diterbitkan oleh ISO/IEC terkait teknologi QKD, yaitu ISO/IEC 23837-1:2023 dan ISO/IEC 23837-2:2023. Kedua standar tersebut disusun untuk memberikan acuan teknis mengenai persyaratan keamanan serta metode pengujian dan evaluasi terhadap sistem QKD. Dalam penyusunannya, standar ini mengadopsi kerangka ISO/IEC 15408 dan dapat digunakan sebagai pelengkap terhadap metodologi evaluasi keamanan ISO/IEC 18045.

A. ISO/IEC 23837-1:2023 *Information security — Security requirements, test and evaluation methods for quantum key distribution Part 1: Requirements*

ISO/IEC 23837-1:2023 [1] merupakan bagian dari seri ISO/IEC 23837 yang menetapkan persyaratan keamanan, metode pengujian, dan evaluasi untuk QKD, dalam kerangka ISO/IEC 15408. Fokus utama dokumen ini adalah merumuskan seperangkat persyaratan fungsional keamanan (*Security Functional Requirements* (SFRs)) yang menjadi dasar umum bagi modul QKD. QKD secara teoretis menawarkan metode untuk memperpanjang kunci simetris dari kunci awal yang telah dibagikan, dengan tingkat keamanan yang tidak bergantung pada kekuatan komputasi pihak penyerang. Kunci tersebut kemudian dapat digunakan untuk tujuan kriptografi, seperti enkripsi guna menciptakan saluran komunikasi yang aman.

Meskipun protokol QKD didasarkan pada model keamanan matematis yang ketat dengan asumsi kedua pihak telah berbagi kunci secara rahasia (berbasis pada prinsip kuantum), dalam praktiknya masih sering terjadi perbedaan antara model teoretis dan implementasi aktual sepanjang siklus hidup modul QKD. Penyimpangan ini dapat menimbulkan kerentanan keamanan, termasuk potensi serangan *side-channel* yang telah terbukti secara eksperimental dalam beberapa kasus

peretasan QKD. Oleh karena itu, sebagaimana perangkat kriptografi konvensional, modul QKD juga harus menjalani pengujian dan evaluasi keamanan yang ketat sebelum dapat digunakan dalam aplikasi nyata.

Untuk mengatasi hal tersebut, seri ISO/IEC 23837 menyediakan spesifikasi keamanan yang ketat dan seragam bagi produsen modul QKD agar dapat mengikuti prosedur standar dalam perancangan dan implementasi produk teknologi informasi berbasis QKD. Selain itu, dokumen ini juga memandu evaluator dalam proses pengujian keamanan modul QKD guna meminimalkan risiko kegagalan sistem saat dioperasikan. ISO/IEC 23837-1 mengadopsi model dan bahasa yang distandarkan dari ISO/IEC 15408 dalam mendefinisikan SFR dasar, mencakup keseluruhan komponen QKD mulai dari jaringan konvensional hingga komponen optik kuantum. Lampiran A memberikan informasi tambahan untuk membantu penyusunan *protection profile* bagi modul QKD, sedangkan bagian ISO/IEC 23837-2 akan membahas kegiatan evaluasi yang diperlukan pada berbagai tingkat jaminan evaluasi. Format dan gaya penulisan SFR dalam dokumen ini mengikuti konvensi ISO/IEC 15408-2, sehingga memudahkan pengguna yang telah terbiasa dengan seri ISO/IEC 15408 dalam mengadaptasi dan menyusun dokumen evaluasi keamanan untuk modul QKD.

Struktur dokumen ISO/IEC 23837-1:2023 terdiri atas:

1. Ruang lingkup
2. Acuan normatif
3. Istilah dan definisi
4. Singkatan
5. Aspek Teoretis Protokol QKD
6. Implementasi Modul Protokol QKD yang terdiri atas antarmuka eksternal modul QKD, struktur internal modul QKD dan ruang lingkup *Target of Evaluation* (TOE) untuk Modul QKD. Dalam ruang lingkup, TOE untuk Modul QKD dijelaskan beserta fungsionalitas keamanan TOE (*TOE security functionality* (TSF)).

7. Analisis Masalah Keamanan QKD yang terdiri atas asumsi keamanan, analisis aset, ancaman terhadap komponen jaringan konvensional dari perspektif serangan klasik berbasis jaringan serta ancaman terhadap komponen optik kuantum karena cacat pada sumber optik, kerentanan deteksi optik dan karena kerentanan penyesuaian parameter
8. Komponen Fungsional Keamanan yang diperluas untuk Implementasi QKD
9. Persyaratan Fungsional Keamanan untuk Modul QKD yang terdiri atas persyaratan umum untuk komponen jaringan konvensional dalam modul QKD, persyaratan umum untuk implementasi protokol QKD dan persyaratan umum untuk komponen optik kuantum dalam modul QKD
10. Pernyataan Kepatuhan yang terdiri atas pernyataan kepatuhan terkait definisi masalah keamanan dan pernyataan kepatuhan terkait persyaratan fungsional keamanan.
11. Lampiran A yang berupa Panduan (informatif) untuk Mengembangkan *Protection Profile* bagi Modul QKD

Berikut adalah ringkasan dari dokumen ISO/IEC 23837-1:2023.

1. Ruang Lingkup

Dokumen ini menetapkan kerangka kerja umum untuk evaluasi keamanan QKD berdasarkan seri standar ISO/IEC 15408. Secara khusus, dokumen ini menetapkan seperangkat persyaratan fungsional keamanan atau SFR dasar yang berlaku umum untuk modul-modul QKD. Persyaratan ini mencakup baik komponen jaringan konvensional maupun komponen optik kuantum, serta keseluruhan implementasi protokol QKD.

Untuk mendukung analisis terhadap SFR, permasalahan keamanan yang dapat dihadapi oleh modul QKD dalam lingkungan operasionalnya dianalisis melalui pendekatan struktural terhadap fungsionalitas keamanannya dan klasifikasi berbagai jenis protokol

QKD. SFR yang berlaku pada komponen jaringan konvensional dalam modul QKD dirumuskan terutama berdasarkan kerangka kerja ISO/IEC 15408. Selain itu, metodologi dari ISO/IEC 19790 dan standar-standar lain yang relevan terkait pengujian modul kriptografi dan perangkat jaringan juga dijadikan rujukan.

2. Acuan normatif

Dokumen-dokumen berikut dirujuk dalam teks ini sedemikian rupa sehingga sebagian atau seluruh isinya merupakan persyaratan dalam dokumen ini. Untuk referensi yang mencantumkan tahun terbit, hanya edisi yang disebutkan yang berlaku. Untuk referensi tanpa tahun terbit, edisi terbaru dari dokumen yang dirujuk (termasuk setiap amendemen) yang berlaku.

- a. ISO/IEC 15408-1:2022 — Keamanan informasi, keamanan siber, dan perlindungan privasi — Kriteria evaluasi untuk keamanan TI — Bagian 1: Pendahuluan dan model umum
- b. ISO/IEC 15408-2:2022 — Keamanan informasi, keamanan siber, dan perlindungan privasi — Kriteria evaluasi untuk keamanan TI — Bagian 2: Komponen fungsional keamanan

3. Istilah dan definisi

Untuk dokumen ini, istilah dan definisi yang tercantum dalam ISO/IEC 15408-1 serta definisi tambahan akan digunakan. ISO dan IEC menyediakan basis data terminologi yang digunakan dalam proses standardisasi, yang dapat diakses melalui alamat berikut:

- a. ISO Online Browsing Platform: <https://www.iso.org/obp>
- b. IEC Electropedia: <https://www.electropedia.org>

Pada dokumen ini terdapat 37 (tiga puluh tujuh) buah definisi.

4. Singkatan

Berikut adalah beberapa singkatan yang terdapat dalam dokumen

APD	<i>avalanche photodiode</i>
CV-QKD	<i>continuous-variable quantum key distribution</i>
DV-QKD	<i>discrete-variable quantum key distribution</i>

EB-QKD	<i>entanglement-based quantum key distribution</i>
FTP	<i>trusted path/channels</i>
FUN_QKD	<i>quantum key distribution function</i>
FUN_SCM	<i>system control and management function</i>
FUN_SP	<i>self-protection function</i>
IT	<i>information technology</i>
KM	<i>key manager</i>
MDI-QKD	<i>measurement-device-independent quantum key distribution</i>
NRBG	<i>non-deterministic random bit generator</i>
PM-QKD	<i>prepare-and-measure quantum key distribution</i>
PP	<i>protection profile</i>
QBER	<i>quantum bit error rate</i>
QKD	<i>quantum key distribution</i>
QRBG	<i>quantum random bit generator</i>

5. Aspek Teoretis Protokol QKD

a. Bagian 5.1 Umum

Bagian ini menjelaskan konsep QKD dalam sebuah model teoretis yang dibatasi pada pembahasan aspek-aspek teoretis dari protokol QKD, tanpa mempertimbangkan kerentanan implementasi yang mungkin terjadi dalam praktik. Dengan kata lain, dalam model ini seluruh bagian dari implementasi QKD diasumsikan sepenuhnya sesuai dengan model teoretis tersebut, dan tidak terdapat kemungkinan serangan melalui kerentanan implementasi.

Jenis serangan yang diperbolehkan dalam model teoretis hanya mencakup serangan yang telah dipertimbangkan dalam model keamanan protokol QKD itu sendiri. Konsep dan prinsip dasar protokol QKD dibahas pada Bagian 5.2, klasifikasi protokol QKD dan arsitekturnya disajikan dalam Bagian 5.3 dan 5.4, sedangkan untuk mendukung analisis terhadap implementasi QKD dijelaskan pada bagian-bagian berikutnya.

b. Bagian 5.2 Prinsip

Secara garis besar, protokol QKD digunakan untuk memperluas kunci simetris yang telah dibagikan sebelumnya antara dua pihak menjadi kunci rahasia yang lebih panjang dan layak digunakan dalam kriptografi. Dalam model umum protokol QKD, dua pihak terhubung melalui dua saluran komunikasi, yaitu:

- 1) Saluran kuantum: digunakan untuk transmisi sinyal kuantum.
- 2) Saluran klasik: digunakan untuk transmisi sinyal klasik, dan biasanya memerlukan autentikasi data.

Untuk sesi QKD pertama, kedua pihak membutuhkan kunci simetris awal yang telah dibagikan sebelumnya (*pre-shared key*), yang digunakan sebagai kunci autentikasi QKD untuk mengamankan komunikasi pada saluran klasik. Karena kunci autentikasi yang digunakan dalam tiap sesi QKD umumnya jauh lebih pendek dibandingkan kunci yang dihasilkan, sesi-sesi QKD berikutnya dapat menggunakan bagian tertentu dari kunci yang dihasilkan sebelumnya sebagai kunci autentikasi baru. Dengan demikian, QKD berfungsi sebagai protokol ekspansi kunci dua pihak yang memungkinkan pengembangan kunci rahasia bersama dari ukuran pendek ke panjang sesuai kebutuhan aplikasi.

Catatan 1: Kunci awal dapat dimasukkan secara manual atau diunduh dari pengelola kunci eksternal pada tahap pengembangan, pra-operasional, atau pemeliharaan sistem QKD. Umumnya, sekumpulan kunci simetris dibagikan sebelum sistem QKD mulai beroperasi, bukan hanya satu kunci tunggal.

Secara umum, protokol QKD terdiri atas dua prosedur utama:

- 1) Prosedur pertama: Pembangkitan data mentah (*raw data generation*)

Dalam tahap ini, sinyal kuantum ditransmisikan melalui kanal kuantum dan dideteksi oleh pihak yang berwenang.

- a) Pihak yang mengirim sinyal kuantum disebut pihak pengirim QKD (*transmitter*).
- b) Pihak yang menerima/deteksi sinyal disebut pihak penerima QKD (*receiver*).

2) Prosedur kedua: Pemrosesan pasca transmisi (*post-processing*)

Data mentah diproses untuk menghasilkan kunci simetris akhir. Proses ini umumnya melibatkan empat tahap:

- a) *Sifting*: mengekstraksi data yang layak dari data mentah.
- b) Estimasi parameter: memperkirakan parameter yang diperlukan untuk koreksi kesalahan dan penguatan privasi.
- c) Koreksi kesalahan: memperbaiki kesalahan dalam data yang telah disaring.
- d) Penguatan privasi: menghasilkan kunci akhir dari data yang telah disaring.

Catatan 2: Sistem QKD yang praktis juga dapat mencakup prosedur tambahan, seperti inisialisasi, untuk mendukung fungsionalitas sistem.

Catatan 3: Dalam beberapa kasus, batas antara prosedur tidak selalu tegas. Misalnya, estimasi tingkat kesalahan bit kuantum (*Quantum Bit Error Rate* (QBER)) bisa dilakukan selama koreksi kesalahan, bukan dalam estimasi parameter.

c. Bagian 5.3 Klasifikasi

Selain protokol generik yang dibahas dalam Bagian 5.2, protokol QKD dapat diklasifikasikan dari berbagai sudut pandang. Seri ISO/IEC 23837 menetapkan dua metode klasifikasi utama untuk protokol QKD, yaitu:

- 1) Berdasarkan metode pengukuran keadaan kuantum:
 - a) QKD variabel diskret (*Discrete-Variable* QKD (DV-QKD)): Pihak penerima biasanya menggunakan detektor foton tunggal untuk mengukur pulsa optik.
 - b) QKD variabel kontinu (*Continuous-Variable* QKD (CV-QKD)): Pihak penerima umumnya menggunakan teknik deteksi koheren untuk mengukur pulsa optik.

Untuk perbandingan detail, dapat dilihat pada Tabel 2.1.

Tabel 2.1 Klasifikasi protokol QKD berdasarkan metode pengodean balik (*decoding*) keadaan kuantum.

Tipe	DV-QKD	CV-QKD
Deskripsi	Pihak pengirim biasanya mengkodekan informasi menggunakan variabel diskret berdimensi hingga, seperti fasa, polarisasi, atau celah waktu (<i>time-bin</i>). Untuk mendekode informasi, pihak penerima umumnya menggunakan detektor foton tunggal.	Pihak pengirim biasanya mengkodekan informasi menggunakan variabel konjugat (kuadratur) dari medan elektromagnetik terkuantisasi dalam ruang Hilbert berdimensi tak hingga. Contohnya adalah keadaan optik koheren. Pihak penerima umumnya menggunakan teknik deteksi koheren, seperti deteksi homodin atau heterodin, untuk melakukan

Tippe	DV-QKD	CV-QKD
		pengukuran kuadratur pada keadaan kuantum tersebut.

2) Berdasarkan arsitektur protokol QKD (ditunjukkan pada Tabel 2.2):

- a) Protokol *prepare-and-measure* (PM-QKD): Pihak pengirim mengkodekan informasi ke dalam keadaan kuantum dan mengirimkannya melalui kanal kuantum ke pihak penerima, yang kemudian melakukan pengukuran untuk menghasilkan data mentah. (ditunjukkan pada Gambar 2.1.)
- b) Protokol *measurement-device-independent* (MDI-QKD): Terdapat dua pihak pengirim dan satu pihak penerima. Masing-masing pihak pengirim terhubung ke pihak penerima melalui saluran kuantum. Kedua pengirim menyiapkan dan mengirimkan keadaan kuantum, dan pihak penerima melakukan pengukuran bersama atas keadaan tersebut. (Lihat Gambar 2.2.)
- c) Protokol berbasis keterjeratan (*Entanglement-Based* QKD (EB-QKD)): Terdapat satu pihak pengirim dan dua pihak penerima. Pihak pengirim menyiapkan keadaan kuantum keterikatan dua bagian (bipartit) dan mengirimkan masing-masing bagian ke pihak penerima yang berbeda. Kedua penerima kemudian melakukan pengukuran secara independen untuk menghasilkan data mentah. (Lihat Gambar 2.3.)

Catatan: DV-QKD dan CV-QKD keduanya dapat mencakup jenis protokol PM-QKD, MDI-QKD, dan EB-QKD.

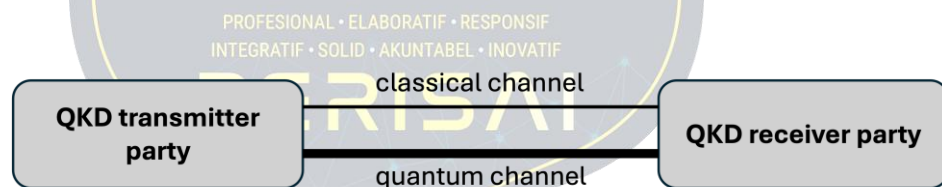
Tabel 2.2 Klasifikasi protokol QKD berdasarkan arsitektur protokol.

Tipe	PM-QKD	MDI-QKD	EB-QKD
Deskripsi	Pihak pengirim QKD dan pihak penerima QKD. Pihak pengirim menyiapkan dan mengirimkan <i>quantum state</i> kepada pihak penerima melalui kanal kuantum. Pihak penerima mengukur <i>quantum state</i> tersebut. Hasilnya (setelah pemrosesan pasca-transmisi) adalah kunci akhir bersama yang tersedia bagi pihak pengirim dan pihak penerima.	Protokol ini melibatkan dua pihak pengirim QKD dan satu pihak penerima QKD. Kedua pihak pengirim menyiapkan dan mengirimkan <i>quantum state</i> kepada pihak penerima melalui kanal kuantum. Pihak penerima melakukan pengukuran gabungan terhadap <i>quantum state</i> yang diterima dari kedua pihak pengirim. Hasilnya (setelah pemrosesan	Protokol ini melibatkan satu pihak pengirim QKD dan dua pihak penerima QKD. Pihak pengirim menyiapkan <i>quantum state</i> keterikatan bipartit dan mengirimkan masing-masing bagiannya kepada kedua pihak penerima secara terpisah. Kedua pihak penerima secara individual melakukan pengukuran terhadap <i>quantum state</i> tersebut. Hasilnya (setelah

Tipe	PM-QKD	MDI-QKD	EB-QKD
		pasca-transmisi) adalah kunci akhir bersama yang tersedia bagi kedua pihak pengirim.	pemrosesan pasca-transmisi) adalah kunci akhir bersama yang tersedia bagi kedua pihak penerima.

d. Bagian 5.4 Arsitektur

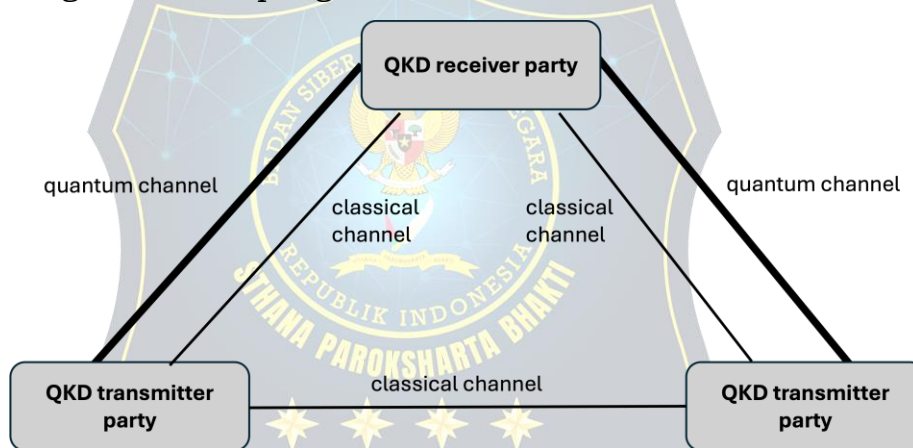
Bagian 5.3 membahas tiga arsitektur berbeda dari protokol QKD yang ditampilkan dalam Gambar 2.1, 2.2, dan 2.3. Secara umum, ruang lingkup evaluasi keamanan sangat berkaitan erat dengan arsitektur protokol QKD yang diimplementasikan. Pada protokol PM-QKD, sebagaimana ditunjukkan dalam Gambar 2.1, terdapat satu pihak pengirim dan satu pihak penerima yang terhubung melalui kanal kuantum dan klasik.



Gambar 2.1 Protokol PM-QKD digambar ulang dari [1].

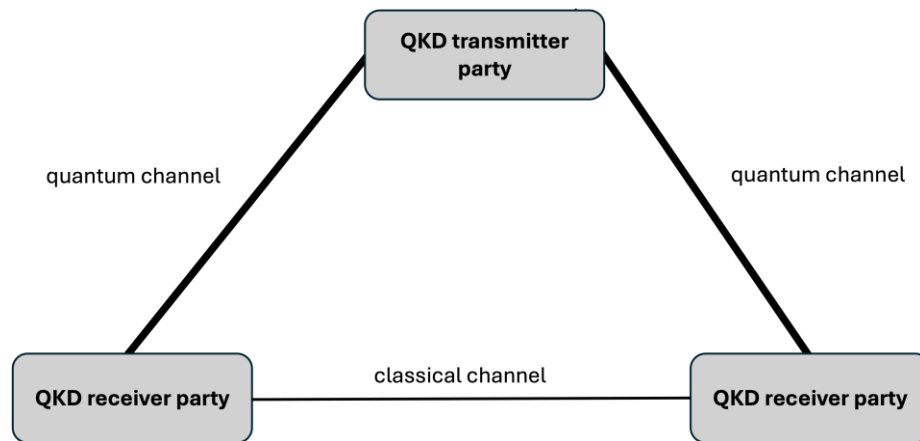
Pada protokol MDI-QKD yang digambarkan dalam Gambar 2.2, terdapat satu pihak penerima di tengah yang terhubung dengan dua pihak pengirim melalui kanal kuantum dan klasik, sementara kedua pihak pengirim juga saling terhubung melalui kanal klasik. Setelah sesi QKD berhasil dilakukan, hanya kedua pihak pengirim yang mengetahui kunci akhir. Dalam arsitektur ini, pihak penerima hanya diharapkan mengikuti spesifikasi protokol untuk menjamin keberhasilan pertukaran kunci,

namun tidak diasumsikan memiliki peran dalam pembuktian keamanan protokol. Oleh karena itu, modul implementasi pihak penerima tidak termasuk dalam ruang lingkup evaluasi keamanan sebagaimana dijelaskan dalam Bagian 6.4.3. Selain itu, terdapat dua jenis saluran klasik dalam MDI-QKD: saluran antara dua pihak pengirim yang perlu diautentikasi tergantung pada protokol QKD yang digunakan, dan saluran antara masing-masing pihak pengirim dan pihak penerima, yang digunakan untuk menyampaikan hasil pengukuran, tetapi tidak memerlukan autentikasi. Artinya, penyerang diasumsikan dapat mengubah hasil pengukuran tersebut.



Gambar 2.2 Protokol MDI-QKD
digambar ulang dari [1].

Sementara itu, pada protokol EB-QKD yang digambarkan dalam Gambar 2.3, satu pihak pengirim mengirimkan keadaan keterikatan kuantum kepada dua pihak penerima melalui kanal kuantum. Kedua pihak penerima kemudian terhubung melalui kanal klasik. Setelah sesi QKD berhasil, hanya kedua pihak penerima yang mengetahui kunci akhir. Dalam protokol ini, pihak pengirim hanya diharapkan mengikuti spesifikasi protokol, namun tidak ada asumsi keamanan yang diberlakukan terhadap protokol dalam pembuktian keamanan. Oleh karena itu, modul implementasi pihak pengirim dikecualikan dari ruang lingkup evaluasi keamanan, seperti dijelaskan dalam Bagian 6.4.3.



Gambar 2.3 Protokol EB-QKD
digambar ulang dari [1].

Lebih lanjut, dalam beberapa implementasi, peran pihak di tengah dan salah satu dari dua pihak lainnya dapat digabungkan menjadi satu entitas. Dalam kasus ini, penyusun PP atau ST harus mempertimbangkan tingkat integrasi tersebut untuk menjamin keamanan sistem secara keseluruhan. Secara khusus, bila sebuah komponen yang memerlukan evaluasi digabungkan dalam satu modul dengan komponen yang tidak memerlukan evaluasi, metode pemisahan fungsional harus dijelaskan dengan jelas dalam dokumen PP, ST, dan definisi TOE. Sebagai contoh, dalam protokol EB-QKD, pihak pengirim dan salah satu pihak penerima dapat diimplementasikan dalam satu modul yang sama.

6. Implementasi Modul Protokol QKD

a. Umum

Dalam konteks protokol QKD, komponen-komponen implementasi disebut sebagai modul pengirim QKD dan modul penerima QKD. Model keamanan protokol QKD pada umumnya mengasumsikan bahwa agen ancaman hanya akan melakukan aksi jahat melalui kanal kuantum dan kanal klasik. Namun, dalam praktiknya, apabila agen ancaman dapat mengakses perangkat komputasi secara jarak jauh melalui antarmuka jaringan atau bahkan secara fisik mendekati perangkat dan

mengakses perangkat kerasnya, informasi penting mengenai proses komputasi dapat bocor dan membatalkan asumsi-asumsi dalam model keamanan tersebut.

Serangan melalui *side channel*, seperti pengukuran konsumsi daya atau pancaran elektromagnetik, merupakan contoh nyata dari risiko ini. Evaluasi terhadap kebocoran *side channel* pada modul QKD membutuhkan upaya besar. Namun, upaya ini dapat diminimalkan jika asumsi lingkungan operasional memungkinkan pengecualian atas beberapa jenis serangan *side channel*, sebagaimana dijelaskan dalam Bagian 7 (khususnya 7.2 dan 7.4.2).

Untuk menjembatani kesenjangan antara model keamanan teoretis dan kondisi praktis, pendekatan praktis dapat dilakukan melalui asumsi lingkungan yang wajar serta penggunaan pengendalian keamanan baik yang berkaitan dengan TI maupun non-TI. Evaluasi modul QKD berdasarkan seri ISO/IEC 15408 bertujuan untuk memastikan bahwa tingkat keamanan praktis telah tercapai, dan bahwa tidak terdapat celah antara protokol QKD dan implementasi nyatanya yang dapat dimanfaatkan oleh penyerang sebagaimana diasumsikan.

Seri ISO/IEC 23837 berfokus untuk menjawab tiga pertanyaan utama berikut:

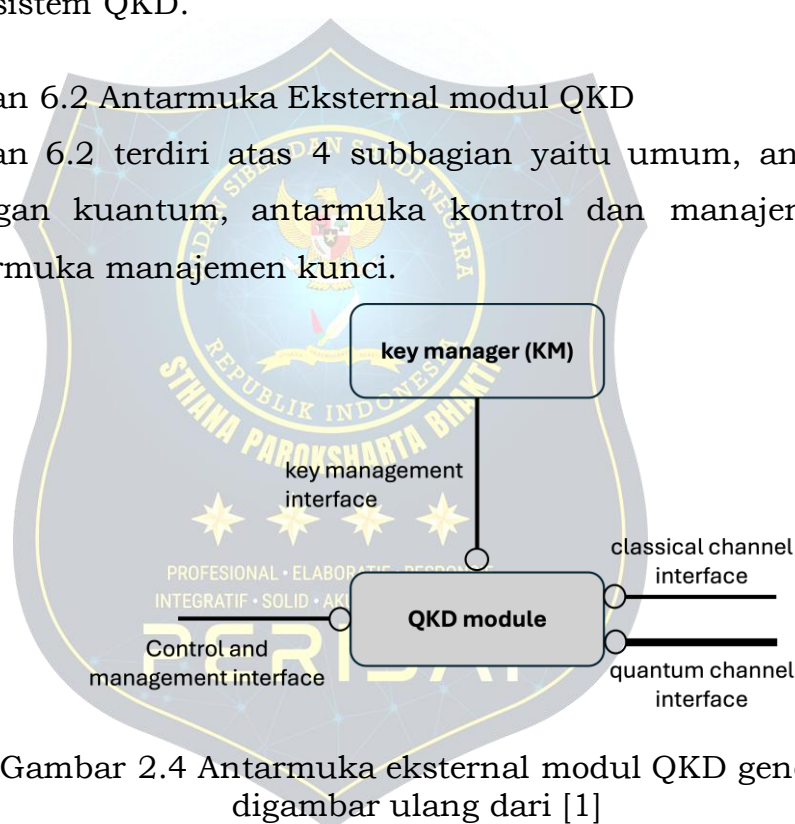
- 1) Asumsi lingkungan operasional apa yang perlu dibuat dan ancaman apa saja yang harus ditangani dari perspektif keamanan praktis? (terdapat pada Bagian 7)
- 2) Pengendalian keamanan TI apa yang harus diterapkan untuk menghadapi ancaman tersebut dan mencapai tujuan keamanan, atau lebih spesifik, persyaratan keamanan apa yang perlu dikenakan terhadap modul QKD? (terdapat pada Bagian 9)

- 3) Bagaimana cara memvalidasi bahwa pengendalian keamanan dan fungsionalitas inti dari modul QKD telah diimplementasikan dengan benar? (lihat ISO/IEC 23837-2)

Untuk memahami ketiga pertanyaan tersebut, antarmuka eksternal dari modul QKD dijelaskan dalam Bagian 6.2, komponen internal sistem QKD dianalisis dalam Bagian 6.3, Bagian 6.4 memberikan definisi umum mengenai ruang lingkup TOE dan TSF, dan Bagian 6.5 menggambarkan alur kerja umum dari sistem QKD.

b. Bagian 6.2 Antarmuka Eksternal modul QKD

Bagian 6.2 terdiri atas 4 subbagian yaitu umum, antarmuka jaringan kuantum, antarmuka kontrol dan manajemen dan antarmuka manajemen kunci.



Gambar 2.4 Antarmuka eksternal modul QKD generik digambar ulang dari [1]

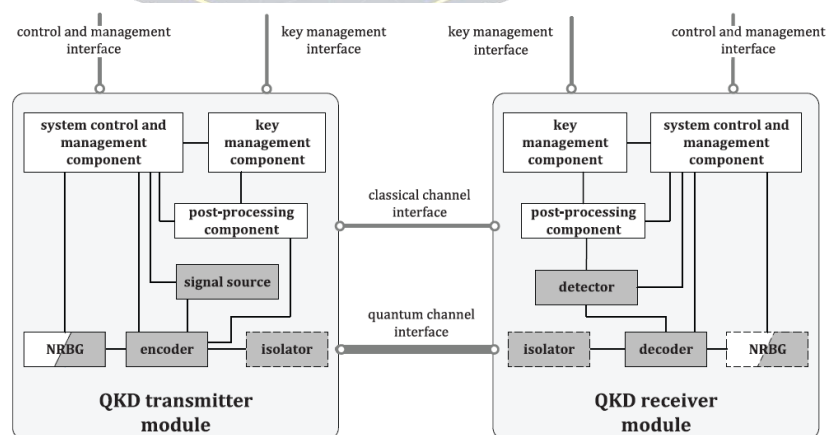
Antarmuka eksternal dari modul QKD (ditunjukkan pada Gambar 2.4) merepresentasikan pihak pengirim maupun penerima bergantung pada arsitektur protokol QKD yang digunakan. Selain antarmuka untuk kanal kuantum dan kanal klasik, modul QKD juga memerlukan antarmuka tambahan guna mendukung fungsionalitas operasionalnya. Antarmuka tambahan ini mencakup antarmuka kontrol dan manajemen yang memungkinkan operator mengatur dan memantau modul, serta antarmuka manajemen kunci untuk mengunggah kunci

final ke Manajer Kunci (*Key Manager* (KM)). Dalam beberapa strategi implementasi, kunci yang telah dibagikan sebelumnya (*pre-shared key*) untuk autentikasi QKD dapat diunduh dari KM atau dimasukkan secara manual oleh operator melalui antarmuka kontrol. Antarmuka kanal klasik berfungsi untuk pertukaran pesan dan proses pasca-pemrosesan antara modul QKD, yang serupa dengan perangkat jaringan konvensional. Antarmuka kanal kuantum direkomendasikan menggunakan serat optik mode tunggal untuk mencegah potensi serangan yang memanfaatkan karakteristik multi-mode. Antarmuka kontrol dan manajemen memungkinkan konfigurasi sistem, pengelolaan informasi audit, pembaruan perangkat lunak atau perangkat keras, pemantauan status operasional, serta pemasukan kunci awal dalam kasus tertentu. Untuk melindungi akses antarmuka tersebut dari pihak yang tidak berwenang, kontrol akses berbasis autentikasi sangat diperlukan. Sementara itu, antarmuka manajemen kunci memungkinkan komunikasi antara modul QKD dan KM untuk mengunggah kunci akhir yang baru dan, dalam strategi tertentu, mengunduh kunci awal. Jalur komunikasi ini harus dilindungi dari kebocoran informasi dan gangguan, karena dapat melewati berbagai jaringan internal.

c. Bagian 6.3 Struktur internal modul QKD

Bagian 6.3 terdiri atas 3 subbagian yaitu umum, komponen dalam modul *transmitter* QKD dan komponen modul *receiver* QKD. Dalam praktiknya, implementasi protokol QKD dapat bervariasi secara signifikan, terutama karena perbedaan komponen penyusunnya seperti sumber foton, detektor, modulator, serta sistem pemrosesan pasca-transmisi. Untuk memberikan pemahaman menyeluruh tanpa terjebak dalam rincian teknis, struktur internal modul QKD dijelaskan secara umum berdasarkan pendekatan abstrak tingkat tinggi, dengan penekanan khusus pada elemen fungsional dalam modul PM-

QKD seperti yang ditampilkan dalam Gambar 2.5. Struktur ini dapat disesuaikan untuk protokol QKD lainnya, misalnya struktur modul pemancar dan penerima pada PM-QKD; dua modul pemancar pada protokol MDI-QKD yang serupa dengan modul dalam Gambar 2.5, sementara struktur penerima tidak relevan dari sudut pandang keamanan; serta dua modul penerima pada protokol EB-QKD yang menyerupai modul penerima dalam Gambar 2.5, dengan modul pemancar yang juga tidak diperhitungkan dalam analisis keamanan. Pembagian komponen ini menjadi landasan untuk analisis ancaman (Bagian 7), penetapan persyaratan fungsional keamanan (Bagian 9), dan kegiatan evaluasi sesuai dengan standar ISO/IEC 23837-2. Dalam konteks ini, komponen dalam modul QKD diklasifikasikan menjadi dua jenis: komponen jaringan konvensional (ditunjukkan dengan latar putih) dan komponen optik kuantum (dengan latar solid). Sementara itu, komponen *Non-Deterministic Random Bit Generator* (NRBG), yang karakteristiknya bergantung pada implementasinya, digambarkan dengan kotak setengah solid. Penting untuk dicatat bahwa pembagian komponen ini bersifat instruksional, dan dapat disesuaikan atau diperinci lebih lanjut oleh penulis PP atau ST sesuai dengan kebutuhan representasi struktur modul QKD secara lebih spesifik.



Gambar 2.5 Struktur internal generik dari implementasi protokol PM-QKD digambar ulang dari [1].

Modul pemancar dalam sistem QKD terdiri atas berbagai komponen fungsional yang dirancang untuk mendukung proses pembangkitan dan pengiriman kunci kuantum secara aman. Komponen utama pertama adalah *signal source*, yang berfungsi menghasilkan foton sesuai dengan protokol QKD yang digunakan. Sumber ini juga dapat dilengkapi dengan kemampuan untuk mengatur intensitas sinyal optik dan melakukan pengkodean informasi. Jika fungsi pengkodean tidak terdapat dalam sumber sinyal, maka foton akan dialirkan ke komponen *encoder* untuk diubah statusnya sesuai dengan skema pengkodean, seperti berdasarkan fasa, polarisasi, atau waktu, tergantung pada protokol QKD yang digunakan.

Beberapa modul pemancar QKD juga dilengkapi dengan komponen isolator yang berfungsi mencegah masuknya kembali pulsa optik dari kanal kuantum ke dalam sistem. Komponen ini bersifat opsional dan umumnya juga mampu mengatur intensitas sinyal optik. Selain itu, komponen penting lainnya adalah NRBG, yang digunakan untuk memilih basis dan nilai bit secara acak dalam proses pengkodean dan pembangkitan material kunci. NRBG dapat diimplementasikan dengan pendekatan berbasis derau fisik konvensional (mengacu pada ISO/IEC 18031) atau dengan prinsip kuantum QRBG. Oleh karena itu, NRBG dikategorikan sebagai komponen jaringan konvensional jika menggunakan desain fisik, atau sebagai komponen optik kuantum jika menggunakan prinsip kuantum.

Selanjutnya, terdapat komponen *post-processing* yang bertugas menangani proses pemrosesan pasca-transmisi, termasuk penyaringan (*sifting*), estimasi parameter, koreksi kesalahan, dan amplifikasi privasi dalam satu sesi QKD. Manajemen dan koordinasi sistem secara keseluruhan dikendalikan oleh

komponen *system control and management*, yang biasanya berbasis sistem tertanam (*embedded*) dan mendukung fungsi kontrol aliran data serta layanan administratif, seperti audit, autentikasi operator, kontrol akses terhadap informasi sensitif, konfigurasi parameter sistem, pengelolaan siklus hidup modul, *debugging* sistem, dan pembaruan perangkat lunak/*firmware*.

Siklus hidup modul QKD meliputi fase desain, pengembangan, pra-operasional, operasional, hingga pemeliharaan. Transisi antar fase ini harus disertai dengan konfigurasi sistem yang sesuai guna menjaga keamanan, yang dapat dikendalikan oleh produsen atau operator. Komponen terakhir yang tak kalah penting adalah manajemen kunci (*Key Management (KM)*), yang memungkinkan komunikasi antara modul QKD dan sistem manajemen kunci eksternal. Fungsinya mencakup pengunggahan sebagian kunci akhir yang dihasilkan ke KM eksternal, pengunduhan kunci awal yang telah dibagikan sebelumnya untuk sesi autentikasi QKD pertama, penyimpanan kunci, serta penghancuran kunci yang sudah tidak diperlukan.

Dokumen ini secara eksplisit mengatur fungsi akses dan penghancuran kunci dalam modul QKD, namun menyerahkan detail fungsi lainnya, seperti derivasi dan penyimpanan kunci, kepada dokumen PP atau ST. Dalam praktiknya, keamanan akses terhadap kunci sangat bergantung pada mekanisme kontrol akses yang diterapkan oleh modul QKD, baik oleh sistem manajemen maupun komponen manajemen kunci itu sendiri, sehingga hanya proses-proses tertentu yang memiliki hak istimewa yang dapat mengakses atau menggunakan material kunci tersebut.

Struktur internal modul penerima dalam sistem QKD pada dasarnya memiliki kesamaan dengan modul pemancar, namun terdapat perbedaan mendasar terkait fungsi dan komponen

utamanya. Modul penerima dilengkapi dengan komponen *decoder* dan *detector* yang bertugas untuk mendekode sinyal optik yang sebelumnya telah diencode oleh komponen sumber sinyal dan encoder pada modul pemancar. Selain itu, terdapat komponen isolator yang berfungsi untuk meredam pulsa optik secara signifikan di dalam modul penerima, guna mencegah keluarnya pulsa tersebut kembali ke kanal kuantum, sehingga menjaga integritas sistem dari gangguan eksternal.

Dalam hal pemilihan basis dekode yang bersifat acak, blok NRBG dalam modul penerima dapat diimplementasikan melalui metode pasif, seperti menggunakan *passive beam splitter*, alih-alih menggunakan NRBG konvensional. Terlepas dari metode implementasi yang digunakan, fungsi utamanya tetap sama, yaitu melakukan pemilihan basis dekode secara acak. Namun, karena pendekatan ini dapat menimbulkan potensi ketidaksempurnaan dalam implementasinya, evaluasi teknis harus selalu dilakukan untuk menjamin keandalannya. Oleh karena itu, dalam representasi diagram seperti pada Gambar 2.5, blok NRBG ini ditampilkan sebagai komponen opsional dan digambarkan dengan garis putus-putus.

d. Bagian 6.4 Lingkup TOE untuk modul QKD

Bagian 6.4 terdiri atas 3 subbagian yaitu umum, definisi TSF, dan definisi TOE.

1) Umum

Berdasarkan analisis struktur dari modul QKD yang bersifat umum, dimungkinkan untuk merumuskan fungsi keamanan TOE yang bersifat umum, serta menetapkan ruang lingkup TOE dalam rangka evaluasi keamanan modul QKD. Hal ini tetap dapat dilakukan meskipun arsitektur protokol QKD dan strategi implementasinya sangat bervariasi dalam praktik. Pendekatan ini memungkinkan proses evaluasi keamanan

yang konsisten dan terstandarisasi terhadap berbagai bentuk modul QKD yang berbeda.

2) Definisi TSF

Dalam mendefinisikan TSF, seperangkat fungsi umum dari modul QKD dapat dirumuskan dengan mengacu pada peran komponen-komponen yang telah dijelaskan pada Bagian 6.3. Secara umum, TSF mencakup setidaknya tiga jenis fungsi utama. Pertama, *Quantum key distribution function* (FUN_QKD), yang meliputi proses pembangkitan data mentah serta prosedur pemrosesan pasca-transmisi. Dalam beberapa kasus, modul QKD juga dapat melaksanakan penyesuaian parameter sebagai bagian dari fungsi ini. Kedua, *system control and management function* (FUN_SCM), yang diimplementasikan oleh komponen manajemen dan kontrol modul QKD, mencakup fungsi pengendalian aliran serta layanan manajerial lain yang relevan sebagaimana diuraikan dalam 6.3. Ketiga, *key management function* (FUN_KM), yang dijalankan oleh komponen manajemen kunci dalam modul QKD untuk melaksanakan proses unggah dan unduh kunci ke dan dari sistem manajemen kunci eksternal, serta penghancuran kunci sesuai kebutuhan.

Ketiga fungsi di atas mencerminkan fungsionalitas dasar yang memungkinkan modul QKD menghasilkan kunci akhir, asalkan sistem berjalan dalam kondisi normal tanpa gangguan atau serangan. Namun, dari perspektif keamanan praktis, setiap komponen dalam modul QKD berpotensi memiliki kerentanan yang mungkin baru teridentifikasi setelah sistem dioperasikan, seiring berkembangnya metode serangan. Karena serangan biasanya dilakukan melalui antarmuka eksternal, modul QKD harus dilengkapi dengan *self-protection function* (FUN_SP) untuk melindungi TSF dari

eksploitasi. Fungsi ini mencakup mekanisme perlindungan terhadap serangan *side-channel* melalui kanal kuantum, fungsi uji mandiri (*self-testing*), kontrol terhadap penyimpanan informasi, pemulihan sistem dari kegagalan, serta penyesuaian parameter.

Perlu dicatat bahwa cakupan spesifik dari setiap fungsi TSF tidak dapat sepenuhnya dirinci dalam dokumen ini karena sangat bergantung pada protokol QKD yang digunakan serta strategi implementasinya. Oleh karena itu, dokumen ini hanya memberikan deskripsi umum mengenai definisi TSF. Penulis dokumen PP atau ST bertanggung jawab untuk merumuskan definisi TSF yang lebih konkret berdasarkan informasi teknis yang lebih lengkap. Sebagai tambahan, meskipun fungsi penyesuaian parameter diklasifikasikan dalam dokumen ini sebagai bagian dari proses pembangkitan data mentah, secara logis fungsi tersebut juga merupakan bagian dari mekanisme perlindungan diri, karena bertujuan untuk memastikan kinerja modul QKD tetap optimal. Namun, fungsi ini tidak termasuk dalam kategori *self-testing* sebagaimana didefinisikan dalam persyaratan fungsional keamanan FPT_TST.1 dan FTP_QKD.1.

3) Definisi TOE

Meskipun dokumen ini tidak menetapkan secara rinci ruang lingkup TOE untuk sistem QKD (karena hal tersebut merupakan tanggung jawab dari dokumen PP atau ST) cakupan umum TOE tetap dapat dirumuskan dengan mempertimbangkan seluruh fungsi esensial sebagaimana dijelaskan dalam Bagian 6.4.2. Secara prinsip, TOE mencakup seluruh komponen yang menjalankan fungsi *Quantum Key Distribution* (FUN_QKD), *System Control and Management* (FUN_SCM), *Key Management* (FUN_KM), dan *Self-Protection* (FUN_SP). Namun demikian, TOE tidak

mencakup kanal kuantum maupun kanal klasik yang meskipun dibutuhkan untuk operasi sistem QKD, tidak menjadi bagian dari objek evaluasi keamanan. Yang termasuk dalam TOE adalah komponen implementasi dari antarmuka eksternal yang berinteraksi langsung dengan kedua kanal tersebut.

Dengan pendekatan ini, TOE yang dimaksud merupakan sistem terdistribusi yang definisinya bergantung pada arsitektur protokol QKD yang diimplementasikan. Untuk protokol PM-QKD, TOE meliputi dua modul yang terpisah, yaitu modul pemancar dan modul penerima, beserta komponen antarmuka eksternal masing-masing sebagaimana ditunjukkan pada Gambar 2.4. Oleh karena itu, TOE yang hanya mencakup satu modul secara individual (baik pemancar maupun penerima saja) tidak sesuai dengan cakupan yang didukung oleh seri standar ISO/IEC 23837.

Dalam konteks protokol MDI-QKD, TOE mencakup dua modul pemancar beserta komponen antarmuka eksternal dari masing-masing modul tersebut. Modul penerima tidak termasuk dalam cakupan TOE, karena meskipun penting untuk menjalankan fungsi QKD, modul ini tidak dianggap sebagai bagian yang harus dipercaya dari sudut pandang keamanan sistem. Sebaliknya, dalam protokol EB-QKD, TOE mencakup dua modul penerima dan komponen antarmuka eksternal yang terkait, sementara modul pemancar tidak termasuk dalam evaluasi keamanan karena tidak dianggap sebagai bagian yang harus dipercaya.

Catatan penting dalam definisi ini adalah bahwa pengecualian modul penerima pada MDI-QKD dan modul pemancar pada EB-QKD dari ruang lingkup evaluasi keamanan memberikan fleksibilitas. Artinya, TOE yang telah

dievaluasi keamanannya dapat digunakan bersamaan dengan modul penerima atau pemancar lain selama modul tersebut berfungsi secara benar, tanpa harus melalui evaluasi ulang. Namun, pendekatan ini tidak menutup kemungkinan untuk memasukkan modul-modul tersebut ke dalam TOE, misalnya sebagai bagian non-TSF berdasarkan kesepakatan antara pengembang dan evaluator.

Selain itu, beberapa strategi implementasi tertentu dapat menjadikan beberapa komponen pada Gambar 2.5 sebagai opsional. Jika suatu komponen tidak diimplementasikan dalam modul QKD, maka secara otomatis komponen tersebut tidak termasuk dalam cakupan TOE. Sebagai contoh, jika modul penerima QKD tidak menggunakan NRBG karena fungsinya digantikan oleh *passive beam splitter*, maka NRBG tidak dianggap sebagai bagian dari TOE.

e. Bagian 6.5 Alur kerja umum modul QKD

Alur kerja dari suatu modul QKD yang berperan dalam membentuk sistem QKD secara umum terdiri atas tiga tahapan utama. Tahap pertama adalah tahap inisialisasi, di mana setiap modul QKD melakukan proses *bootstrapping*, menginisialisasi dirinya, serta menjalankan pengujian awal terhadap komponen-komponen fungsional utama, seperti komponen kriptografi, integritas perangkat lunak dan *firmware*, serta, jika termasuk dalam ruang lingkup TOE, komponen NRBG. Selain itu, pada beberapa implementasi, prosedur autentikasi mutual antar modul QKD dalam sistem mungkin diperlukan sebelum melanjutkan ke tahap selanjutnya.

Tahap kedua adalah tahap pembangkitan data mentah (*raw data generation*), di mana sinyal kuantum dikirimkan melalui kanal kuantum dan dideteksi oleh pihak yang sah untuk menghasilkan data mentah, yaitu data yang saling berkorelasi namun masih

mengandung derau. Pada tahap ini, modul QKD dapat melakukan penyesuaian parameter tertentu secara terbatas guna menjamin kestabilan dan keamanan sistem selama proses transmisi berlangsung.

Tahap ketiga adalah tahap pasca-pemrosesan (*post-processing*), yang berfungsi untuk mengolah data mentah menjadi kunci simetris yang lebih pendek dan aman, yang kemudian menjadi kunci akhir (*final key*). Secara umum, tahap ini mencakup empat sub-tahapan utama, yaitu *sifting*, estimasi parameter, koreksi kesalahan, dan amplifikasi privasi, sebagaimana dijelaskan dalam Bagian 5.2 b). Perlu dicatat bahwa tahap kedua dan ketiga masing-masing merepresentasikan pelaksanaan dari prosedur pertama dan kedua dalam protokol QKD generik yang dijelaskan pada Bagian 5.2.

7. Analisis Masalah Keamanan QKD

a. Bagian 7.1 Umum

Bagian ini bertujuan untuk memberikan landasan dalam merumuskan definisi permasalahan keamanan (*security problem definition*) pada dokumen PP atau ST untuk modul QKD. Mengingat keragaman strategi implementasi modul QKD, dokumen ini secara khusus memfokuskan pembahasan pada permasalahan keamanan yang bersifat umum dan relevan dengan berbagai bentuk implementasi. Permasalahan keamanan yang melampaui kasus umum tersebut tidak dibahas dalam dokumen ini.

Bagian 7.2 dan 7.3 menjadi dasar dari analisis ancaman yang lebih lanjut diuraikan dalam Bagian 7.4 dan 7.5. Secara khusus, ancaman yang timbul akibat kerentanan modul QKD diklasifikasikan ke dalam dua jenis, sesuai dengan metode pembagian komponen yang dijelaskan dalam Bagian 6.3, yaitu: ancaman terhadap komponen jaringan konvensional dan

ancaman terhadap komponen optik kuantum. Perlu dicatat bahwa pembagian ini tidak menutup kemungkinan adanya serangan nyata yang mengeksploitasi kerentanan secara lintas-komponen antara keduanya.

b. Bagian 7.2 Asumsi keamanan

Secara teoretis, protokol QKD mampu membentuk kunci dengan klaim keamanan yang tidak bergantung pada kekuatan komputasi pihak penyerang, selama asumsi-asumsi dalam model pembuktian keamanannya terpenuhi. Namun, dalam konteks keamanan praktis, asumsi-asumsi tersebut perlu ditransformasikan secara tepat. Secara khusus, beberapa asumsi dalam model pembuktian keamanan dapat diterjemahkan menjadi persyaratan fungsional keamanan (*security functional requirements*) yang harus diimplementasikan melalui mekanisme tertentu dan divalidasi dalam proses evaluasi keamanan modul QKD. Di sisi lain, sebagian asumsi lainnya tidak dapat diuji secara langsung dalam evaluasi keamanan, melainkan harus dipertahankan sebagai asumsi terhadap lingkungan operasional. Asumsi-asumsi lingkungan ini merupakan kondisi yang harus dipenuhi agar modul QKD dapat berfungsi dengan baik dalam skenario tertentu, meskipun tidak menjadi objek evaluasi. Secara lebih rinci, asumsi mengenai lingkungan operasional modul QKD mencakup paling tidak tiga aspek utama, yaitu:

1) Modul QKD terproteksi secara fisik pada lingkungan operasionalnya

Asumsi operasional utama dalam modul TOE QKD adalah bahwa modul tersebut beroperasi dalam lingkungan terlindungi yang mencegah agen ancaman mendekati secara fisik dan menjaga jarak geografis minimum melalui langkah-langkah keamanan dan jaminan lingkungan operasional. Hal ini meniadakan kemungkinan serangan fisik invasif maupun

non-invasif parsial yang dapat mengganggu keamanan maupun operasi fisik perangkat, sehingga standar ISO/IEC 23837 tidak mencakup persyaratan perlindungan terhadap manipulasi fisik dan beberapa serangan *side channel* tertentu. Namun, asumsi ini tidak meniadakan ancaman melalui antarmuka eksternal modul QKD; misalnya, komunikasi antara modul QKD dan manajemen kunci yang terkadang berada dalam lingkungan terlindungi secara fisik, tetapi dalam kasus lain rentan terhadap penguping atau manipulasi oleh pelaku internal. Oleh karena itu, mekanisme perlindungan komunikasi pada antarmuka eksternal tersebut wajib diimplementasikan. Pendekatan ini pragmatis dengan mengasumsikan hanya modul QKD yang secara fisik terlindungi, sedangkan antarmuka eksternal rentan terhadap serangan jarak jauh, sehingga SFR seperti perlindungan komunikasi pada antarmuka manajemen kunci dan kontrol manajemen perlu ditegakkan. Penulis PP atau ST dapat memperkuat asumsi ini dengan menganggap seluruh modul dan antarmuka terlindungi secara fisik, sehingga beberapa SFR dapat dikesampingkan. Selain itu, dalam konteks daya komputasi pelaku ancaman, model pembuktian keamanan QKD menganggap kekuatan komputasi pada saluran kuantum dan klasik tidak terbatas, sedangkan untuk antarmuka manajemen kunci dan kontrol diasumsikan terbatas, sehingga mekanisme keamanan komputasi dapat diterapkan untuk melindunginya. Akhirnya, penulis PP atau ST tidak boleh menghilangkan atau mengurangi asumsi ini kecuali ada mekanisme khusus yang mengatasi serangan fisik dalam TOE.

2) Operator tepercaya

Operator dianggap tepercaya dalam pengoperasian TOE, termasuk administrator sistem, auditor, maupun peran sah

lainnya yang menjalankan TOE. Diasumsikan bahwa para operator bertindak demi kepentingan terbaik keamanan organisasi dengan menjalani pelatihan yang memadai, mematuhi kebijakan keamanan, serta mengikuti panduan pengguna secara ketat. Selain itu, administrator diharapkan melaksanakan prosedur konfigurasi sistem serta melakukan pembaruan *firmware* dan perangkat lunak secara rutin sebagai respons terhadap rilis *patch* atau pembaruan produk yang berkaitan dengan kerentanan yang diketahui dan peningkatan teknis. Hal ini penting dalam konteks keamanan QKD, terutama untuk meminimalkan risiko yang timbul dari serangan *side channel*.

- 3) Diasumsikan *pre-shared key* dirahasiakan dan dibangkitkan secara acak sebelum menjadi input modul QKD.

c. Bagian 7.3 Analisis aset

Beberapa data dan fungsi dalam modul QKD harus dilindungi dari kebocoran atau kerusakan guna menjamin keamanan modul QKD tersebut. Dalam dokumen ini, aset-aset umum modul QKD diidentifikasi sebagai berikut, meskipun daftar aset yang konkret dalam suatu PP atau ST hanya dapat disesuaikan berdasarkan implementasi spesifik modul QKD. Pertama, kunci akhir yang dihasilkan dari pelaksanaan protokol QKD harus dijaga keamanannya, termasuk semua informasi terkait keamanan yang dianggap sebagai aset individual dan harus dilindungi dari kebocoran atau kerusakan sepanjang siklus hidup yang telah ditetapkan. Secara rinci, bahan kunci meliputi data mentah, data *sifting*, dan data yang sudah dikoreksi kesalahannya selama eksekusi sistem QKD; kunci autentikasi QKD untuk autentikasi pesan melalui saluran klasik; serta kunci yang digunakan untuk menjaga kerahasiaan dan integritas komunikasi antara manajemen kunci dan modul QKD saat proses pengunggahan kunci akhir atau pengunduhan kunci yang

sudah dibagikan sebelumnya secara opsional. Protokol QKD mengasumsikan bahwa sebagian data mentah, data *sifting*, dan data yang telah dikoreksi dapat diketahui oleh agen ancaman setelah transmisi keadaan kuantum dan beberapa bagian dapat terungkap selama tahap pasca-pemrosesan, namun kebocoran dan pengungkapan tersebut telah diperkirakan pada estimasi parameter agar amplifikasi privasi yang sesuai dapat dilakukan untuk menghasilkan kunci akhir. Seluruh aset harus dilindungi dari kebocoran atau kerusakan akibat potensi serangan lainnya. Perlu dicatat bahwa tahap *sifting* (dan data *sifting*) tidak selalu diperlukan pada beberapa protokol CV-QKD yang menggunakan pengukuran *heterodyne*. Kedua, data autentikasi pengguna seperti kata sandi, PIN, kredensial, dan data terkait untuk autentikasi operator juga termasuk aset yang harus dilindungi. Ketiga, informasi lain yang berkaitan dengan keamanan seperti catatan audit, data audit, informasi kontrol dan manajemen yang dikomunikasikan melalui antarmuka kontrol dan manajemen, serta informasi lain yang mendukung keamanan TOE juga termasuk dalam aset. Kunci akhir, bahan kunci, data autentikasi, dan informasi terkait keamanan tersebut diakui sebagai bagian dari data TSF pada TOE. Selain itu, fungsi-fungsi modul QKD yang harus dilindungi agar tidak disalahgunakan oleh pengguna yang tidak sah juga merupakan bagian penting dalam menjaga keamanan modul tersebut, khususnya dalam konteks mitigasi risiko terhadap serangan *side channel*.

- d. Bagian 7.4 Ancaman terhadap komponen jaringan konvensional
Bagian 7.4 terdiri atas 2 subbagian yaitu *overview* dan ancaman terhadap perspektif serangan klasik berbasis-jaringan.

1) *Overview*

Sebagai salah satu jenis perangkat jaringan, modul QKD secara potensial rentan terhadap serangan yang serupa dengan perangkat jaringan konvensional. Kerentanan

signifikan yang tersembunyi dalam modul QKD dapat menarik perhatian serangan praktis dalam konteks praktik rekayasa kriptografi. Dengan meninjau lebih dekat struktur dari modul QKD yang umum, dimungkinkan untuk mengidentifikasi jalur potensial bagi agen ancaman dalam melakukan tindakan merugikan melalui antarmuka jaringan modul, termasuk dengan mengubah lingkungan operasional atau bahkan menyelidiki sirkuit *chip* internal perangkat tersebut (misalnya melalui serangan berbasis jaringan, serangan *side channel*, dan serangan perusakan fisik). Secara khusus, agen ancaman dapat memanfaatkan berbagai strategi untuk mengompromikan aset dengan cara menghindari mekanisme pengendalian akses, merusak skema autentikasi pesan, atau menyalahgunakan fungsi pemeliharaan pada modul QKD. Keberagaman jalur serangan ini membuat sulit untuk mencantumkan seluruh ancaman yang mungkin terjadi terhadap modul QKD. Namun demikian, dari sudut pandang praktis, ancaman-ancaman yang dirinci dalam bagian 7.4.2 harus diatasi oleh modul QKD dan lingkungan operasionalnya, baik melalui kontrol yang berbasis teknologi informasi (*IT-related controls*) maupun kontrol non-IT, seperti perlindungan lingkungan atau prosedur dan kebijakan organisasi.

2) Ancaman terhadap perspektif serangan klasik berbasis-jaringan

Sebagai perangkat jaringan khusus, modul QKD berpotensi mengalami serangan yang serupa dengan perangkat jaringan konvensional. Deskripsi ancaman pada perangkat jaringan yang terdapat dalam *Collaborative Protection Profile for Network Devices* dapat dijadikan referensi dalam analisis ancaman terhadap modul QKD. Serangan berbasis jaringan konvensional umumnya dilakukan melalui antarmuka

eksternal klasik dari modul QKD, seperti antarmuka kontrol dan manajemen, antarmuka manajemen kunci, serta antarmuka saluran klasik. Serangan ini dapat dilakukan dari jarak jauh tanpa perlu pendekatan fisik terhadap TOE. Untuk kepraktisan, dokumen ini mengelompokkan ancaman berdasarkan jalur serangan dan menyajikannya secara alfabetis.

Perlu dicatat bahwa daftar ancaman berikut tidak dimaksudkan sebagai daftar lengkap, melainkan mencerminkan pemahaman akademik dan industri terkini tentang keamanan perangkat jaringan dan modul QKD. Ancaman-ancaman ini juga dapat saling bergantung, berinteraksi, dan berkonvergensi, meskipun pada akhirnya bertujuan sama yaitu mengompromikan aset modul QKD.

- a) *Audit circumvention*: Ancaman ini terjadi ketika fungsi audit sistem dimanipulasi oleh agen ancaman agar dapat melewati, mengakses, atau mengubah data audit tanpa otorisasi, memungkinkan kompromi aset tanpa terdeteksi oleh administrator.
- b) *Eksplorasi kerentanan kriptografi*: Agen ancaman dapat mengeksploitasi kelemahan tersembunyi dalam algoritma kriptografi, atau pada desain dan implementasi protokol kriptografi untuk menyerang fungsi-fungsi penting seperti autentikasi pesan, amplifikasi privasi, unggah kunci, dan autentikasi pengguna.
- c) *Eksplorasi kegagalan*: Kegagalan operasional TOE akibat kesalahan sistem, ketidakstabilan lingkungan, atau gangguan dari agen ancaman dapat dimanfaatkan untuk mengakses aset TOE. Oleh karena itu, modul QKD harus mempertahankan kondisi aman meskipun terjadi kegagalan.

- d) Penyalahgunaan fungsi: Fungsi pengujian, debugging, atau manajemen yang tidak dinonaktifkan dengan benar setelah tahap pengembangan dapat dimanfaatkan oleh agen ancaman untuk mengakses aset TOE secara tidak sah.
- e) Pelanggaran keamanan fisik: Meskipun serangan fisik invasif dan non-invasif dengan akses langsung dikecualikan dalam cakupan dokumen ini karena asumsi perlindungan fisik oleh lingkungan operasional, dokumen ini tetap mempertimbangkan serangan non-invasif jarak jauh seperti *timing attacks* dan *cache-timing attacks* yang dapat mengeksploitasi informasi dari *side channel*.
- f) Eksploitasi cacat keacakan (*randomness defect exploitation*): Kelemahan dalam NRBG (pembangkitan bit acak) dapat dimanfaatkan untuk memprediksi atau mengakses informasi sensitif, yang berpengaruh pada berbagai fungsi seperti pengkodean kuantum, pemilihan basis pengukuran, serta amplifikasi privasi.
- g) Penyalahgunaan data residual: Informasi sensitif yang tidak dihapus secara permanen setelah masa berlaku berakhir dapat diekstrak oleh agen ancaman, memungkinkan kompromi terhadap aset historis TOE.
- h) Akses tidak sah: Agen ancaman dapat menembus mekanisme kontrol akses melalui berbagai metode seperti penyusupan dari antarmuka manajemen, konfigurasi salah, penggunaan kredensial yang dicuri, atau menyamar sebagai modul QKD yang sah. Ini memungkinkan pengambilan data tanpa otorisasi dan akses ke aset sensitif.

Contohnya, modul QKD dapat memerlukan autentikasi pengguna sebelum masuk ke sistem, dan mengatur agar bahkan administrator tidak memiliki akses ke kunci akhir

dalam bentuk teks polos, demi menjaga kerahasiaan kunci secara maksimal.

e. Bagian 7.5 Ancaman terhadap komponen optik kuantum

Bagian 7.5 terdiri atas 4 subbagian yaitu *overview*, ancaman yang mengeksploitasi kelemahan sumber optik, ancaman yang mengeksploitasi kerentanan deteksi optik dan ancaman mengeksploitasi kerentanan penyesuaian parameter.

1) *Overview*

Untuk menganalisis secara lebih baik ancaman yang berkaitan dengan eksploitasi kerentanan keamanan pada komponen optik kuantum dalam modul QKD, kerentanan dibedakan menjadi dua jenis utama, yaitu kerentanan aktif dan pasif. Kedua jenis ini secara umum mewakili dua strategi serangan berbeda yang dilakukan oleh agen ancaman. Kerentanan aktif merujuk pada kebocoran informasi yang disebabkan oleh serangan aktif, seperti *Trojan horse attack*, *source tampering attack*, atau *blinding attack*. Sebaliknya, kerentanan pasif mencakup kerentanan terhadap serangan *side channel* yang muncul akibat ketidaksempurnaan komponen optik, seperti modulasinya yang tidak sempurna, fluktuasi intensitas pulsa, serta ketidaksesuaian efisiensi deteksi pada detektor foton tunggal. Penjelasan berikutnya dalam dokumen ini secara khusus didedikasikan untuk menganalisis kedua jenis kerentanan tersebut secara rinci.

Catatan: Survei yang lebih komprehensif mengenai berbagai jenis serangan terhadap sistem QKD dapat ditemukan dalam ETSI *White Paper* tentang Keamanan Implementasi Kriptografi Kuantum.

2) Ancaman yang mengeksploitasi kelemahan sumber optik

Agen ancaman dapat mencoba mengeksploitasi kerentanan pada komponen optik kuantum (termasuk sumber sinyal dan

encoder) dari modul pemancar QKD untuk membahayakan kunci final. Kategori ancaman ini dapat berkaitan dengan modul pemancar QKD pada protokol PM-QKD maupun MDI-QKD. Sebagai contoh, dalam modul DV-QKD, fase dari setiap pulsa sinyal seharusnya diacak secara merata. Namun, dalam praktiknya, pengacakan sempurna ini tidak selalu dapat dicapai. Ketika pengacakan tidak sepenuhnya tercapai, agen ancaman dapat mencoba membedakan sebagian keadaan kuantum yang dipersiapkan oleh modul pemancar QKD dengan melakukan pengukuran pada ruang fase. Selain itu, serangan lain untuk mencapai tujuan yang sama juga telah ditemukan, yang memanfaatkan kelemahan pada sumber, seperti *source tampering attack*, *Trojan-horse attack*, ketidaksempurnaan dalam persiapan keadaan kuantum, dan kegagalan dalam mengacak fase sinyal secara benar.

- 3) Ancaman yang mengeksploitasi kerentanan deteksi optik
Agen ancaman dapat mencoba mengeksploitasi kerentanan pada satu atau lebih komponen optik kuantum (termasuk dekoder dan detektor) dari modul penerima QKD. Jika berhasil, serangan ini berpotensi mengkompromikan kunci final. Jenis ancaman ini dapat ditujukan pada modul penerima QKD yang mengoperasikan baik protokol PM-QKD maupun beberapa protokol EB-QKD. Sebagai contoh, diketahui bahwa sebagian besar modul penerima QKD menggunakan dua detektor foton tunggal. Namun, sangat sulit untuk mencocokkan kedua detektor tersebut secara sempurna dalam semua derajat kebebasan, seperti waktu, frekuensi, dan polarisasi. Berdasarkan ketidaksesuaian ini, agen ancaman dapat sepenuhnya atau sebagian mengendalikan klik dari detektor foton tunggal dengan mengatur parameter keadaan kuantum yang masuk. Selain itu, berbagai serangan lainnya juga telah ditemukan yang

memanfaatkan kelemahan pada proses deteksi, seperti *blinding attack*, *faked state attack*, *dead-time attack*, dan *wavelength attack*.

4) Ancaman mengeksploitasi kerentanan penyesuaian parameter

Agen ancaman dapat berupaya mengeksploitasi kerentanan yang tersembunyi dalam implementasi prosedur penyesuaian parameter. Dalam situasi ini, agen ancaman dapat berhasil menipu modul-modul QKD untuk beroperasi seolah-olah sistem QKD berada dalam kondisi aman, padahal sebenarnya tidak demikian. Jika serangan ini berhasil, maka dapat menyebabkan kompromi terhadap kunci final yang dihasilkan oleh modul-modul QKD. Jenis ancaman ini dapat ditujukan pada modul pemancar atau penerima QKD yang menjalankan protokol PM-QKD, modul pemancar dalam protokol MDI-QKD, atau modul penerima dalam protokol EB-QKD. Sebagai contoh, sebelum atau selama sesi QKD, modul pemancar dan penerima QKD diharapkan mampu menyesuaikan parameter sistem mereka, seperti menyelaraskan waktu deteksi foton tunggal dengan waktu kedatangan keadaan kuantum. Agen ancaman dapat secara aktif mengubah waktu dari berbagai sinyal yang digunakan untuk menyesuaikan waktu detektor, sehingga menciptakan kerentanan *time-mismatch* yang aktif dan dapat dieksploitasi.

8. Komponen Fungsional Keamanan yang Diperluas untuk Implementasi QKD

a. Bagian 8.1 Umum

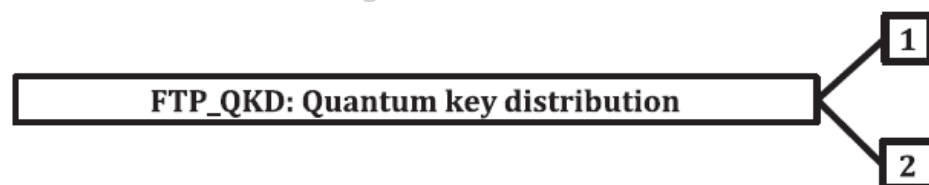
Secara umum, komponen fungsional keamanan standar yang didefinisikan dalam ISO/IEC 15408-2 dapat digunakan untuk menggambarkan kebutuhan keamanan dari modul QKD. Namun demikian, karena komponen-komponen fungsional keamanan

tersebut tidak dapat disesuaikan secara langsung untuk menangani seluruh karakteristik khusus yang dimiliki oleh modul QKD, maka diperlukan definisi terhadap komponen fungsional keamanan yang diperluas. Kelas fungsional keamanan standar FTP (*Trusted Path/Channels*) dalam ISO/IEC 15408-2 digunakan untuk menetapkan persyaratan terkait pembentukan saluran komunikasi tepercaya antara pihak-pihak yang terhubung dalam jaringan (secara khusus antara TSF dan produk TI tepercaya lainnya). Mengingat bahwa protokol QKD dapat digunakan untuk mencapai tujuan serupa (yaitu dengan menggunakan kunci akhir yang dihasilkan untuk membentuk saluran komunikasi yang tepercaya antar pengguna) maka relevan untuk memperluas komponen fungsional keamanan dalam kelas FTP guna mencakup fungsi-fungsi keamanan yang dimiliki oleh QKD. Secara khusus, komponen fungsional keamanan yang diperluas tersebut adalah FTP_QKD.1 dan FTP_QKD.2 yang dirancang untuk menentukan implementasi protokol QKD sebagaimana dijelaskan dalam Bagian 8.2.

b. Bagian 8.2 Komponen Fungsional Keamanan yang Diperluas ke kelas FTP: *Trusted path/channels*

1) Pelevelan komponen dan deskripsinya

Gambar 2.6 menunjukkan pelevelan komponen untuk *family* ini.



Gambar 2.6 FTP_QKD *quantum key distribution* digambar ulang dari [1].

FTP_QKD.1 Protokol QKD dan pembangkitan data mentah mensyaratkan pembentukan kunci simetris sesuai dengan protokol yang ditentukan yang melibatkan transmisi dan

deteksi sinyal kuantum. Hal ini mencakup negosiasi konfigurasi dan penyesuaian parameter jika diperlukan.

FTP_QKD.2 Proses pasca-pemrosesan QKD mensyaratkan kunci simetris dibentuk secara aman oleh modul QKD dari data mentah sesuai dengan protokol QKD. Penjelasan secara lengkap mengenai pelevelan pada *family* ini dapat dilihat pada dokumen ISO/IEC 23837-1:2023.

9. Persyaratan Fungsional Keamanan untuk Modul QKD

Bagian ini menjabarkan *baseline* SFR yang wajib dipenuhi oleh modul QKD. Pemenuhan terhadap SFR ini sangat penting agar TOE dapat mempertahankan perlindungan terhadap potensi ancaman yang telah dianalisis dalam Subbagian 7.4 dan 7.5. Oleh karena itu, SFR ini bersifat wajib dan menjadi dasar penyusunan PP serta ST. Namun demikian, mengingat beragamnya implementasi modul QKD dan lingkungan operasionalnya, Bagian 10 memberikan ketentuan khusus yang memperbolehkan penulis PP atau ST untuk menghilangkan atau menyesuaikan SFR tertentu, dengan syarat disertai justifikasi yang memadai terhadap perubahan atau penghilangan tersebut.

SFR diklasifikasikan ke dalam tiga kelompok, yaitu: persyaratan terhadap komponen jaringan konvensional (Lihat 9.2), persyaratan terhadap implementasi protokol QKD (Lihat 9.3), dan persyaratan terhadap komponen optik kuantum (Lihat 9.4). Dari perspektif fungsionalitas keamanan, setiap SFR dapat dikaitkan dengan satu atau lebih fungsi dari TSF, dan setiap fungsi tersebut dapat direalisasikan melalui komponen jaringan konvensional, komponen optik kuantum, atau kombinasi keduanya. Hubungan antara fungsi dan komponen-komponen ini dijelaskan dalam kolom ketiga dan keempat pada Tabel 2.3.

Untuk memberikan fleksibilitas yang cukup dalam implementasi modul QKD, sebagian besar operasi dalam SFR belum dirinci dalam

dokumen ini. Dalam penyusunan PP atau ST, setiap operasi pada SFR harus diselesaikan sesuai dengan ketentuan dalam ISO/IEC 15408-1:2022, Bagian 8.2, serta sesuai dengan ketentuan terkait penggunaan komponen fungsional keamanan dalam ISO/IEC 15408-2. Secara khusus, dalam menyelesaikan *assignments* dan *selections* pada SFR yang bersumber dari komponen fungsional keamanan terstandardisasi dalam ISO/IEC 15408-2, harus merujuk pada prinsip-prinsip relevan dalam standar tersebut untuk menentukan apakah penggunaan nilai "None" sah atau tidak. Selain itu, catatan aplikasi di bawah setiap SFR memberikan panduan dalam pemilihannya serta rekomendasi atau persyaratan lebih rinci untuk penyelesaiannya.

Metode evaluasi dan aktivitas yang berkaitan dengan SFR dijelaskan dalam ISO/IEC 23837-2. Seri ISO/IEC 23837 secara umum menyediakan kerangka kerja untuk evaluasi keamanan modul QKD dalam kerangka kerja seri ISO/IEC 15408, dan dapat digunakan untuk memfasilitasi pengembangan PP bagi modul QKD. Panduan penyusunan *protection profile* untuk modul QKD disediakan dalam Lampiran A.

Tabel 2.3 *Overview baseline* kumpulan SFR untuk modul QKD.

Subbagian	SFR	Fungsi keamanan	Komponen implementasi
9.2.1	FAU_GEN.1	FUN_SCM	Komponen jaringan konvensional
9.2.2	FCS_CKM.6	FUN_KM	
9.2.3	FCS_COP.1	FUN_QKD, FUN_SCM, FUN_KM	
9.2.4	FCS_RNG.1	FUN_QKD	
9.2.5	FDP_ACC.1	FUN_SCM	
9.2.6	FDP_ACF.1	FUN_SCM	
9.2.7	FDP_IRC.1	FUN_SP	

Subbagian	SFR	Fungsi keamanan	Komponen implementasi
9.2.8	FDP_ITC.1	FUN_SCM	
9.2.9	FIA_UAU.2	FUN_SCM	
9.2.10	FIA_UID.1	FUN_SCM	
9.2.11	FMT_LIM.1	FUN_SCM	
9.2.12	FMT_LIM.2	FUN_SCM	
9.2.13	FMT_MSA.1	FUN_SCM	
9.2.14	FMT_MTD.1	FUN_SCM	
9.2.15	FMT_SMF.1	FUN_SCM	
9.2.16	FMT_SMR.1	FUN_SCM	
9.2.17	FMT_EMS.1/ Convention	FUN_SP	
9.2.18	FPT_FLS.1	FUN_SP	
9.2.19	FPT_ITC.1	FUN_KM	
9.2.20	FPT_ITL.1	FUN_KM	
9.2.21	FPT_RCV.2	FUN_SP	
9.2.22	FPT_TST.1	FUN_SP	
9.3.2	FTP_QKD.1	FUN_QKD	Komponen jaringan konvensional dan komponen optik kuantum
9.3.3	FTP_QKD.2	FUN_QKD	Komponen jaringan konvensional
9.4.2	FPT_EMS.1/Quantum	FUN_SP	komponen optik kuantum
9.4.3	FPT_PHP.3	FUN_SP	Komponen jaringan konvensional

Subbagian	SFR	Fungsi keamanan	Komponen implementasi
			dan komponen optik kuantum

Penjelasan Tabel 2.3 secara lengkap dapat dilihat pada dokumen ISO/IEC 23837-1:2023 Subbab 9.2.1 sampai dengan Subbab 9.2.22.

- a. Bagian 9.2 Persyaratan umum untuk komponen jaringan konvensional dalam modul QKD

Bagian 9.2 terdiri atas 22 subbagian yang berisi penjelasan setiap SFR mulai dari FAU_GEN.1 *Audit data generation* sampai dengan FPT_TST.1 TSF *self-testing* yang terdiri atas persyaratan dan catatan aplikasi (*application note*). Penjelasan secara lengkap dapat dilihat pada dokumen ISO/IEC 23837-1:2023 Subbab 9.2.1 sampai dengan Subbab 9.2.22.

- b. Bagian 9.3 Persyaratan umum untuk penerapan protokol QKD Implementasi protokol QKD mendorong perlunya perumusan definisi SFR yang baru, khususnya SFR yang mencakup tahap pembangkitan data mentah dan tahap pasca-pemrosesan. Definisi baru ini membentuk kumpulan dasar SFR yang harus dipenuhi oleh TOE. Kumpulan ini merupakan syarat fundamental agar TSF dapat berfungsi secara efektif. Terkait dengan kegiatan evaluasi atas SFR tersebut, metode evaluasi yang relevan telah ditetapkan dalam standar ISO/IEC 23837-2. Ketentuan ini menjadi penting dalam menghadapi tantangan keamanan, termasuk potensi serangan *side channel*, sehingga integritas dan efektivitas sistem distribusi kunci kuantum dapat terjaga dengan baik. Pada bagian ini dijelaskan mulai dari FTP_QKD.1 QKD *protocol and raw data generation* sampai dengan FTP_QKD.2 QKD *post-processing* masing-masing terdiri atas persyaratan dan catatan aplikasi. Penjelasan secara lengkap

dapat dilihat pada dokumen ISO/IEC 23837-1:2023 Subbab 9.3.2 sampai dengan Subbab 9.3.3.

c. Bagian 9.4 Persyaratan umum untuk komponen optik kuantum modul QKD

Upaya untuk menghadapi serangan *side channel* yang saat ini telah diketahui, yang sebagian besar dilakukan melalui kanal kuantum, memerlukan penerapan persyaratan keamanan yang mencakup dua aspek utama. Pertama, adalah persyaratan untuk menahan serangan *side channel* pasif (FPT_EMS.1), dan kedua, persyaratan untuk menahan serangan *side channel* aktif (FPT_PHP.3). Kedua jenis persyaratan ini dirancang untuk memperkuat keamanan komponen optik kuantum dalam sistem QKD. Terkait dengan kegiatan evaluasi atas SFR tersebut, metode evaluasi yang relevan telah ditetapkan secara resmi dalam standar ISO/IEC 23837-2, yang berfungsi sebagai acuan teknis dalam menjamin efektivitas dan keandalan sistem terhadap ancaman keamanan yang bersifat fisik maupun pasif. Penjelasan secara lengkap dapat dilihat pada dokumen ISO/IEC 23837-1:2023 Subbab 9.4.2 sampai dengan Subbab 9.4.3.

10. Komponen Fungsional Keamanan yang Diperluas untuk Implementasi QKD

a. Bagian 10.1 Umum

Seri standar ISO/IEC 23837 memberikan dasar untuk pengembangan PP atau ST bagi modul QKD. Oleh karena itu, penting untuk menjelaskan persyaratan konformitas bagi PP, ST, maupun metode evaluasi yang mengklaim kepatuhan terhadap standar ini. Persyaratan konformitas untuk PP dan ST dijelaskan secara spesifik pada Bagian 10.2 dan Bagian 10.3, sedangkan persyaratan konformitas untuk metode pengujian dan evaluasi dibahas secara rinci dalam ISO/IEC 23837-2. Secara umum, ketika suatu PP atau ST menyatakan kepatuhan terhadap dokumen ini, maka dokumen tersebut harus menawarkan solusi

atas permasalahan keamanan umum yang diuraikan dalam standar. Solusi tersebut dapat disusun dengan cara yang setara atau lebih ketat dibandingkan dengan persyaratan yang tercantum dalam dokumen ini. Dengan demikian, PP atau ST dapat berisi pernyataan yang berbeda selama secara keseluruhan tetap menetapkan pembatasan yang setara atau lebih kuat terhadap TOE, disertai dengan asumsi terhadap lingkungan operasional TOE yang setara atau lebih lemah. Untuk memberikan fleksibilitas dalam implementasi, sejumlah pengecualian tambahan dijelaskan dalam Bagian 10.2 dan Bagian 10.3. Pernyataan konformitas dalam dokumen ini secara utama berkaitan dengan definisi permasalahan keamanan dan persyaratan fungsional keamanan, termasuk dalam konteks perlindungan terhadap serangan *side channel* dalam sistem QKD.

- b. Bagian 10.2 pernyataan kesesuaian khusus untuk definisi masalah keamanan

Kepatuhan terhadap dokumen ini mensyaratkan bahwa definisi permasalahan keamanan dalam PP atau ST harus setara, ekuivalen, atau lebih ketat dibandingkan dengan yang ditetapkan dalam Klausul 7, serta disertai justifikasi terhadap penggunaan beberapa pengecualian yang diizinkan.

- 1) Pertama, PP/ST harus mencantumkan semua asumsi sebagaimana dijelaskan dalam Klausul 7.2, dengan sejumlah pengecualian, yaitu:
 - a) asumsi mengenai lingkungan operasional dapat digantikan dengan kontrol keamanan terkait TI dalam TOE, sepanjang seluruh bagian yang terdampak digantikan secara memadai oleh kontrol tersebut;
 - b) asumsi baru dapat ditambahkan selama tidak memengaruhi kontrol keamanan TI dan tidak digunakan

untuk mengatasi ancaman yang seharusnya ditangani oleh kontrol tersebut;

- c) asumsi baru terkait lingkungan operasional dapat dimasukkan jika dapat dibuktikan bahwa asumsi tersebut realistis dalam lingkungan operasional TOE dan lebih praktis dibandingkan penerapan kontrol keamanan TI.

Sebagai contoh, pada skenario praktis di mana modul QKD dan sistem manajemen kunci ditempatkan dalam lingkungan fisik yang terlindungi, maka antarmuka manajemen dan kendali tidak lagi memerlukan perlindungan melalui kontrol keamanan TI. Dengan demikian, SFR seperti FPT_ITC.1 dan FPT_ITI.1 dapat dilonggarkan berdasarkan ketentuan pada Poin 1)c).

- 2) PP/ST harus mencantumkan ancaman-ancaman yang dianalisis dalam Klausul 7.4 dan 7.5, dengan pengecualian sebagai berikut:
 - a) ancaman baru dapat ditambahkan jika berkaitan dengan karakteristik spesifik dari TOE;
 - b) ancaman yang tercantum dalam bagian 7.4 atau 7.5 dapat dihilangkan dari PP/ST apabila terdapat asumsi baru mengenai lingkungan operasional TOE sebagai mana yang dijelaskan dalam 1)b) atau 1)c) yang dapat menangkal ancaman tersebut.

- c. Bagian 10.3 pernyataan kesesuaian khusus terhadap persyaratan fungsional keamanan

SFR yang ditetapkan dalam Bagian 9 bertujuan untuk menjaga ketahanan TOE terhadap ancaman yang telah diidentifikasi. Kepatuhan terhadap dokumen ini mengharuskan SFR yang dirumuskan dalam PP atau ST memiliki tingkat ketat yang setara, ekuivalen, atau lebih tinggi dibandingkan dengan SFR

dalam Bagian 9. Oleh karena itu, PP/ST wajib mencantumkan seluruh SFR yang ditetapkan dalam Bagian 9, dengan beberapa pengecualian yang diizinkan sebagaimana berikut:

- 1) Penghapusan SFR dapat dilakukan apabila alasan konformitas dalam PP/ST menunjukkan bahwa
 - a) SFR tersebut tidak lagi dibutuhkan karena adanya asumsi baru atau yang diperluas mengenai lingkungan operasional TOE, sebagaimana dijelaskan dalam Butir 10.2 a) 2) atau 10.2 a) 3);
 - b) SFR tersebut tidak lagi relevan karena karakteristik spesifik TOE; atau
 - c) SFR tersebut telah digantikan dengan SFR lain yang secara hierarkis lebih kuat atau SFR yang diperluas untuk memenuhi kebutuhan yang sama.
- 2) Penyesuaian SFR terhadap TOE diperbolehkan apabila alasan konformitas menunjukkan bahwa:
 - a) penyelesaian operasi untuk setiap SFR sesuai dengan catatan aplikasinya, dan
 - b) persyaratan yang disesuaikan tetap memberlakukan pembatasan yang sebanding dengan yang ditetapkan dalam Bagian 9, kecuali TOE memiliki karakteristik yang memungkinkan pelanggaran.
- 3) PP/ST juga dapat mengklaim SFR tambahan atau SFR yang lebih kuat secara hierarkis, asalkan dapat dibuktikan bahwa SFR tersebut konsisten secara internal dengan SFR relevan dalam Bagian 9. Pendekatan ini memastikan bahwa sistem QKD tetap memiliki ketahanan yang tinggi terhadap berbagai ancaman, termasuk serangan *side channel*, sambil memberikan fleksibilitas dalam penyusunan dan evaluasi PP/ST.

11. Lampiran A Panduan (informatif) untuk mengembangkan *Protection Profile* bagi Modul QKD

Seri ISO/IEC 23837 menyediakan kerangka umum untuk evaluasi keamanan modul QKD dalam kerangka kerja ISO/IEC 15408, dan dapat digunakan untuk memfasilitasi pengembangan PP bagi modul QKD. PP untuk modul QKD merupakan spesifikasi persyaratan keamanan pada jenis modul QKD tertentu yang digunakan untuk mengungkapkan ekspektasi pengguna terkait aspek keamanan modul tersebut, serta memastikan kelayakan teknis dari persyaratan tersebut. Beberapa deskripsi umum namun rinci mengenai struktur PP dan panduan penyusunannya telah dijelaskan dalam ISO/IEC 15408-1:2022 Lampiran B dan ISO/IEC TR 15446. Informasi tambahan dalam lampiran A bertujuan untuk melengkapi konten yang diperlukan dalam penulisan PP untuk jenis modul QKD tertentu. Penjabaran tersebut mengikuti struktur konten wajib dari PP standar sebagaimana dijelaskan dalam ISO/IEC 15408-1:2022, Bagian B.3.

B. ISO/IEC 23837-2:2023 *Information security — Security requirements, test and evaluation methods for quantum key distribution Part 2: Evaluation and testing methods*

Dokumen ini menetapkan metode pengujian dan evaluasi untuk evaluasi keamanan QKD [2]. Dokumen ini juga menjelaskan aktivitas evaluasi yang merupakan bagian dari metode pengujian dan evaluasi terhadap persyaratan fungsional keamanan pada implementasi protokol QKD, komponen *quantum optic* dan komponen jaringan konvensional dalam modul QKD. Selain itu juga terdapat kegiatan evaluasi tambahan untuk persyaratan jaminan keamanan untuk mendukung evaluasi keamanan QKD dengan tingkat jaminan yang sesuai.

Adapun struktur dokumen ini terdiri atas beberapa bab sebagai berikut:

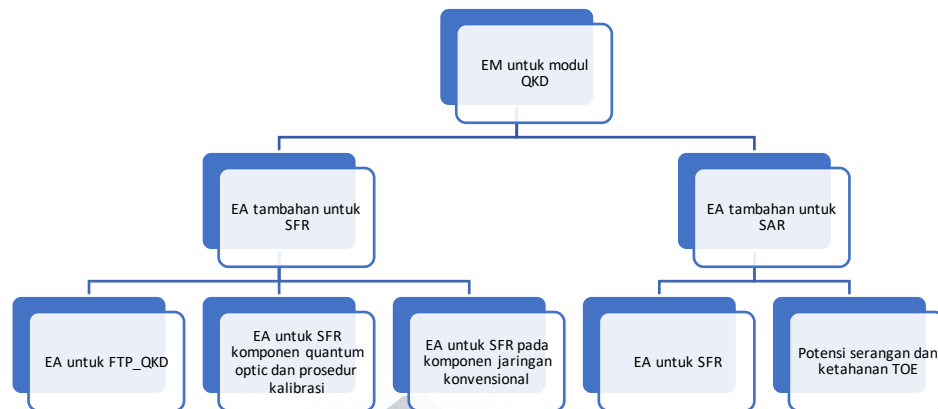
1. Pendahuluan
2. Ruang lingkup

3. Referensi acuan
4. Istilah dan definisi
5. Singkatan
6. Gambaran umum metode evaluasi untuk model QKD
7. Kegiatan evaluasi untuk FTP_QKD
8. Kegiatan evaluasi untuk mengevaluasi komponen *quantum optical* dalam modul transmitter
9. Kegiatan evaluasi untuk evaluasi komponen *quantum optical* dalam modul *receiver*
10. Kegiatan evaluasi untuk evaluasi prosedur parameter *adjustment*
11. Kegiatan tambahan untuk evaluasi *Security Functional Requirement* (SFR) pada komponen jaringan konvensional
12. Kegiatan tambahan untuk *Security Assurance Requirements* (SAR)
13. Pernyataan kesesuaian
14. Lampiran A Panduan (informatif) perhitungan potensi serangan untuk evaluasi modul QKD
15. Lampiran B Contoh penilaian (informatif) untuk perhitungan potensi serangan AVA
16. Lampiran C Kumpulan (informatif) ambang batas
17. Lampiran D Korespondensi (informatif) antara kegiatan evaluasi dan serangan yang dikenal terhadap komponen *quantum optic* dan prosedur parameter *adjustment* pada modul QKD.

Tujuan utama dari evaluasi keamanan modul QKD adalah untuk memverifikasi apakah implementasi fungsi keamanan TI dari modul QKD memenuhi persyaratan keamanan pada tingkat jaminan evaluasi (*Evaluation Assurance Level* (EAL)) yang diharapkan.

Dokumen ini memberikan metode evaluasi (*evaluation method* (EM)) untuk melengkapi ISO/IEC 18045 dengan mempertimbangkan karakteristik khusus modul QKD. EM ini mencakup beberapa kegiatan evaluasi spesifik untuk SFR yang didefinisikan dalam ISO/IEC 23837-1, serta persyaratan jaminan keamanan (*Security Assurance Requirement* (SAR)) yang didefinisikan berdasarkan ISO/IEC 18045. Gambar 2.7

berikut merupakan struktur EM spesifik untuk modul QKD dan komponen kegiatan evaluasinya (*Evaluation activities* (EA)).



Gambar 2.7 Struktur EM spesifik untuk modul QKD digambar ulang dari [2]

Berdasarkan Gambar 2.7, berikut dijelaskan lebih lanjut EA tambahan untuk SFR dan SAR untuk protokol QKD.

1. EA tambahan untuk SFR
 - a. EA untuk mengevaluasi FTP_QKD

SFR yang digunakan pada implementasi protokol QKD yaitu FTP_QKD. Adapun SFR ini memiliki 2 (dua) komponen) yaitu FTP_QKD.1 *raw data generation* dan FTP_QKD.2 *post-processing*. Tabel 2.4 berikut menjelaskan EA untuk mengevaluasi FTP_QKD.

Tabel 2.4 EA untuk mengevaluasi FTP_QKD.

EA	Deskripsi	SFR	Protokol yang berlaku
Uji prosedur transmisi dan penyaringan status kuantum	Uji kebenaran fungsionalitas pembuatan data mentah terkait antara modul Tx dan	FTP_QKD.1 FTP_QKD.2	DV-PM-QKD; DV-MDI-QKD; DV-EB-QKD; CV-PM-QKD; CV-MDI-QKD; CV-EB-QKD

EA	Deskripsi	SFR	Protokol yang berlaku
	modul Rx, dan fungsionalitas penyaringan data yang dihasilkan saat penyaringan merupakan bagian dari protokol QKD.		
Uji prosedur pasca-pemrosesan lainnya	Uji kebenaran implementasi prosedur pasca-pemrosesan dalam TOE, setelah penyaringan apa pun yang menjadi bagian dari protokol QKD.	FTP_QKD.2	DV-PM-QKD; DV-MDI-QKD; DV-EB-QKD; CV-PM-QKD; CV-MDI-QKD; CV-EB-QKD
Uji prosedur <i>parameter adjustment</i>	Uji kebenaran implementasi prosedur <i>parameter adjustment</i> dalam TOE	FTP_QKD.1	DV-PM-QKD; DV-MDI-QKD; DV-EB-QKD; CV-PM-QKD; CV-MDI-QKD; CV-EB-QKD

- b. EA untuk mengevaluasi komponen *quantum optic* pada modul *transmitter* (TX)

EA ini membahas potensi kelemahan pada komponen *quantum optic* modul QKD yang dapat membahayakan fungsi keamanan FPT_EMS.1/Quantum dan FPT_PHP.3 pada modul Tx. Tabel 2.5 menjelaskan EA untuk mengevaluasi keamanan komponen *quantum optic* pada modul TX.

Tabel 2.5 EA untuk mengevaluasi keamanan komponen *quantum optic* pada modul TX

EA	Deskripsi	SFR	Protokol yang berlaku
Uji distribusi jumlah foton dari pulsa optik	Uji apakah emisi yang dihasilkan konsisten dengan distribusi jumlah foton dari pulsa optik yang diharapkan untuk dipancarkan oleh modul TX yang diuji	FPT_EMS.1/Quantum	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD
Uji rata-rata jumlah foton dan kestabilan pulsa optik	Uji apakah rata-rata jumlah foton dari pulsa optik yang dihasilkan dalam modul TX yang diuji, serta kestabilannya terhadap waktu, konsisten dengan persyaratan dari protokol QKD yang diimplementasikan.	FPT_EMS.1/Quantum	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD

EA	Deskripsi	SFR	Protokol yang berlaku
Uji independensi intensitas pulsa optik	Uji apakah intensitas dari pulsa yang dipancarkan untuk setiap intensitas yang dimaksud independen terhadap pola modulasi intensitas yang mendasarinya.	FPT_EMS.1/ Quantum	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD
Uji akurasi encoding status kuantum	Uji apakah status kuantum yang dipancarkan oleh modul TX yang diuji dikodekan dengan cukup akurat untuk sesuai dengan yang disyaratkan oleh protokol QKD yang diimplementasikan.	FPT_EMS.1/ Quantum	DV-PM-QKD; DV-MDI-QKD
Uji ketakterbedakan (indistinguishability) status yang dikodekan	Uji apakah status-status kuantum yang berbeda namun dikodekan dalam derajat kebebasan yang sama dapat dibedakan dari perspektif derajat kebebasan lain yang	FPT_EMS.1/ Quantum	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD

EA	Deskripsi	SFR	Protokol yang berlaku
	tidak digunakan untuk encoding.		
Uji distribusi uniform dari fase global pulsa optik	Uji apakah fase global dari pulsa optik terdistribusi secara acak, sebagaimana disyaratkan oleh protokol QKD yang diimplementasikan.	FPT_EMS.1/ Quantum	DV-PM-QKD; DV-MDI-QKD
Uji tingkat isolasi optik dari modul TX	Uji apakah kemampuan isolasi yang disediakan oleh modul TX yang diuji cukup untuk mencegah cahaya yang disuntikkan dari saluran kuantum ke dalam modul.	FPT_PHP.3	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD
Uji sensitivitas <i>injected light</i> monitor pada modul TX	Uji apakah <i>injected light</i> monitor yang dipasang untuk mendeteksi cahaya yang disuntikkan oleh pihak lawan melalui antarmuka saluran kuantum berfungsi dengan baik. Karakterisasi	FPT_PHP.3	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD

EA	Deskripsi	SFR	Protokol yang berlaku
	sensitivitasnya terhadap emisi gelombang kontinu (<i>continuous-wave</i>) dan pulsa optik dengan frekuensi tinggi/lebar-sempit.		
Uji ketahanan modul TX terhadap injeksi laser	Uji ketahanan modul TX yang diuji terhadap cahaya laser yang disuntikkan melalui antarmuka saluran kuantum	FPT_PHP.3	DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD

- c. EA untuk mengevaluasi komponen *quantum optic* pada modul *Receiver (RX)*

EA ini membahas potensi kelemahan pada komponen *quantum optic* modul QKD yang dapat membahayakan fungsi keamanan FPT_EMS.1/Quantum dan FPT_PHP.3 pada modul Rx. Tabel 2.6 menjelaskan EA untuk mengevaluasi keamanan komponen *quantum optic* pada modul RX.

Tabel 2.6 EA untuk mengevaluasi keamanan komponen *quantum optic* pada modul RX.

EA	Deskripsi	SFR	Protokol yang berlaku
Uji konsistensi probabilitas deteksi pada modul RX	Uji apakah probabilitas deteksi yang dihasilkan dari modul RX yang diuji	FPT_EMS.1/ Quantum	DV-PM-QKD; DV-EB-QKD

EA	Deskripsi	SFR	Protokol yang berlaku
	konsisten dengan model dari protokol QKD yang diimplementasikan.		
Uji kebocoran informasi akibat <i>back-flashes</i> dari modul RX	Uji apakah modul RX yang diuji memancarkan kembali foton ke saluran kuantum, yang dapat mengungkapkan informasi tentang status yang terdeteksi setelah deteksi foton.	FPT_EMS.1/ Quantum	DV-PM-QKD; DV-EB-QKD
Uji tingkat isolasi optik dari modul RX	Uji apakah kemampuan isolasi yang disediakan oleh modul RX yang diuji cukup untuk mencegah cahaya yang terpantul kembali dari modul tersebut ke saluran kuantum.	FPT_PHP.3	DV-PM-QKD; DV-EB-QKD; CV-PM-QKD; CV-EB-QKD
Uji sensitivitas <i>injected light</i> monitor pada modul RX	Uji apakah <i>injected light</i> monitor yang dipasang untuk mendeteksi cahaya yang disuntikkan	FPT_PHP.3	DV-PM-QKD; DV-EB-QKD; CV-PM-QKD; CV-EB-QKD

EA	Deskripsi	SFR	Protokol yang berlaku
	melalui antarmuka saluran kuantum berfungsi dengan baik.		
Uji ketahanan modul RX terhadap blinding oleh cahaya terang	Uji apakah output deteksi dari modul Rx yang diuji dapat dikendalikan oleh cahaya terang yang disuntikkan.	FPT_PHP.3	DV-PM-QKD; DV-EB-QKD
Uji kesesuaian pengaturan <i>dead time</i> pada detektor foton tunggal	Uji apakah data mentah yang dihasilkan oleh modul RX yang diuji tidak mencakup peristiwa deteksi yang terjadi selama periode <i>dead time</i> pada salah satu detektor foton tunggal (Single Photon Detector - SPD).	FPT_PHP.3	DV-PM-QKD; DV-EB-QKD
Uji profil temporal dari efisiensi deteksi pada detektor foton tunggal	Uji apakah profil temporal efisiensi deteksi saat mendeteksi pulsa pada tingkat foton tunggal sama dengan profil saat	FPT_PHP.3	DV-PM-QKD; DV-EB-QKD

EA	Deskripsi	SFR	Protokol yang berlaku
	mendeteksi pulsa dengan rata-rata jumlah foton yang lebih tinggi untuk setiap SPD.		
Uji ketahanan modul RX terhadap injeksi laser	Uji apakah probabilitas deteksi dari modul Rx yang diuji dapat diubah dengan menyinari cahaya tambahan ke dalam modul RX melalui antarmuka saluran kuantum.	FPT_PHP.3	DV-PM-QKD; DV-EB-QKD;
Uji batas deteksi detektor homodin pada modul RX	Uji apakah modul RX yang diuji menolak data atau melaporkan kejadian luar biasa ketika detektor homodin beroperasi dalam wilayah saturasi.	FPT_PHP.3	CV-PM-QKD; CV-EB-QKD
Uji kesesuaian penanganan kejadian <i>double-click</i>	Uji apakah kejadian <i>double click</i> ditangani dengan tepat selama tahap <i>post-processing</i> , misalnya dengan memberikan	FPT_PHP.3	DV-PM-QKD; DV-EB-QKD

EA	Deskripsi	SFR	Protokol yang berlaku
	nilai bit secara acak untuk kejadian tersebut.		

d. EA untuk evaluasi prosedur *parameter adjustment*

EA ini bertujuan untuk memverifikasi efektivitas langkah keamanan (*security countermeasures*) yang diterapkan oleh modul *transmitter* (TX) dan *Receiver* (RX) QKD untuk menangkal serangan terhadap prosedur *parameter adjustment* perangkat.

TOE harus diuji dalam kondisi operasi normal, tanpa modifikasi besar atau penggunaan antarmuka tambahan. Hal ini bertujuan agar hasil pengujian mencerminkan kondisi nyata keamanan modul QKD saat beroperasi. Untuk efektivitas EM, beberapa EA dapat memperbolehkan modifikasi terbatas pada TOE misalnya modul Rx harus menyediakan tingkat jumlah deteksi (*detection count rates*) dalam output, atau menyediakan data *time-tagged* dari output, sehingga *detection count rates* dapat dihitung. Tabel 2.7 menjelaskan EA yang terkait dengan prosedur *parameter adjustment*.

Tabel 2.7 EA yang terkait dengan prosedur *parameter adjustment*.

EA	Deskripsi	SFR	Protokol yang berlaku
Uji prosedur transmisi dan penyaringan	Uji kebenaran fungsionalitas pembuatan data mentah	FTP_QKD.1 FTP_QKD.2	DV-PM-QKD; DV-MDI-QKD; DV-EB-QKD; CV-PM-QKD;

EA	Deskripsi	SFR	Protokol yang berlaku
status kuantum	terkait antara modul TX dan modul RX, dan fungsionalitas penyaringan data yang dihasilkan saat penyaringan merupakan bagian dari protokol QKD.		CV-MDI-QKD; CV-EB-QKD
Uji prosedur pasca-pemrosesan lainnya	Uji kebenaran implementasi prosedur pasca-pemrosesan dalam TOE, setelah penyaringan apa pun yang menjadi bagian dari protokol QKD.	FTP_QKD.2	DV-PM-QKD; DV-MDI-QKD; DV-EB-QKD; CV-PM-QKD; CV-MDI-QKD; CV-EB-QKD
Uji prosedur <i>parameter adjustment</i>	Uji kebenaran implementasi prosedur <i>parameter</i>	FTP_QKD.1	DV-PM-QKD; DV-MDI-QKD; DV-EB-QKD; CV-PM-QKD; CV-MDI-QKD;

EA	Deskripsi	SFR	Protokol yang berlaku
	<i>adjustment</i> dalam TOE		CV-EB-QKD

- e. EA untuk evaluasi SFR pada komponen jaringan konvensional

Berikut merupakan persyaratan umum untuk evaluasi komponen jaringan:

- Input umum, TOE perlu disesuaikan agar memungkinkan pengujian, misalkan dengan melakukan akses output langsung dari NRBG untuk pengujian *randomness* FCS-RNG.1.
- Alat yang dibutuhkan, diantaranya yaitu alat pemantau lalu lintas jaringan (*network sniffer*), alat *protocol fuzzing*, dan kesesuaian terhadap algoritma kriptografi.
- Kompetensi evaluator, memiliki pemahaman yang memadai tentang protokol QKD dan eksper dalam evaluasi perangkat jaringan.
- Pelaporan, hasil pengujian fungsional dari setiap EA harus dilaporkan.

Adapun evaluasi SFR terkait fungsi kriptografi (FCS) yaitu untuk evaluasi FCS_COP.1 merujuk ke ISO/IEC 18367 dan ISO/IEC 24759, sedangkan untuk pengujian *randomness* FCS_RNG.1 menggunakan metode sesuai EAL yang ditentukan berdasarkan ISO/IEC 20543.

Evaluasi untuk kelas FAU, FDP, FIA, dan FMT dapat mengacu pada dokumen CC untuk CPP perangkat jaringan. Sedangkan SFR lainnya yang belum memiliki panduan eksplisit, evaluator dianjurkan menyusun EA baru

berdasarkan pengalaman dalam mengevaluasi keamanan perangkat jaringan.

2. EA tambahan untuk SAR

Tujuan dari aktivitas tambahan ini adalah untuk memberikan persyaratan baru kepada evaluator, atau menyempurnakan aktivitas evaluasi yang telah di standardisasi dalam ISO/IEC 18045, sehingga metode evaluasi untuk modul QKD menjadi lebih lengkap dan lebih praktis.

a. EA tambahan untuk kelas APE: Evaluasi *Protection Profile*

Tabel 2.8 menunjukkan EA tambahan untuk kelas APE.

Tabel 2.8 EA tambahan untuk kelas APE.

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
APE_INT.1.1E	APE_INT.1-3	Evaluator harus memeriksa TOE <i>overview</i> untuk memastikan bahwa PP menjelaskan fitur keamanan dari fungsi <i>key establishment</i> yang disediakan oleh TOE. Jarak komunikasi yang diharapkan dapat didukung oleh TOE serta prasyarat <i>pre-sharing a secret key</i> agar TOE dapat berfungsi juga harus dijelaskan secara jelas.

Evaluator action element	Work unit	Aktivitas tambahan
	APE_INT.1-4	Evaluators harus memeriksa TOE <i>overview</i> untuk memastikan bahwa jenis TOE mengidentifikasi protokol QKD tertentu dan arsitektur yang diimplementasikan dalam TOE. Evaluators juga harus mengidentifikasi modul TX dan modul RX yang terpisah, yang membentuk TOE untuk pelaksanaan fungsi QKD secara tepat [sesuai dengan arsitektur dari protokol QKD yang diimplementasikan].
	APE_INT.1-5	Evaluators harus memeriksa TOE <i>overview</i> untuk memastikan bahwa saluran eksternal serta <i>platform</i> perangkat keras dan perangkat lunak yang mendasari, seperti <i>chip</i> dan sistem operasi, yang mendukung

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		fungsionalitas namun dikecualikan dari cakupan TOE, telah diidentifikasi dengan jelas. Selain itu, jika TOE mengimplementasikan protokol MDI-QKD atau EB-QKD, evaluator harus memeriksa apakah modul penerima QKD pada MDI-QKD dan modul pemancar QKD pada EB-QKD secara jelas dikecualikan dari TOE, atau telah diberikan penjelasan yang jelas untuk membenarkan penyertaan modul-modul tersebut.
APE_CCL.1.1E	APE_CCL.1-19	Jika <i>conformance statement</i> dalam PP yang dievaluasi menyatakan kesesuaian terhadap dokumen ini, evaluator harus memeriksa <i>conformance statement</i> tersebut untuk

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		menentukan apakah pernyataan berikut tercantum atau tidak: “PP ini mewajibkan penggunaan metode evaluasi dan/atau aktivitas evaluasi yang didefinisikan dalam ISO/IEC 23837-2.” Jika tercantum, evaluator harus menunjukkan bahwa modifikasi terhadap metode/aktivitas evaluasi (jika ada) konsisten dengan dan memenuhi persyaratan dalam dokumen ini.
	APE_CCL.1-20	Jika PP atau ST menyatakan kesesuaian terhadap ISO/IEC 23837-1, evaluator harus memeriksa PP/ST tersebut untuk memastikan bahwa modifikasi terhadap definisi permasalahan keamanan (<i>security</i>

Evaluator action element	Work unit	Aktivitas tambahan
		<i>problem definition</i>) atau SFRs (jika ada) konsisten dengan dan memenuhi persyaratan yang ditetapkan dalam ISO/IEC 23837-1:2023
APE_SPD.1.1E	APE_SPD.1-1	Evaluators harus memeriksa bahwa definisi permasalahan keamanan (<i>security problem definition</i>) mencakup semua ancaman yang telah diidentifikasi dalam ISO/IEC 23837-1:2023, Klausul 7, dengan beberapa pengecualian yang diperbolehkan sebagaimana dijelaskan dalam ISO/IEC 23837-1:2023, Klausul 10. Jika pengecualian dinyatakan, maka pemeriksaan atas justifikasi rasional harus dilakukan dalam unit kerja APE_CCL.1-20.

- b. EA tambahan untuk kelas ASE : Evaluasi *Security Target*

Tabel 2.9 menunjukkan EA tambahan untuk kelas ASE.

Tabel 2.9 EA tambahan untuk kelas ASE.

Evaluator action element	Work unit	Aktivitas tambahan
ASE_INT.1.1E	ASE_INT.1-5	Evaluator harus memeriksa TOE <i>overview</i> untuk memastikan bahwa ST. menjelaskan fitur keamanan dari fungsi <i>key establishment</i> yang disediakan oleh TOE, termasuk jarak komunikasi yang diharapkan. Pra kondisi dari <i>pre-sharing secret key</i> agar TOE dapat berfungsi juga harus dijelaskan secara jelas.
	ASE_INT.1-6	Evaluator harus memeriksa gambaran umum TOE untuk memastikan <i>TOE overview</i> untuk memastikan bahwa jenis TOE mengidentifikasi protokol QKD dan arsitektur spesifik yang diimplementasikan dalam TOE. Evaluator juga mengidentifikasi

Evaluator action element	Work unit	Aktivitas tambahan
		modul TX dan modul RX yang terpisah, yang membentuk TOE untuk pelaksanaan fungsi QKD secara tepat [sesuai dengan arsitektur protokol QKD yang diimplementasikan].
	ASE_INT.1-8	Evaluator harus memeriksa gambaran umum TOE untuk memastikan bahwa saluran eksternal (seperti <i>quantum channel</i> dan <i>classical channel</i>) serta <i>platform</i> perangkat keras dan perangkat lunak yang mendasarinya (seperti <i>chip</i> dan sistem operasi), yang mendukung fungsionalitas namun dikecualikan dari cakupan TOE, telah diidentifikasi dengan jelas. Selain itu, jika TOE mengimplementasikan protokol MDI-QKD atau EB-QKD, evaluator harus

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		memeriksa apakah modul penerima QKD pada MDI-QKD dan modul pemancar QKD pada EB-QKD secara jelas dikecualikan dari TOE, atau apakah telah disediakan penjelasan yang jelas untuk membenarkan inklusi modul-modul tersebut.
	ASE_INT.1-10	Evaluators harus memeriksa gambaran umum TOE untuk memastikan bahwa TOE mencakup modul-modul yang diperlukan oleh protokol QKD yang diimplementasikan. Harus dinyatakan dengan jelas bahwa beberapa modul dianggap sebagai bagian non-TOE jika relevan, seperti modul penerima QKD pada MDI-QKD dan modul pemancar QKD pada EB-QKD

Evaluator action element	Work unit	Aktivitas tambahan
ASE_TSS.1.1E	ASE_TSS.1-1	Evaluator harus memeriksa TSS untuk memastikan bahwa dokumen tersebut menjelaskan kontrol terkait TI yang digunakan oleh TOE untuk memenuhi tujuan keamanan, khususnya kontrol yang digunakan untuk menahan serangan <i>side channel</i> dari antarmuka <i>quantum channel</i> .

c. EA tambahan untuk kelas ADV: *Development*

Tabel 2.10 merupakan EA tambahan untuk kelas ADV.

Tabel 2.10 EA tambahan untuk kelas ADV.

Evaluator action element	Work unit	Aktivitas tambahan
ADV_ARC.1.1E	ADV-ARC.1-2	Evaluator harus memeriksa deskripsi arsitektur keamanan untuk memastikan bahwa ruang proses sistem dan bagian memori untuk prosedur pasca-pemrosesan serta

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		<i>final key</i> (dan material kunci yang relevan) dipisahkan dari ruang proses sistem dan bagian memori lainnya, sehingga akses terhadap <i>final key</i> dan material kunci yang relevan dibatasi oleh langkah-langkah kontrol akses sistem.
	ADV-ARC.1-3	Evaluator harus memeriksa deskripsi arsitektur keamanan untuk memastikan bahwa pada tahap inisialisasi, TOE tidak menjalankan sesi QKD sampai parameter sistem berhasil disejajarkan dan sistem mencapai kondisi stabil.
	ADV-ARC.1-4	Evaluator harus memeriksa deskripsi arsitektur keamanan untuk memastikan bahwa semua serangan <i>active side channel</i> yang diketahui

Evaluator action element	Work unit	Aktivitas tambahan
		dari <i>quantum channel</i> telah dipertimbangkan dan ditangani, sehingga TSF mampu melindungi dirinya dari serangan <i>physical tampering</i> .
	ADV-ARC.1-5	Evaluators harus memeriksa deskripsi arsitektur keamanan untuk memastikan bahwa semua antarmuka yang digunakan untuk tujuan pengujian telah ditutup atau dibatasi, dan semua serangan <i>passive side channel</i> yang diketahui dari <i>quantum channel</i> telah dipertimbangkan dan ditangani, sehingga mekanisme yang menegakkan SFR tidak dapat dilewati.
ADV_FSP.1.1E	ADV_FSP.1-1	Evaluators harus memeriksa spesifikasi fungsional untuk

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		memastikan bahwa tujuan dari antarmuka eksternal pada modul QKD telah dijelaskan dengan jelas. Secara khusus, antarmuka kontrol dan manajemen dapat diimplementasikan melalui seperangkat antarmuka spesifik yang dirancang untuk berbagai aspek fungsi kontrol dan manajemen sistem, dan diwujudkan melalui porta fisik yang berbeda, seperti porta USB atau porta jaringan. Dokumen FSP menyediakan ruang bagi pengembang untuk menjelaskan antarmuka-antarmuka ini secara jelas.
ADV_FSP.2.1E	ADV_FSP.2-2	Evaluators harus memeriksa spesifikasi fungsional untuk memastikan bahwa tujuan dari antarmuka

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		eksternal modul QKD telah dijelaskan dengan jelas. Secara khusus, antarmuka kontrol dan manajemen dapat diimplementasikan melalui seperangkat antarmuka spesifik yang dirancang untuk berbagai aspek fungsi kontrol dan manajemen sistem, dan diwujudkan melalui porta fisik yang berbeda, seperti porta USB atau porta jaringan. Dokumen FSP menyediakan ruang bagi pengembang untuk menjelaskan antarmuka-antarmuka ini secara jelas.
ADV_FSP.3.1E	ADV_FSP.3-2	Evaluator harus memeriksa spesifikasi fungsional untuk memastikan bahwa tujuan dari antarmuka eksternal modul QKD telah dijelaskan dengan jelas. Secara khusus,

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		antarmuka kontrol dan manajemen dapat diimplementasikan melalui seperangkat antarmuka spesifik yang dirancang untuk berbagai aspek dari fungsi kontrol dan manajemen sistem, dan diimplementasikan melalui porta fisik yang berbeda, seperti porta USB atau porta jaringan. Dokumen FSP menyediakan tempat bagi pengembang untuk menjelaskan antarmuka-antarmuka tersebut secara jelas.
ADV_FSP.4.1E	ADV_FSP.4-2	Evaluators harus memeriksa spesifikasi fungsional untuk memastikan bahwa tujuan dari antarmuka eksternal modul QKD telah dijelaskan dengan jelas. Secara khusus, antarmuka kontrol dan manajemen dapat

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		diimplementasikan melalui seperangkat antarmuka spesifik yang dirancang untuk berbagai aspek dari fungsi kontrol dan manajemen sistem, dan diwujudkan melalui porta fisik yang berbeda, seperti porta USB atau porta jaringan. Dokumen FSP menyediakan wadah bagi pengembang untuk menjelaskan antarmuka-antarmuka tersebut secara jelas.
ADV_FSP.5.1E	ADV_FSP.5-3	Evaluator harus memeriksa spesifikasi fungsional untuk memastikan bahwa tujuan dari antarmuka eksternal modul QKD telah dijelaskan dengan jelas. Secara khusus, antarmuka kontrol dan manajemen dapat diimplementasikan melalui seperangkat antarmuka spesifik yang

<i>Evaluator action element</i>	<i>Work unit</i>	Aktivitas tambahan
		dirancang untuk berbagai aspek dari fungsi kontrol dan manajemen sistem, dan diwujudkan melalui porta fisik yang berbeda, seperti porta USB atau porta jaringan. Dokumen FSP menyediakan ruang bagi pengembang untuk menjelaskan antarmuka-antarmuka tersebut secara jelas.

- d. EA tambahan untuk kelas AGD: *Guidance document*

Tabel 2.11 menunjukkan EA tambahan pada kelas AGD.

Tabel 2.11 EA tambahan pada kelas AGD.

<i>Evaluator action element</i>	<i>Work unit</i>	Aktivitas tambahan
AGD_OPE.1.1E	AGD_OPE.1-3	Evaluator harus memeriksa panduan operasional pengguna untuk memastikan bahwa parameter keamanan sistem yang berada di bawah kendali operator beserta nilai defaultnya telah

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		dijelaskan dengan jelas. Karena parameter-parameter ini dapat diubah oleh operator, deskripsi parameter harus mencantumkan nilai-nilai yang wajar untuk operasi TOE yang aman.
	AGD_OPE.1-5	Evaluator harus memeriksa panduan operasional pengguna untuk memastikan bahwa panduan tersebut mengidentifikasi semua mode operasi sistem yang mungkin (termasuk mode kegagalan dan mode operasi normal) serta metode untuk membedakan mode-mode tersebut dari tampilan TOE (misalnya lampu sinyal), sehingga operator dapat mengambil tindakan tepat waktu jika terjadi insiden darurat.

<i>Evaluator action element</i>	<i>Work unit</i>	Aktivitas tambahan
AGD_PRE.1.1E	AGD_PRE.1-2	Evaluators harus memeriksa prosedur instalasi yang disediakan untuk memastikan bahwa langkah-langkah yang diperlukan untuk penerapan TOE secara aman dan persiapan lingkungan operasional yang aman telah dijelaskan, sehingga dapat memvalidasi apakah asumsi yang ditetapkan pada lingkungan operasional dapat terpenuhi.

e. EA tambahan untuk kelas ATE: *Test*

Tabel 2.12 menunjukkan EA tambahan untuk kelas ATE.

Tabel 2.12 EA tambahan untuk kelas ATE.

<i>Evaluator action element</i>	<i>Work unit</i>	Aktivitas tambahan
ATE_FUN.1.1E	ATE_FUN.1-2	Evaluators harus memeriksa rencana pengujian untuk memastikan bahwa rencana tersebut

<i>Evaluator action element</i>	<i>Work unit</i>	Aktivitas tambahan
		menjelaskan informasi mengenai peralatan uji dan persiapan khusus terhadap TOE. Beberapa EA untuk aspek-aspek ini memerlukan persiapan khusus terhadap TOE guna memperoleh data antara selama eksekusi atau mempermudah penyusunan lingkungan pengujian. Oleh karena itu, pengembang diwajibkan untuk menjelaskan konfigurasi pengujian secara jelas.
	ATE_FUN.1-4	Terkait evaluasi terhadap EA, evaluator harus memeriksa rencana pengujian untuk memastikan bahwa dependensi EA telah dipertimbangkan dalam pengujian fungsional. Hal ini harus konsisten dengan item dependensi dari setiap EA untuk evaluasi

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		FTP_QKD, komponen <i>quantum optical</i> untuk modul <i>transmitter</i> dan <i>receiver</i> , serta prosedur parameter <i>adjustment</i> atau hubungan dependensi lain yang dapat dianggap masuk akal.
	ATE_FUN.1-5	Terkait evaluasi terhadap EA, evaluator harus memeriksa dokumentasi pengujian untuk memastikan bahwa semua hasil uji yang diharapkan konsisten dengan nilai ambang batas yang telah ditetapkan sebelumnya dalam ST atau dokumen relevan lainnya untuk keperluan evaluasi.
	ATE_FUN.1-6	Terkait evaluasi terhadap EA, evaluator harus memeriksa bahwa hasil penilaian lulus/gagal yang tercantum dalam dokumentasi pengujian

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		konsisten dengan kriteria lulus/gagal yang terdapat dalam dokumen ini atau dokumen relevan lainnya untuk keperluan evaluasi.
ATE_IND.1.1E	ATE_IND.1-1	Evaluators harus memeriksa prosedur instalasi yang disediakan untuk memastikan bahwa langkah-langkah yang diperlukan untuk penerapan TOE secara aman dan persiapan lingkungan operasional yang aman telah dijelaskan, sehingga dapat memvalidasi apakah asumsi yang ditetapkan pada lingkungan operasional dapat terpenuhi.
ATE_IND.1.2E	ATE_IND.1-3	Terkait evaluasi terhadap EA, evaluator harus memasukkan EA yang ditentukan dalam EA untuk evaluasi FTP_QKD, komponen <i>quantum optical</i> untuk

<i>Evaluator action element</i>	<i>Work unit</i>	Aktivitas tambahan
		modul <i>transmitter</i> dan <i>receiver</i> , serta prosedur parameter <i>adjustment</i> ke dalam subset pengujian yang dirancang apabila metode evaluasi yang diterapkan secara aktual diklaim sesuai dengan dokumen ini.
	ATE_IND.1-7	Terkait evaluasi terhadap EA, evaluator harus memeriksa apakah hasil pengujian aktual konsisten dengan nilai ambang batas yang telah ditetapkan sebelumnya dalam ST dan/atau dokumen relevan lainnya untuk keperluan evaluasi, apabila metode evaluasi yang diterapkan secara aktual diklaim sesuai dengan dokumen ini.
ATE_IND.2.1E	ATE_IND.2-1	Evaluator harus memeriksa TOE untuk memastikan bahwa konfigurasi pengujian dan persiapan khusus

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		terhadap TOE sesuai untuk evaluasi EA. Hal ini didasarkan pada persyaratan bahwa TOE mungkin memerlukan beberapa modifikasi guna memfasilitasi penyusunan lingkungan evaluasi untuk EA.
ATE_IND.2.2E	ATE_IND.2-5	Terkait evaluasi terhadap EA, evaluator harus memeriksa apakah hasil pengujian aktual dari pengujian yang diambil sampelnya konsisten dengan nilai ambang batas yang telah ditetapkan sebelumnya dalam ST dan/atau dokumen relevan lainnya untuk keperluan evaluasi, apabila metode evaluasi yang diterapkan secara aktual diklaim sesuai dengan dokumen ini.
ATE_IND.2.3E	ATE_IND.2-6	Terkait evaluasi terhadap EA, evaluator harus memasukkan EA

<i>Evaluator action element</i>	<i>Work unit</i>	Aktivitas tambahan
		yang ditentukan dalam EA untuk evaluasi FTP_QKD, komponen <i>quantum optical</i> untuk modul <i>transmitter</i> dan <i>receiver</i> , serta prosedur parameter <i>adjustment</i> ke dalam subset pengujian yang dirancang, apabila metode evaluasi yang diterapkan secara aktual diklaim sesuai dengan dokumen ini.
	ATE_IND.2-10	Terkait evaluasi terhadap EA, evaluator harus memeriksa apakah hasil pengujian aktual konsisten dengan nilai ambang batas yang telah ditetapkan sebelumnya dalam ST dan/atau dokumen relevan lainnya untuk keperluan evaluasi, apabila metode evaluasi yang diterapkan secara aktual diklaim sesuai dengan dokumen ini.

- f. EA tambahan untuk kelas AVA: *Vulnerability assessment*

Tabel 2.13 menunjukkan EA tambahan untuk kelas AVA.

Tabel 2.13 EA tambahan untuk kelas AVA.

Evaluator action element	Work unit	Aktivitas tambahan
AVA_VAN.1.2E	AVA_VAN.1-3	Evaluators harus memeriksa sumber informasi yang tersedia untuk publik guna mengidentifikasi potensi kerentanan dalam TOE, yang mencakup kerentanan yang terkait dengan perangkat jaringan konvensional maupun yang spesifik terhadap teknologi QKD.
AVA_VAN1.3E	AVA_VAN.1-10	Evaluators harus memeriksa hasil dari seluruh pengujian penetrasi untuk memastikan bahwa TOE, dalam lingkungan operasionalnya, tahan terhadap penyerang yang memiliki potensi serangan dasar (<i>basic attack potential</i>). Jika tidak ada pendekatan alternatif yang ditentukan oleh otoritas evaluasi, maka panduan perhitungan potensi serangan harus digunakan

Evaluator action element	Work unit	Aktivitas tambahan
		untuk menentukan potensi serangan yang diperlukan guna mengeksploitasi suatu kerentanan tertentu, dan apakah kerentanan tersebut dapat dieksploitasi dalam lingkungan yang dimaksud. Tidak selalu diperlukan untuk menghitung potensi serangan dalam setiap kasus, kecuali jika terdapat keraguan apakah kerentanan tersebut dapat dieksploitasi oleh penyerang dengan potensi serangan di bawah <i>Enhanced-Basic</i>.
AVA_VAN.2.2E	AVA_VAN.2-3	Evaluator harus memeriksa sumber informasi yang tersedia untuk umum guna mengidentifikasi potensi kerentanan dalam TOE, yang mencakup kerentanan yang terkait dengan perangkat jaringan konvensional maupun yang spesifik terhadap teknologi QKD.

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
AVA_VAN.2.4E	AVA_VAN.2-11	Evaluators must check results from all penetration tests to ensure that TOE, in the operational environment, is resistant to attackers who have basic attack potential (<i>Basic attack potential</i>). If there are no alternative approaches determined by the evaluation authority, then the guidance for calculating attack potential must be used to determine the attack potential that is needed to exploit a specific vulnerability and whether the vulnerability can be exploited in the intended environment. Attack potential calculations may not be needed in every case, except if there is doubt whether the vulnerability can be exploited by

Evaluator action element	Work unit	Aktivitas tambahan
		penyerang dengan potensi serangan di bawah <i>Enhanced-Basic</i> .
AVA_VAN.3.2E	AVA_VAN.3-3	Evaluator harus memeriksa sumber informasi yang tersedia untuk umum guna mengidentifikasi potensi kerentanan dalam TOE, yang mencakup kerentanan yang terkait dengan perangkat jaringan konvensional maupun yang spesifik terhadap teknologi QKD.
AVA_VAN.3.4E	AVA_VAN.3-11	Evaluator harus memeriksa hasil dari seluruh pengujian penetrasi untuk memastikan bahwa TOE, dalam lingkungan operasionalnya, tahan terhadap penyerang yang memiliki potensi serangan <i>Enhanced-Basic</i> . Jika tidak ada pendekatan alternatif yang ditentukan oleh otoritas evaluasi, maka panduan dalam menghitung potensi serangan harus digunakan

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		untuk menentukan potensi serangan yang diperlukan guna mengeksploitasi suatu kerentanan tertentu dan apakah kerentanan tersebut dapat dieksploitasi dalam lingkungan yang dimaksud. Perhitungan potensi serangan mungkin tidak diperlukan dalam setiap kasus, kecuali jika terdapat keraguan apakah kerentanan tersebut dapat dieksploitasi oleh penyerang dengan potensi serangan di bawah tingkat <i>Moderate</i>.
AVA_VAN.4.2E	AVA_VAN.4-3	Evaluator harus memeriksa sumber informasi yang tersedia untuk umum guna mengidentifikasi potensi kerentanan dalam TOE, yang mencakup kerentanan yang terkait dengan perangkat jaringan konvensional maupun yang spesifik terhadap teknologi QKD.

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
AVA_VAN.4.4E	AVA_VAN.4-11	Evaluators must check results from all penetration tests to ensure that TOE, in its operational environment, is resistant to attackers who have the potential for a <i>Moderate</i> attack. If there are no alternative approaches determined by the evaluation authority, then the guidance in calculating the potential for attack must be used to determine the potential for attack that is needed to exploit a specific vulnerability and whether the vulnerability can be exploited in the intended environment. Attack potential calculations may not be needed in every case, except if there is doubt whether the vulnerability can be exploited by the attacker with the potential

Evaluator action element	Work unit	Aktivitas tambahan
		serangan di bawah tingkat <i>High</i> .
AVA_VAN.5.2E	AVA_VAN.5-3	Evaluator harus memeriksa sumber informasi yang tersedia untuk umum guna mengidentifikasi potensi kerentanan dalam TOE, yang mencakup kerentanan yang terkait dengan perangkat jaringan konvensional maupun yang spesifik terhadap teknologi QKD.
AVA_VAN.5.4E	AVA_VAN.5-11	Evaluator harus memeriksa hasil dari seluruh pengujian penetrasi untuk memastikan bahwa TOE, dalam lingkungan operasionalnya, tahan terhadap penyerang yang memiliki potensi serangan <i>High</i> . Jika tidak ada pendekatan alternatif yang ditentukan oleh otoritas evaluasi, maka panduan dalam menghitung potensi serangan harus digunakan untuk menentukan potensi serangan yang diperlukan

<i>Evaluator action element</i>	<i>Work unit</i>	<i>Aktivitas tambahan</i>
		guna mengeksploitasi suatu kerentanan tertentu dan apakah kerentanan tersebut dapat dieksploitasi dalam lingkungan yang dimaksud. Perhitungan potensi serangan mungkin tidak diperlukan dalam setiap kasus, kecuali jika terdapat keraguan apakah kerentanan tersebut dapat dieksploitasi oleh penyerang dengan potensi serangan kurang dari atau sama dengan tingkat <i>High</i> .

EM dan EA tambahan untuk SFR dan SAR dalam dokumen ini dapat dihilangkan jika tidak relevan dengan protokol QKD yang sedang dievaluasi, atau jika telah digantikan oleh EA baru yang lebih sesuai. Sedangkan penambahan EA baru dapat ditambahkan jika tidak ada RA standar yang cocok, atau jika EA baru lebih efisien/teknis/menguntungkan. Setiap EA baru harus memenuhi struktur EA menurut ISO/IEC 15408.

BAB III

STANDAR ETSI



BAB III

STANDAR ETSI

Bab ini membahas sejumlah standar yang diterbitkan oleh ETSI yang berkaitan dengan implementasi dan keamanan teknologi QKD. Standar ETSI ini memberikan panduan teknis yang lebih terperinci mengenai terminologi, kasus penggunaan (*use case*), pembuktian keamanan, parameter perangkat dan kanal komunikasi, serta spesifikasi keamanan modul QKD. Selain itu, standar ETSI juga mencakup PP berbasis *Common Criteria* serta *interface control* untuk integrasi dengan infrastruktur SDN. Informasi yang disajikan dalam standar-standar ini dapat menjadi acuan yang komprehensif dalam penerapan sistem QKD.

A. ETSI GR QKD 007 V.1.1.1 Quantum Key Distribution (QKD): Vocabulary

Dokumen ini berisi kumpulan definisi istilah dan singkatan yang berkaitan dengan QKD [3]. Karena QKD membawa konsep baru dari ranah fisika kuantum dan kriptografi klasik ke dalam dunia telekomunikasi, maka diperlukan standar istilah agar komunikasi teknis menjadi konsisten dan mudah dipahami.

Tujuan dokumen ini adalah untuk menstandarkan terminologi yang digunakan dalam dokumen-dokumen *Industry Specification Group on Quantum Key Distribution* (ISG-QKD), menjadi referensi acuan khususnya yang belum familiar dengan QKD, mengurangi kebingungan akibat makna istilah yang dapat bervariasi. Istilah-istilah yang dimuat umumnya bersifat umum dan diperkirakan akan digunakan secara luas dalam dokumen QKD di masa depan. Istilah yang hanya muncul dalam satu dokumen khusus tidak dimasukkan ke dalam dokumen ini, kecuali jika dianggap penting untuk pemahaman secara keseluruhan.

Dokumen ini memuat 2 (dua) bagian utama yaitu:

1. Istilah (Pasal 3.1: *Terms*)

Istilah disusun berdasarkan abjad dari A sampai dengan Z dengan jumlah total 119 (seratus sembilan belas) istilah. Contoh istilah dapat dilihat pada Tabel 3.1.

Tabel 3.1 Istilah.

Huruf	Istilah	Terjemahan
A	<i>Adversary: malicious entity in cryptography whose aim is to prevent the users of the cryptosystem from achieving their goals</i> ...	Pihak lawan: Entitas jahat dalam kriptografi yang bertujuan menggagalkan pengguna sistem dalam mencapai tujuan ...
B	<i>bit error rate: percentage of bits with errors divided by the total number of bits that have been transmitted, received or processed over a given time period</i> ...	Tingkat kesalahan bit: persentase bit yang mengalami kesalahan dibagi dengan jumlah total bit yang telah ditransmisikan, diterima, atau diproses selama periode waktu tertentu. ...
C	<i>classical channel: communication channel that is used by two communicating parties for exchanging data encoded in a form that may be non-destructively read and fully reproduced</i>	Saluran klasik: saluran komunikasi yang digunakan oleh dua pihak yang berkomunikasi untuk bertukar data yang dikodekan dalam bentuk yang dapat dibaca tanpa merusak dan dapat direproduksi sepenuhnya.

Huruf	Istilah	Terjemahan
	...	...
D	<i>dark count probability: probability that a detector registers a detection event within a stated duration time, in the absence of optical illumination</i> ...	Probabilitas hitungan gelap : probabilitas bahwa sebuah detektor mencatat sebuah peristiwa deteksi dalam jangka waktu tertentu, dalam keadaan tanpa pencahayaan optik. ...
E	<i>eavesdropping: act of attempting to listen to the private conversation of others without their consent</i> ...	Penyadapan: tindakan mencoba mendengarkan percakapan pribadi orang lain tanpa persetujuan mereka ...
F s.d G	Void	Tidak ada
H	<i>homodyne detection: method of detecting a weak frequency-modulated signal through mixing with a strong reference frequency-modulated signal (so-called local oscillator)</i>	Deteksi homodin: metode untuk mendeteksi sinyal lemah yang dimodulasi frekuensi dengan mencampurkannya dengan sinyal referensi kuat yang juga dimodulasi frekuensi (disebut osilator lokal).
I	<i>individual attack: attack where Eve lets each signal interact separately with its own ancilla, and keeps the</i>	Serangan individual: serangan di mana Eve membiarkan setiap sinyal berinteraksi secara terpisah dengan ancillanya masing-masing, dan menjaga agar

Huruf	Istilah	Terjemahan
	<i>ancillas apart at later times</i> ...	ancilla-ancilla tersebut tetap terpisah pada waktu-waktu berikutnya. ...
J	<i>Void</i>	Tidak ada
K	<i>key rate: rate of shared secret key generation resulting from a Quantum Key Distribution process</i>	Laju kunci: laju pembangkitan kunci rahasia bersama yang dihasilkan dari proses Distribusi Kunci Kuantum
L	<i>Void</i>	Tidak Ada
M	<i>mean spectral frequency: average frequency of spectral measurement</i> ...	Frekuensi spektral rata-rata: frekuensi rata-rata dari pengukuran spektral. ...
N s.d O	<i>Void</i>	Tidak ada
P	<i>partial detector recovery time (high): time duration after a photon detection event for the detection efficiency to return to 90 % (or some other specified fraction) of its steady-state value</i> ...	Waktu pemulihan sebagian detektor (tinggi): durasi waktu setelah suatu peristiwa deteksi foton hingga efisiensi deteksi kembali mencapai 90% (atau fraksi tertentu lainnya) dari nilai keadaan mantapnya. ...
Q	<i>QKD Entity: entity providing key distribution functionality including</i>	Entitas QKD: entitas yang menyediakan fungsi distribusi kunci, termasuk bertindak sebagai titik akhir

Huruf	Istilah	Terjemahan
	<i>acting as an endpoint for the distribution of keys to at least one other QKD Entity using QKD protocols</i> ...	untuk mendistribusikan kunci kepada setidaknya satu entitas QKD lainnya menggunakan protokol QKD. ...
R	<i>radiation hardening: improving the ability of a device or piece of equipment to withstand nuclear or other radiation; applies mainly to dielectric and semiconductor materials</i> ...	Penguatan terhadap radiasi: peningkatan kemampuan suatu perangkat atau peralatan untuk bertahan terhadap radiasi nuklir atau jenis radiasi lainnya; terutama diterapkan pada material dielektrik dan semikonduktor. ...
S	<i>security analysis: analysis of a cryptographic protocol to relate the security parameters with the exact security claim of the protocol</i> ...	Analisis keamanan: analisis terhadap sebuah protokol kriptografi untuk mengaitkan parameter-parameter keamanan dengan klaim keamanan yang spesifik dari protokol tersebut ...
T	<i>threshold detector: photon detector that can tell the difference between i) having no photon and ii) having one or more photons,</i>	Detektor ambang: detektor foton yang dapat membedakan antara i) tidak adanya foton dan ii) adanya satu atau lebih foton, tetapi tidak dapat menentukan

Huruf	Istilah	Terjemahan
	<i>but cannot tell the number of photons</i> ...	jumlah foton yang ada. ...
U s.d V	<i>Void</i>	Tidak ada
W	<i>weak laser pulse: optical pulse obtained through attenuating a laser emission</i> ...	Pulsa laser lemah: pulsa optik yang diperoleh dengan melemahkan emisi laser. ...
X	<i>X-type error: bit-flip error</i>	Kesalahan tipe-X: galat pembalikan bit
Y	<i>Y-type error: phase error</i>	Kesalahan tipe-Y: galat fasa
Z	<i>zeroization: method of erasing electronically stored data to prevent the recovery of the data</i> ...	Zeroisasi: metode untuk menghapus data yang disimpan secara elektronik guna mencegah pemulihan data tersebut.

2. Singkatan (Pasal 3.2: Abbreviations)

Bagian ini juga disusun alfabetis dari A sampai Z, dan memuat sekitar 127 (seratus dua puluh tujuh) singkatan. Daftar singkatan dilihat pada Tabel 3.2:

Tabel 3.2 Singkatan

Huruf	Singkatan	Kepanjangan
A	AC	<i>Alternating Current</i>
	AMZI	<i>Asymmetric Mach-Zehnder Interferometer</i>
	APC	<i>Angled Physical Contact</i>
	APD	<i>Avalanche PhotoDiode</i>
	API	<i>Application Programming Interface</i>

Huruf	Singkatan	Kepanjangan
	APPA APPB	<i>Application A</i> <i>Application B</i>
B	BB84 BNC BS BW	<i>QKD protocol published by Bennett and Brassard in 1984</i> <i>Bayonet Neill-Concelman connector</i> <i>British Standard</i> <i>Band Width</i>
C	CHSH CIE CML CMS COW CSP CV CV-QKD CW	<i>Clauser-Horne-Shimony-Holt</i> <i>International Commission on Illumination (Commission Internationale de l'Eclairage)</i> <i>Current Mode Logic</i> <i>Configuration Management System</i> <i>Coherent One-Way</i> <i>Critical Security Parameter</i> <i>Continuous Variable</i> <i>Continuous Variable Quantum Key Distribution</i> <i>Continuous Wave</i>
D	DAC DC DE DPA DPS DSA DSP DUT DV DVM	<i>Digital-to-Analogue Converter</i> <i>Direct Current</i> <i>Detection Efficiency</i> <i>Differential Power Analysis</i> <i>Differential Phase Shift</i> <i>Digital Signature Algorithm</i> <i>Digital Signal Processor</i> <i>Device Under Test</i> <i>Discrete Variable</i> <i>Digital VoltMeter</i>
E	ECDSA ECL EDC	<i>Elliptic Curve Digital Signature Algorithm</i> <i>Emitter Coupled Logic</i> <i>Error Detection Code</i>

Huruf	Singkatan	Kepanjangan
	EFP EFT EME EPR ESD	<i>Environmental Failure Protection</i> <i>Environmental Failure Testing</i> <i>ElectroMagnetic Emanation</i> <i>Einstein-Podolsky-Rosen</i> <i>Electrostatic Discharge</i>
F	FC FC/PC FIPS FPGA FSM FSR FW FWHM	<i>Ferrule Connector or Fibre Channel</i> <i>Ferrule Connector/Physical Contact</i> <i>Federal Information Processing Standard</i> <i>Field Programmable Gate Array</i> <i>Finite State Model</i> <i>Free Spectral Range</i> <i>Full-width</i> <i>Full Width at Half Maximum</i>
G	GG02 GM GMCS GSPD	<i>QKD protocol published by Grosshans and Grangier in 2002</i> <i>Gaussian Modulation</i> <i>Gaussian Modulated Coherent State</i> <i>Gated Single Photon Detector</i>
H	HBT HDL HMAC	<i>Hanbury Brown-Twiss</i> <i>Hardware Description Language</i> <i>Hash-Based Message Authentication Code</i>
I	I/O IR IV	<i>Inputs and Outputs</i> <i>Infrared</i> <i>Initial Value / Initialization Vector</i>
J	JSON	<i>JavaScript Object Notation</i>
K	KAT KME KMIP	<i>Known Answer Test</i> <i>Key Management Entity</i> <i>Key Management Interoperability Protocol</i>
L	LDPC LED	<i>Low-Density Parity-Check</i> <i>Light-Emitting Diode</i>

Huruf	Singkatan	Kepanjangan
	LLO LO	<i>Local Local Oscillator</i> <i>Local Oscillator</i>
M	MAC MCA MDI MM MRI MSI	<i>Message Authentication Code</i> <i>Multi-Channel Analyser</i> <i>Measurement-Device Independent</i> <i>Multi-Mode</i> <i>Magnetic Resonance Imaging</i> <i>Module Software Interface</i>
N	NA NFAD NIM NIST	<i>Numerical Aperture</i> <i>Negative Feedback Avalanche Photodiode</i> <i>Nuclear Instrumentation Module</i> <i>National Institute of Standards and Technology</i>
O	OASIS OTDR OS	<i>Organization for the Advancement of Structured Information Standards</i> <i>Optical Time Domain Reflectometry</i> <i>Operative System</i>
P	PBS PC PDE PIN PM PNS PSP PSK	<i>Polarizing Beamsplitter</i> <i>Physical Contact</i> <i>Photon Detection Efficiency</i> <i>Personal Identification Number / Positive Intrinsic Negative</i> <i>Polarization-Maintaining</i> <i>Photon Number Splitting</i> <i>Public Security Parameter</i> <i>Phase Shift Keying</i>
Q	QBER QKD QKDE QoS QPSK	<i>Quantum Bit Error Rate</i> <i>Quantum Key Distribution</i> <i>QKD Entity</i> <i>Quality of Service</i> <i>Quadrature Phase Shift Keying</i>

Huruf	Singkatan	Kepanjangan
R	REST RBG RP-SMA RRDPS RX	<i>RE</i> presentational State Transfer <i>R</i> andom Bit Generator <i>R</i> everse Polarity Sub-Miniature version A connector <i>R</i> ound Robin DPS <i>R</i> eceiver
S	SAE SDE SI SM SMA SMB SMK SNR SNSPD SPA SPAD SPDC SSP	<i>S</i> ecure Application Entity <i>S</i> ystem Detection Efficiency <i>I</i> nternational System of Units (<i>S</i> ystème <i>I</i> nternational d' <i>U</i> nités) <i>S</i> ingle-Mode <i>S</i> ub-Miniature version A connector <i>S</i> ub-Miniature version B connector <i>S</i> ub-Miniature version K connector <i>S</i> ignal-to-Noise Ratio <i>S</i> uperconducting Nanowire Single-Photon Detector <i>S</i> imple Power Analysis <i>S</i> ingle-Photon Avalanche Photodiode <i>S</i> pontaneous Parametric Down-Conversion <i>S</i> ensitive Security Parameter
T	TA TAC TAT TCSPC TLO TLS TN TTL TX	<i>T</i> iming Analysis <i>T</i> ime-to-Amplitude Converter <i>T</i> rap-Assisted Tunnelling <i>T</i> ime-Correlated Single-Photon Counting <i>T</i> ransmitted Local Oscillator <i>T</i> ransport Layer Security <i>T</i> rusted Node <i>T</i> ransistor-Transistor Logic <i>T</i> ransmitter

Huruf	Singkatan	Kepanjangan
U	URI	<i>Uniform Resource Identifier</i>
	URL	<i>Uniform Resource Locator</i>
	UUID	<i>Universally Unique Identifier</i>
V	VHDL	<i>VHSIC Hardware Description Language</i>
	VHSIC	<i>Very-High-Speed Integrated Circuits</i>
	VOA	<i>Variable Optical Attenuator</i>
W	WDM	<i>Wavelength Division Multiplexing</i>

B. ETSI GS QKD 002 V.1.1.1 *Quantum Key Distribution (QKD): Use Cases*

Dokumen ETSI GS QKD 002 V1.1.1 memberikan gambaran umum mengenai skenario penerapan teknologi QKD sebagai komponen dasar dalam membangun sistem keamanan teknologi informasi dan komunikasi (TIK) yang sangat aman [4]. Dokumen ini menekankan bahwa QKD memungkinkan distribusi kunci kriptografi dengan tingkat keamanan teoretis tertinggi berdasarkan hukum fisika kuantum, yang menjamin ketidakmungkinan penyadapan tanpa terdeteksi. Selain membahas prinsip dasar dan variasi implementasi teknis QKD, dokumen ini juga menyusun *use cases* di berbagai konteks seperti *backup* data, jaringan infrastruktur kritis, dan komunikasi jarak jauh, serta mendorong pengembangan sertifikasi keamanan sebagai syarat penggunaan QKD yang dapat diandalkan dan layak diadopsi.

Struktur utama dokumen ini terdiri atas :

1. Ruang Lingkup

Berisi gambaran umum tentang skenario aplikasi potensial di mana sistem QKD dapat digunakan sebagai elemen dasar dalam membangun sistem TIK dengan keamanan tinggi.

2. Referensi

Bagian referensi dalam dokumen ini mengklasifikasikan rujukan menjadi dua jenis, yaitu referensi spesifik dan non-spesifik.

Referensi spesifik hanya berlaku untuk versi dokumen yang disebutkan secara jelas dan rinci, sedangkan referensi non-spesifik merujuk pada versi terbaru yang tersedia, termasuk segala amandemennya. ETSI juga mencantumkan bahwa beberapa dokumen referensi dapat diakses melalui repositori daring mereka, meskipun tidak menjamin keabsahan tautan dalam jangka panjang.

3. Definisi dan Singkatan

Dokumen ini tidak mencantumkan bagian definisi dan singkatan, karena seluruh terminologi telah diselaraskan dengan dokumen ETSI GR QKD 007 V.1.1.1 *Quantum Key Distribution (QKD): Vocabulary*, yang dalam dokumen QKD 002 disebut sebagai QKD: *Ontology, Vocabulary, and Terms of Reference*.

4. QKD – Inovasi Teknologi Keamanan

Bagian ini menjelaskan bahwa QKD merupakan *primitive* kriptografi yang bersifat atomik, yang berarti QKD hanya mencakup salah satu bagian dari keseluruhan fungsi kriptografi yang dibutuhkan untuk membangun sistem komunikasi yang aman. QKD bukanlah pengganti kriptografi klasik, melainkan pelengkap yang dirancang untuk memenuhi kebutuhan distribusi kunci dengan tingkat keamanan yang sangat tinggi. Dalam sistem komunikasi yang aman, dibutuhkan tiga komponen utama yaitu enkripsi untuk menjaga kerahasiaan pesan, autentikasi untuk menjamin keaslian pengirim dan integritas pesan, serta distribusi kunci untuk membagikan kunci rahasia secara aman. Karena keamanan sistem secara keseluruhan tergantung pada bagian terlemahnya, maka penting agar ketiga komponen tersebut memiliki tingkat keamanan yang seimbang dan kuat.

Bagian ini mengevaluasi *primitive* kriptografi yang digunakan untuk enkripsi, distribusi kunci, dan autentikasi pesan dalam sistem komunikasi yang aman. Enkripsi modern seperti AES dan RSA bergantung pada asumsi komputasi yang dapat dilemahkan oleh kemajuan teknologi, termasuk komputer kuantum. Satu-satunya

metode enkripsi yang terbukti aman secara teori adalah *One-Time Pad*, namun penggunaannya memerlukan distribusi kunci yang aman dan sepanjang pesan. Di sinilah QKD berperan penting, yaitu sebagai *primitive* distribusi kunci berbasis hukum fisika kuantum, yang memungkinkan dua pihak membentuk kunci rahasia secara bersamaan dan mendeteksi upaya penyadapan. Untuk autentikasi pesan, metode seperti tanda tangan digital dan *Message Authentication Code* (MAC) juga bergantung pada asumsi komputasi, sedangkan fungsi *hash universal-2*, sebagaimana diperkenalkan oleh Wegman-Carter, memungkinkan autentikasi yang aman secara teoretis tanpa bergantung pada asumsi komputasi. Untuk memperjelas perbandingan, Tabel 3.3 menyajikan klasifikasi dasar keamanan dari masing-masing *primitive* kriptografi.

Tabel 3.3 Dasar Keamanan dari *primitive* kriptografi.

Kategori	Jenis <i>Primitive</i> Kriptografi	Dasar Keamanan
Enkripsi	<i>Block cipher</i> atau <i>stream cipher</i> (kunci lebih pendek dari pesan)	Asumsi komputasi
	Kriptografi kunci publik	Asumsi komputasi
	<i>One-Time Pad</i>	Teori informasi
Distribusi Kunci	Saluran aman	Asumsi komputasi
	Kriptografi kunci publik	Asumsi komputasi
	QKD	Teori informasi kuantum
Otentikasi Pesan	Kriptografi kunci publik	Asumsi komputasi
	MAC	Asumsi komputasi

Kategori	Jenis <i>Primitive</i> Kriptografi	Dasar Keamanan
	Fungsi <i>hash universal-2</i> (Wegman-Carter)	Teori informasi

Dari Tabel 3.3 dapat disimpulkan bahwa sebagian besar metode kriptografi konvensional baik untuk enkripsi, distribusi kunci, maupun autentikasi pesan masih bergantung pada asumsi komputasi yang bisa menjadi lemah di masa depan. Sebaliknya, metode seperti *One-Time Pad*, QKD, dan fungsi *hash universal-2* menawarkan keamanan berbasis teori informasi yang terbukti secara matematis dan tahan terhadap ancaman jangka panjang, termasuk dari komputer kuantum.

Kombinasi ketiga komponen kriptografi yang aman secara teori informasi tersebut QKD, *One-Time Pad*, dan autentikasi *hash universal-2* telah menjadi salah satu pencapaian utama dari proyek SECOQC dalam program *6th Framework* Uni Eropa. Jaringan SECOQC menggabungkan QKD dengan implementasi fungsi *hash universal-2* yang efisien untuk otentikasi, serta menggunakan *One-Time Pad* atau AES (dengan pergantian kunci yang sangat sering) untuk enkripsi data (*payload encryption*).

5. Rencana Kerja ISG-QKD

Bagian ini menjelaskan rencana kerja dari ETSI ISG-QKD dalam mengembangkan kerangka standar dan spesifikasi teknis yang dibutuhkan untuk mendukung penerapan nyata dan penggunaan yang memenuhi syarat dari sistem QKD. Terdiri atas 3 sub bagian:

a. Sertifikasi Keamanan QKD

Subbagian ini menguraikan kebutuhan untuk mengembangkan sistem sertifikasi keamanan bagi QKD agar dapat digunakan secara profesional. Sertifikasi ini mencakup evaluasi sistem

secara menyeluruh baik perangkat keras, perangkat lunak, hingga subsistem optik kuantumnya dan meminimalkan risiko dari sisi implementasi maupun serangan. Dokumennya meliputi:

- 1) QKD; *Ontology, Vocabulary, Terms of Reference*
- 2) QKD; *Assurance requirements*
- 3) QKD; *Module security specification*
- 4) *List of approved QKD technologies*
- 5) QKD; *Threats and Attacks*
- 6) QKD; *Security Proofs*
- 7) QKD; *Components and Internal Interfaces*

b. Integrasi QKD ke Infrastruktur yang Ada

Subbagian ini fokus pada bagaimana QKD dapat diintegrasikan secara praktis ke dalam sistem komunikasi konvensional, seperti jaringan optik dan sistem aplikasi. Hal ini penting karena sistem QKD tidak dapat berdiri sendiri namun harus dapat berfungsi bersama dengan infrastruktur TIK yang sudah ada. Dokumennya meliputi :

- 1) QKD; *Use Cases*
- 2) QKD; *Application Interface*
- 3) QKD *devices integration within standard optical networks*

c. Penelitian Pelengkap

Subbagian ini melengkapi pengembangan teknis QKD dengan menyoroti faktor-faktor non teknis yang sangat penting bagi adopsi teknologi secara luas melalui penelitian tambahan. Penelitian ini mencakup analisis terhadap faktor-faktor yang dapat mendorong maupun menghambat implementasi QKD serta kajian prospektif mengenai kebutuhan pengguna, tantangan regulasi, dan potensi penerapannya di kawasan Eropa.

6. Skenario Aplikasi untuk QKD

Bagian ini menyajikan beragam skenario penerapan QKD dalam sistem TIK, dengan mengacu pada model referensi lapisan *Open*

Systems Interconnection (OSI). Penempatan QKD dalam arsitektur sistem tidak terbatas pada satu lapisan tertentu, karena seperti halnya *primitive* distribusi kunci lainnya QKD dapat diintegrasikan pada berbagai level protokol sesuai dengan kebutuhan sistem.

Pendekatan ini menunjukkan bahwa QKD memiliki fleksibilitas tinggi dan dapat diadaptasikan dalam berbagai jenis sistem dan arsitektur komunikasi, mulai dari koneksi antar perangkat hingga aplikasi pada lapisan tertinggi.

a. *Data Link Layer*

Pada lapisan ini, QKD dapat digunakan sebagai mekanisme pertukaran kunci dalam protokol komunikasi seperti *Point-to-Point Protocol* (PPP) dan MACsec (IEEE 802.1). PPP biasanya digunakan untuk menghubungkan dua node jaringan, sedangkan MACsec menyediakan layanan keamanan data seperti kerahasiaan, integritas, dan autentikasi dalam jaringan lokal.

Karena QKD saat ini umumnya diimplementasikan sebagai tautan *point-to-point*, teknologi ini sangat sesuai jika dikombinasikan dengan perangkat enkripsi tautan (*link encryptor*). Hasil kombinasi ini dikenal sebagai QKD *Link Encryptor*, yang berfungsi seperti VPN *tunnel* untuk melindungi lalu lintas data antara dua titik jaringan. Kunci yang dihasilkan oleh QKD digunakan dalam algoritma *cipher* simetris (seperti AES) atau *One-Time Pad* untuk tingkat keamanan maksimum.

QKD *Link Encryptor* dapat digunakan baik untuk komunikasi langsung antar node jaringan maupun untuk perlindungan komunikasi ujung-ke-ujung (*end-to-end*) di seluruh jaringan. Sistem ini juga memiliki manajemen kunci terintegrasi, sehingga dapat digunakan untuk mengamankan koneksi jaringan seperti *Fast Ethernet* secara transparan.

b. *Network Layer*

Pada lapisan ini, QKD dapat diintegrasikan ke dalam protokol IPsec, yang berfungsi mengamankan komunikasi IP melalui autentikasi dan enkripsi paket data. Biasanya, IPsec menggunakan protokol *Internet Key Exchange* (IKE) yang memanfaatkan algoritma *Diffie-Hellman* untuk menghasilkan *shared secret* sebagai dasar pembentukan kunci kriptografi.

Dalam skenario berbasis QKD, protokol IKE dimodifikasi agar *shared secret* diperoleh dari hasil pertukaran kunci kuantum, bukan dari metode kriptografi klasik. Kunci yang dihasilkan QKD ini dapat digunakan dalam *cipher* blok, *stream cipher*, atau *One-Time Pad* untuk tingkat keamanan tinggi.

Integrasi ini memungkinkan IPsec tetap digunakan secara umum, namun dengan keamanan distribusi kunci yang jauh lebih kuat dan tahan terhadap ancaman jangka panjang, termasuk dari komputer kuantum.

c. *Transport Layer*

Pada lapisan *transport*, protokol seperti TLS dan SSL digunakan untuk memberikan keamanan *end-to-end* dalam komunikasi jaringan, misalnya saat melakukan transaksi *e-commerce*. Biasanya, protokol ini menggunakan kunci sesi yang dibentuk melalui pertukaran kunci publik. Dalam skenario QKD, kunci sesi tersebut dapat digantikan oleh kunci hasil QKD, atau digunakan langsung untuk enkripsi *One-Time Pad* agar keamanan lebih maksimal. Selain itu, kunci QKD juga dapat digunakan untuk otentikasi pesan, sebagai pengganti HMAC atau fungsi acak pada TLS/SSL.

d. *Application Layer*

Di atas lapisan *transport*, sistem QKD juga dapat diintegrasikan pada lapisan aplikasi (Lapisan 7) dalam model OSI. Integrasi ini

berguna untuk aplikasi yang menggunakan *pre-shared key* untuk autentikasi pengguna, akses terhadap hak tertentu, atau sebagai kunci enkripsi dalam proses pengiriman data antar aplikasi.

7. Skenario Penggunaan (*Use Cases*)

Bagian ini membahas beberapa contoh kasus penggunaan nyata (*use cases*) dari QKD dalam berbagai sektor dan kebutuhan komunikasi, baik di lingkungan komersial, pemerintahan, maupun infrastruktur kritis. Setiap *use cases* menunjukkan bagaimana QKD dapat memperkuat keamanan komunikasi dengan menyediakan kunci kriptografi yang aman secara teori informasi.

a. *Use Case 1: Backup di Lokasi Terpisah dan Kelangsungan Bisnis (Offsite Backup/Business Continuity)*

Skenario ini menggambarkan penggunaan QKD untuk mengamankan komunikasi antar pusat data (*data center*) yang digunakan dalam strategi *backup* dan kelangsungan bisnis (*business continuity*). Umumnya, organisasi seperti perusahaan besar atau instansi pemerintah mengoperasikan dua atau lebih pusat data yang terhubung melalui jaringan serat optik untuk memungkinkan replikasi dan sinkronisasi data secara berkala atau *real-time*. Dalam konteks ini, QKD digunakan untuk mendistribusikan kunci kriptografi secara terus-menerus dan aman, guna mengenkripsi seluruh lalu lintas data antar lokasi. Operasional enkripsi dilakukan di lapisan data *link* (Lapisan 2 OSI) menggunakan perangkat QKD *Link Encryptor*, yang bekerja secara transparan tanpa perlu modifikasi pada aplikasi. Kunci yang dihasilkan QKD digunakan oleh *cipher* simetris (seperti AES) atau *One-Time Pad*, tergantung pada tingkat keamanan yang diinginkan. Integrasi ini tidak hanya memperkuat perlindungan data, tetapi juga memastikan bahwa sistem tetap berjalan meski terjadi serangan siber, bencana alam, atau kegagalan sistem, sebagai bagian dari strategi *disaster recovery*.

Aktor utama dalam skenario ini adalah organisasi yang memiliki atau menyewa perangkat QKD dan infrastruktur komunikasi antar pusat data. Mereka perlu mempertimbangkan kesiapan operasional, seperti pengelolaan jaringan, kompatibilitas dengan sistem yang ada, dan kapasitas QKD untuk menangani lalu lintas data berintensitas tinggi. Meskipun ada kebutuhan investasi awal, manfaat jangka panjangnya mencakup peningkatan keamanan terhadap serangan kuantum, kepatuhan terhadap regulasi perlindungan data, serta peningkatan kepercayaan pemangku kepentingan.

Selain memberikan *perfect forward secrecy* yang tidak tersedia pada sistem kriptografi konvensional, penggunaan QKD dalam skenario ini mendukung perlindungan jangka panjang atas data sensitif yang ditransmisikan antar pusat data. Pertimbangan kualitas layanan, seperti kecepatan pembaruan kunci dan latensi jaringan, juga harus diperhatikan agar sistem dapat berjalan efisien dan tidak mengganggu proses *backup* otomatis yang berlangsung terus-menerus.

b. *Use Case 2: Jaringan Area Metropolitan Perusahaan (Enterprise Metropolitan Area Network)*

Skenario ini menggambarkan sebuah perusahaan besar atau lembaga pemerintah mengelola jaringan pribadi atau menyewa jaringan serat optik untuk menghubungkan satu atau lebih pusat data dengan sejumlah kantor cabang dalam satu wilayah metropolitan. Jaringan ini digunakan untuk berbagai aplikasi penting seperti email, telekonferensi, akses basis data, dan layanan berbasis server lainnya. Karena kantor cabang tidak saling terhubung langsung, komunikasi antar cabang harus melalui pusat data. Dalam skenario ini, organisasi tersebut memerlukan tingkat keamanan yang tinggi terhadap kerahasiaan, integritas, dan autentikasi data, sehingga sistem keamanan khusus sangat dibutuhkan.

Untuk itu, QKD *Link Encryptor* digunakan pada setiap koneksi antar lokasi (pusat data dan kantor cabang), beroperasi di lapisan *data link* (Lapisan 2 OSI). Kunci kriptografi yang dihasilkan secara kontinu oleh perangkat QKD dimanfaatkan untuk melakukan enkripsi lalu lintas jaringan secara transparan, menggunakan *cipher* simetris seperti AES atau *stream cipher*. Karena dilakukan di lapisan bawah, pendekatan ini tidak memerlukan modifikasi pada aplikasi yang digunakan, tetapi justru memungkinkan pengembangan aplikasi komunikasi baru dengan tingkat keamanan yang lebih tinggi, seperti sistem berbasis *One-Time Pad*.

Aktor utama dalam skenario ini adalah organisasi pemilik jaringan dan fasilitas, yang bisa memilih untuk mengelola sendiri perangkat QKD dan infrastrukturnya, atau menyewanya dari penyedia infrastruktur. Mereka juga harus mempertimbangkan isu spesifik seperti kesiapan integrasi QKD ke dalam jaringan yang ada, serta keandalan operasionalnya. Selain itu, mereka perlu mengkaji kebutuhan kualitas layanan (QoS) yang berbeda antara koneksi pusat data ↔ kantor cabang dibandingkan dengan pusat data ↔ pusat data. Hal ini karena lalu lintas data antara cabang bisa lebih bervariasi dalam volume, frekuensi, dan pola transmisinya.

Penerapan QKD dalam jaringan area metropolitan seperti ini memberikan banyak manfaat. Selain menjaga keamanan komunikasi internal perusahaan dari ancaman canggih, QKD juga meningkatkan resiliensi dan fleksibilitas arsitektur jaringan. Organisasi dapat menambah *node* baru atau memperluas jangkauan jaringan dengan tetap mempertahankan standar keamanan tertinggi, sekaligus mendukung kepatuhan terhadap regulasi perlindungan data dan keamanan nasional.

c. *Use Case 3: Kendali dan Akuisisi Data Infrastruktur Kritis (Critical Infrastructure Control and Data Acquisition)*

Skenario ini menggambarkan penggunaan QKD untuk mengamankan komunikasi pada sistem kendali dan pemantauan infrastruktur kritis, seperti pembangkit listrik, jaringan air, sistem transportasi, dan fasilitas energi nasional. Sistem seperti ini biasanya menggunakan *Supervisory Control and Data Acquisition* (SCADA) atau sistem kendali industri lainnya yang melibatkan komunikasi dua arah antara pusat pengendali dan perangkat-perangkat lapangan (sensor, aktuator, *controller*).

Komunikasi dalam sistem infrastruktur kritis sangat sensitif terhadap penyadapan dan manipulasi data karena dapat mengakibatkan gangguan sistem berskala luas. Dengan mengintegrasikan QKD *Link Encryptor* pada koneksi antara pusat kendali dan stasiun-stasiun lapangan, seluruh lalu lintas data dapat dienkripsi dan diautentikasi secara aman secara teori informasi, menggunakan kunci kriptografi yang diperoleh melalui saluran kuantum. Proses ini dilakukan secara transparan di lapisan data *link*, sehingga tidak mengganggu sistem aplikasi dan protokol SCADA yang berjalan.

Aktor dalam skenario ini biasanya adalah operator infrastruktur kritis baik dari sektor publik maupun privat yang bertanggung jawab atas operasi berkelanjutan dan keamanan sistem nasional. Operator dapat memiliki sendiri infrastruktur QKD atau bermitra dengan penyedia layanan khusus. Mereka perlu mempertimbangkan faktor-faktor seperti integrasi dengan perangkat lapangan, reliabilitas sistem QKD di lingkungan yang kompleks, dan efektivitasnya dalam skenario waktu-nyata (*real-time control*).

QKD menghadirkan keuntungan besar bagi sistem ini karena dapat menjamin integritas dan kerahasiaan data kontrol, bahkan terhadap ancaman jangka panjang seperti komputer kuantum. Selain itu, penerapan QKD mendukung regulasi keamanan industri, meningkatkan resiliensi nasional, serta mengurangi risiko terhadap serangan siber yang ditargetkan pada sistem-sistem penting negara.

d. *Use Case 4: Perlindungan Jaringan Backbone (Backbone Protection)*

Skenario ini membahas penerapan QKD untuk mengamankan jaringan *backbone*, yaitu infrastruktur komunikasi utama yang menghubungkan berbagai pusat data, wilayah geografis, atau institusi nasional. Jaringan *backbone* merupakan tulang punggung komunikasi modern, dan gangguan terhadapnya dapat berdampak luas terhadap layanan pemerintahan, keuangan, energi, dan komunikasi publik. Oleh karena itu, perlindungan terhadap saluran *backbone* menjadi prioritas utama dalam strategi keamanan nasional dan korporat.

QKD digunakan untuk menghasilkan kunci kriptografi secara terus-menerus di sepanjang jalur *backbone*, yang kemudian dimanfaatkan oleh *link encryptor* untuk mengenkripsi lalu lintas data antar simpul. Karena QKD bekerja di lapisan data *link*, perlindungan ini bersifat transparan terhadap sistem dan aplikasi yang berjalan di atasnya. Model ini dapat digunakan untuk komunikasi antar kota, antar negara, atau antar lembaga strategis nasional, termasuk militer, kementerian, atau operator jaringan nasional.

QKD memungkinkan distribusi kunci dengan keamanan jangka panjang dan memberikan perlindungan terhadap ancaman komputer kuantum, sekaligus mendukung interoperabilitas antar sistem lembaga dan penyedia infrastruktur. Solusi ini mendukung komunikasi antar *backbone* lintas sektor dengan

standar keamanan yang seragam dan dapat diperluas secara bertahap sesuai kebutuhan.

e. *Use Case 5: Jaringan Akses dengan Keamanan Tinggi (High Security Access Network)*

Skenario ini mengarah pada penggunaan QKD untuk melindungi jalur komunikasi antara pengguna akhir dan jaringan pusat, khususnya untuk pengguna-pengguna dengan kebutuhan keamanan tinggi seperti pejabat negara, unit intelijen, militer, atau layanan publik strategis. Dalam sistem komunikasi tradisional, titik akses pengguna merupakan salah satu titik paling rentan terhadap serangan. Oleh karena itu, penggunaan QKD untuk mengamankan koneksi dari terminal pengguna ke jaringan utama menjadi solusi strategis.

QKD memungkinkan pengamanan komunikasi mulai dari *gateway* akses hingga pusat data, tanpa mengubah aplikasi atau perangkat pengguna. Kunci yang dihasilkan dapat digunakan untuk mengenkripsi data atau mengautentikasi pengguna, memberikan proteksi ujung ke ujung terhadap penyadapan atau pemalsuan identitas. Sistem ini juga dapat digabungkan dengan enkripsi *One-Time Pad* untuk kasus penggunaan yang memerlukan tingkat kerahasiaan maksimal.

Penerapan QKD pada jaringan akses menjadikan sistem komunikasi aman bukan hanya pada level *backbone* atau pusat data, tetapi juga hingga ke sisi pengguna, yang sangat penting untuk menjaga keutuhan sistem misi kritis dan informasi sensitif nasional.

f. *Use Case 6: Layanan Jarak Jauh (Long-Haul Service)*

Skenario ini membahas tantangan dan penerapan QKD dalam layanan komunikasi jarak jauh, seperti koneksi antar negara, antar benua, atau antar pusat data nasional yang terpaut

ratusan kilometer. Karena kanal kuantum memiliki batasan fisik terkait jarak (misalnya atenuasi pada serat optik), QKD untuk *long-haul* membutuhkan pendekatan seperti *trusted repeater nodes* atau eksplorasi *quantum repeater* di masa depan.

Dalam praktiknya, jaringan QKD disusun dalam bentuk *multi-hop*, di mana simpul QKD perantara digunakan untuk meneruskan kunci antar jalur. Ini memungkinkan integrasi QKD pada sistem komunikasi global seperti kabel bawah laut internasional, *backbone* fiber optik nasional, atau sistem komunikasi internasional antar kedutaan dan markas besar lembaga internasional.

Keuntungan utamanya adalah kemampuan QKD untuk menyediakan keamanan jangka panjang lintas wilayah yang tidak bisa dijamin oleh metode konvensional. Meskipun implementasinya menantang secara teknis, manfaat strategisnya sangat besar dalam konteks perlindungan data lintas batas, kedaulatan siber, dan komunikasi diplomatik rahasia.

8. Persyaratan (*Requirements*)

Bagian *Requirements* belum disajikan dalam dokumen pada edisi ini.

C. ETSI GS QKD 005 V1.1.1 *Quantum Key Distribution (QKD): Security Proofs*

Dokumen ETSI GS QKD 005 mendefinisikan persyaratan umum untuk pembuktian keamanan teoretis dalam kriptografi kuantum [5]. Dokumen ini bertujuan sebagai referensi dalam pembuatan persyaratan dan kriteria evaluasi untuk penilaian keamanan sistem QKD secara praktis.

Berbeda dengan kriptografi konvensional yang sering didasarkan pada asumsi komputasional, kriptografi kuantum, khususnya QKD, menawarkan "keamanan tanpa syarat" berdasarkan hukum fisika.

Untuk memenuhi janji tersebut, pembuktian keamanan menjadi aspek penting dalam kriptografi kuantum. Pembuktian keamanan dan penerapannya harus dilakukan dengan sangat hati-hati karena dua alasan utama:

1. Kerumitan dalam definisi keamanan pada kriptografi kuantum;
2. Tantangan dalam menerapkan asumsi-asumsi pada pembuktian keamanan dalam sistem QKD yang nyata/praktikal.

Setiap pelanggaran asumsi sekecil apa pun dalam pembuktian keamanan dapat dimanfaatkan oleh penyerang dengan konsekuensi yang berpotensi merusak keamanan sistem QKD secara nyata. Misalnya dalam protokol BB84, ada asumsi bahwa detektor hanya mendeteksi satu foton. Tetapi jika di dunia nyata detektor tersebut dapat bereaksi terhadap lebih dari satu foton (*multiphoton pulse*), maka penyerang bisa melakukan *Photon Number Splitting (PNS) attack* dan membobol sistem, padahal pelanggaran asumsi tersebut terlihat “sepele”.

1. Ruang Lingkup

QKD merupakan teknologi yang menggunakan efek mekanika kuantum untuk mendistribusikan kunci rahasia antara pihak yang berjauhan. Tujuan dari dokumen ETSI GS QKD 005 adalah:

- a. Menjelaskan secara rinci sifat klaim keamanan, termasuk komponennya yang bersifat statistik.
- b. Mendaftar batasan yang bermakna terkait aksi penyerang.
- c. Menjelaskan perbedaan antara klaim keamanan protokol (berdasarkan model) dan klaim keamanan implementasi.
- d. Mendaftar semua komponen utama dari protokol QKD beserta karakterisasi kritisnya.

Dokumen ini disusun oleh kelompok ISG QKD yang terdiri atas para ahli dalam teori dan praktik QKD. Dengan tujuan-tujuan di atas, dokumen ini diharapkan dapat:

- a. Menjelaskan peran perangkat QKD dalam infrastruktur keamanan berdasarkan sifat klaim keamanan mereka.

- b. Mengklasifikasikan perangkat QKD berdasarkan tingkat keamanan yang dapat dicapai.
- c. Menentukan parameter yang harus dipantau secara berkala untuk menjamin pembuatan kunci rahasia sesuai dengan tingkat keamanan yang berbeda.

Dokumen ini tidak bertujuan untuk:

- a. Menentukan parameter spesifik untuk keberhasilan QKD karena parameter tersebut dapat berubah seiring waktu.
- b. Mengesahkan pembuktian keamanan tertentu.

2. Definisi Keamanan

- a. Apa yang dihasilkan QKD

Pernyataan keamanan: Pernyataan keamanan dari protokol QKD bersifat probabilistik. Kunci akhir dapat diklaim sepenuhnya acak dan rahasia, kondisi kebalikannya memiliki probabilitas kecil, ϵ . Dalam skenario terburuk, dengan probabilitas ϵ , diasumsikan bahwa penyerang mengetahui seluruh kunci. Oleh karena itu, setiap perangkat QKD harus menyebutkan panjang kunci yang dihasilkan dalam rentang waktu tertentu dan parameter ϵ yang terkait dengan kunci tersebut.

Asal Parameter Keamanan ϵ : Beberapa faktor yang berkontribusi terhadap sifat probabilistik dari kunci rahasia meliputi estimasi parameter perangkat dan data, misalnya estimasi tingkat kesalahan. Ada juga faktor lain yang tidak terkait langsung dengan estimasi parameter.

Contoh: Serangan *Intercept/Resend*: Dalam protokol QKD, seorang penyerang dapat mencegat semua sinyal dan mengirim ulang sinyal baru ke penerima, berdasarkan hasil pengukurannya. Dalam beberapa kasus kecil, serangan ini dapat

berhasil tanpa meninggalkan jejak yang terdeteksi, yaitu ketika semua sinyal yang dikirim ulang identik dengan sinyal aslinya.

Mengurangi Parameter Keamanan ϵ : Suatu pembuktian keamanan harus menyebutkan untuk parameter sistem (misalnya kehilangan sinyal, tingkat kesalahan) yang memungkinkan sebuah kunci rahasia dapat diperoleh, dan berapa nilai ϵ yang sesuai.

Jika laju kunci rahasia positif dapat dicapai untuk nilai ϵ tertentu, maka nilai ϵ dapat dikurangi dengan cara meningkatkan jumlah sinyal kuantum yang dipertukarkan, sambil menjaga parameter sistem yang lain tetap sama.

Untuk mencapai hal ini, pembuktian keamanan harus menjelaskan secara tepat parameter-parameter protokol (seperti jumlah *privacy amplification*) yang diperlukan untuk mencapai target tersebut.

Interpretasi: Parameter keamanan ϵ memiliki interpretasi yang jelas, sehingga dari suatu kasus penggunaan tertentu, seseorang dapat menentukan nilai ϵ yang perlu ditargetkan.

Hal ini penting karena ϵ dapat dianggap sebagai probabilitas kegagalan, yang kemudian dapat dikombinasikan dalam suatu analisis risiko.

Contoh: Misal sebuah perusahaan asuransi yang futuristik bersedia memberikan perlindungan terhadap kejadian kegagalan yang sangat tidak mungkin terjadi.

Protokol yang Dapat Dibatalkan: Dalam menentukan nilai ϵ , perlu dicatat bahwa protokol QKD dapat dibatalkan (*abort*), misalnya jika tingkat kesalahan yang diamati terlalu tinggi. Dalam kasus-kasus seperti ini, keluaran dari protokol QKD adalah kunci dengan panjang nol, namun upaya untuk

menghasilkan kunci tetap harus diperhitungkan dalam pemilihan nilai ε .

Contoh: Penyerang cukup memutus saluran kuantum dan melakukan serangan *denial-of-service*. Perlu dicatat bahwa jenis serangan yang sama juga dapat terjadi pada saluran komunikasi klasik, sehingga hal ini bukan merupakan kelemahan khusus dari QKD.

Komposabilitas (Composability): Dalam properti ini, protokol QKD dengan probabilitas kegagalan ε dapat digabungkan dengan protokol lain yang memiliki probabilitas kegagalan ε' , di mana kunci tersebut digunakan. Probabilitas kegagalan gabungan ε'' dari protokol yang digabungkan diperoleh dari jumlah $\varepsilon + \varepsilon'$. Properti komposabilitas ini sangat penting, karena kunci rahasia secara alami akan digunakan oleh aplikasi lain.

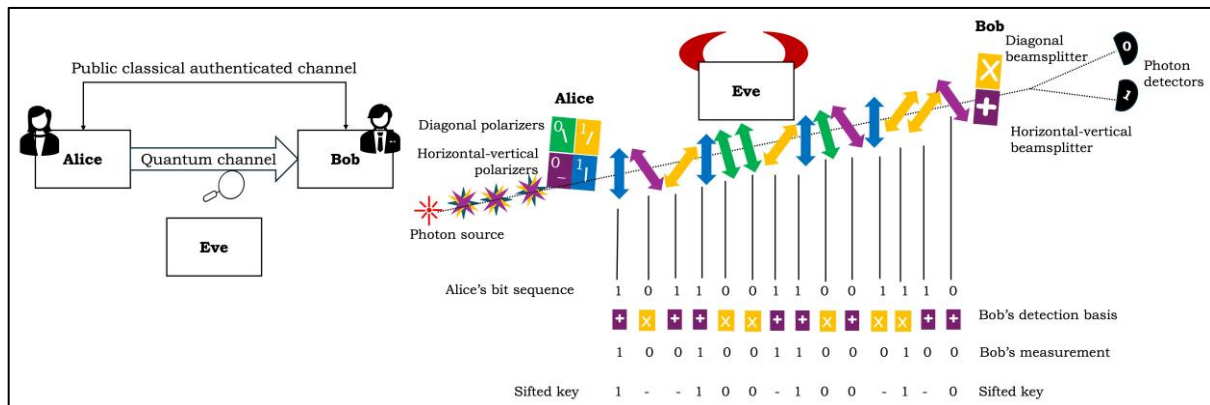
Contoh: Jika selama masa pakai suatu sistem QKD, protokol QKD dijalankan sebanyak N kali, dengan masing-masing memiliki probabilitas kegagalan ε , maka total probabilitas kegagalan untuk gabungan N kali percobaan adalah $N \times \varepsilon$. Oleh karena itu, tidak cukup hanya memastikan bahwa ε kecil, tetapi juga harus memastikan bahwa $N \times \varepsilon$ tetap kecil.

b. Struktur Protokol QKD

Protokol QKD menggunakan berbagai sumber daya:

- 1) Kanal Kuantum (*quantum channel*): yaitu kanal yang mempertahankan sifat-sifat mekanika kuantum.
- 2) Contoh: Serat optik telekomunikasi standar dan transmisi optik melalui ruang bebas.
- 3) Kanal Klasik yang Terautentikasi (*authenticated classical channel*): yaitu kanal publik yang telah terautentikasi, artinya semua pesan yang dikirim melalui kanal ini telah diautentikasi berasal dari pihak yang sesuai.

- 4) Sumber Keacakan: yaitu generator angka acak fisik (bukan PRNG).



Gambar 3.1 Alur komunikasi dalam QKD
digambar ulang dari [5].

QKD terdiri atas dua fase utama:

1) Fase Kuantum

Pada fase ini, sinyal kuantum dikirim melalui saluran kuantum dan diukur oleh pengirim dan penerima. Pada akhir fase ini, kedua pihak memiliki data klasik yang dapat diproses lebih lanjut.

Ada dua jenis protokol utama:

- Protokol *Prepare and Measure*: Pengirim menyiapkan sinyal yang dipilih secara acak, dan penerima mengukurnya dengan metode mekanika kuantum tertentu.
- Protokol Berbasis Keterjeratan (*Entanglement-based Protocols*): Sumber pihak ketiga menyediakan sistem bipartit kepada pengirim dan penerima, yang kemudian diukur.

2) Fase Komunikasi Klasik

Data klasik diproses melalui saluran komunikasi klasik yang diautentikasi. Tahapan dalam fase ini meliputi penyaringan data, koreksi kesalahan, dan amplifikasi privasi untuk memperoleh kunci rahasia akhir.

c. Kerangka Pernyataan Keamanan Pada Implementasi QKD

Dalam bagian ini dijelaskan keterkaitan antara pembuktian keamanan ilmiah dan pengujian terhadap implementasi, untuk memperoleh tingkat keamanan yang dapat diterima. Memahami hubungan ini sangat penting dalam mengembangkan prosedur yang akan memungkinkan sertifikasi implementasi QKD.

Pernyataan keamanan dari suatu implementasi QKD memiliki dua komponen utama, yaitu:

1) Pembuktian Keamanan Ilmiah (*Scientific Security Proof*):

Sebuah Pembuktian Keamanan Ilmiah mencakup:

- a) Model dari perangkat fisik yang digunakan;
- b) Protokol yang dijalankan menggunakan perangkat model tersebut.

Pembuktian ini membuktikan secara konklusif bahwa protokol yang dijalankan pada perangkat model tersebut adalah aman. Pembuktian ini menghasilkan parameter-parameter relevan dari protokol serta menyusun pernyataan keamanan secara tepat.

Sebagai contoh, dalam definisi keamanan yang *composable*, pembuktian ini memberikan bentuk eksak dari parameter keamanan ϵ sebagai fungsi dari parameter-parameter protokol.

Pembuktian Keamanan Ilmiah mengikuti kaidah pembuktian ilmiah yang telah diterima secara umum dan tidak memerlukan spesifikasi tambahan.

2) Verifikasi Implementasi (*Implementation Verification*)

Untuk melengkapi pernyataan keamanan dari suatu implementasi QKD, kita perlu memverifikasi bahwa:

- a) Implementasi aktual sesuai dengan model yang diasumsikan dalam pembuktian keamanan;

- b) Protokol yang dijalankan di dalam perangkat telah diimplementasikan dengan benar.

Verifikasi terhadap kedua langkah ini harus dilakukan berdasarkan standar rekayasa terbaik yang tersedia, menggunakan pengetahuan dan pemahaman terbaik kita terhadap perangkat.

Hasil dari verifikasi bisa berupa:

- a) Lulus/Gagal (misalnya dengan memverifikasi bahwa elemen tertentu telah diimplementasikan, atau melalui pengujian yang memiliki hasil lulus/gagal secara langsung), atau
- b) Pengujian kuantitatif, yang menghasilkan parameter keamanan yang dapat dimasukkan ke dalam pembuktian keamanan.

Penting untuk memahami perbedaan antara:

- a) Pembuktian Keamanan Ilmiah: konsep yang telah diterima secara umum dalam dunia ilmiah.
- b) Verifikasi Implementasi: didasarkan pada praktik terbaik (*best practices*) yang dapat berubah seiring waktu, karena bergantung pada pengetahuan dan pengalaman terbaik yang tersedia saat itu.

Oleh karena itu perlu dirumuskan dalam standar, apa saja praktik terbaik tersebut. Pengujian pada prinsipnya tidak pernah bisa dilakukan secara menyeluruh, dan secara definisi, perangkat nyata selalu memiliki perbedaan dibandingkan model. Namun demikian, tidak semua penyimpangan berdampak pada keamanan.

d. Kerangka Pembuktian Keamanan Ilmiah

Bagian ini menjelaskan ciri-ciri umum dari pembuktian keamanan, sebagaimana diterapkan pada protokol QKD, dan

perlu dihubungkan dengan implementasi tertentu dengan memverifikasi asumsi-asumsi yang dibuat dalam protokol.

Tugas dari sebuah pembuktian keamanan adalah untuk menunjukkan parameter protokol mana yang harus dipilih agar, berdasarkan parameter yang diamati, sebuah kunci rahasia dengan parameter keamanan ϵ dapat dihasilkan. Setiap pembuktian semacam itu dilakukan pada sebuah protokol yang membuat asumsi tertentu tentang implementasinya.

1) Asumsi Keamanan pada Perangkat

- a) Perimeter yang Aman: Perangkat QKD diasumsikan terlindungi dari akses penyerang. Jika tidak, mereka bisa membaca kunci rahasia saat sedang dihasilkan. Oleh karena itu, diasumsikan adanya perimeter yang aman.
- b) Antarmuka Klasik: Antarmuka harus dirancang sedemikian rupa sehingga tidak memungkinkan kebocoran data internal. Contoh sederhananya adalah bahwa antarmuka data klasik dapat dimodelkan dengan sinyal digital, sehingga tidak ada kanal samping (*side-channel*) yang memungkinkan pembacaan proses internal dari perangkat.
- c) Antarmuka Kuantum: Tidak boleh ada kanal samping (*side-channel*) yang memungkinkan serangan terhadap perangkat QKD.
- d) Perangkat Kuantum: Model perangkat harus sesuai dengan asumsi dalam pembuktian keamanan.
- e) Perbedaan Model dan Perangkat Nyata: Pada umumnya, selalu ada penyimpangan antara model dengan perangkat nyata. Penyimpangan ini harus diukur dan diperhitungkan dalam pembuktian keamanan.
- f) Pembuktian Keamanan yang Tidak Bergantung pada Perangkat Nyata: Sebagai alternatif dari kuantifikasi

penyimpangan, terdapat pendekatan yang memungkinkan protokol QKD diselesaikan tanpa model fisik dari perangkat. Dalam kasus ini, protokol QKD harus berbasis keterjeratan (*entanglement-based*) dengan pilihan pengukuran yang aktif. Perlu dicatat bahwa semua asumsi lain tentang perimeter dan antarmuka tetap berlaku. Oleh karena masih terbatasnya implementasi *device-independent QKD*, dokumen ETSI GS QKD 005 fokus pada pendekatan yang memodelkan perangkat mekanika kuantum.

g) Asumsi Terhadap Penyerang

Meskipun QKD dapat diterapkan tanpa menetapkan batasan teknologi pada pihak lawan, dalam kondisi tertentu diperbolehkan menetapkan asumsi mengenai kemampuan pihak lawan, asalkan asumsi tersebut dinyatakan secara jelas dan konsisten. Salah satu contoh asumsi tersebut adalah *noisy and bounded storage model* untuk berbagai tugas kriptografi kuantum.

2) Asumsi Terhadap Penyerang

Bagian ini mencantumkan beberapa asumsi yang dibuat terkait kemampuan penyerang. Perlu dicatat bahwa pembatasan-pembatasan ini tidak dapat diverifikasi, tetapi diasumsikan berlaku. Penting untuk selalu mengevaluasi kembali apakah asumsi-asumsi ini masih masuk akal dari waktu ke waktu.

CATATAN 1: Berbeda dengan kriptografi klasik, pembatasan teknologi seperti yang disebutkan di atas hanya perlu berlaku selama tahap pembentukan kunci. Jika di kemudian hari penyerang memperoleh kemampuan yang melampaui pembatasan tersebut, keamanan kunci yang telah dihasilkan tetap tidak terpengaruh.

Pembatasan terhadap Kemampuan Penyimpanan Kuantum:

- a) Tanpa memori kuantum: Penyerang harus langsung mengukur keadaan kuantum tambahan (ancilla) miliknya segera setelah berinteraksi dengan sistem.
- b) Memori kuantum jangka pendek: Penyerang menyimpan sistem ancillanya hingga pengumuman publik dilakukan (misalnya, basis yang digunakan), tetapi setelah itu ia harus melakukan pengukuran.
- c) Memori terbatas: Dalam model ini, pada tahap tertentu dari protokol, jumlah memori kuantum yang dimiliki penyadap dibatasi hingga sejumlah tertentu. Artinya, kapasitas memori jangka panjang dibatasi, meskipun memori jangka pendek di awal protokol bisa tidak terbatas.
- d) *Noisy memory*: Diasumsikan bahwa setiap penyimpanan memori kuantum selalu disertai dengan gangguan (*noise*) tertentu yang dapat mempengaruhi integritas data kuantum.

CATATAN 2: Konsep memori terbatas dan *noisy memory* dapat dikombinasikan menjadi suatu pembatasan umum atas kemampuan penyimpanan kuantum seorang penyadap.

Asumsi tanpa memori kuantum kadang-kadang menghasilkan laju kunci (*key rate*) yang lebih tinggi, yang dapat dijelaskan oleh perbedaan antara batas Holevo atas informasi yang bisa didapat oleh Eve dan informasi yang sebenarnya dapat diakses.

Model memori terbatas dan memori berisik merupakan perkembangan yang lebih baru, yang memiliki manfaat tambahan yaitu mampu digunakan dalam primitif kriptografi yang melampaui QKD, seperti *oblivious transfer*, *bit commitment*, dll.

Diketahui bahwa oblivious transfer bisa digunakan untuk membangun sistem komputasi dua-pihak yang aman secara umum.

Contoh: Contoh aplikasi praktis adalah identifikasi aman dengan mesin ATM yang tidak dipercaya.

e) Serangan Spesifik

Dalam literatur, cukup sering ditemukan klaim mengenai laju kunci yang aman terhadap serangan tertentu.

CATATAN 3: Analisis terhadap serangan spesifik bisa menjadi alat yang baik untuk menguji batasan protokol, namun tidak cukup untuk menyatakan keamanan secara menyeluruh.

Pernyataan keamanan selalu harus dikaitkan dengan serangkaian alat (*toolbox*) yang tersedia untuk penyadap. Artinya, penyadap tidak hanya dapat menggunakan alat-alat tersebut secara individu, tetapi juga menggabungkannya dengan berbagai cara.

Protokol QKD yang hanya aman terhadap serangan tertentu sering kali gagal saat menghadapi penyadap yang menggabungkan elemen-elemen dari serangan-serangan tersebut dengan cara yang berbeda.

e. Pemodelan, Asumsi, dan Kanal Samping (*Side Channels*)

Bagian ini membahas asumsi yang dibuat dalam protokol QKD mengenai komponen mekanika kuantum pada perangkat QKD serta bagaimana cara verifikasinya. Selain itu, dibahas pendekatan pemodelan perangkat dalam pembuktian keamanan QKD sebagaimana disebutkan pada bagian “Asumsi Keamanan pada Perangkat”.

Produsen perangkat QKD harus:

- 1) Menentukan model fisik secara rinci dari sistem QKD yang digunakan dalam praktik.

- 2) Membuktikan atau memverifikasi bahwa model tersebut benar-benar sesuai dengan sistem fisik yang sebenarnya.

Meskipun suatu protokol QKD memiliki pembuktian keamanan yang ketat, jika model sistemnya salah, tidak ada jaminan bahwa sistem QKD tersebut aman. Selain itu, ada kemungkinan terdapat celah implementasi yang dapat dimanfaatkan oleh penyadap untuk membobol sistem.

Meskipun telah terjadi banyak kemajuan dalam bidang ini, tetap masih terdapat kesenjangan besar antara teori dan praktik QKD. Berikut adalah prinsip umum dalam pemodelan sistem QKD:

- 1) Menuliskan semua asumsi yang dibuat dengan eksplisit.
- 2) Memverifikasi semua asumsi melalui eksperimen dan pengujian.
- 3) Mengukur penyimpangan dari model ideal dan mempertimbangkannya dalam proses amplifikasi privasi.
- 4) Membuat pembuktian keamanan berdasarkan model yang lebih realistis, bukan hanya model ideal.

1) Sumber Cahaya dalam QKD

Komponen sumber cahaya dalam sistem QKD memiliki beberapa asumsi utama:

a) Fase Randomisasi

Diasumsikan bahwa sinyal yang dipancarkan bersifat *fase-randomized* sehingga bisa dianggap sebagai campuran klasik dari sinyal dengan jumlah foton tertentu.

Namun, dalam beberapa kasus, asumsi ini bisa gagal, misalnya ketika *mode-locking* digunakan atau dalam skenario *Plug&Play*.

Jika sumber cahaya tidak mengalami randomisasi fase, maka sistem harus mempertimbangkannya dalam

analisis keamanan atau menerapkan randomisasi fase aktif.

b) Distribusi Foton

Dalam protokol QKD, penting untuk mengetahui distribusi jumlah foton yang dihasilkan untuk mengantisipasi serangan *photon-number splitting* (PNS). Statistik foton harus diuji dan dipastikan tetap stabil sepanjang umur perangkat QKD.

c) Derajat Kebebasan (*Degrees of Freedom* (DoF))

DoF merupakan jumlah parameter yang digunakan untuk mengkodekan informasi. Biasanya, sumber sinyal dimodelkan sebagai mode tunggal (frekuensi, waktu, mode spasial) dengan satu derajat kebebasan (misalnya polarisasi atau fase).

d) Batas Keamanan di Saluran Optik

Tidak boleh ada cara bagi pihak luar untuk membaca pengaturan internal unit pengirim atau memodifikasi komponennya (misalnya laser, modulator).

Isolator optik yang dimonitor harus digunakan sebagai langkah keamanan minimal.

2) Unit Deteksi Dalam QKD

Pada bagian deteksi, ada beberapa asumsi penting:

a) Derajat Kebebasan

Diasumsikan bahwa unit deteksi hanya bereaksi terhadap derajat kebebasan tempat sinyal kuantum diencode.

Misalnya, dalam sistem dengan polarisasi sebagai DoF, detektor tidak boleh menunjukkan respons yang berbeda terhadap derajat kebebasan lainnya (frekuensi, waktu, mode spasial).

b) Efisiensi Deteksi

Diasumsikan bahwa probabilitas deteksi tidak bergantung pada pengaturan pengukuran. Dalam praktiknya, efisiensi deteksi foton tunggal bisa berbeda, sehingga perlu dilakukan pengaturan khusus atau dimasukkan dalam pembuktian keamanan.

c) Batas Keamanan di Kanal Optik

Tidak boleh ada cara bagi pihak luar untuk membaca atau mengubah pengaturan internal unit penerima.

Isolator optik yang dimonitor harus digunakan sebagai tindakan keamanan dasar.

f. Asumsi Klasik (*Shielding, Electronic Side-Channels*)

Asumsi-asumsi dalam konteks klasik, seperti perlindungan terhadap *electronic side-channels* dan *shielding* perangkat, dibahas dalam dokumen keamanan ETSI GS QKD 008.

g. Protokol Klasik Dalam QKD

Setelah fase kuantum selesai, bagian klasik dari protokol QKD bertujuan untuk membangun kunci rahasia berdasarkan data yang diperoleh. Langkah-langkah dalam protokol klasik meliputi:

- 1) Pengujian Data
- 2) Pemilihan Data yang Valid (*Sifting*)
- 3) Estimasi Kesalahan
- 4) Rekonsiliasi (Koreksi Kesalahan)
- 5) Amplifikasi Privasi
- 6) Autentikasi

Semua elemen ini harus sesuai dengan pembuktian keamanan perangkat secara keseluruhan.

1) *Sifting*

Contoh berikut ini termasuk proses *presifting* dan *inverse sifting*:

- a) Bob membalas dengan serangkaian nomor slot waktu yang menunjukkan di slot waktu mana ia berhasil mengukur sinyal. Untuk setiap slot waktu, ia juga mengirimkan basis pengukuran yang digunakan.
 - b) Alice membalas secara urutan yang terdiri atas: “Basis Sama”, atau “Basis Tidak Sama”.
 - c) Alice dan Bob menyimpan bit-bit yang sesuai dengan basis yang sama. Ini disebut *sifted key*.
- 2) Estimasi Kesalahan
- a) Alice secara acak memilih sebagian (*sub-string*) dari *sifted key* dan mengirimkan kepada Bob posisi dan nilai bit yang sesuai. Bob membandingkan *sub-string* ini dengan bagian yang sama dari *sifted key* miliknya, lalu mengumumkan hasilnya. Alice dan Bob menggunakan hasil ini untuk memperkirakan tingkat galat (*error rate*).
 - b) Jika tingkat galat berada di bawah batas tertentu yang telah ditentukan oleh pembuktian keamanan (*security proof*), maka protokol dilanjutkan. Jika tidak, protokol dibatalkan.
 - c) Bit-bit yang telah dipertukarkan secara terbuka dibuang dari *sifted key*.

Tahapan ini dapat dilakukan secara kebalikan (Bob yang mengirim, Alice yang memverifikasi), atau secara simetris (keduanya mengirim sebagian *sifted key*).

Jumlah total dari bit yang dibuka sangat penting untuk menghasilkan estimasi statistik yang baik.

3) Rekonsiliasi (Koreksi Kesalahan)

Berikut ini contoh langkah-langkah pada tahap rekonsiliasi:

- a) Alice menggunakan estimasi tingkat galat dan sebuah *error correction code* untuk menghasilkan bit-bit paritas yang dijamin cukup untuk menyelaraskan (*reconcile*)

kunci Bob dengan miliknya berdasarkan *error correction code* tersebut.

- b) Alice mengirimkan bit-bit paritas kepada Bob.

Jika pesan ini tidak dienkripsi, maka informasi ini harus dihitung dan diperhitungkan dalam tahap privasi amplifikasi (*privacy amplification*), karena membuka informasi ke publik.

Jika dienkripsi, maka penggunaan kunci tambahan untuk enkripsi ini harus dihitung saat menentukan laju akhir pembangkitan kunci.

- c) Bob menerapkan prosedur *error correction* pada *sifted key*-nya. *Sifted key* Alice dan kunci hasil koreksi Bob menjadi kunci yang sudah direkonsiliasi.

- d) Bob membandingkan kunci hasil rekonsiliasi dengan *sifted key*-nya sendiri. Berdasarkan perbandingan ini, dia menghitung tingkat galat pasca-rekonsiliasi dan mengirimkan hasil estimasi itu ke Alice. Jika tingkat galat berada di bawah batas yang ditentukan oleh bukti keamanan, protokol dilanjutkan; jika tidak, maka dihentikan.

4) Konfirmasi

Alice dan Bob dapat memeriksa dengan probabilitas tinggi apakah koreksi kesalahan berhasil dengan melakukan *confirmation test* (uji konfirmasi). Salah satu cara untuk melakukannya adalah dengan menghitung dan membandingkan nilai hash dari fungsi yang dipilih secara tepat terhadap kunci yang telah direkonsiliasi.

Keuntungan dari uji konfirmasi adalah memastikan bahwa Alice dan Bob memiliki kunci yang identik, bahkan jika hanya dilakukan estimasi kasar terhadap tingkat kesalahan dalam proses estimasi kesalahan.

Penting untuk secara jelas menyebutkan protokol konfirmasi yang digunakan beserta parameternya, dan memverifikasi bahwa protokol tersebut konsisten dengan bukti keamanan yang menyediakan probabilitas kegagalan yang diinginkan.

CATATAN: Perlu secara jelas memperhitungkan kebocoran informasi ke Eve (penyadap) selama uji konfirmasi ini.

5) Amplifikasi Privasi

Tujuan dari amplifikasi privasi adalah untuk mengurangi kemungkinan bahwa penyadap (*eavesdropper*) memiliki pengetahuan tentang kunci di bawah batas atas tertentu, yaitu ϵ . Untuk mencapai tujuan ini, proses yang dilakukan:

- a) Alice dan Bob secara independen menghitung panjang akhir kunci, yang tergantung pada bukti keamanan, parameter protokol (termasuk tingkat kesalahan/*error rate*), dan panjang blok kunci yang telah direkonsiliasi (dikonfirmasi).
- b) Alice secara acak memilih fungsi *hash* yang menjamin bahwa probabilitas dua input berbeda menghasilkan *output* yang sama sangat kecil, lalu mengkomunikasikan pilihan tersebut kepada Bob.
- c) Alice dan Bob melakukan proses *hashing* pada kunci yang telah direkonsiliasi (dikonfirmasi) menggunakan fungsi tersebut. Hasil dari *hashing* inilah yang menjadi kunci akhir milik Alice dan Bob.

Catatan: Perlu ditentukan apakah akan menggunakan fungsi *hash* yang baru atau yang sama pada putaran baru QKD, dan berkaitan dengan itu, apakah perlu dilakukan pengacakan ulang (*reshuffling*) terhadap bit atau tidak.

6) Autentikasi

Komunikasi melalui kanal publik perlu diautentikasi untuk mencegah serangan *man-in-the-middle*. Ada berbagai metode yang dapat digunakan, antara lain:

a) Autentikasi Berdasarkan Teori Informasi (*Information Theoretic Authentication*)

Metode ini menggunakan fungsi *hash* yang menjamin bahwa probabilitas dua input berbeda menghasilkan *output* yang sama sangat kecil. Membutuhkan rahasia bersama (*shared secret*) untuk putaran QKD yang pertama. Sebelum QKD dimulai, Alice dan Bob harus sudah memiliki sejumlah kecil kunci rahasia bersama terlebih dahulu. Setelah QKD berjalan, kunci dari QKD sebelumnya dapat digunakan untuk autentikasi putaran QKD berikutnya. Parameter keamanan ϵ secara keseluruhan tetap terjaga ketika dua protokol (QKD + autentikasi) digabung.

b) Metode Autentikasi Lainnya

Saat ini, berbagai metode autentikasi lain sedang dikembangkan dan dibahas dalam penelitian. Mekanisme autentikasi hanya perlu aman sampai kunci diterima. Setelah kunci akhir diterima oleh kedua pihak, autentikasi bisa dibobol tanpa membahayakan keamanan kunci tersebut. Ini karena yang dilindungi adalah proses komunikasi saat pertukaran kunci, bukan isi kunci itu sendiri setelah proses selesai.

7) Kesalahan Umum Dalam Protokol Klasik

Beberapa kesalahan umum yang dapat membahayakan keamanan sistem QKD:

a) Tidak mengautentikasi semua informasi yang dipertukarkan.

- b) Menggunakan protokol dua arah tanpa pembuktian keamanan yang sesuai.
- c) Parameter koreksi kesalahan atau amplifikasi privasi tidak ditentukan dengan jelas.
- d) Mengabaikan efek ukuran terbatas (*finite-size effects*) dalam perhitungan tingkat keamanan.
- e) Tidak menangani *multiple-clicks* (misalnya akibat *dark counts* atau *multi-foton*).
- f) Tidak mempertimbangkan kebocoran informasi selama fase klasik.
- g) Secara tidak sengaja mengungkapkan informasi tambahan dalam protokol *post-processing*.

D. ETSI GS QKD 008 V1.1.1 *Quantum Key Distribution (QKD): QKD Module Security Specification*

ETSI GS QKD 008 V1.1.1 adalah standar internasional yang menetapkan persyaratan keamanan minimum untuk modul QKD yang digunakan dalam sistem keamanan telekomunikasi guna melindungi informasi sensitif sesuai dengan ISO/IEC 19790 [6]. Dokumen ini disusun oleh kelompok ETSI QKD-ISG yang terdiri atas operator dan penyedia layanan. Sebanyak sebelas aspek keamanan telah diidentifikasi dengan mengacu pada metodologi sistem kriptografi konvensional. Namun, dokumen ini tidak membedakan tingkatan keamanan, tingkat sensitivitas data, atau lingkungan aplikasi karena kekhususan sistem QKD. Persyaratan perangkat lunak mendapat perhatian besar karena perangkat lunak mengendalikan seluruh sistem pengukuran dan komunikasi, serta menjadi dasar utama keamanan sistem secara keseluruhan. Selain itu, persyaratan perlindungan terhadap serangan non-invasif juga disertakan.

Meskipun kepatuhan terhadap persyaratan keamanan yang tercantum penting, hal itu tidak cukup untuk menjamin keamanan modul secara keseluruhan. Operator modul QKD bertanggung jawab untuk

memastikan keamanan modul dapat diterima oleh pemilik informasi dan menyadari risiko yang masih tersisa. Penggunaan modul QKD yang telah divalidasi juga tidak menjamin keamanan sistem secara keseluruhan. Oleh karena itu, kesadaran akan pentingnya keamanan informasi harus menjadi prioritas manajemen dan dikomunikasikan kepada seluruh pihak terkait. Setiap organisasi perlu mengidentifikasi sumber daya informasi mereka, menilai tingkat sensitivitas dan dampak kerugian, serta menerapkan pengendalian yang tepat berdasarkan risiko, termasuk kebijakan administratif, kontrol fisik dan lingkungan, pengendalian data, serta perencanaan cadangan dan kontingensi.

Struktur dokumen ETSI GS QKD 008 V1.1.1 terdiri atas:

1. Ruang lingkup
2. Referensi
3. Definisi dan singkatan
4. Tujuan keamanan fungsional
5. Lampiran A (normatif): Ringkasan persyaratan dokumentasi
6. Lampiran B (normatif): QKD *Module Security Policy*
7. Lampiran C (informatif): Praktik Pengembangan Perangkat Lunak yang Direkomendasikan
8. Lampiran D (informatif): Fungsi Keamanan yang Disetujui Contoh: BB84
9. Lampiran E (informatif): Penentu Lokasi Sumber Daya Seragam Internet yang Berlaku
10. Lampiran F (informatif): Bibliografi
11. Lampiran G (informatif): Penulis dan kotributor.

Penjelasan singkatnya adalah sebagai berikut:

1. Ruang lingkup

Dokumen ETSI GS QKD 008 V1.1.1 bertujuan untuk menetapkan persyaratan yang diperlukan agar modul QKD memiliki probabilitas tinggi untuk mendeteksi dan merespons secara tepat dan tepat waktu terhadap upaya akses fisik langsung, dan penggunaan atau modifikasi modul di dalamnya. Tujuan utamanya adalah untuk

mendeteksi setiap kemungkinan penetrasi dengan probabilitas tinggi, dan menghasilkan zeroisasi segera semua Parameter Keamanan Kritis (*Critical Security Parameter*) dalam bentuk *plainteks*.

Tujuan ini memerlukan mekanisme untuk menyediakan perlindungan menyeluruh di sekitar modul QKD, sensor serta sirkuit untuk mendeteksi dan merespons tepat waktu terhadap semua upaya akses fisik yang tidak sah. Ini dapat diperoleh dengan menggunakan pelindung (*enclosure*) yang cukup kuat, sirkuit deteksi dan respons gangguan redundan yang menolak semua *Critical Security Parameter* yang berbentuk *plainteks*. Integritas pelindung dapat dikontrol menggunakan lapisan atau segel anti-gangguan (*tamper-evident*), dan kunci anti-bobol pada semua penutup atau pintu modul yang dapat dilepas.

Pelindung yang kuat harus tak tembus cahaya (*opaque*) terhadap semua pemeriksaan radiasi visual dan non-visual dan sirkuit deteksi gangguan serta zeroisasi dilindungi terhadap penonaktifan. Ketika zeroisasi diperlukan, Parameter Keamanan Publik (*Public Security Parameter*) dan *Critical Security Parameter* dinolkan.

Akses dan pengoperasian modul harus memerlukan mekanisme autentikasi berbasis-identitas yang meningkatkan organisasi berbasis-peran. Autentikasi ini harus memerlukan setidaknya autentikasi dua faktor untuk autentikasi operator (*password* rahasia, kunci atau token fisik, biometrik). Pengoperasian yang tepat memerlukan autentikasi identitas operator dan untuk memverifikasi bahwa ia berwenang untuk mengambil peran tertentu dan melakukan serangkaian layanan yang sesuai.

Entri atau *output Critical Security Parameter* harus dilakukan menggunakan porta yang secara fisik terpisah dari porta lain, atau

melalui antarmuka yang secara logis dipisahkan menggunakan saluran tepercaya dari antarmuka lain mana pun.

Semua modul QKD harus dilindungi terhadap kondisi lingkungan atau fluktuasi di luar rentang operasi normal modul, karena penyimpangan tersebut dapat dilihat sebagai serangan, atau dapat meningkatkan kemungkinan kegagalan modul dan dapat membahayakan keamanan modul dan pengoperasiannya. Besaran lingkungan yang harus dikontrol harus berupa kegelapan (bila diperlukan), suhu, tegangan, tekanan, kelembapan, komposisi kimia atmosfer, getaran mekanis, dan keberadaan nuklir serta radiasi pengion lainnya. Karena modul QKD mencakup subsistem optik dan elektro-optik, maka perlu untuk mengendalikan setiap variabel lingkungan yang dapat memengaruhi secara khusus komponen tersebut dan cara kerjanya, baik secara sementara maupun permanen.

Modul QKD diharuskan untuk menyertakan fitur perlindungan lingkungan khusus yang dirancang untuk mendeteksi fluktuasi dan meniadakan *Critical Security Parameter*, atau menjalani Pengujian Kegagalan Lingkungan (*Environmental Failure Testing*) yang ketat untuk memberikan jaminan yang masuk akal bahwa modul tidak akan terpengaruh oleh fluktuasi di luar rentang operasi normal dengan cara yang dapat membahayakan keamanannya.

Secara khusus, semua modul QKD memerlukan perlindungan *Critical Security Parameter* terhadap serangan Analisis Waktu (*Timing Analysis Attacks*), Analisis Daya Sederhana (*Simple Power Analysis*), serangan Analisis Daya Diferensial (*Differential Power Analysis Attacks*), Serangan Emanasi Elektromagnetik (*Electromagnetic Emanation Attacks*), dan serangan apa pun yang dilakukan melalui kanal optik.

Modul QKD harus menggunakan perlindungan kriptografi yang kuat untuk mendeteksi dan mencegah pengungkapan dan modifikasi *Public Security Parameter* serta *Critical Security Parameter* saat modul tidak aktif. Untuk memastikan bahwa setiap kali modul beroperasi dalam mode aman (*safe mode*), modul harus memiliki indikasi yang jelas bahwa modul beroperasi dalam Mode yang Disetujui (*Approved Mode*). Karena perangkat lunak memiliki kontrol akhir dalam setiap modul QKD, komponen ini harus menyediakan solusi yang kuat dan teruji untuk enkripsi dan autentikasi semua *Critical Security Parameter*, semua Parameter Keamanan Sensitif (*Sensitive Security Parameters*) dalam sistem dan juga untuk menyediakan uji integritas yang aman untuk kode perangkat lunak saat modul tidak digunakan.

Komponen perangkat lunak modul QKD dapat dijalankan pada sistem komputasi umum jika sistem operasi menyediakan audit semua akses operator ke data audit, semua permintaan untuk menggunakan mekanisme manajemen data autentikasi, semua penggunaan Fungsi Petugas Kripto yang relevan dengan keamanan, dan semua permintaan untuk mengakses data autentikasi yang terkait dengan modul QKD. Secara khusus, sistem operasi yang menjalankan sistem komputasi umum harus:

- a. mencegah operator dalam peran pengguna memodifikasi perangkat lunak, *Sensitive Security Parameters* (SSP) sistem, dan data audit yang disimpan dalam lingkungan operasional modul;
- b. mengomunikasikan semua SSP, data autentikasi, input kontrol, dan output status melalui saluran tepercaya; dan
- c. mengaudit pengoperasian saluran tepercaya apa pun.

2. Referensi

Tidak ada acuan normatif dan acuan informatif pada dokumen ini.

3. Definisi dan singkatan

a. Definisi

Terdapat 108 buah definisi pada dokumen ETSI GS QKD 008 V1.1.1. Berikut adalah beberapa definisi yang terdapat dalam dokumen ini:

- 1) mode operasi yang disetujui: mode modul QKD yang hanya menggunakan fungsi keamanan yang disetujui atau diizinkan

CATATAN: Jangan sampai tertukar dengan mode khusus dari fungsi keamanan yang disetujui.

CONTOH: AES pada mode CBC

- 2) pengujian bersyarat: pengujian yang dilakukan oleh modul QKD ketika kondisi yang ditentukan untuk pengujian terjadi.
- 3) *Configuration Management System* (CMS): manajemen fitur dan jaminan keamanan melalui kontrol perubahan yang dilakukan pada perangkat keras, perangkat lunak, dan dokumentasi modul QKD
- 4) *Critical Security Parameter* (CSP): informasi terkait keamanan (misalnya kunci kriptografi rahasia dan pribadi, konfigurasi perangkat keras optik dan data otentikasi seperti password dan PIN) yang pengungkapan atau modifikasinya dapat membahayakan keamanan modul QKD
- 5) *Cryptographically protected Critical Security Parameter* (CSP): *Critical Security Parameter* (CSP) yang dilindungi secara kriptografi terhadap pengungkapan, modifikasi, dan penggantian yang tidak sah, dan yang alasan kekuatan mekanisme perlindungannya hanya bergantung pada Fungsi Keamanan yang Disetujui
- 6) *Cryptographically protected Public Security Parameter* (PSP): *Public Security Parameter* (PSP) yang dilindungi secara kriptografi terhadap modifikasi dan penggantian yang tidak sah dan yang alasan kekuatan mekanisme perlindungannya hanya bergantung pada Fungsi Keamanan yang Disetujui.

- 7) *Cryptographically protected Sensitive Security Parameter* (SSP): baik *cryptographically protected Critical Security Parameter* (CSP) atau *Cryptographically protected Public Security Parameter* (PSP).
- 8) mikrokode: instruksi prosesor dasar yang sesuai dengan instruksi program yang dapat dieksekusi.
- 9) pasivasi: proses dalam konstruksi perangkat semikonduktor di mana sambungan, permukaan komponen dan sirkuit terpadu diberikan sarana perlindungan terhadap modifikasi perilaku sirkuit.
- 10) Modul QKD: seperangkat komponen perangkat keras dan perangkat lunak yang mengimplementasikan fungsi kriptografi dan proses optik kuantum, termasuk algoritma dan protokol kriptografi serta pembangkitan kunci, dan terkandung dalam batas kriptografi yang ditentukan.

b. Singkatan

Terdapat 32 buah singkatan pada dokumen ETSI GS QKD 008 V1.1.1 diantaranya:

- 1) *CMS Configuration Management System*
- 2) *CSP Critical Security Parameter*
- 3) *DPA Differential Power Analysis*
- 4) *HDL Hardware Description Language*
- 5) *LDPC Low-Density Parity-Check*
- 6) *PSP Public Security Parameter*
- 7) *RBG Random Bit Generator*
- 8) *SPA Simple Power Analysis*
- 9) *SSP Sensitive Security Parameter*
- 10) *TA Timing Analysis*
- 11) *URL Uniform Resource Locator*
- 12) *VHDL VHSIC Hardware Description Language*
- 13) *VHSIC Very-High-Speed Integrated Circuits*

4. Tujuan keamanan fungsional

Persyaratan keamanan yang ditetapkan dalam dokumen ini terkait dengan desain dan implementasi modul QKD yang aman. Persyaratan tersebut berasal dari tujuan keamanan fungsional tingkat tinggi berikut:

- a. Untuk menggunakan protokol QKD yang benar dan implementasinya yang benar, yang memungkinkan pengguna untuk memastikan bahwa hanya dua entitas yang berkomunikasi yang menghasilkan dan berbagi barisan biner acak rahasia yang sama, dan tidak ada informasi terkait lainnya yang tersedia bagi orang lain; artinya pengguna adalah orang yang memilih tingkat keamanan apa pun definisinya selama pengguna menyetujuinya.
- b. Untuk menggunakan dan mengimplementasikan dengan benar fungsi keamanan, komunikasi kriptografi dan kuantum yang terkait, yang diperlukan untuk perlindungan informasi sensitif yang termuat atau dihasilkan di dalam modul QKD.
- c. Untuk melindungi modul QKD dari operasi atau penggunaan yang tidak sah.
- d. Untuk mencegah pengungkapan isi modul QKD yang tidak sah.
- e. Untuk mencegah modifikasi modul QKD dan algoritma kriptografi yang tidak sah dan tidak terdeteksi, termasuk modifikasi, penggantian, penyisipan, dan penghapusan SSP yang tidak sah.
- f. Untuk memberikan indikasi yang benar tentang status operasional modul QKD.
- g. Untuk memastikan bahwa modul QKD selalu berfungsi dengan baik saat beroperasi dalam Mode Operasi yang Disetujui dari modul tersebut.
- h. Untuk mendeteksi kesalahan dalam pengoperasian modul QKD dan untuk mencegah kompromi atau modifikasi data sensitif dan SSP yang diakibatkan oleh kesalahan ini.

- i. Untuk memastikan desain, distribusi, dan implementasi modul QKD yang tepat.

Pasal ini berisi 14 pasal, dengan penjelasan singkat dari masing-masing subpasal adalah sebagai berikut:

a. Pasal 4.1 Persyaratan keamanan

Subpasal ini menetapkan persyaratan keamanan yang harus dipenuhi oleh modul QKD yang sesuai dengan dokumen ini. Protokol QKD secara keseluruhan, khususnya bagian optik kuantum dan algoritmiknya, tidak secara langsung disebutkan dalam dokumen ini. Keamanan dari setiap protokol QKD alternatif yang mungkin ada harus diuji dan diselidiki sebelum dimasukkan dalam rangkaian Fungsi Keamanan yang Disetujui, dan parameter serta penggunaannya akan dijelaskan dalam dokumen Mode Operasi yang Disetujui. Dokumen ini menetapkan persyaratan dan langkah-langkah yang akan memastikan bahwa kondisi yang diperlukan selalu terpenuhi, atau jika tidak, sistem harus direset, dihentikan, dan dimasukkan dalam status kesalahan. Persyaratan keamanan dalam dokumen ini mencakup aspek-aspek terkait desain, implementasi, dan operasi modul QKD. Aspek-aspek tersebut meliputi spesifikasi modul QKD; porta dan antarmuka modul; peran, layanan, dan autentikasi; keamanan perangkat lunak; lingkungan operasional; keamanan fisik; perlindungan terhadap serangan non-invasif; manajemen *sensitive security parameter*; *self-test*; dan jaminan siklus hidup. Modul QKD harus diuji sesuai dengan persyaratan setiap area yang dibahas dalam subpasal ini dan divalidasi secara independen di setiap area. Validasi keseluruhan akan menunjukkan hasil validasi independen minimum yang diterima di setiap area. Semua dokumentasi, termasuk salinan manual pengguna dan instalasi, harus disediakan kepada laboratorium pengujian oleh vendor. Persyaratan keamanan dalam dokumen ini mencakup

persyaratan dokumentasi khusus yang dirangkum dalam Lampiran A dan C.

b. Pasal 4.2 Spesifikasi modul QKD

Modul QKD harus merupakan sekumpulan komponen perangkat keras dan perangkat lunak yang mengimplementasikan fungsi kriptografi dan proses optik kuantum, termasuk algoritma dan protokol kriptografi serta pembangkitan kunci, dan berada dalam batas kriptografis yang terdefinisi.

Dalam Mode Operasi yang Disetujui, modul QKD harus mengimplementasikan minimal satu Fungsi Keamanan yang Disetujui atau Diperbolehkan (lihat persyaratan spesifikasi Modul QKD yang tercantum dalam Lampiran A).

Fungsi Keamanan yang Diperbolehkan yang digunakan dalam Mode Operasi yang Disetujui harus memenuhi semua persyaratan yang berlaku yang ditentukan dalam lampiran B. Operator harus dapat menentukan kapan mode operasi yang disetujui dipilih. Semua mode operasi yang disetujui harus dijelaskan dalam Kebijakan Keamanan modul (lihat Lampiran B). Perangkat keras dan perangkat lunak modul QKD dapat dikecualikan dari persyaratan dokumen ini jika vendor dapat menunjukkan bahwa perangkat keras dan perangkat lunak yang dikecualikan tidak mempengaruhi keamanan modul.

Kebijakan Keamanan modul QKD harus menetapkan kapan modul QKD beroperasi dalam mode operasi yang disetujui. Selain itu, modul QKD harus menunjukkan kapan mode operasi yang disetujui dipilih.

1) Pasal 4.2.1 Tipe modul QKD

Modul QKD harus didefinisikan sebagai modul Hibrida; yaitu modul yang fungsinya terutama terdapat dalam perangkat lunak, yang juga mencakup dan menggunakan beberapa

perangkat keras optik dan kriptografis dengan tujuan khusus dalam batasan kriptografis modul.

2) Pasal 4.2.2 Batasan kriptografis

Batasan kriptografis harus terdiri atas perimeter yang ditetapkan secara eksplisit yang menetapkan batas fisik modul QKD. Persyaratan dokumen ini harus diterapkan untuk semua komponen dalam batas ini, termasuk semua perangkat keras dan perangkat lunak. Batasan kriptografis harus mencakup prosesor, optik, dan komponen perangkat keras lainnya yang menyediakan lingkungan operasional modul.

3) Pasal 4.2.3 Beberapa mode operasi yang disetujui

Modul QKD boleh dirancang untuk mendukung beberapa mode operasi yang disetujui. Agar modul QKD dapat menerapkan lebih dari satu mode operasi yang disetujui, berikut ini harus berlaku:

- a) Keamanan modul secara keseluruhan harus tidak diubah saat dikonfigurasi untuk berbagai mode operasi yang disetujui.
- b) Kebijakan Keamanan harus menjelaskan setiap mode operasi yang disetujui yang diterapkan dalam modul QKD dan bagaimana setiap mode dikonfigurasi.
- c) Setelah konfigurasi ulang dari satu mode operasi yang disetujui ke mode operasi lain, modul QKD harus melakukan uji mandiri pra-operasional (pasal 4.10.1).
- d) *Pre-operational self-tests* harus dilakukan untuk semua fungsi keamanan yang disetujui dan diizinkan yang digunakan dalam mode operasi yang disetujui yang dipilih.
- e) Jika konfigurasi ulang dari satu mode operasi yang disetujui ke mode operasi lain mengubah keamanan fisik modul tanpa mengubah keamanan keseluruhan modul

kriptografi, maka modul kriptografi harus melakukan zeroisasi semua CSP dalam modul.

4) Pasal 4.2.4 *Degraded functionality*

Modul QKD boleh dirancang untuk mendukung fungsionalitas yang terdegradasi dalam mode operasi yang disetujui. Contohnya adalah beralih dari satu algoritma enkripsi ke algoritma lain jika algoritma awal gagal dalam *self-test*. Kasus lain dapat terjadi jika komunikasi kuantum melalui *band* tertentu tidak mencapai tingkat kualitas minimum, dan dialihkan untuk menggunakan yang lain. Setiap perubahan dalam mode operasi yang disetujui akan menurunkan fungsionalitasnya.

Agar modul QKD dapat menerapkan fungsionalitas yang terdegradasi dalam mode operasi yang disetujui, hal berikut ini berlaku:

- a) Operasi yang terdegradasi harus terjadi setelah kegagalan *pre-operational self-tests*.
- b) Ketika modul QKD beroperasi dengan fungsionalitas yang terdegradasi, setiap fungsi keamanan operasional harus lulus semua *self-tests* yang berlaku.
- c) Fungsi keamanan non-operasional harus diisolasi dari fungsi keamanan modul QKD yang tersisa.
- d) Modul harus tetap dalam mode terdegradasi hingga semua uji yang gagal, telah lulus.

5) Pasal 4.2.5 Kekuatan keamanan modul

Kekuatan keamanan modul QKD harus ditentukan. Kekuatan keamanan modul QKD harus tidak lebih besar dari kekuatan keamanan minimum Fungsi Keamanan dan SSP yang Disetujui dan Diizinkan dalam Mode Operasi yang Disetujui

c. Pasal 4.3 Porta fisik dan antarmuka logis modul QKD

Modul QKD didefinisikan di atas sebagai yang termuat dalam batas kriptografi yang didefinisikan sebagai perimeter fisik berkelanjutan yang memuat semua perangkat keras dan perangkat lunak. Modul QKD harus membatasi semua aliran informasi dan titik akses fisik ke porta fisik dan antarmuka logis yang menentukan semua titik masuk dan keluar ke dan dari batas kriptografinya. Antarmuka modul QKD harus berbeda secara logis satu sama lain meskipun mereka dapat berbagi satu port fisik (misalnya data masukan dapat masuk dan data keluaran dapat keluar melalui porta yang sama) atau dapat didistribusikan melalui satu atau lebih porta fisik (misalnya data masukan dapat masuk melalui porta serial dan paralel).

Modul QKD boleh menggunakan beberapa saluran komunikasi independen. Keluaran data, untuk semua saluran komunikasi, harus dinonaktifkan saat melakukan pembangkitan kunci, entri kunci manual, *self-test*, *loading* perangkat lunak, dan zeroisasi.

d. Pasal 4.4 Peran, autentikasi, dan layanan

1) Peran

Modul QKD harus mendukung peran yang sah bagi operator serta layanan yang terkait dengan masing-masing peran. Salah satu peran utama yang harus didukung adalah Peran Petugas Kriptografi, yang bertanggung jawab untuk melakukan seluruh fungsi inisialisasi, manajemen, serta layanan keamanan umum seperti pengelolaan kunci kriptografi, CSP, dan fungsi audit. Selain itu, modul QKD dapat mendukung Peran Pengguna. Jika peran ini tersedia, maka operator dengan peran tersebut harus menjalankan layanan keamanan umum termasuk operasi kriptografi dan fungsi keamanan lain yang telah disetujui. Modul QKD juga dapat mendukung peran tambahan selain dua peran utama tersebut. Seorang operator dapat menjalankan lebih dari satu

peran, dan jika modul mendukung beberapa operator secara bersamaan, maka sistem modul harus dapat memisahkan peran dan layanan yang diemban oleh masing-masing operator secara internal. Peran sah ini berlaku untuk seluruh layanan yang menggunakan fungsi keamanan yang telah disetujui atau yang berdampak pada keamanan modul. Namun, operator tidak diwajibkan memegang peran sah untuk menjalankan layanan yang tidak menggunakan, mengubah, atau mengungkap CSP maupun PSP, misalnya untuk menampilkan status modul. Seluruh peran sah yang didukung oleh modul QKD harus dicantumkan dan dijelaskan secara lengkap dalam dokumentasi resmi.

2) Autentikasi Petugas

Modul QKD harus mendukung mekanisme autentikasi untuk memverifikasi identitas operator yang mengakses modul dan memastikan bahwa operator memiliki wewenang untuk menjalankan peran yang diminta serta layanan yang terkait. Mekanisme kontrol akses yang harus didukung oleh modul QKD meliputi autentikasi berbasis peran dan autentikasi berbasis identitas. Pada autentikasi berbasis peran, operator harus memilih satu atau lebih peran secara eksplisit maupun implisit, dan modul harus mengautentikasi pengambilan peran tersebut. Sedangkan dalam autentikasi berbasis identitas, operator harus diidentifikasi secara unik dan individu, memilih satu atau lebih peran, dan modul harus mengautentikasi baik identitas maupun otorisasi operator atas peran yang dipilih. Jika operator diizinkan untuk mengganti peran, modul juga harus memverifikasi otorisasi terhadap peran baru tersebut. Operator yang telah diautentikasi dapat diizinkan untuk menjalankan seluruh layanan dalam peran yang sah, atau dapat diwajibkan untuk menjalani autentikasi terpisah untuk setiap layanan. Setiap

kali modul dimatikan dan dinyalakan kembali, autentikasi sebelumnya tidak boleh disimpan, dan operator harus diautentikasi ulang. Berbagai jenis data autentikasi dapat digunakan, seperti kata sandi, PIN, kunci kriptografi, token fisik, atau biometrik. Data autentikasi dalam modul QKD harus dilindungi dari pengungkapan, modifikasi, dan penggantian yang tidak sah. Jika data autentikasi tidak tersedia saat pertama kali modul diakses, metode lain seperti kontrol prosedural atau data autentikasi bawaan harus digunakan, namun data autentikasi bawaan tersebut harus diganti setelah autentikasi pertama. Data autentikasi bawaan tidak wajib memenuhi persyaratan pemusnahan (*zeroization*). Mekanisme autentikasi dapat terdiri atas beberapa metode yang secara kolektif memenuhi kekuatan autentikasi yang disyaratkan. Jika fungsi kriptografi digunakan dalam autentikasi, maka harus menggunakan Fungsi Kriptografi yang Disetujui atau Diizinkan. Kekuatan autentikasi harus memenuhi ketentuan sebagai berikut:

- a) kemungkinan keberhasilan autentikasi dalam satu percobaan tidak boleh lebih dari satu dalam 2^{27} (sekitar 1 banding 134 juta);
- b) untuk beberapa percobaan dalam satu menit, kemungkinan berhasil tidak boleh lebih dari satu dalam 2^{32} (sekitar 4,3 miliar), dengan jeda minimal 2 detik antarpercobaan;
- c) implementasi modul harus memenuhi kekuatan autentikasi ini tanpa bergantung pada kontrol prosedural;
- d) jika digunakan kata sandi, modul harus membatasi pemilihan kata sandi untuk mencegah penggunaan kata sandi lemah;

- e) umpan balik data autentikasi kepada operator harus disamarkan selama proses autentikasi (misalnya, tidak menampilkan karakter yang diketik); dan
- f) umpan balik autentikasi tidak boleh melemahkan kekuatan mekanisme autentikasi.

Jika modul menggunakan data autentikasi bawaan saat pertama kali diakses, maka data tersebut harus unik untuk setiap unit modul. Selain itu, modul QKD harus menerapkan autentikasi berbasis identitas dan secara khusus juga harus menerapkan autentikasi dua faktor berbasis identitas untuk mengontrol akses ke modul.

3) Layanan

Modul QKD harus menyediakan berbagai layanan bagi operator, antara lain: menampilkan status terkini dari modul, menampilkan nama dan nomor versi modul, menjalankan uji mandiri sebelum operasi sebagaimana diatur dalam pasal 4.10, menjalankan minimal satu fungsi keamanan yang Disetujui atau Diizinkan dalam mode operasi yang Disetujui sebagaimana dijelaskan dalam pasal 4.1, serta melakukan proses zeroisasi sesuai ketentuan dalam pasal 4.9.6. Modul juga harus mendukung kemampuan *bypass*, yaitu kemampuan suatu layanan untuk sebagian atau sepenuhnya melewati fungsi kriptografi. Jika modul dapat mengeluarkan data atau status dalam bentuk yang dilindungi secara kriptografis, tetapi juga dapat mengeluarkannya dalam bentuk tidak terlindungi akibat konfigurasi modul atau intervensi operator, maka kemampuan *bypass* tersebut harus ditentukan secara jelas. Dalam hal ini, operator harus terlebih dahulu berada dalam peran yang sah sebelum dapat mengatur kemampuan *bypass*. Selain itu, dua tindakan internal yang independen harus dilakukan untuk menonaktifkan mekanisme yang dirancang guna mencegah

bypass keamanan yang tidak disengaja akibat kesalahan tunggal. Tindakan ini harus mengubah perilaku perangkat lunak dan/atau perangkat keras yang secara khusus mengatur proses *bypass*. Modul juga harus menampilkan status untuk menunjukkan apakah layanan yang diberikan menggunakan fungsi kriptografi (*bypass* tidak diaktifkan) atau tidak (*bypass* diaktifkan). Jika modul memiliki kemampuan untuk memuat perangkat lunak dari sumber eksternal, maka logika pemuatannya harus terpisah secara logis dari seluruh keluaran data. Modul tidak boleh mengeksekusi kode yang dimuat hingga pengujian pemuatan perangkat lunak sebagaimana diatur dalam pasal 4.10.2 berhasil memverifikasi validitas kode tersebut. Modul juga tidak boleh menjalankan fungsi keamanan yang Disetujui sampai pengujian algoritma kriptografi dalam pasal 4.10.1 telah berhasil dilakukan. Selain itu, modul harus menggunakan teknik autentikasi yang Disetujui untuk memverifikasi validitas perangkat lunak eksternal yang akan dimuat. Tidak diperkenankan untuk menetapkan lingkungan operasional yang terbatas atau tidak dapat diubah hanya dengan aturan keamanan prosedural guna melarang penggunaan kemampuan pemuatan perangkat lunak eksternal. Di luar layanan-layanan utama tersebut, modul QKD juga dapat menyediakan layanan lainnya, baik yang Disetujui maupun yang tidak, dan layanan tertentu dapat tersedia dalam lebih dari satu peran, seperti layanan entri kunci yang dapat diakses baik oleh pengguna maupun petugas kriptografi.

e. Pasal 4.5 Keamanan perangkat lunak

Ketentuan berikut harus diterapkan pada perangkat lunak yang terdapat dalam modul QKD. Seluruh kode kriptografi dalam modul harus berada dalam bentuk yang dapat dijalankan. Setiap

perangkat lunak dalam modul harus dilindungi oleh mekanisme kriptografi menggunakan teknik integritas yang Disetujui, seperti kode autentikasi pesan atau algoritma tanda tangan digital, yang menggunakan kunci kriptografi; kunci tersebut dapat berada di dalam modul. Input dan *output* modul harus diarahkan melalui Antarmuka Perangkat Lunak Modul (*Module Software Interface* (MSI)) yang telah ditentukan. MSI tidak boleh mengizinkan operator layanan untuk membaca perangkat lunak atau memodifikasi perangkat lunak modul tanpa menjalankan Uji Pemuatan Perangkat Lunak sebagaimana diatur dalam pasal 4.10.2. Setiap modifikasi terhadap perangkat lunak modul, selain pemuatan ulang secara menyeluruh, juga harus melewati uji tersebut. Apabila modul menerima data dari sumber eksternal dalam format tertentu, maka modul harus memverifikasi kesesuaian format tersebut.

Teknik integritas yang Disetujui dalam Uji Integritas Perangkat Lunak harus melibatkan pembuatan tanda tangan digital menggunakan algoritma tanda tangan digital yang Disetujui. Entitas yang meminta validasi harus menghasilkan kunci privat untuk menandatangani kode dan kunci publik untuk memverifikasi tanda tangan. Kunci privat tidak boleh berada di dalam modul, sedangkan kunci publik dapat disimpan bersama perangkat lunak modul. Modul juga harus menyediakan perintah MSI (layanan yang dapat dipanggil) yang memungkinkan Petugas Kriptografi menjalankan Uji Integritas Perangkat Lunak tanpa mematikan daya modul. Perintah ini harus mengembalikan informasi apakah uji berhasil serta nilai *hash* yang baru dihitung. Nilai *hash* awal dari perangkat lunak modul dapat dikirimkan terlebih dahulu secara terpisah kepada Petugas Kriptografi, yang kemudian dapat membandingkan nilai *hash* baru dengan nilai yang diberikan oleh penyedia modul. Jika nilai *hash* tidak cocok atau tanda tangan digital tidak valid, maka

perangkat lunak modul harus dianggap tidak sah. Nilai *hash* tersebut harus dihapus dari modul setelah perintah MSI untuk Uji Integritas selesai dijalankan.

Modul harus memiliki kemampuan untuk mendekripsi bagian perangkat lunak yang terenkripsi saat pertama kali dimuat. Semua CSP, perangkat lunak Uji Integritas (termasuk kunci publik dan tanda tangan digital) harus dienkripsi oleh penyedia menggunakan kunci simetris. Kunci simetris tersebut, atau komponennya, harus dihasilkan oleh penyedia (pasal 4.9.2) dan dikirim ke lokasi modul (pasal 4.9.3 dan 4.9.4), namun tidak boleh disimpan di dalam modul selama pengangkutan ke pelanggan. Setelah perangkat lunak dimuat ke dalam modul, Petugas Kriptografi harus memasukkan kunci simetris atau komponennya (sesuai pasal 4.9.4) untuk mendekripsi bagian yang terenkripsi, kemudian menjalankan Uji Integritas sebagai bagian dari pengujian pra-operasional. Sebelum modul beralih ke status pra-operasional, Petugas Kriptografi dapat menyediakan kunci simetris baru atau komponennya; jika tidak, maka kunci simetris yang ada akan digunakan. Semua CSP dan perangkat lunak Uji Integritas (termasuk kunci publik dan tanda tangan digital) harus dienkripsi kembali dan seluruh salinan dalam bentuk jelas (*plaintext*) di dalam modul harus dihapus secara otomatis. Untuk setiap instansi modul QKD, sepasang kunci baru untuk Uji Integritas serta kunci enkripsi simetris baru juga harus dihasilkan (pasal 4.9.2). Mode enkripsi yang digunakan untuk melindungi CSP dan perangkat lunak Uji Integritas harus berupa enkripsi Disetujui dengan mode autentikasi. Selain CSP dan perangkat lunak Uji Integritas, enkripsi simetris juga harus diterapkan pada seluruh PSP.

f. Pasal 4.6 Lingkungan operasional

Persyaratan dalam pasal ini hanya berlaku untuk modul yang berisi perangkat lunak yang berjalan dalam lingkungan

operasional yang dapat dimodifikasi. Lingkungan operasional dari modul QKD adalah kumpulan seluruh perangkat lunak dan perangkat keras yang diperlukan agar modul dapat beroperasi secara aman. Contohnya, lingkungan operasional dari suatu modul perangkat lunak mencakup modul itu sendiri, prosesor tempat perangkat lunak dijalankan, dan sistem operasi yang mengontrol eksekusi perangkat lunak. Lingkungan operasional dapat berupa lingkungan yang tidak dapat dimodifikasi atau yang dapat dimodifikasi. Lingkungan yang tidak dapat dimodifikasi dirancang untuk hanya memuat perangkat lunak yang telah tervalidasi, misalnya pada kartu pintar atau kartu PC yang tidak dapat diprogram, atau perangkat lunak yang hanya dapat diperbarui melalui proses autentikasi data yang Disetujui, seperti Uji Pemuatan Perangkat Lunak (*Software Load Test*) dalam pasal 4.10.2. Dalam hal ini, komponen lingkungan operasional yang menjamin ketidakmampuan modifikasi harus terikat pada modul perangkat lunak. Sementara itu, lingkungan operasional yang dapat dimodifikasi memungkinkan pemuatan perangkat lunak yang belum tervalidasi, seperti dalam sistem operasi umum (contoh: sistem operasi komputer atau kartu pintar yang dapat dikonfigurasi). Sistem operasi dianggap sebagai lingkungan yang dapat dimodifikasi apabila perangkat lunak dapat dimodifikasi oleh operator dan/atau operator dapat memuat serta menjalankan perangkat lunak yang tidak termasuk dalam paket validasi awal.

Tujuan dari persyaratan dalam pasal 4.5 adalah untuk melindungi secara logis modul QKD yang berjalan dalam lingkungan operasional yang dapat dimodifikasi dari akses tidak sah (eksekusi, modifikasi, atau pembacaan) oleh proses yang tidak tepercaya. Pasal ini tidak mencakup perlindungan fisik terhadap modul. Dokumentasi harus menjelaskan lingkungan

operasional dari modul QKD, termasuk sistem operasi yang digunakan bila relevan.

Untuk lingkungan operasional yang membatasi sesi hanya untuk satu operator pada satu waktu, persyaratan berikut harus diterapkan: semua perintah MSI dalam sesi harus dijalankan atas nama satu operator; semua CSP harus dihapus sebelum sesi operator berakhir dan sebelum sesi operator baru dimulai; dan proses yang dijalankan oleh modul QKD harus dimiliki oleh modul itu sendiri, bukan oleh proses eksternal atau operator lain. Jika sistem operasi memungkinkan beberapa operator berjalan secara bersamaan, maka harus dipenuhi bahwa semua perangkat lunak kriptografi, SSP, serta informasi kontrol dan status berada di bawah kendali sistem operasi yang menerapkan kontrol akses diskresioner guna mencegah eksekusi, modifikasi, dan pembacaan tidak sah. Mekanisme kontrol akses sistem operasi harus dikonfigurasi untuk menegakkan hak akses terhadap peran yang dapat menjalankan, memodifikasi, atau membaca perangkat lunak kriptografi, data audit, CSP, data teks terang, serta SSP. Selain itu, sistem operasi harus mencegah semua operator dan proses yang berjalan dari memodifikasi proses kriptografi yang sedang berjalan, mencegah akses baca atau tulis terhadap SSP milik operator lain, serta mencegah proses eksternal membaca perangkat lunak kriptografi dalam batas kriptografi. Konfigurasi sistem operasi untuk memenuhi persyaratan ini harus dijelaskan dalam pedoman Petugas Kriptografi, yang menyatakan bahwa sistem operasi harus dikonfigurasi sebagaimana dijelaskan sebelum isi modul dianggap terlindungi.

Sistem operasi juga harus menyediakan mekanisme audit untuk mencatat modifikasi, akses, penghapusan, dan penambahan data kriptografi dan SSP. Jika informasi audit disimpan di luar modul, maka modul harus menggunakan mekanisme kriptografi

yang Disetujui untuk melindungi informasi tersebut dari pengungkapan dan modifikasi tidak sah. Peristiwa yang harus dicatat meliputi: percobaan memberikan input tidak sah ke fungsi Petugas Kriptografi, serta penambahan atau penghapusan operator dari peran Petugas Kriptografi. Mekanisme audit juga harus mampu mencatat seluruh akses baca/tulis operator terhadap data audit, permintaan penggunaan mekanisme manajemen data autentikasi, penggunaan fungsi Petugas Kriptografi yang relevan terhadap keamanan, permintaan akses data autentikasi, serta permintaan eksplisit untuk mengambil alih peran Petugas Kriptografi.

Kebijakan Keamanan Modul harus menetapkan apakah identifikasi dan autentikasi operator dilakukan oleh kode sistem operasi atau oleh kode yang disediakan vendor. Dalam kedua kasus, mekanisme identifikasi dan autentikasi harus memenuhi persyaratan pasal 4.4.2. Sistem operasi juga harus dikonfigurasi untuk mencegah operator dalam peran pengguna (jika didukung) dari memodifikasi perangkat lunak kriptografi, SSP sistem, dan data audit yang tersimpan dalam lingkungan operasional modul. Selain itu, Kanal Terpercaya (*Trusted Channel*) harus diterapkan antara operator yang telah diautentikasi dan modul QKD. Semua SSP, data autentikasi, input kontrol, dan output status harus dikomunikasikan melalui Saluran Terpercaya ini, yang hanya boleh diaktifkan oleh operator atau modul QKD. Saluran ini harus menyediakan autentikasi sumber serta mencegah modifikasi, penggantian, pengungkapan, dan pengulangan parameter keamanan secara tidak sah.

Sebagai tambahan atas semua persyaratan audit sebelumnya, mekanisme audit juga harus mencatat: upaya penggunaan fungsi saluran terpercaya, serta identifikasi dari penginisiasi dan target saluran terpercaya. Mekanisme audit harus dikonfigurasi secara permanen agar selalu mencatat: seluruh akses baca/tulis

oleh operator terhadap data audit, permintaan penggunaan mekanisme manajemen data autentikasi, penggunaan fungsi Petugas Kriptografi yang penting untuk keamanan, serta permintaan akses terhadap data autentikasi yang terkait dengan modul QKD.

g. Pasal 4.7 Keamanan fisik

Modul QKD harus menerapkan mekanisme keamanan fisik guna membatasi akses fisik tidak sah terhadap isi modul dan mencegah penggunaan atau modifikasi tidak sah setelah modul dipasang. Seluruh perangkat keras, perangkat lunak, dan SSP dalam batas kriptografi modul harus dilindungi. Mekanisme keamanan fisik ini, tergantung pada jenisnya, harus mampu mendeteksi upaya akses fisik tidak sah, baik setelah kejadian melalui bukti kerusakan (*tamper evidence*), maupun saat kejadian berlangsung melalui mekanisme tanggap kerusakan (*tamper response*).

Perlindungan fisik umumnya mencakup penyediaan mekanisme bukti kerusakan, opasitas area kritis dalam modul, dan penggunaan penutup kuat yang dilengkapi dengan deteksi dan respons kerusakan terhadap bagian yang dapat dilepas seperti pintu atau penutup.

Jika modul QKD dirancang untuk memungkinkan akses fisik, seperti oleh vendor atau individu berwenang lainnya, maka antarmuka akses pemeliharaan harus ditentukan, mencakup jalur akses fisik dan dilindungi dengan mekanisme keamanan fisik yang sesuai. Seluruh CSP dan PSP harus dihapus (*zeroize*) saat antarmuka ini diakses. Zeroisasi juga harus dilakukan dalam jangka waktu yang cukup cepat untuk mencegah pemulihan data sensitif antara deteksi dan pelaksanaan penghapusan. Modul harus terdiri atas komponen berkualitas produksi (*production-grade components*) dan dilengkapi teknik

pelindung standar seperti pelapis konformal (*conformal coating*). Saat pemeliharaan fisik dilakukan, seluruh CSP dalam modul harus dihapus, baik secara prosedural oleh operator atau secara otomatis oleh modul.

Modul kriptografi harus menunjukkan bukti kerusakan fisik melalui penutup, segel, atau lapisan pelindung yang buram dalam spektrum cahaya tampak guna mencegah pengamatan operasi internal. Lubang ventilasi harus dirancang agar tidak memungkinkan pengamatan atau penyelidikan fisik tanpa terdeteksi. Modul juga harus dilindungi dengan lapisan pelindung tahan bongkar (*hard opaque removal-resistant coating*) atau amplop deteksi kerusakan (*tamper detection envelope*) yang mampu merespons kerusakan dan segera menghapus seluruh CSP saat akses fisik tidak sah terdeteksi.

Untuk **modul QKD tertanam multi-chip**, selain memenuhi persyaratan umum di pasal 4.7.1, modul harus berada dalam penutup yang kuat, dan komponen-komponennya harus dilindungi dengan lapisan atau amplop bukti kerusakan seperti *potting*, pelapis tahan ukir, atau amplop (*envelope*) deteksi berbentuk sirkuit fleksibel. Amplop ini harus mampu mendeteksi gangguan fisik seperti pemotongan, pengeboran, atau pelarutan. Modul harus memiliki sirkuit tanggap kerusakan dan zeroisasi yang secara terus-menerus memantau amplop deteksi dan segera menghapus seluruh CSP jika kerusakan terdeteksi. Perlindungan terhadap pengungkapan CSP harus tetap berlaku jika sirkuit deteksi rusak, kecuali jika CSP telah dihancurkan atau dihapus bersamaan dengan kerusakan sirkuit tersebut.

Untuk **modul QKD standalone multi-chip**, persyaratannya serupa, yakni harus berada dalam penutup kuat berbahan logam atau plastik keras, dengan pintu atau penutup yang dikunci atau dilindungi oleh segel bukti kerusakan yang bernomor unik.

Amplop deteksi kerusakan harus mencakup mekanisme seperti sakelar penutup, detektor gerak, dan lainnya. Sirkuit tanggap kerusakan dan zeroisasi harus selalu aktif dan mampu menghapus seluruh CSP saat kerusakan terdeteksi. Jika sirkuit tanggap kerusakan dinonaktifkan, maka CSP tetap harus terlindungi dari pengungkapan.

Pasal 4.7.4 membahas perlindungan dan pengujian terhadap kegagalan lingkungan (*Environmental Failure protection/ Testing*). Modul QKD harus memiliki fitur *Environmental Failure Protection* (EFP) untuk suhu dan tegangan. Fitur ini melibatkan sirkuit elektronik yang terus memantau suhu dan tegangan operasi modul. Jika terjadi fluktuasi di luar rentang normal, sirkuit harus mematikan modul atau segera menghapus seluruh CSP dan PSP. Dokumentasi harus menetapkan rentang suhu dan tegangan operasi normal, serta fitur EFP yang digunakan.

Prosedur *Environmental Failure Testing* (EFT) mencakup analisis, simulasi, dan pengujian untuk menjamin bahwa kondisi ekstrem tidak akan mengkompromikan keamanan modul. Pengujian harus mencakup suhu dari -100°C hingga $+200^{\circ}\text{C}$, serta tegangan yang meningkat atau menurun dari nilai normal, termasuk pembalikan polaritas. Uji dihentikan jika modul dimatikan, CSP dan PSP dihapus, atau modul memasuki mode gagal. Dokumentasi harus mencakup semua kondisi lingkungan yang relevan seperti tekanan, kelembaban, getaran mekanis, radiasi pengion, dan komposisi kimia atmosfer, khususnya mengingat komponen optik dan elektro-optik dalam sistem QKD.

h. Pasal 4.8 Keamanan fisik - Serangan Non-Invasif

Serangan terhadap operasi modul yang bersifat fisik (bukan logis) dan tidak memerlukan kontak fisik atau observasi langsung terhadap modul dijelaskan dalam pasal ini. Serangan-serangan ini meliputi *Simple Power Analysis* (SPA), *Differential Power*

Analysis, (DPA), *Electromagnetic Emanation* (EME) dan *Timing Analysis* (TA). Serangan non-invasif lainnya mungkin ada, namun perlindungan terhadapnya saat ini dianggap opsional.

Modul QKD harus melindungi CSP dari serangan TA. Dokumentasi harus menyebutkan teknik mitigasi terhadap serangan TA yang relevan. Modul QKD harus melindungi CSP dari serangan SPA. Dokumentasi harus menyebutkan teknik mitigasi terhadap serangan SPA yang relevan. Modul kriptografi harus melindungi CSP dari serangan DPA. Dokumentasi harus menyebutkan teknik mitigasi terhadap serangan DPA yang relevan. Modul QKD harus melindungi CSP dari serangan EME. Dokumentasi harus menyebutkan teknik mitigasi terhadap serangan EME yang relevan.

i. Pasal 4.9 Manajemen SSP

SSP terdiri atas CSP dan PSP. Persyaratan keamanan untuk manajemen SSP mencakup seluruh siklus hidup SSP yang digunakan oleh modul. Manajemen SSP mencakup pembangkit bit acak (*Random Bit Generator* (RBG)), pembuatan SSP, pembentukan SSP, entri/keluarannya SSP, penyimpanan SSP, dan pengosongan SSP. Sebuah modul dapat berisi satu atau lebih modul terpasang yang masing-masing menjalankan fungsi manajemen SSP. CSP yang terenkripsi merujuk pada CSP yang dienkripsi menggunakan fungsi keamanan yang disetujui. CSP yang dienkripsi dengan fungsi keamanan yang tidak disetujui dianggap sebagai *plaintext* dalam lingkup dokumen ini.

CSP harus dilindungi dalam modul dari pengungkapan, modifikasi, dan penggantian yang tidak sah. PSP harus dilindungi dalam modul dari modifikasi dan penggantian yang tidak sah. Kunci yang hanya digunakan untuk menguji algoritma kriptografi sebagaimana yang dijelaskan dalam pasal 4.10.2 adalah PSP. Untuk modul perangkat lunak, kunci Uji Integritas

Perangkat Lunak (*Software Integrity Test*) adalah CSP. Untuk modul perangkat keras yang mengandung komponen perangkat lunak, kunci Uji Integritas Perangkat Lunak adalah PSP. Untuk modul hibrid, kunci yang digunakan untuk Uji Integritas Perangkat Lunak adalah CSP. Jika kunci lain digunakan untuk menguji integritas perangkat lunak dalam bagian perangkat keras dari modul hibrid, kunci ini bukanlah SSP. Dokumentasi harus menyebutkan semua SSP yang digunakan oleh suatu modul.

1) Pembangkit bit acak

Modul QKD harus mengandung RBG, rangkaian RBG, dan/atau satu atau lebih sumber entropi RBG. Modul QKD dapat dianggap sebagai satu RBG atau sumber entropi RBG untuk sistem lainnya. Dokumentasi harus mencantumkan setiap RBG dan sumber entropi RBG yang terdapat dalam modul. Semua RBG yang digunakan dalam mode Disetujui harus disetujui dan terdaftar dalam lampiran A.

Jika suatu modul mengandung RBG atau sumber entropi RBG dalam mode Disetujui, maka:

- a) Sumber entropi RBG harus tunduk pada Uji Sumber Entropi RBG seperti yang ditentukan dalam Pasal 4.10.2.
- b) Komponen deterministik dari RBG harus tunduk pada Uji Algoritma Kriptografi dalam Pasal 4.10.1.
- c) Data yang dihasilkan dari RBG harus lulus Uji RBG Berkelanjutan seperti yang ditentukan dalam Pasal 4.10.2.

Jika entropi disediakan dari luar modul, maka nilai entropi minimum yang diklaim harus diberikan kepada modul. Modul harus memverifikasi bahwa nilai entropi minimum yang diklaim oleh sumber entropi RBG cukup untuk mendukung kekuatan keamanan yang dimaksudkan dari RBG yang menggunakan entropi tersebut.

Jika nilai acak dibutuhkan dalam Nilai Awal (*Initial Value* (IV)), yang digunakan oleh fungsi keamanan Disetujui, maka RBG yang disetujui harus digunakan untuk menghasilkan Nilai Awal ini.

2) Pembangkitan SSP

Suatu modul dapat membangkitkan SSP secara internal atau memuatnya dari sumber eksternal. Dokumentasi harus menyebutkan setiap metode pembangkitan SSP yang digunakan oleh modul, termasuk metode pembangkitan SSP yang menggunakan RBG.

Setiap SSP (selain *seed* dan kunci *seed*) yang dibangkitkan dalam mode disetujui modul menggunakan RBG harus dibangkitkan dengan menggunakan pembangkit yang disetujui dan memenuhi persyaratan sebagaimana ditetapkan dalam pasal 4.10.1.

Dalam menggunakan RBG yang disetujui untuk membangkitkan SSP, kekuatan keamanan dari RBG tersebut harus cukup untuk mendukung kekuatan keamanan dari fungsi keamanan kriptografi yang menggunakan SSP tersebut. SSP (selain kunci *seed*) yang dibangkitkan oleh modul untuk digunakan oleh fungsi keamanan yang disetujui harus dibangkitkan dengan menggunakan metode pembangkitan SSP yang disetujui.

3) Penetapan SSP

Dokumentasi modul QKD harus mencantumkan semua metode pembentukan SSP yang digunakan oleh modul. Pembentukan SSP dapat dilakukan melalui metode elektronik, seperti skema transportasi SSP (*SSP transport scheme*) atau skema kesepakatan SSP (*SSP agreement schemes*). Semua metode elektronik pembentukan SSP yang

digunakan dalam mode operasi yang disetujui harus merupakan metode yang disetujui atau diizinkan untuk digunakan dalam mode tersebut.

Jika suatu metode pembentukan SSP dalam mode yang disetujui membutuhkan nilai acak sebagai masukan, maka RBG yang disetujui harus digunakan untuk menyediakan nilai-nilai tersebut. Apabila metode transportasi SSP digunakan oleh modul, maka SSP yang ditransportasikan dalam proses tersebut harus memenuhi persyaratan sebagaimana ditetapkan dalam Pasal 4.9.4.

- 4) Enti dan keluaran SSP
- Proses keluaran SSP dapat dilakukan secara manual (misalnya melalui entri menggunakan papan ketik atau tampilan visual) maupun secara elektronik (misalnya melalui *smart card*/token, kartu PC, perangkat pemuatan kunci elektronik lainnya, atau sistem operasi modul), atau kombinasi keduanya. Dokumentasi harus mencantumkan metode entri dan keluaran SSP yang digunakan oleh suatu modul.

Modul harus mengaitkan setiap SSP yang dimasukkan ke dalam atau dikeluarkan dari modul dengan entitas yang benar (seperti individu, kelompok, peran, atau proses) yang ditetapkan untuk SSP tersebut. Semua SSP terenkripsi yang dimasukkan ke dalam atau dikeluarkan dari modul dan digunakan dalam mode operasi yang disetujui, harus dienkripsi menggunakan fungsi keamanan yang disetujui.

Selama entri SSP secara manual, nilai yang dimasukkan dapat ditampilkan sementara untuk verifikasi visual guna meningkatkan akurasi. Jika CSP terenkripsi dimasukkan secara manual ke dalam modul, maka nilai *plaintext* dari CSP

tidak boleh ditampilkan. Kunci kriptografi yang dimasukkan secara manual, baik dalam bentuk *plaintext* maupun terenkripsi (termasuk kunci *seed*), harus diverifikasi keakuratannya selama proses entri ke dalam modul menggunakan Uji Entri Kunci Manual (*Manual Key Entry Test*) sebagaimana ditetapkan dalam pasal 4.10.2.

Untuk modul perangkat lunak, CSP dapat dimasukkan ke dalam atau dikeluarkan dari modul dalam bentuk terenkripsi maupun *plaintext* di bawah kendali sistem operasi modul, asalkan CSP tetap berada dalam lingkungan operasional. PSP dapat dimasukkan ke dalam atau dikeluarkan dari modul dalam bentuk *plaintext*.

CSP yang ditransportasikan secara elektronik harus masuk dan keluar dari modul dalam bentuk terenkripsi dan integritasnya harus dilindungi (misalnya dengan fungsi keamanan yang disetujui atau metode pembentukan kunci yang disetujui atau diizinkan). PSP yang ditransportasikan secara elektronik harus masuk dan keluar dari modul dengan integritas yang dilindungi menggunakan algoritma tanda tangan digital yang disetujui, MAC yang disetujui, atau metode transportasi kunci yang disetujui.

PSP yang tidak ditransportasikan secara elektronik dapat dimasukkan ke dalam atau dikeluarkan dari modul dalam bentuk *plaintext* dan tidak perlu diautentikasi secara kriptografis, baik dimasukkan secara manual maupun elektronik. CSP yang tidak ditransportasikan secara elektronik harus dimasukkan atau dikeluarkan dari modul baik:

- a) dalam bentuk terenkripsi atau
- b) menggunakan prosedur pembagian pengetahuan (yaitu dalam dua atau lebih komponen *plaintext*).

Jika prosedur pembagian pengetahuan digunakan:

- a) Modul harus mengautentikasi secara terpisah operator yang memasukkan atau mengeluarkan setiap komponen sebagai identitas yang terpisah.
- b) Modul harus memverifikasi bahwa tidak ada dua operator yang memasukkan atau mengeluarkan komponen kunci memiliki identitas yang sama.
- c) Untuk mencegah penyalahgunaan SSP, modul QKD harus menggunakan Kanal Terpercaya untuk entri atau keluaran semua SSP, terlepas dari apakah dilindungi secara kriptografis atau tidak. Jika Kanal Terpercaya dibentuk dan dipertahankan menggunakan algoritma kriptografi, maka algoritma tersebut harus disetujui dan memiliki kekuatan keamanan yang setara atau lebih tinggi dari yang didokumentasikan oleh modul.
- d) Setidaknya dua komponen harus diperlukan untuk merekonstruksi CSP asli.
- e) Dokumentasi harus menunjukkan bahwa jika pengetahuan tentang n komponen diperlukan untuk merekonstruksi CSP asli, maka pengetahuan tentang $n-1$ komponen tidak memberikan informasi apa pun tentang CSP asli selain panjangnya.
- f) Dokumentasi harus mencantumkan prosedur pembagian pengetahuan yang digunakan oleh modul.

5) Penyimpanan SSP

SSP yang disimpan di dalam suatu modul dapat disimpan dalam bentuk *plaintext* maupun bentuk terenkripsi. Modul harus mengaitkan setiap SSP yang disimpan di dalamnya dengan entitas yang sesuai, seperti operator, peran, atau proses yang ditetapkan untuk SSP tersebut. Sebuah SSP juga dapat disimpan di dalam modul kriptografi tertanam yang

memenuhi atau melampaui persyaratan standar yang berlaku terhadap modul induknya.

Dokumentasi harus mencantumkan: SSP yang disimpan dalam modul; cara modul melindungi CSP dari akses tidak sah saat disimpan; cara modul melindungi PSP dari modifikasi tidak sah saat disimpan; serta cara modul mengaitkan PSP yang disimpan dengan entitas (operator, peran, atau proses) yang ditetapkan untuk parameter tersebut.

CSP dalam bentuk *plaintext* tidak boleh dapat diakses oleh operator yang tidak berwenang dari luar modul. PSP juga tidak boleh dapat dimodifikasi oleh operator tidak sah dari luar modul.

6) Zeroisasi SSP

Modul QKD harus menyediakan metode untuk secara aktif melakukan zeroisasi terhadap semua CSP, termasuk nilai yang disimpan sementara, di dalam modul. Setelah CSP dilakukan zeroisasi, nilai tersebut tidak boleh dapat diambil kembali dari modul. Zeroisasi terhadap PSP, CSP terenkripsi, atau CSP yang dilindungi secara fisik maupun logis dalam modul tertanam yang telah tervalidasi dan memenuhi ketentuan dalam dokumen ini juga merupakan persyaratan yang harus dipenuhi.

Kunci yang hanya digunakan untuk melakukan uji mandiri sebelum operasi (*pre-operational self-tests*) dianggap sebagai PSP. Nilai hash dari *password* yang jika diketahui dapat menjadi target serangan ekshaustif secara *offline* (*off-line exhaustion attack*) harus dianggap sebagai CSP. Informasi status RBG juga dikategorikan sebagai CSP.

Dokumentasi harus mencantumkan metode zeroisasi CSP yang digunakan oleh modul dan alasan yang menjelaskan bahwa metode tersebut mencegah pengambilan kembali maupun penggunaan ulang CSP yang telah dizeroisasi. CSP sementara, seperti kunci ephemeris (*ephemeral keys*), harus segera dizeroisasi setelah tidak digunakan lagi.

Zeroisasi CSP dapat dilakukan secara prosedural dan tidak bergantung pada kendali langsung modul. Sebagai contoh, operator dapat melakukan penghancuran modul secara fisik, seperti memformat ulang *hard disk* atau penghancuran atmosferik saat modul memasuki kembali atmosfer. Modul QKD juga harus mengendalikan proses zeroisasi terhadap CSP.

Adapun persyaratan keamanan yang harus dipenuhi mencakup:

- a) modul harus menyediakan metode untuk melakukan zeroisasi terhadap semua PSP, termasuk yang disimpan sementara;
- b) dokumentasi harus menjelaskan metode zeroisasi PSP yang digunakan beserta alasan bahwa metode tersebut mencegah pengambilan kembali dan penggunaan ulang data yang telah dizeroisasi; serta
- c) PSP sementara harus dizeroisasi segera setelah tidak lagi dibutuhkan.

j. Pasal 4.10 *Self-test*

Modul QKD harus melaksanakan pengujian mandiri sebelum operasional, pengujian mandiri kondisional (*conditional self-tests*), dan jika relevan, pengujian terhadap fungsi kritis (*critical functions tests*) untuk memastikan bahwa modul berfungsi dengan benar. Pengujian mandiri sebelum operasional harus

dilakukan dan lulus dengan sukses sebelum modul dapat menyediakan layanan apa pun. Pengujian mandiri kondisional harus dilakukan setiap kali fungsi keamanan tertentu dijalankan, yakni fungsi-fungsi yang memerlukan pengujian mandiri. Modul QKD juga dapat melakukan pengujian tambahan selain yang ditentukan dalam dokumen ini.

Jika modul QKD gagal dalam pengujian mandiri, modul tersebut harus memasuki status kesalahan dan menampilkan indikator kesalahan melalui antarmuka keluaran status. Dalam kondisi kesalahan, modul QKD tidak boleh melakukan operasi kriptografi atau mengeluarkan data melalui antarmuka keluaran data. Modul juga tidak boleh menggunakan fungsi apa pun yang bergantung pada algoritma atau fungsi yang gagal dalam pengujian mandiri, kecuali jika pengujian tersebut telah diulang dan lulus dengan sukses.

Dokumentasi harus mencantumkan pengujian mandiri yang dilakukan oleh modul QKD, status kesalahan yang dapat terjadi saat pengujian mandiri gagal, serta kondisi dan tindakan yang diperlukan untuk keluar dari status kesalahan dan mengembalikan modul ke operasi normal. Tindakan ini dapat mencakup pemeliharaan modul, menghidupkan ulang modul, pemulihan otomatis, atau pengembalian modul ke pihak vendor untuk diperbaiki.

k. Pasal 4.11 Jaminan siklus hidup

Jaminan siklus hidup mengacu pada penggunaan praktik terbaik oleh penyedia modul QKD selama perancangan, penyebaran, dan pengoperasian modul QKD, yang memberikan kepastian bahwa modul tersebut dikembangkan, diuji, dikonfigurasi, diserahkan, dan dipasang dengan benar, serta dokumentasi panduan operator yang tepat disediakan. Persyaratan keamanan ditentukan untuk manajemen

konfigurasi, perancangan, model status terbatas, pengembangan, pengujian, pengiriman dan pengoperasian, serta dokumentasi panduan.

1) Manajemen Konfigurasi

Manajemen konfigurasi menetapkan persyaratan keamanan untuk sistem manajemen konfigurasi yang diterapkan oleh penyedia modul QKD, yang memberikan kepastian bahwa integritas modul QKD terjaga dengan memerlukan disiplin dan kontrol dalam proses perbaikan dan modifikasi modul QKD serta dokumentasi terkait. Sistem manajemen konfigurasi diterapkan untuk mencegah modifikasi yang tidak sengaja atau tidak sah, serta menyediakan jejak perubahan untuk modul QKD dan dokumentasi terkait.

Persyaratan keamanan berikut harus diterapkan pada modul QKD:

- a) Sistem manajemen konfigurasi harus diterapkan untuk modul QKD dan komponen modul di dalam batas kriptografi, serta untuk dokumentasi modul terkait.
- b) Setiap versi item konfigurasi (misalnya modul QKD, bagian perangkat keras modul, komponen perangkat lunak modul, HDL modul, panduan pengguna, Kebijakan Keamanan, dll.) yang mencakup modul dan dokumentasi terkait harus diberi nomor identifikasi unik.
- c) Sistem manajemen konfigurasi harus melacak dan memelihara perubahan pada identifikasi dan versi atau revisi setiap item konfigurasi sepanjang siklus hidup modul QKD yang tervalidasi.
- d) Dokumentasi harus menyebutkan dan menjelaskan sistem manajemen konfigurasi yang digunakan untuk modul QKD.
- e) Item konfigurasi harus dikelola menggunakan sistem manajemen konfigurasi otomatis.

2) Perancangan

Perancangan adalah solusi rekayasa yang menangani Spesifikasi Fungsional untuk modul QKD. Perancangan dimaksudkan untuk memberikan kepastian bahwa spesifikasi fungsional modul QKD sesuai dengan fungsionalitas yang dimaksud dalam Kebijakan Keamanan. Modul QKD harus dirancang untuk memungkinkan pengujian fungsionalitas yang diterapkan sesuai dengan dokumen ini, bila memungkinkan tanpa mengorbankan keamanan modul, sehingga semua layanan modul QKD dapat diuji.

Persyaratan berikut harus diterapkan pada modul QKD:

- a) Dokumentasi harus menyebutkan hubungan antara desain perangkat keras dan/atau perangkat lunak modul QKD, serta Kebijakan Keamanan dan Model Status Terbatas modul QKD.
- b) Dokumentasi harus menyebutkan Spesifikasi Fungsional yang menggambarkan secara informal modul QKD, fungsionalitasnya, porta fisik eksternal dan antarmuka logis modul QKD, serta tujuan porta fisik dan antarmuka logis tersebut.
- c) Dokumentasi harus menyebutkan desain rinci yang menggambarkan fungsionalitas internal dari komponen utama modul QKD, antarmuka komponen internal, tujuan antarmuka komponen, dan aliran informasi internal (di dalam batas kriptografi secara keseluruhan dan juga dalam komponen utama).
- d) Dokumentasi harus menyebutkan bukti informal (termasuk prasyarat dan pasca-kondisi) dari hubungan antara desain modul QKD dan spesifikasi fungsional.
- e) Dokumentasi harus menyebutkan model formal yang menggambarkan aturan dan karakteristik Kebijakan

Keamanan modul QKD. Model formal harus ditentukan menggunakan bahasa spesifikasi formal yang merupakan notasi ketat yang didasarkan pada matematika yang mapan, seperti logika orde pertama atau teori himpunan.

- f) Dokumentasi harus menyebutkan alasan yang menunjukkan konsistensi dan kelengkapan model formal terkait dengan Kebijakan Keamanan modul QKD.
- g) Dokumentasi harus menyebutkan bukti informal dari hubungan antara model formal dan spesifikasi fungsional.

3) Model Status Terbatas

Operasi modul QKD harus ditentukan menggunakan Model Status Terbatas (atau yang setara) yang diwakili oleh diagram transisi status dan/atau tabel transisi status serta deskripsi status. FSM harus cukup rinci untuk menunjukkan bahwa modul QKD memenuhi semua persyaratan dokumen ini.

Dokumentasi harus menyertakan FSM (atau yang setara) menggunakan diagram transisi status dan/atau tabel transisi status dan deskripsi status yang harus menyebutkan:

- a) Status operasional dan status kesalahan dari modul QKD.
- b) Transisi yang sesuai dari satu status ke status lainnya.
- c) Peristiwa input, termasuk input data dan input kontrol, yang menyebabkan transisi dari satu status ke status lainnya.
- d) Peristiwa *output*, termasuk kondisi modul internal, *output* data, dan *output* status, yang dihasilkan dari transisi dari satu status ke status lainnya.

4) Pengembangan

Proses pengembangan yang tepat memberikan kepastian bahwa implementasi modul QKD sesuai dengan spesifikasi

fungsional dan Kebijakan Keamanan modul, bahwa modul QKD dapat dipelihara, dan bahwa modul QKD yang tervalidasi dapat direproduksi.

Persyaratan berikut harus diterapkan pada modul QKD:

- a) Jika modul QKD mengandung perangkat lunak, dokumentasi harus menyebutkan kompiler, pengaturan konfigurasi, dan metode untuk mengompilasi kode sumber menjadi bentuk yang dapat dieksekusi. Dokumentasi juga harus menyertakan kode sumber perangkat lunak yang diberi komentar yang menggambarkan hubungan perangkat lunak dengan desain modul.
- b) Jika modul kriptografi mengandung perangkat keras, dokumentasi harus menyebutkan skematik dan/atau *Hardware Description Language* (HDL), jika relevan. HDL harus diberi komentar yang menggambarkan hubungan perangkat keras dengan desain modul.

5) Pengujian Vendor

Pasal ini menetapkan persyaratan keamanan untuk pengujian vendor pada modul QKD, termasuk pengujian fungsionalitas keamanan yang diterapkan dalam modul QKD, yang memberikan kepastian bahwa modul berfungsi sesuai dengan Kebijakan Keamanan modul dan spesifikasi fungsional.

Dokumentasi modul QKD harus menyebutkan pengujian fungsional yang dilakukan pada modul QKD.

6) Pengiriman dan Operasi

Pasal ini menetapkan persyaratan keamanan untuk pengiriman, pemasangan, dan pengaktifan modul QKD secara aman, memberikan kepastian bahwa modul dikirim dengan aman kepada operator yang sah, dan dipasang serta diinisialisasi dengan cara yang benar dan aman. Dokumentasi

modul QKD harus menyebutkan prosedur untuk pemasangan, inisialisasi, dan pengaktifan modul QKD dengan aman.

7) Dokumen Panduan

Persyaratan dalam bagian ini dimaksudkan untuk memastikan bahwa semua entitas yang menggunakan modul QKD memiliki panduan dan prosedur yang memadai untuk mengelola dan menggunakan modul dengan cara yang aman. Dokumentasi panduan terdiri atas panduan administrator dan non-administrator.

Panduan administrator harus menyebutkan:

- a) Fungsi administratif, peristiwa keamanan, parameter keamanan, porta fisik, dan antarmuka logis modul QKD yang tersedia untuk *Crypto-Officer* dan/atau peran administratif lainnya.
- b) Panduan non-administrator harus menyebutkan: Fungsi keamanan yang disetujui dan tidak disetujui, porta fisik, dan antarmuka logis yang tersedia bagi pengguna modul QKD.

1. Pasal 4.12 Mitigasi serangan lainnya

Kerentanan sebuah modul QKD terhadap serangan yang tidak dijelaskan di bagian lain dari dokumen ini bergantung pada jenis modul, implementasinya, dan lingkungan implementasinya. Serangan-serangan ini menjadi perhatian khusus terutama jika modul QKD digunakan di lingkungan yang berbahaya, seperti ketika penyerang adalah operator sah dari modul itu sendiri. Serangan semacam ini umumnya bergantung pada analisis informasi yang diperoleh dari sumber eksternal secara fisik terhadap modul, dan pada semua kasus bertujuan untuk memperoleh pengetahuan tentang CSP yang berada di dalam modul QKD.

Apabila sebuah modul QKD dirancang untuk mengatasi satu atau lebih jenis serangan tertentu, maka Kebijakan Keamanan (*Security Policy*) modul tersebut atau dokumen pendukung lainnya harus mencantumkan secara rinci serangan-serangan yang dimaksud. Keberadaan dan fungsi dari mekanisme keamanan yang digunakan untuk mengatasi serangan tersebut akan divalidasi ketika persyaratan dan pengujian terkait dikembangkan.

Selain itu, persyaratan berikut juga harus dipenuhi oleh modul QKD yaitu jika modul mengklaim mampu mengatasi jenis serangan lainnya, maka dokumentasi harus menjelaskan metode yang digunakan untuk mengatasi serangan tersebut serta metode yang digunakan untuk menguji efektivitas teknik mitigasinya.

5. Lampiran A (normatif): Ringkasan persyaratan dokumentasi
Berisi ringkasan daftar pemeriksaan yang mencakup seluruh persyaratan dokumentasi dalam dokumen ini. Seluruh dokumentasi harus disampaikan kepada fasilitas pengujian oleh penyedia modul QKD.
6. Lampiran B (normatif): QKD *Module Security Policy*
Berisi informasi tentang Kebijakan Keamanan modul QKD yang harus disertakan dalam dokumentasi yang disediakan oleh penyedia.
7. Lampiran C (informatif): Praktik Pengembangan Perangkat Lunak yang Direkomendasikan
Lampiran ini disediakan hanya untuk tujuan informasi dan tidak memuat persyaratan keamanan yang berlaku untuk modul QKD dalam cakupan dokumen ini.

Rekomendasi rekayasa perangkat lunak sepanjang siklus hidup (terkait dengan spesifikasi, pembangunan, verifikasi, pengujian, pemeliharaan, dan dokumentasi perangkat lunak) harus diikuti.

Praktik rekayasa perangkat lunak dapat mencakup pengujian unit yang terdokumentasi, tinjauan kode, dokumen desain tingkat tinggi dan rendah yang eksplisit, spesifikasi dan persyaratan fungsional yang eksplisit, diagram struktur dan alur data, analisis titik fungsi, pelacakan cacat dan resolusi, manajemen konfigurasi, dan proses pengembangan perangkat lunak yang terdokumentasi. Untuk semua pengembangan perangkat lunak, baik besar maupun kecil, teknik pemrograman berikut sesuai dengan praktik terkini dan harus digunakan untuk memfasilitasi analisis komponen perangkat lunak dari modul kriptografi dan mengurangi kemungkinan kesalahan pemrograman.

8. Lampiran D (informatif): Fungsi Keamanan yang Disetujui Contoh: BB84

Lampiran ini berisi contoh dari fungsi keamanan QKD yang disetujui. Karena BB84 adalah protokol QKD yang paling dikenal, protokol ini dipilih untuk mencontohkan fungsi tersebut. Persyaratan contoh diberikan untuk menggambarkan beberapa parameter utama yang perlu dikendalikan dalam fungsi keamanan QKD, namun tidak dimaksudkan untuk mencakup seluruh parameter.

9. Lampiran E (informatif): *Uniform Resource Locator (URL) Internet* yang berlaku

Berisi informasi tentang *Uniform Resource Locator (URL) Internet* yang berlaku.

E. ETSI GS QKD 012 V1.1.1 Quantum Key Distribution (QKD): Device and Communication Channel Parameters for QKD Deployment

Dokumen ETSI GS QKD 012 *Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment* diterbitkan oleh ETSI pada bulan Februari 2019 [7].

Struktur dokumen tersebut adalah sebagai berikut:

1. Ruang Lingkup

Dokumen ini membahas sumber daya komunikasi utama dan arsitektur yang dapat digunakan untuk penerapan QKD pada jaringan serat optik dengan komunikasi titik-ke-titik. Dokumen juga mendefinisikan entitas yang terlibat dan konteks penerapan, khususnya konteks di mana entitas QKD_O mengoperasikan modul QKD dan merencanakan penerapan pada jaringan optik yang dioperasikan oleh entitas NET_O. Parameter sistem QKD dan jaringan yang perlu dipertukarkan dijelaskan dan diprioritaskan, dengan tabel standar di akhir dokumen sebagai panduan pertukaran informasi antara QKD_O dan NET_O.

2. Referensi

Tidak ada acuan normatif dan acuan informatif pada dokumen ini.

3. Definisi Istilah, simbol, dan singkatan

Bab ini berisi tentang daftar istilah sejumlah 15 istilah dan 13 daftar singkatan yang digunakan pada dokumen.

4. Arsitektur dan kanal komunikasi QKD

a. Proses QKD

Subbab ini menjelaskan tentang bagaimana proses QKD itu dapat berjalan. Sistem QKD terdiri atas dua Modul QKD yang terkoneksi menggunakan kanal komunikasi (Kanal kuantum, Kanal distilasi, dan dimungkinkan Kanal Sinkronisasi). Dua modul ini mengikuti sebuah protokol yang dapat dijelaskan sebagai serangkaian proses yang dijalankan secara paralel atau berurutan untuk membentuk kunci simetris yang aman di kedua sisi, A dan B. Proses QKD terdiri atas tiga proses utama yang dijalankan oleh sistem QKD (Deskripsi proses dapat dilihat pada Tabel 1 dokumen ETSI GS QKD 012).

b. Kanal komunikasi QKD

Subbab ini menjelaskan tentang kanal komunikasi QKD. Sistem QKD menjalankan berbagai proses secara lokal di A dan B, dan beberapa proses memerlukan komunikasi antara A dan B. Komunikasi ini dapat terjadi melalui hingga tiga jenis kanal yang berbeda, yaitu:

- 1) Kanal Kuantum QKD.
- 2) Kanal Sinkronisasi QKD (merupakan kanal optik klasik berupa sinyal analog).
- 3) Kanal Distilasi QKD (merupakan kanal digital konvensional dua arah).

c. Kanal Kuantum QKD

Kanal Kuantum biasanya merupakan kanal optik satu arah. Kanal optik ini dapat berbasis serat optik atau ruang bebas (*free-space*). Kanal Kuantum biasanya digunakan dalam protokol QKD untuk mengirimkan keadaan kuantum non-ortogonal yang membawa informasi klasik dari A ke B.

Protokol QKD umumnya mengandalkan pemantauan gangguan saat mengirim data klasik acak melalui kanal kuantum. Jika gangguan terlalu tinggi, sistem QKD mengasumsikan gangguan tersebut bisa disebabkan oleh pihak yang tidak berwenang (*adversary*) dan tidak dapat menghasilkan kunci yang aman. Parameter seperti kerugian optik dan kebisingan sangat memengaruhi keberhasilan distribusi kunci aman, sehingga penting untuk meminimalkan kebisingan sepanjang kanal.

d. Kanal Sinkronisasi QKD

Kanal Sinkronisasi biasanya digunakan untuk bertukar informasi antara A dan B, menggunakan sinyal klasik yang mengandung banyak foton. Informasi tersebut dapat digunakan khususnya untuk:

- 1) Sinkronisasi jam.

- 2) Berbagi dan kompensasi referensi fase (terutama dalam CV-QKD).
- 3) Pemantauan dan kompensasi pergeseran polarisasi.

Kanal Sinkronisasi harus diimplementasikan pada jalur optik yang karakteristik propagasinya (durasi, dispersi, pergeseran polarisasi, dll.) mendekati atau berkorelasi erat dengan karakteristik propagasi pada kanal kuantum. Oleh karena itu, kanal Sinkronisasi sering kali dimultiplex bersama dengan kanal Kuantum, meskipun implementasi lain juga memungkinkan.

e. Kanal Distilasi QKD

Kanal Distilasi biasanya merupakan kanal digital optik konvensional dua arah yang digunakan untuk mengirim informasi klasik dari A ke B atau dari B ke A. Komunikasi klasik dua arah antara A dan B biasanya diperlukan untuk proses *sifting* dan pasca-pemrosesan, seperti koreksi kesalahan dan amplifikasi privasi. Kanal Distilasi QKD dapat benar-benar berbeda secara fisik dari kanal Kuantum dan tidak harus berupa kanal optik. Namun, batasan pada kinerja protokol dapat menetapkan persyaratan pada karakteristik kanal, seperti *throughput* dan latensi.

5. Arsitektur QKD

a. Definisi arsitektur QKD

Penerapan sistem QKD memerlukan alokasi sumber daya jaringan (kanal komunikasi) yang dikelola oleh operator jaringan (NET_O). Seperti yang dibahas pada klausul 4.2, kebutuhan komunikasi QKD dapat dikategorikan menjadi tiga kelompok berbeda yaitu distilasi, sinkronisasi, dan kuantum.

Arsitektur QKD adalah desain yang memungkinkan penentuan bagaimana setiap kebutuhan komunikasi tersebut diakomodasi. Pilihan arsitektur yang mungkin disusun berdasarkan

keputusan untuk melakukan multiplexing pada serat yang sama antara kanal kuantum dan sinkronisasi dengan kanal distilasi yang biasanya membawa sinyal dengan daya jauh lebih tinggi. Terdapat dua varian, yaitu *Dedicated-link* dan *Dedicated-to-quantum*.

b. Penerapan QKD dengan kanal kuantum khusus

Penerapan QKD dengan kanal kuantum khusus (*Dedicated quantum channel*) merujuk pada arsitektur di mana kanal QKD dan Sinkronisasi ditempatkan pada jalur khusus (*dedicated link*). Arsitektur seperti ini memiliki keuntungan memberikan isolasi yang baik untuk kanal QKD dari gangguan yang disebabkan oleh kanal Distilasi QKD. Namun, arsitektur ini memerlukan alokasi serat gelap (*dark fibre*) untuk memasang kanal komunikasi kuantum tersebut.

Terdapat dua varian kanal kuantum, yaitu *Dedicated-link* dan *Dedicated-to-quantum*. Dalam arsitektur *dedicated-link*, sebuah jalur khusus dialokasikan untuk kanal QKD Kuantum dan kanal Sinkronisasi QKD. Kanal Distilasi QKD dan kanal lainnya ditempatkan pada jalur yang berbeda (dijelaskan dalam Gambar 1 dokumen ETSI GS QKD 012). Dalam arsitektur *dedicated-to-quantum*, kanal Kuantum ditempatkan pada jalur khusus, sementara kanal Sinkronisasi dan Distilasi ditempatkan pada jalur yang berbeda (dijelaskan dalam Gambar 2 dokumen ETSI GS QKD 012).

c. Arsitektur penerapan QKD dimultipleks

Penerapan QKD yang dimultiplexing merujuk pada arsitektur di mana saluran QKD dan saluran Distilasi dimultiplex pada jalur komunikasi yang sama. Arsitektur seperti ini memiliki keuntungan mengurangi sumber daya fisik (misalnya serat optik) yang dibutuhkan untuk mengimplementasikan saluran komunikasi. Namun, arsitektur *multiplexed* juga menimbulkan

kebutuhan untuk menyaring dengan efisien gangguan yang disebabkan oleh saluran Distilasi QKD atau saluran lain yang dimultiplex. Selain itu, dapat menimbulkan kerugian tambahan akibat perangkat tambahan di dalam serat, seperti *multiplexer*, *splitter*, dan sebagainya. Arsitektur ini terdiri atas dua, yaitu arsitektur *multiplexed* khusus QKD (*QKD-only multiplexed architecture*) dan arsitektur *fully multiplexed*. Arsitektur *multiplexed* khusus QKD (*QKD-only multiplexed architecture*) merujuk pada alokasi tiga saluran, di mana ketiganya terkait QKD dimultiplex pada satu jalur tunggal, sementara saluran klasik eksternal ditempatkan pada jalur fisik yang berbeda. Dalam arsitektur seperti ini, diperlukan upaya khusus untuk memultiplex saluran Distilasi dan Kuantum, dengan keuntungan bahwa saluran Distilasi dikendalikan oleh QKD_O. Oleh karena itu, parameter saluran Distilasi, termasuk daya peluncuran (*launch power*), dapat dioptimalkan oleh QKD_O dan diturunkan secara signifikan di bawah 0 dBm, guna meminimalkan gangguan pada saluran Kuantum, dengan syarat saluran Distilasi tetap berfungsi.

Arsitektur *fully multiplexed* merujuk pada alokasi tiga saluran, di mana ketiganya terkait QKD serta beberapa saluran eksternal dimultiplex pada satu jalur tunggal. Dalam arsitektur ini, daya peluncuran optik dari saluran klasik eksternal tidak dikendalikan oleh operator QKD, sehingga arsitektur *fully multiplexed* memungkinkan penerapan bersama QKD dan komunikasi WDM standar pada serat yang sama. Sebaliknya, prosedur pengendalian gangguan menjadi lebih menantang dibandingkan dengan arsitektur *QKD-only multiplexed*, karena harus mengatasi daya peluncuran saluran klasik eksternal sekitar 0 dBm atau lebih.

6. Perencanaan Penerapan QKD : Entitas dan Konteks

a. Entitas dan perang pada perencanaan penerapan

Klausul ini menjelaskan entitas yang dapat terlibat dalam penerapan QKD: Operator QKD (QKD_O), Operator Jaringan (NET_O), dan Pengguna (USER). Konteks penerapan yang mungkin, yaitu "peran umum" yang dimainkan oleh QKD_O, NET_O, dan USER, juga dijelaskan beserta bagaimana peran tersebut menentukan informasi yang harus dipertukarkan. Definisi-definisi ini kemudian digunakan dalam templat (klausul 7) yang menentukan informasi yang harus dipertukarkan saat melakukan penerapan QKD pada infrastruktur jaringan optik. Penjelasan lengkap dari setiap entitas dapat dilihat pada Subbab 6.1 dokumen ETSI GS QKD 012.

b. Konteks

Sebuah konteks atau "konteks penerapan" adalah sebuah skenario yang menjelaskan beberapa aspek peran yang dimainkan oleh berbagai entitas, serta interaksi di antara mereka. Di dalam dokumen ETSI GS QKD juga ditampilkan contoh skenario, yaitu Konteks1, di mana pengembangan diatur oleh QKD_O dan entitas di dalamnya yaitu USER dan QKD_O.

7. Templat perubahan informasi

Pada Bab ini menjelaskan tentang skenario Konteks1, di mana QKD_O dan USER adalah entitas yang sama yang bertanggung jawab merencanakan penerapan QKD pada infrastruktur jaringan optik yang dioperasikan oleh NET_O. Daftar informasi yang harus dipertukarkan antara Operator QKD (QKD_O) dan Operator Jaringan (NET_O) dijelaskan dalam tabel yang ada.

Tabel-tabel tersebut dapat digunakan sebagai templat standar untuk pertukaran informasi antara entitas QKD_O dan NET_O yang terlibat dalam penerapan QKD. Prioritas dikategorikan dari yang terendah (1) hingga tertinggi (3), yaitu:

- a. 3: informasi yang diperlukan dan harus dikomunikasikan.
- b. 2: informasi yang berguna dan sebaiknya dikomunikasikan.
- c. 1: informasi yang mungkin berguna dan boleh dikomunikasikan.

Pada praktiknya, tabel–tabel tersebut dapat disesuaikan jika diperlukan untuk diterapkan dalam konteks lain:

- a. Tabel dapat diformat ulang dan item-item dapat diatur ulang.
- b. Informasi yang diperlukan (prioritas level 3) secara umum harus tetap ada.
- c. Tingkat prioritas harus tetap sama.
- d. Informasi tambahan dengan tingkat prioritas yang disesuaikan dapat ditambahkan.

Tabel yang memuat tentang klasifikasi dan daftar parameter jaringan dan tabel tentang daftar parameter QKD dapat dilihat pada Tabel 2 dan 3 dokumen ETSI GS QKD 012.

F. ETSI GK QKD 016 V.1.1.1 Quantum Key Distribution (QKD): Common Criteria Protection Profile – Pair of Prepare and Measure Quantum Key Distribution Modules

Dokumen ini menetapkan *Protection Profile* (PP) untuk evaluasi keamanan pasangan modul QKD berdasarkan *Common Criteria for Information Technology Security Evaluation* (CC:2022 Revisi 1) [8]. Dokumen ini berlaku untuk sepasang modul QKD yang mengimplementasikan protokol QKD berbasis metode persiapan dan pengukuran, yang dapat membentuk satu sistem QKD lengkap ketika dihubungkan melalui setiap titik tautan QKD yang sesuai. PP ini menetapkan persyaratan tingkat tinggi, mulai dari implementasi fisik hingga keluaran *secret key* akhir.

Adapun struktur dokumen ETSI GK QKD 016 V.2.1.1 terdiri atas beberapa bab sebagai berikut:

1. Ruang lingkup
2. Referensi
3. Istilah definisi, simbol dan singkatan
4. Catatan Penerapan dalam PP
5. Pendahuluan PP
6. Klaim kesesuaian
7. Definisi permasalahan keamanan
8. Tujuan keamanan
9. Definisi komponen tambahan
10. Persyaratan keamanan
11. Paket
12. Panduan untuk SFR terkait RNG
13. Lampiran A (informatif): Peran, Pengguna TOE dan TSF
14. Lampiran B (informatif): Bibliografi

Berikut merupakan ringkasan PP sebagaimana tercantum dalam dokumen ini. Untuk penjelasan dan informasi detail dapat merujuk pada dokumen ETSI ETSI GK QKD 016 V.2.1.1[9].

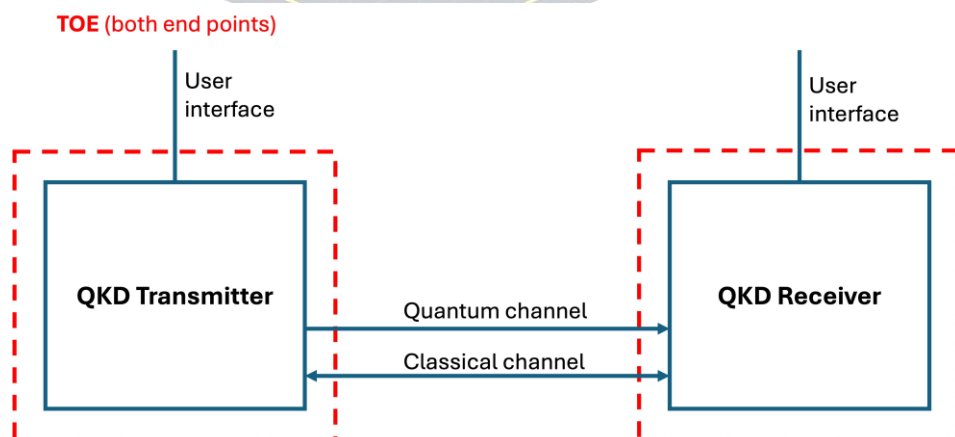
1. Pendahuluan PP

Judul	<i>Common Criteria Protection Profile – Pair of Prepare and Measure Quantum Key Distribution Modules</i>
Versi CC	CC:2022 Revisi 1
Penyusun	ETSI (ISG QKD)
Level Asurans	EAL4 <i>augmented</i> dengan AVA_VAN.5 dan ALC_DVS.2
Tanggal kompilasi	2023-11-27
Nomor versi	V2.1.1
Registrasi	BSI-CC-PP-0120-2024

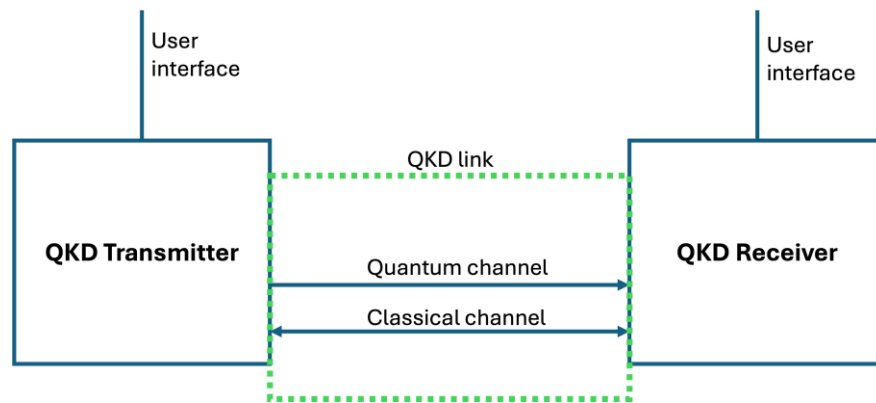
Kata kunci *Cryptographic Module, Cryptography, Quantum Key Distribution*

PP ini menjelaskan persyaratan keamanan untuk modul QKD yang menggunakan protokol QKD *Prepare and Measure* (P&M). PP ini mempertimbangkan situasi dimana kedua modul berada dalam lingkungan dengan persyaratan keamanan yang identik. PP ini memberikan fleksibilitas bagi penyusun *Security Target* (ST) untuk menyesuaikan dengan standar QKD yang akan datang dan mendukung solusi inovatif. Pengembangan disarankan untuk berkomunikasi dengan Badan Sertifikasi sebelum dan selama pengembangan untuk memastikan interpretasi yang konsisten.

TOE adalah sepasang modul QKD yang dapat dihubungkan melalui tautan QKD untuk membentuk sistem QKD, namun tautan yang digunakan bukan merupakan ruang lingkup TOE sebagaimana ditunjukkan pada Gambar 3.2. Tautan QKD dapat melewati lingkungan yang tidak terkendali tanpa pelindung fisik, dan tidak menyediakan layanan keamanan. Tautan QKD setidaknya mencakup saluran klasik yang terotentikasi dan saluran kuantum seperti ditunjukkan pada Gambar 3.3. Komunikasi yang menggunakan tautan QKD dianggap sebagai komunikasi Inter-TSF.

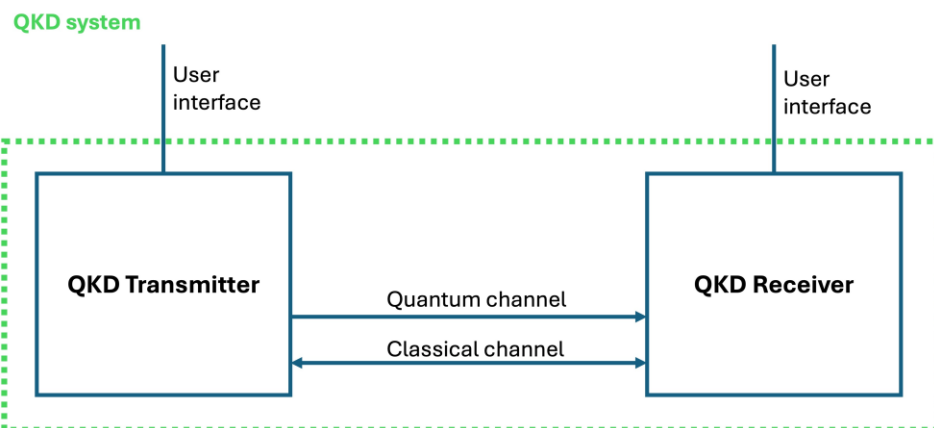


Gambar 3.2 Ruang lingkup TOE
digambar ulang dari [9]



Gambar 3.3 QKD *link*
digambar ulang dari [9]

Tujuan dari sistem QKD adalah untuk membangun kunci QKD, berupa sepasang modul QKD berperan sebagai pemancar dan penerima QKD yang dihubungkan dan saling berbagi kredensial autentikasi sebagaimana ditunjukkan pada Gambar 3.4.



Gambar 3.4 Sistem QKD.
digambar ulang dari [9].

Berikut merupakan layanan keamanan yang disediakan oleh TOE:

- Menyediakan mode kalibrasi untuk sistem QKD
- Menetapkan kunci QKD berdasarkan permintaan pengguna yang sah menggunakan protokol P&M.
- Mengekspor kunci QKD untuk pengguna yang ditentukan
- Menerapkan kontrol akses berbasis peran yang ditentukan oleh administrator

- e. Menghasilkan dan mengeksport data audit sesuai dengan auditor yang ditunjuk
- f. Melindungi data konfigurasi dan inisialisasi yang terkait dengan fungsi keamanan.

Sedangkan entitas yang digunakan untuk pemodelan dalam pendefinisian masalah keamanan yaitu sebagai berikut:

- a. Pengguna yang Sah (*Legitimate User*), merupakan entitas yang diperbolehkan menggunakan TOE dalam peran apapun. Izin tersebut diberikan oleh pemilik atau operator TOE melalui organisasi
- b. Pengguna Terotorisasi (*Authorized User*), merupakan pengguna sah yang berinteraksi dengan TOE sesuai dengan kebijakan keamanan yang ditentukan oleh pemilik atau operator TOE dalam batasan peran pengguna yang dimaksud
- c. Pengguna Tidak Terotorisasi (*Unauthorized User*), merupakan pengguna sah yang tidak diotorisasi untuk berinteraksi dengan TOE sesuai dengan peran yang dimaksud.
- d. Penyerang (*Attacker*), merupakan entitas yang berusaha merusak TSF.

TOE menghubungkan peran kepada pengguna yang teridentifikasi ke dalam beberapa peran berikut:

- a. Administrator, memiliki izin untuk mengasosiasikan identitas pengguna dengan peran
- b. *Maintainer*, dapat mengakses, memodifikasi, dan mengubah nilai *default* untuk data kalibrasi
- c. Auditor, dapat mendefinisikan aktivitas yang dapat diaudit serta mengeksport dan menghapus catatan audit dari TOE setelah diekspor
- d. *Key requester*, dapat meminta pembangkitan dan ekspor kunci QKD.

PP ini mendefinisikan model siklus hidup umum untuk TOE yang terdiri atas beberapa fase sebagai berikut:

- a. Fase pengembangan
- b. Fase manufakturing
- c. Fase pra-operasional
- d. Fase operasional
- e. *End of life*.

Adapun dalam fase operasional, PP mengasumsikan adanya 4 keadaan (*state*) utama, sebagai berikut:

- a. *Calibration state*
- b. *QKD state*
- c. *Failure state*
- d. *End of life*

2. Klaim kesesuaian

PP ini bersesuaian terhadap CC:2022 revisi 1, sebagai berikut:

- a. Kesesuaian terhadap CC Bagian 2 *extended*
- b. Kesesuaian terhadap CC Bagian 3
- c. Tingkat asurans keamanan untuk PP ini adalah EAL4 *augmented* AVA_VAN.5 dan ALC_DVS.2
- d. PP tidak mengklaim kesesuaian terhadap PP lain
- e. ST dan PP yang mengklaim kesesuaian terhadap PP ini harus mengikuti kesesuaian dengan ketat (*strict conformance*) terhadap PP ini.

3. Definisi permasalahan keamanan

- a. Aset, data TSF, pengguna, subjek, objek, dan atribut keamanan Aset TOE yang dilindung terdiri atas Kunci QKD terhadap integritas dan kerahasiaan dan Layanan distribusi kunci terhadap penggunaan yang tidak sah. Sedangkan data TSF yang dipelihara oleh TOE meliputi:

- 1) *Audit Data Records* (ADR)

- 2) QKD *Authentication Key* (QAK), *share secret* yang digunakan untuk mengautentikasi komunikasi klasik pada saluran klasik yang diautentikasi dari tautan QKD;
- 3) ADR *Signing Key* (ASK), kunci untuk menandatangani catatan ADR saat diekspor
- 4) *User Definition Records* (UDR), informasi terkait pengguna yang dikenal dan peran yang terkait
- 5) *Calibration Data* (CD), parameter fisik dari platform yang mendasari, yang dapat disesuaikan dan diverifikasi oleh pengguna agar TOE dapat menjalankan protokol QKD dengan aman.

TOE membedakan subjek sebagai berikut:

- 1) Pengguna tidak teridentifikasi, merupakan pengguna yang tidak terkait dengan UDR apapun
- 2) Pengguna teridentifikasi, merupakan pengguna yang memiliki UDR terkait, dengan minimal peran sebagai berikut:
 - a) Administrator, mendefinisikan pengguna baru dan menetapkan peran kepada pengguna dengan membuat, memodifikasi, dan menghapus UDR;
 - b) Auditor, mengeksport ADR dan menghapus data audit yang telah diekspor dari TOE
 - c) *Maintainer*, dapat mengonfigurasi, mengkalibrasi atau melakukan perbaikan terbatas pada memodifikasi CD
 - d) *Key Requester*, pengguna yang berwenang atas layanan distribusi kunci dan penerima kunci QKD

Adapun atribut keamanan dari pengguna yang dikenal oleh TOE disimpan dalam UDR dengan memuat User-ID dan peran pengguna.

b. Ancaman (*Threat*)

Berikut adalah identifikasi ancaman yang harus dimitigasi oleh TOE untuk melindungi aset.

- 1) T.ServAcc akses tidak sah ke data dan fungsi dalam TOE
Pengguna yang teridentifikasi memperoleh akses tidak sah ke layanan distribusi kunci pada TOE atau kunci QKD dan dapat mengeksploitasi aturan yang tidak konsisten/ambigu terkait penerima yang sah dari kunci QKD di masing-masing modul QKD.
- 2) T.Session Pembajakan Sesi
Penyerang atau pengguna sah dapat menggunakan sesi terbuka dari pengguna teridentifikasi lain untuk mendapatkan akses tidak sah ke layanan distribusi kunci pada TOE atau kunci QKD.
- 3) T.QKDEave Penyadapan data tautan QKD
Penyerang menyadap komunikasi yang dikirimkan melalui link QKD untuk mengkompromikan kerahasiaan kunci QKD.
- 4) T. QKDMani Manipulasi data link QKD
Penyerang menghasilkan atau memanipulasi data pada link QKD untuk mengkompromikan kerahasiaan kunci QKD.
- 5) T.ExplMal Eksploitasi Malfungsi TOE
Penyerang atau pengguna yang tidak sah memperoleh pengetahuan tentang kunci QKD dengan mengeksploitasi malfungsi TOE yang disebabkan baik secara sengaja, spontan, atau karena kalibrasi yang tidak benar.
- 6) T.Observe Pengamatan Karakteristik TSF
Penyerang mengamati emisi, termasuk sinyal atau menginjeksi sinyal *probe* melalui antarmuka yang dapat diakses oleh TOE atau menerapkan metode inspeksi non-destruktif lainnya untuk memperoleh informasi tentang keadaan internal TSF yang dapat digunakan untuk mengkompromikan kerahasiaan kunci QKD

c. Kebijakan keamanan organisasi

Berikut merupakan kebijakan yang disusun dan disahkan untuk ditaati dan dijalankan oleh pengguna TOE, meliputi:

1) OSP.QKDSERVICE, Layanan Distribusi Kunci TOE

TOE menyediakan layanan distribusi kunci kepada pengguna yang sah berdasarkan protokol P&M untuk distribusi kunci kuantum dan membangun bit-string acak yang dibagikan dan bersifat rahasia di setiap modul QKD.

2) OSP Audit, Audit untuk operasi keamanan

TOE mendukung audit keamanan untuk operasi administrasi, kalibrasi, dan layanan distribusi kunci. Konfigurasi cakupan data yang diaudit dan izin untuk menghapus data audit dibatasi pada peran Auditor. Pengguna dengan peran Auditor tidak memegang peran Administrator atau *Maintainer*. Data audit yang diekspor disimpan dengan aman untuk keperluan forensik.

3) OSP.SEC.EoL, Status *end of life* yang aman

TOE menghapus semua data rahasia atau memastikan bahwa data rahasia tidak dapat diambil kembali. Administrator diizinkan untuk sengaja menempatkan TOE ke dalam status *End of Life* untuk proses dekomisioning.

d. Asumsi

Asumsi keamanan yang dijadikan sebagai justifikasi untuk menyatakan bahwa tujuan keamanan lingkungan operasional dipenuhi yaitu sebagai berikut:

1) A.Maint, pemeliharaan yang teliti

Administrator dan *Maintainer* adalah pengguna yang terpercaya. *Maintainer* melakukan kalibrasi dengan cermat. Administrator tidak akan menambahkan pengguna atau menetapkan peran kepada pengguna yang tidak berwenang. Administrator juga akan menetapkan pengguna sebagai

Auditor. Auditor akan mengonfigurasi dan melakukan audit terhadap TOE.

2) A.SecureOp, operasi di area yang aman

TOE dipasang dan dioperasikan di area yang aman, yaitu hanya personel yang berwenang yang dapat memperoleh akses fisik ke TOE. Personel yang berwenang ini tidak akan menyalahgunakan TOE. Lingkungan di sekitar TOE akan mendeteksi setiap akses tidak sah, dan TOE akan dihentikan dari layanan jika deteksi tersebut terjadi.

4. Tujuan keamanan

a. Tujuan keamanan TOE, terdiri atas beberapa hal sebagai berikut:

1) O.Identify, Identifikasi pengguna

TSF harus secara unit mengidentifikasi pengguna sebelum memberikan akses ke sumber daya yang tidak dikendalikan

2) O.AccCtrl, Kontrol akses

TSF harus menyediakan kontrol akses terhadap layanan distribusi kunci dan kunci QKD, ADR, manajemen TSF dan data TSF

3) O.QKD, Distribusi Kunci Kuantum

TSF harus menyediakan layanan distribusi kunci berdasarkan protokol P&M untuk distribusi kunci kuantum dan menghapus kunci QKD setelah diekspor atau setelah waktu habis dari masing-masing modul.

4) O.QKDAuth, Saluran klasik yang diautentikasi.

TSF menyediakan autentikasi mutual antara kedua modul QKD, dan memastikan keaslian data yang dipertukarkan untuk tujuan O.QKD melalui saluran klasik yang diautentikasi pada tautan QKD.

5) O.Audit, audit untuk TSF kriptografi

TSF menyediakan audit keamanan atas administrasi, kalibrasi, dan layanan distribusi kunci dengan mengenali, mencatat, dan menyimpan secara andal kejadian-kejadian audit tertentu menggunakan catatan audit yang berkaitan dengan aktivitas-aktivitas yang dikendalikan oleh TSF

6) O.TST, Pengujian mandiri

TSF melakukan pengujian mandiri terhadap fungsi-fungsi keamanan penting dan memantau parameter operasionalnya, termasuk parameter dari tautan QKD.

TSF menolak akses ke layanan distribusi kunci dan kunci QKD kecuali apabila fungsi-fungsi keamanan telah dipastikan berjalan dengan baik.

TSF juga menekan atau mendeteksi sinyal-sinyal pada tautan QKD yang dapat digunakan untuk memeriksa keadaan internal TSF.

7) O.EMSec, Keamanan emisi

TSF dirancang untuk mencegah kebocoran data rahasia pengguna atau data TSF yang dapat dipahami melalui tautan QKD.

8) O.Sanitize, status *end of life* yang aman

TSF memungkinkan penghapusan semua informasi yang tersimpan dalam TOE secara aman sebelum memasuki status *End of life (EoL)*.

9) O.SessionLimit, Pembatasan sesi pengguna

TSF memungkinkan pengguna untuk mengakhiri sesi mereka dan secara otomatis mengakhiri sesi yang tidak digunakan atau tidak aktif.

b. Tujuan keamanan Lingkungan Operasional, terdiri beberapa hal sebagai berikut:

1) OE.*Trust*, Pengguna yang terpercaya

Lingkungan operasional harus memastikan bahwa Administrator dan *Maintainer* adalah pengguna yang terpercaya dan telah terlatih dengan baik.

2) OE.Audit, revidir dan avabilitas catatan audit

Administrator harus menetapkan peran Auditor kepada identitas pengguna yang sesuai. Auditor harus mendefinisikan kejadian yang diaudit dan melakukan audit. Pengguna dengan peran Auditor tidak boleh merangkap sebagai Administrator ataupun *Maintainer*.

3) OE.SecureOP, lingkungan operasional yang aman

TOE harus disimpan dan dioperasikan dalam area yang dikendalikan aksesnya, sehingga hanya personel yang berwenang yang dapat mengakses TOE secara fisik dan antarmuka penggunaannya

4) OE.*Personnel*, personel yang terpercaya

Personel yang berwenang untuk menggunakan TOE harus terpercaya dan terlatih dengan baik.

Tabel 3.4 berikut merupakan korespondensi antara permasalahan dan tujuan keamanan. Justifikasi ini menunjukkan bahwa tujuan keamanan dapat mengatasi permasalahan keamanan yang berkaitan dengan tepat.

Tabel 3.4 Korespondensi antara permasalahan dan tujuan keamanan.

	T.ServAcc	T.Session	T.QKDEave	T.QKDMani	T.ExplMal	T.Observe	OSP.QKDService	OSP.Audit	OSP.SecEoL	A.SecureOp	A.Maint
O.Identify							x	x			
O.AccCtrl	x						x	x			
O.QKD			x	x			x				
O.QKDAuth			x	x			x				
O.Audit								x			
O.TST					x	x					
O.EMSec						x					
O.Sanitize					x				x		
O.SessionLimit		x									
OE.SecureOp					x	x	x	x		x	
OE.Personnel		x					x	x		x	
OE.Trust								x			x
OE.Audit								x			x

5. Definisi komponen tambahan

Berikut merupakan beberapa pendefinisian komponen tambahan yang digunakan dalam PP ini, yaitu:

a. *Quantum Key Distribution* (FCS_QKD)

Klausul ini menggambarkan persyaratan fungsional keamanan untuk pembuatan kunci QKD, yang dapat digunakan untuk tujuan kriptografi. Persyaratan fungsional keamanan TI untuk TOE didefinisikan dalam famili tambahan dari kelas FCS (FCS_QKD), yaitu FCS_QKD.1 *Prepare and Measure Quantum Key Distribution*. Komponen ini mensyaratkan distribusi kunci kuantum antara dua modul QKD untuk dibangun menggunakan protokol P&M, termasuk rekonsiliasi informasi dan penguatan privasi.

b. *Sanitizing on State Change* (FDP_RIP.3)

Komponen tambahan dalam PP ini yaitu FDP_RIP.3 *Sanitizing on State Change*, mengharuskan bahwa TSF harus menghapus sekumpulan data yang terdefinisi dengan baik ketika mendeteksi suatu peristiwa.

c. *Inter-TSF trusted channel – authenticated classical channel* (FTP_ITC.2)

Komponen tambahan dalam PP in yaitu FTP_ITC.2 *Inter-TSF trusted channel – authenticated classical channel*, mengharuskan agar TSF menyediakan saluran komunikasi yang terautentikasi, yang disebut sebagai saluran klasik terautentikasi di dalam tautan QKD antara kedua modul QKD.

6. Persyaratan keamanan

Tabel 3.5 berikut merupakan korespondensi antara tujuan keamanan TOE dengan SFR.

Tabel 3.5 Korespondensi antara tujuan keamanan TOE dengan SFR.

Tujuan Keamanan	SFR	Keterangan
O.Identity	FIA_ATD.1	mengharuskan TSF untuk menjaga daftar atribut keamanan, yaitu Identitas Pengguna dan Peran, dari setiap pengguna untuk memungkinkan identifikasi pengguna
	FIA_UID.1	mengharuskan TSF untuk menolak akses ke sumber daya yang terkontrol sebelum pengguna diidentifikasi. TSF juga mengharuskan untuk mengasosiasikan setiap pengguna dengan peran.
	FIA_USB.1	Mengharuskan TSF untuk mengasosiasikan setiap

Tujuan Keamanan	SFR	Keterangan
		pengguna awal dengan peran pengguna yang tidak teridentifikasi, dan hanya setelah teridentifikasi, mengasosiasikannya dengan peran masing-masing
O.AccCtrl	FDP_ACC.1	mendefinisikan aturan
	FDP_ACF.1	kontrol akses dan membatasi akses ke layanan distribusi kunci, kunci QKD, dan ADR, berdasarkan pengguna yang teridentifikasi, Peran yang terkait, dan status operasional.
	FDP_ETC.1	Mendefinisikan persyaratan untuk mengeksport kunci QKD
	FIA_ATD.1	mendefinisikan atribut keamanan dari pengguna individu, termasuk Peran yang digunakan untuk kontrol akses
	FIA-USB.1	menghubungkan pengguna yang teridentifikasi dengan Peran mereka termasuk nilai awal yang aman.
	FMT_MSA.1	mendefinisikan status operasional dan bagaimana status tersebut dapat diubah.

Tujuan Keamanan	SFR	Keterangan
		memungkinkan <i>Key Requester</i> untuk menentukan pengguna yang sah yang diperbolehkan menerima kunci yang diminta
	FMT_MSA.2	memastikan bahwa TSF melarang <i>User Identity</i> yang sama untuk memegang Peran Administrator dan Auditor sekaligus.
	FMT_MSA.3	mendefinisikan nilai <i>default</i> untuk atribut keamanan. Inisialisasi status operasional tidak diwajibkan karena status ini tidak terikat pada subjek atau objek mana pun yang dapat dibuat
	FMT_MTD.1	mendefinisikan fungsi manajemen dari ADR dan CD. Fungsi ini membatasi manajemen ADR hanya untuk Auditor dan akses ke CD hanya untuk <i>Maintainer</i> .
	FMT_MTD.1/Adm	mendefinisikan manajemen pengguna, manajemen UDR, dan membatasi ini hanya untuk Administrator.
	FMT_MTD/QAK	mendefinisikan QAK sebagai tidak dapat dikelola, karena

Tujuan Keamanan	SFR	Keterangan
		status Personalisasi bukan status operasional dalam PP
	FMT_SMF.1	Mendefinisikan kemampuan untuk pengelolaan data TSF
	FMT_SMR.1	Membatasi nilai yang diperbolehkan untuk atribut keamanan Peran.
	FPT_ITT.1	memastikan bahwa atribut keamanan yang sesuai tidak dapat dimodifikasi saat ditransfer antar modul QKD.
O.QKD	FCS_CKM.6/EXP	menghapus kunci QKD yang disimpan secara internal setelah diekspor (FDP_ETC.1) atau setelah batas waktu yang telah ditentukan.
	FCS_QKD.1	mengimplementasikan protokol P&M yang ditentukan untuk distribusi kunci kuantum.
	FCS_RNG.1	mendefinisikan generator angka acak fisik (<i>physical random number generator</i>) yang diperlukan untuk operasi yang benar dan aman dari FCS_QKD.1.
	FDP_ETC.1	menghapus kunci QKD yang disimpan secara internal setelah diekspor

Tujuan Keamanan	SFR	Keterangan
	FPT_FLS.1/EoL	Memasukkan ke dalam kondisi <i>end of life</i> jika percobaan melampaui batas
	FPT_ITT.1	memastikan bahwa informasi apa pun yang dibutuhkan di luar protokol QKD, misalnya pembagian bit <i>string</i> untuk penggunaan internal dan ekspor sebagai kunci QKD, ditransfer tanpa modifikasi antara kedua modul QKD.
	FPT_ITC.2	mengimplementasikan saluran klasik terautentikasi yang diperlukan untuk komunikasi klasik yang relevan pada tautan QKD.
O.QKDAuth	FCS_CKM.6/QAK	Menutup QKD dengan menghapus <i>Quantum Authentication Key</i> (QAK)
	FCS_COP.1/CCI	mendefinisikan mekanisme kriptografi yang menggunakan QAK dan memastikan keaslian data yang dipertukarkan melalui saluran klasik terautentikasi
	FCS_QKD.1	Menghasilkan dan memperbarui QAK secara aman
	FDP_ACF.1	menolak akses lebih lanjut ke layanan distribusi kunci

Tujuan Keamanan	SFR	Keterangan
	FPT_FLS.1/Fall	mengharuskan TSF untuk beralih ke status Gagal (<i>Failure state</i>)
	FPT_ITC.2	mensyaratkan agar TSF menyediakan saluran komunikasi dengan identifikasi yang terjamin terhadap modul QKD TOE dari mana data saluran tersebut dikirim, serta melindungi integritas data yang dipertukarkan melalui saluran
O.Audit	FAU_GEN.1	mensyaratkan TSF untuk menghasilkan catatan audit dari peristiwa-peristiwa yang dapat diaudit, termasuk administrasi, kalibrasi, dan penggunaan layanan distribusi kunci.
	FAU_STG.2	mensyaratkan TSF untuk menyimpan data audit secara andal guna mencegah hilangnya catatan audit.
	FAU_STG.4	
	FCS_COP.1/Aud	menyediakan mekanisme kriptografi yang diperlukan untuk tujuan ini. Dalam dokumen dasar (<i>base PP</i>), diasumsikan bahwa kunci terkait, yaitu Audit <i>Signing</i>

Tujuan Keamanan	SFR	Keterangan
		<i>Key</i> (ASK), telah diinstal dalam TOE pada saat pengiriman
	FDP_ACF.1	mengizinkan Auditor untuk mengekspor ADR
	FDP_DAU.1	mensyaratkan TSF untuk menyediakan bukti keaslian dan memungkinkan Auditor untuk memverifikasi validitas ADR.
	FMT_MSA.3	memastikan bahwa ADR yang baru dihasilkan tidak ditandai sebagai telah diekspor, sehingga ADR harus diekspor terlebih dahulu sebelum dapat dihapus.
	FMT_MTD.1	menetapkan atribut keamanan " <i>exported</i> " yang kemudian memungkinkan Auditor untuk menghapus entri yang telah diekspor
	FMT_SMR.1	Mendefinisikan peran auditor
O.TST O.EMSec	FPT_FLS.1/EoL	Kondisi yang dapat dipilih sebagai langkah aman jika terdeteksi kondisi berbahaya
	FPT_FLS.1/Fall	
	FPT_PHP.3	mendeteksi penyelidikan aktif menggunakan tautan QKD

Tujuan Keamanan	SFR	Keterangan
	FPT_TST.1	mensyaratkan TSF untuk memantau parameter operasionalnya dengan menjalankan serangkaian tes mandiri (<i>self-test</i>)
	FRU_FLT.2	mensyaratkan TSF untuk beroperasi dengan benar jika FPT_TST.1 tidak mendeteksi kondisi berbahaya.
	FPT_EMS.1	mensyaratkan TSF untuk membatasi emanasi melalui tautan QKD ke tingkat yang tidak dapat dipahami, untuk data pengguna atau data TSF yang bersifat rahasia.
	FPT_PHP.3	mensyaratkan TSF untuk merespons penyelidikan aktif guna mencegah kebocoran paksa.
O.Sanitize	FCS_CKM.6/UDR	menghapus kredensial pengguna bersama dengan UDR
	FCS_CKM.6/ASK	menghapus ASK saat memasuki status EoL
	FMT_MSA.1	memungkinkan siapa saja untuk melakukan sanitasi TOE dari status operasional apa pun.
	FPT_FLS.1/EoL	mensyaratkan TSF untuk memasuki status EoL jika

Tujuan Keamanan	SFR	Keterangan
		tidak dapat memastikan keberlanjutan TSF
O.SessionLimit	FTA_SSL.3	mensyaratkan TSF untuk mengakhiri sesi yang tidak aktif.
	FTA_SSL.4	mensyaratkan TSF untuk memungkinkan setiap pengguna mengakhiri sesi mereka sendiri.

TOE harus dievaluasi pada EAL4 ditambah dengan AVA_VAN.5 dan ALC_DVS. Penambahan AVA_VAN.5 dipilih untuk memberikan jaminan terhadap penyerang yang memiliki potensi serangan tinggi. Paket EAL dipilih karena merupakan paket jaminan terkecil yang memenuhi semua ketergantungan AVA_VAN.5. Sedangkan ALC_DVS.2 dipilih untuk memberikan proses yang lebih ketat untuk mencegah kompromi pada area pengembangan dan manufaktur atau interferensi yang lebih rumit.

7. Panduan untuk SFR terkait RNG

Kualitas bilangan acak yang dihasilkan oleh pembangkit bilangan acak FCS_RNG.1 sangat penting untuk klaim keamanan FCS.QKD.1. Berikut adalah beberapa pendekatan yang dapat digunakan oleh penyusun ST untuk memilih pembagian bilangan acak.

a. RNG berdasarkan AIS 31

German Federal Office for Information Security (BSI) menerbitkan persyaratan evaluasi wajib untuk skema sertifikasi *Common Criteria* Jerman. Dokumen ini menggambarkan kelas pembangkit bilangan acak yang telah

ditentukan, yaitu FCS_RNG.1/PTG3 *Random number generation – Physical random number generation*.

b. RNG berdasarkan NIST 800-90

National Institute of Standard and Technology (NIST) menerbitkan NIST SP 800-90B *Recommendation for the Entropy Sources Used for Random Bit Generation*. Rekomendasi untuk sumber entropi menggambarkan persyaratan keamanan dan prosedur pengujian yang dapat diterapkan pada sumber entropi dari *physical random number generator*. Adapun SFR yang diterapkan menjadi FCS_RNG.1/ES *Random Number Generator*

G. ETSI GR QKD 003 V2.1.1 Quantum Key Distribution (QKD): Components and Internal Interfaces

Dokumen ini menetapkan properti komponen dan antarmuka internal pada sistem QKD [10]. Terdapat perangkat tertentu yang muncul di sebagian besar sistem QKD, misalnya *quantum physical devices* seperti *photon sources* dan *detectors*, atau *classical equipment* seperti *protocol processing computer hardware* dan *operating systems*. Atas hal tersebut, properti yang relevan perlu diidentifikasi yang selanjutnya akan menjadi subyek standardisasi. Selain itu, perlu disusun katalog persyaratan yang relevan untuk antarmuka antar komponen untuk mendukung definisi antarmuka internal yang akan datang.

Adapun struktur dokumen ETSI GK QKD 003 V.2.1.1 terdiri atas beberapa bab sebagai berikut:

1. Ruang lingkup
2. Referensi
3. Definisi, simbol dan singkatan
4. Sistem QKD
5. *Photon Detector*
6. *QKD Source*
7. Modulator

8. Lampiran A Protokol variabel diskrit
9. Lampiran B Protokol variabel berkelanjutan

Sistem QKD terdiri atas sejumlah komponen internal dengan berbagai tingkat kompleksitas dalam implementasinya, diantaranya yaitu sebagai berikut:

- a. Implementasi *Weak Laser Pulse* QKD, nilai qubit dikodekan ke dalam pulsa laser yang telah dilemahkan hingga tingkat foton tunggal. Pengirim menggunakan setidaknya satu sumber laser lemah sebagai pembawa informasi kuantum. Berikut adalah beberapa contoh sistem QKD *Weak Laser Pulse*:
 - 1) *One-Way Mach-Zehnder*
 - 2) Skema *Send-and-return (Mach-Zehnder)*
 - 3) Implementasi *Phase-Intensity Modulator*
 - 4) *Coherent One-Way (COW)*
- b. Implementasi *entanglement* berbasis QKD, sistem ini menggunakan pasangan foton yang terjerat (*entangled*), yang satu dikirim ke penerima dan yang satu diukur oleh penerima. Sistem ini memerlukan sinkronisasi dan kompensasi dinamis terhadap polarisasi selama transmisi. Sistem ini dapat berfungsi dalam lingkungan ekstrem seperti luar angkasa, dan dibuktikan saat peluncuran satelit Micius tahun 2016, dengan *fidelity* sebesar 0,86.
- c. Implementasi CV-QKD
CV-QKD menjamin keamanan dengan menggunakan 2 variabel konjugat dari medan elektromagnetik (real dan imajiner) dari keadaan koheren. Sinkronisasi fase antara pengirim dan penerima dilakukan dengan dua pendekatan, yaitu:
 - 1) *Transmitted Local Oscillator: TLO-CV-QKD scheme*
 - 2) *Local Local Oscillator: LLO-CV-QKD scheme*

Detektor photon yang digunakan dalam sistem QKD, terdiri atas 2 (dua) jenis, sebagai berikut:

- a. Single-Photon Detector, bertujuan untuk mengubah foton tunggal menjadi sinyal yang dapat dideteksi secara makroskopik.

Detektor ini memiliki sejumlah parameter untuk serangkaian kondisi pengoperasian. Tabel 3.6 merupakan parameter yang digunakan untuk menentukan detektor photon-tunggal.

Tabel 3.6 Parameter untuk menentukan detektor photon-tunggal.

No	Parameter	Definisi
1	<i>Detector gate repetition rate</i>	Laju pengulangan dari interval waktu di mana detektor memiliki sensitivitas terhadap foton tunggal.
2	<i>Photon detection probability</i>	Gated detector Probabilitas bahwa sebuah foton yang mengenai input optik akan terdeteksi (dalam sebuah gate deteksi). Free-running detector Probabilitas bahwa sebuah foton yang mengenai input optik akan terdeteksi.
3	<i>Spectral Responsivity</i>	Probabilitas deteksi foton sebagai fungsi dari energi foton
4	<i>Dark count probability</i>	Gated dectector Probabilitas bahwa detektor mencatat kejadian deteksi per gate, dalam kondisi tanpa pencahayaan optik.

No	Parameter	Definisi
		<i>Free-running detector</i> Probabilitas bahwa detektor mencatat kejadian deteksi dalam interval waktu tertentu, dalam kondisi tanpa pencahayaan optik
5	<i>After-pulse probability</i>	Probabilitas bahwa detektor mencatat kejadian deteksi palsu dalam kondisi tanpa pencahayaan, dengan syarat adanya kejadian deteksi pada waktu ΔT sebelumnya.
6	<i>Dead time</i>	Interval waktu setelah kejadian deteksi di mana detektor secara keseluruhan tidak dapat memberikan keluaran sebagai respons terhadap foton yang masuk pada tingkat foton tunggal.
7	<i>Recovery time</i>	Durasi waktu terkecil setelah kejadian deteksi di mana efisiensi deteksi tidak lagi bergantung pada riwayat deteksi foton sebelumnya
8	<i>Partial recovery time</i>	Durasi waktu setelah kejadian deteksi foton untuk efisiensi deteksi kembali ke persentase tertentu dari nilai kondisi stabilnya
9	<i>Maximum count rate</i>	Laju maksimum kejadian deteksi foton dalam rezim foton tunggal

No	Parameter	Definisi
		atau beberapa foton per <i>gate</i> saat terkena pencahayaan kuat
10	<i>Detector signal jitter</i>	Variasi probabilitas deteksi foton terhadap waktu kedatangan sebuah foton tunggal pada porta input <i>Device Under Test</i> (DUT)
11	<i>Photon detection probability profile</i>	Probabilitas deteksi foton sebagai fungsi dari waktu kedatangan pulsa yang masuk.
12	<i>Photon number resolution depth</i>	Untuk detektor yang dapat membedakan jumlah foton dalam pulsa yang datang, ini adalah jumlah maksimum foton yang dapat dibedakan.

- b. Photon Detector untuk CV-QKD, Tabel 3.7 menyajikan parameter yang digunakan untuk menentukan *Receiver* CV_QKD dan kanal receiver.

Tabel 3.7 Parameter untuk menentukan receiver CV_QKD dan kanal receiver.

No	Parameter	Definisi
1	<i>Photon detection probability</i>	Probabilitas bahwa sebuah foton yang mengenai input optik akan terdeteksi.
2	<i>Temporal response indistinguishability</i>	Ketidakmampuan untuk membedakan respons temporal dari dua detektor yang digunakan dalam unit deteksi homodin
3	<i>Supported modulation formats</i>	-

No	Parameter	Definisi
4	<i>Bandwidth</i>	<i>Bandwidth</i> detektor yang digunakan untuk QKD.
5	<i>Detection scheme</i>	Detektor Foton untuk Pengaturan CV-QKD.
6	<i>Supported signal-to-noise ratio</i>	Rasio <i>Signal-to-noise</i> (SNR) terendah yang didukung dari sinyal kuantum pada input penerima, tidak hanya untuk mendeteksi sinyal tetapi juga untuk menghasilkan kunci. Hal ini harus didukung oleh kemampuan koreksi galat yang memadai.
7	<i>Total receiver loss</i>	Kehilangan gabungan dari sistem optik, efisiensi deteksi foton, pemrosesan listrik dan digital, dan lainnya di sisi penerima
8	<i>Excess noise</i>	Diekspresikan dalam satuan shot noise atau milli-shot noise. Untuk deteksi homodin satu kuadratur, nilai ini dinormalisasi terhadap variansi pengukuran shot noise [penerima]. Untuk deteksi homodin dua kuadratur dan heterodin, nilai ini harus dikalikan 2 untuk menyatakan noise berlebih dalam satuan shot noise [kanal penerima].
9	<i>Excess noise uncertainty</i>	Ketidakpastian pengukuran terhadap noise berlebih yang dinormalisasi terhadap nilai noise

No	Parameter	Definisi
		berlebih yang diukur. Ini harus didukung oleh jumlah sampel yang digunakan.
10	<i>Excess noise stability</i>	Frekuensi maksimum dari fluktuasi noise berlebih yang diukur. Hal ini harus didukung oleh estimasi ketidakpastian pengukuran
11	<i>Shot noise</i>	Variansi rata-rata shot noise yang diukur
12	<i>Shot noise uncertainty</i>	Ketidakpastian pengukuran terhadap shot noise yang dinormalisasi terhadap nilai shot noise yang diukur. Hal ini harus didukung oleh jumlah sampel yang digunakan.
13	<i>Shot noise stability</i>	Frekuensi maksimum dari fluktuasi shot noise yang diukur. Ini harus didukung oleh estimasi ketidakpastian pengukuran
14	<i>Electronic noise</i>	Prosedur pengukuran harus mengikuti langkah yang sama seperti shot noise. Dinormalisasi terhadap shot noise yang diukur, dan dinyatakan dalam satuan shot noise atau milli-shot noise.
15	<i>Electronic noise uncertainty</i>	Ketidakpastian pengukuran terhadap noise elektronik yang dinormalisasi terhadap nilai noise elektronik yang diukur. Ini harus

No	Parameter	Definisi
		didukung oleh jumlah sampel yang digunakan
16	<i>Electronic noise stability</i>	Frekuensi maksimum dari fluktuasi noise elektronik yang diukur. Hal ini harus didukung oleh estimasi ketidakpastian pengukuran.

Pemancar QKD dapat berasal dari:

a. Pemancar *Single-photon*

Pemancar ini idealnya hanya mengeluarkan satu foton pada satu waktu, namun implementasi praktis sering menggunakan pendekatan probabilistik untuk menghasilkan dua atau lebih foton. Tabel 3.8 merupakan parameter yang dapat digunakan untuk menentukan kinerja dari pemancar *single-photon*.

Tabel 3.8 Parameter untuk menentukan kinerja dari pemancar *Single-photon*.

No	Parameter	Definisi
1	<i>Optical pulse repetition rate</i>	Frekuensi emisi pulsa cahaya
2	<i>Photon number probability distribution</i>	Distribusi probabilitas jumlah foton dalam suatu pulsa optik
3	<i>Mean photon number</i>	Jumlah rata-rata foton per pulsa sinyal
4	<i>Mean source optical power</i>	Daya optik rata-rata yang dipancarkan selama periode sesi QKD.
5	<i>Long-term power stability</i>	Variasi intensitas sumber cahaya selama sesi QKD atau dalam interval waktu tertentu

No	Parameter	Definisi
6	<i>Short-term power stability</i>	Variasi intensitas pulsa dalam jangka waktu tertentu
7	<i>Number of emitters</i>	Jumlah pemancar cahaya yang membentuk suatu sumber QKD
8	<i>Second order correlation function</i>	Fungsi korelasi orde dua pada selang waktu nol yang mengkuantifikasi statistik jumlah foton
9	<i>Wavelength spectral frequency</i>	Panjang gelombang (atau frekuensi spektral) dari foton yang dipancarkan
10	<i>Spectral linewidth</i>	Lebar pita spektral dari foton yang dipancarkan
11	<i>Emission temporal profile</i>	Distribusi foton dalam pulsa yang dipancarkan sebagai fungsi dari posisi temporal.
12	<i>Timing jitter</i>	Ketidakpastian waktu emisi dari satu pulsa pada output optik
13	<i>Temporal profile</i>	Variasi intensitas dalam satu pulsa sebagai fungsi dari posisi temporal di dalam pulsa tersebut
14	<i>Spectral indistinguishability</i>	Besaran untuk mengkuantifikasi sejauh mana dua qubit dapat dibedakan melalui pengukuran spektral
15	<i>Temporal indistinguishability</i>	Besaran untuk mengkuantifikasi sejauh mana dua qubit dapat dibedakan melalui pengukuran temporal.

b. Pemancar *Continuous-Variable* QKD

Pemancar ini menerapkan laser koheren yang dimodulasi dalam dua kuadratur, yaitu amplitudo dan fase. Tabel 3.9 merupakan parameter yang dapat digunakan untuk menentukan kinerja dari pemancar CV-QKD.

Tabel 3.9 Parameter untuk menentukan kinerja dari pemancar CV-QKD.

No	Parameter	Definisi
1	<i>Bandwidth</i>	Rentang frekuensi di mana sinyal transmisi dikirimkan
2	<i>Modulation format</i>	Jenis modulasi (misalnya QPSK, Gaussian, dll.)
3	<i>Synchronization/phase recovery signal type</i>	Jenis sinyal yang dikirim untuk menyinkronkan <i>Local Oscillator</i> (LO) di sisi penerima (misalnya TLO, <i>pilot tone</i> , dll.)
4	<i>Multiplexing type of synchronization/phase recovery signal</i>	Contoh: polarisasi, frekuensi
5	<i>Synchronization/phase recovery signal strength</i>	Kekuatan sinyal
6	<i>Synchronization/phase recovery signal range</i>	Rentang daya sinyal
7	<i>Accuracy of the transmission power of synchronization/phase recovery signal</i>	Keakuratan daya
8	<i>Accuracy of the transmission power of the quantum signal</i>	Keakuratan daya

Modulator adalah perangkat yang dapat memanipulasi derajat kebebasan tertentu dari cahaya dengan menggunakan sinyal pengendali. Biasanya dalam kriptografi kuantum, modulator digunakan untuk menyandi (mengirimkan) atau menyandi balik (menerima) informasi, tetapi dapat digunakan sebagai elemen peredam. Derajat kebebasan yang digunakan sebagai pembawa informasi kuantum ketika cahaya digunakan sebagai sinyal masukan adalah polarisasi, fase relatif, frekuensi, atau *time-bin*. Sinyal pengendali yang digunakan untuk memodifikasi derajat kebebasan tertentu dari sinyal masukan dapat bervariasi secara kontinu atau diskrit tergantung pada protokol yang digunakan.

Pada sisi pemancar, korelasi antara berbagai derajat kebebasan harus dipertimbangkan sebagai potensi ancaman *side channels*. Korelasi tersebut harus dikuantifikasi untuk diperhitungkan dalam proses penguatan privasi (*privacy amplification*), atau dihilangkan untuk memastikan bahwa berbagai keadaan yang dikirimkan ke unit penerima hanya dapat dibedakan melalui derajat kebebasan yang dipilih. Tabel 3.10 merupakan parameter yang dapat digunakan untuk menentukan modulator.

Tabel 3.10 Parameter untuk menentukan modulator.

No	Parameter	Definisi
1	<i>Modulated degree of freedom</i>	Derajat kebebasan dari cahaya yang dimodulasi. Dapat berupa intensitas, fase, polarisasi, atau panjang gelombang.
2	<i>Deviations</i>	Nilai penyimpangan maksimum dari derajat kebebasan yang dipilih terhadap nilai target.
3	<i>Rise and Fall time</i>	Waktu naik (turun) mengacu pada waktu yang dibutuhkan bagi derajat kebebasan yang dipilih

No	Parameter	Definisi
		untuk berubah dari nilai rendah (tinggi) tertentu ke nilai tinggi (rendah) tertentu.
4	<i>Optical robustness</i>	Daya iluminasi maksimum yang dapat diterima oleh sebuah modulator tanpa mengubah parameternya.

H. ETSI GS QKD 015 V2.1.1 *Quantum Key Distribution (QKD): Control Interface for Software Defined Networks*

Dokumen *ETSI GS QKD 015 Quantum Key Distribution (QKD): Control Interface For Software Defined Networks* diterbitkan oleh ETSI pada bulan April 2022 [11]. Berdasarkan penjelasan pada dokumen ini, *Quantum Key Distribution* menggunakan sinyal pada tingkat kuantum, sehingga transmisi sinyal ini sulit dilakukan apabila harus berbagi media fisik dengan sinyal klasik yang jauh lebih kuat. Oleh karena sinyal kuantum tidak bisa diperkuat atau diregenerasi yang membuat jaraknya terbatas, maka diperlukan *trusted repeater* untuk memperluas jangkauan. Untuk mengoptimalkan pengiriman sinyal kuantum bersamaan dengan komunikasi klasik dalam suatu jaringan, serta mengelola relai kunci yang diperlukan untuk jarak yang lebih jauh, maka diperlukan integrasi sistem QKD agar dapat berkomunikasi dengan pengendali jaringan (*network control*) sekaligus menerima perintah dari pengendali jaringan tersebut.

Integrasi tersebut dapat dilakukan dengan menggunakan pemodelan *Yet Another Next Generation* (YANG) yang digunakan untuk mendeskripsikan elemen jaringan. Tujuan dari integrasi ini adalah untuk menyederhanakan manajemen sumber daya QKD dengan lapisan abstraksi dan mengoptimalkan pembuatan dan penggunaan kunci QKD

melalui SDN *controller* yang memiliki pandangan global terhadap jaringan.

Struktur dokumen tersebut adalah sebagai berikut:

1. Ruang Lingkup

Bab ini berisi tentang ruang lingkup yang dibahas pada dokumen ETSI GS QKD 015. Dokumen ini memberikan definisi mengenai antarmuka manajemen untuk integrasi QKD dalam arsitektur *control plane* jaringan yang terdisagregasi, khususnya yang menggunakan SDN. Dokumen ini menetapkan model abstraksi dan alur kerja antara *node* QKD yang mendukung SDN dan *controller* SDN, termasuk proses penemuan sumber daya, penyebaran kapabilitas, dan operasi konfigurasi sistem.

2. Referensi

Bab ini berisi tentang daftar referensi yang menjadi rujukan dalam penyusunan dokumen ETSI GS QKD 015, yaitu:

- a. IETF RFC 6020 (October 2010): "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)";
- b. IETF RFC 7950 (August 2016): "The YANG 1.1 Data Modeling Language";
- c. IETF RFC 6241 (June 2011): "Network Configuration Protocol (NETCONF)";
- d. IETF RFC 8040 (January 2017): "RESTCONF Protocol"; dan
- e. ETSI GR QKD 007: "Quantum Key Distribution (QKD) Vocabulary".

3. Definisi Istilah, simbol, dan singkatan

Bab ini berisi tentang daftar istilah sejumlah 15 istilah yang digunakan dan mengacu pada dokumen ETSI GS QKD 007: *Vocabulary*, dan 32 daftar singkatan yang ada pada dokumen.

4. *Software-Defined Quantum Key Distribution*

a. Pendahuluan

Bab ini menjelaskan secara umum tentang parameter dan pemodelan *Software-Defined Quantum Key Distribution* (SD-QKD) menggunakan model YANG. Desain arsitektur ini memungkinkan pengendali untuk mengorkestrasi sumber daya QKD secara terpusat, dengan tujuan untuk mengoptimalkan alokasi kunci pada setiap *link* berdasarkan permintaan, dan mengotomatisasi pembuatan *link* QKD, baik yang bersifat langsung (terhubung secara fisik melalui kanal kuantum tanpa putus) maupun virtual (berbasis *multi-hop*), di mana kunci dikirimkan dari satu hop (*link* QKD langsung) ke hop berikutnya dalam rangkaian yang menghubungkan titik awal dan titik akhir. Model YANG ini didesain sebagai model dasar untuk integrasi teknologi QKD ke dalam arsitektur manajemen operator jaringan.

b. SD-QKD node

Sebuah node SD-QKD merupakan gabungan satu atau lebih modul QKD yang terhubung ke pengendali SDN dengan protokol standar. Melalui koneksi ini, memungkinkan pengambilan data QKD dan konfigurasi perilaku sistem QKD secara dinamis untuk membangun, memperbarui, atau menghapus asosiasi kunci, baik pada kanal kuantum langsung maupun jalur multi-hop antar lokasi aman. Node ini harus memenuhi beberapa persyaratan seperti pada Tabel 3.11 berikut.

Tabel 3.11 SD-QKD node.

No.	Deskripsi Persyaratan	Status
1	SD-QKD node harus terdiri atas minimal satu modul QKD, ditampilkan sebagai antarmuka QKD.	Harus (<i>Shall</i>)
2	Dapat terdiri atas beberapa modul QKD, membentuk satu node dengan banyak antarmuka.	Boleh (<i>Optional</i>)

No.	Deskripsi Persyaratan	Status
3	Harus berlokasi di dalam area yang aman.	Harus (<i>Shall</i>)
4	Satu lokasi bisa memiliki satu atau lebih SD-QKD <i>node</i> .	Boleh (Opsional)
5	Harus memiliki sistem manajemen kunci untuk mengumpulkan material kunci dari berbagai asosiasi.	Harus (<i>Shall</i>)
6	Harus menyediakan satu akses API bagi aplikasi untuk mengambil kunci dari <i>key store</i> .	Harus (<i>Shall</i>)
7	Harus terhubung ke minimal satu pengendali SDN menggunakan protokol standar.	Harus (<i>Shall</i>)
8	Sebaiknya menampilkan informasi aplikasi ke <i>controller</i> untuk membantu optimasi penggunaan kunci.	Disarankan (<i>Should</i>)
9	Sebaiknya menampilkan informasi sistem QKD ke <i>controller</i> dan mengizinkan pengaturan parameter untuk kanal kuantum.	Disarankan (<i>Should</i>)
10	Sebaiknya menampilkan informasi hubungan kunci (<i>link</i>) dengan sistem SD-QKD lain.	Disarankan (<i>Should</i>)
11	Sebaiknya menampilkan kebutuhan kanal klasik (misal: redaman, panjang gelombang) dari tiap sistem di <i>node</i> .	Disarankan (<i>Should</i>)

Model abstraksi ini bertujuan untuk:

- 1) Memungkinkan pengelolaan sumber daya QKD secara terpusat berdasarkan permintaan, kapabilitas, dan status jaringan (kuantum maupun klasik).
- 2) Menggabungkan berbagai sistem QKD dalam satu area aman di bawah satu sistem manajemen kunci, untuk mendeteksi kebutuhan dan menyiapkan *link* yang diperlukan.

- 3) Mengurangi kompleksitas pengoperasian modul QKD secara terpisah dan mempermudah pengelolaan statistik sistem QKD.
- 4) Menyederhanakan pengelolaan parameter dan perilaku teknis tiap sistem QKD, karena masing-masing *node* bertanggung jawab untuk konfigurasi level rendah.
- 5) Mengoptimalkan konfigurasi dan distribusi *link* QKD berdasarkan informasi QoS aplikasi dan statistik laju generasi kunci tiap *link*.
- 6) Mengkoordinasikan kanal kuantum dan kanal klasik (baik berbagi media fisik maupun tidak) untuk meningkatkan performa sistem QKD.

Pada subbab ini juga ditampilkan gambar yang menjelaskan tentang jaringan SD-QKD yang merupakan sekumpulan *node* SD-QKD yang saling terhubung dengan SDN *controller*.

Pada Bab 4 ini juga dijelaskan mengenai parameter-parameter yang digunakan dalam model YANG. Berikut beberapa parameter yang dijelaskan pada Bab ini:

- 1) Parameter *node* SD-QKD (Subbab 4.2);
- 2) Parameter kemampuan *node* SD-QKD (Subbab 4.3);
- 3) Parameter tampilan QKD (Subbab 4.4);
- 4) Parameter hubungan asosiasi kunci QKD (QKD *key association link*) (Subbab 4.5); dan
- 5) Parameter aplikasi QKD (Subbab 4.6).

Pada Subbab 4.7 dijelaskan mengenai notifikasi YANG yaitu tentang struktur pemodelan YANG pada model aplikasi, *link*, dan tampilan.

5. Diagram Urutan dan Alur kerja

Bab ini memberikan gambaran tentang beberapa skenario penggunaan dasar yang dirancang untuk ditangani oleh jaringan SD-QKD. Untuk setiap skenario, ditampilkan gambar diagram

urutan alur kerja untuk menunjukkan interaksi dan pertukaran informasi antara *node* SD-QKD dan pengendali SDN (SD-QNC). Skenario dasar yang diidentifikasi berkaitan dengan pengelolaan permintaan masuk (aplikasi baru yang meminta kunci) dari perspektif jaringan, serta pembuatan hubungan kunci baru, baik secara virtual maupun fisik.

Skenario dasar yang dijelaskan pada Bab ini yaitu:

- a. Skenario Registrasi Aplikasi QKD (Subbab 5.2)
 - b. Skenario pembuatan Link (langsung) Fisik QKD (Subbab 5.3)
 - c. Skenario pembuatan Link Virtual QKD (Subbab 5.4)
6. Pertimbangan keamanan
- Bab ini menjelaskan tentang proses pemasangan sistem QKD baru, baik dengan atau tanpa lapisan manajemen SDN. Proses ini memerlukan langkah awal autentikasi dan skema keamanan awal (seperti identitas terpercaya dan kunci rahasia sementara) untuk memastikan keamanan tidak terganggu saat instalasi. Setelah itu, komunikasi dapat diamankan menggunakan kunci yang dihasilkan dari QKD.

Jika pengendali SDN berada di lokasi aman, pemasangan sistem QKD baru harus mengikuti prosedur serupa dengan dua kemungkinan situasi:

- a. Sistem baru dipasang di area yang sudah aman, di mana saluran antara pengendali dan sistem dapat diamankan dengan kunci QKD dari tautan yang ada.
- b. Lokasi aman baru diintegrasikan ke jaringan SDN, memerlukan skema keamanan untuk memperkenalkan Agen SDN lokal ke pengendali agar jaringan mempercayainya, dengan autentikasi awal menggunakan mekanisme konvensional dan kunci QKD untuk autentikasi dan enkripsi selanjutnya.

7. Pertimbangan Protokol

Bab ini menjelaskan bahwa model YANG digunakan sebagai bahasa utama untuk pemodelan data jaringan karena mudah didefinisikan, dibaca, dan diperluas. Modul YANG dalam dokumen ini menggunakan versi 1.0 dan kompatibel dengan versi 1.1.

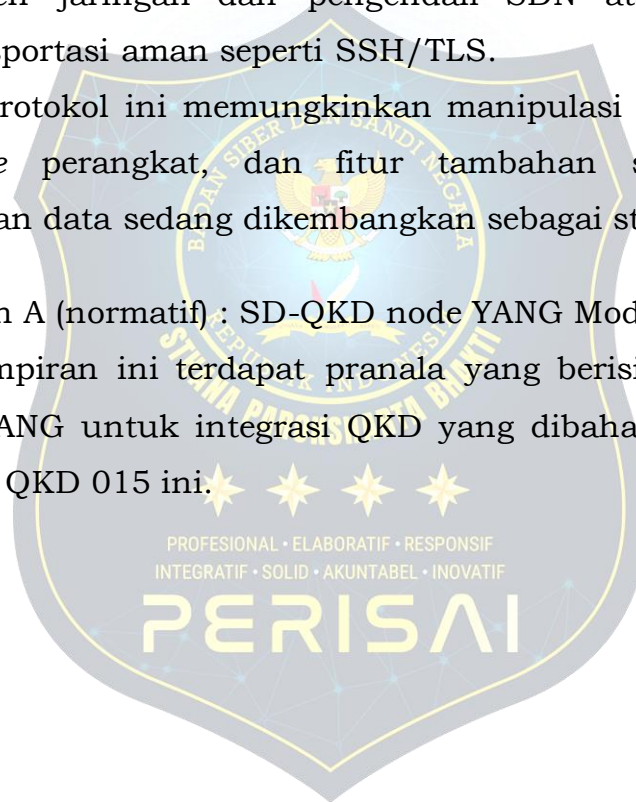
Dua protokol utama manajemen jaringan berbasis YANG adalah:

- a. **RESTCONF**: Berbasis HTTP, digunakan untuk operasi CRUD pada data YANG, biasanya di pengendali SDN.
- b. **NETCONF**: Berbasis XML dan transaksi, digunakan antara elemen jaringan dan pengendali SDN atau NMS, dengan transportasi aman seperti SSH/TLS.

Kedua protokol ini memungkinkan manipulasi data YANG dalam *datastore* perangkat, dan fitur tambahan seperti langganan perubahan data sedang dikembangkan sebagai standar oleh IETF.

8. Lampiran A (normatif) : SD-QKD node YANG Model

Pada lampiran ini terdapat pranala yang berisi tentang struktur model YANG untuk integrasi QKD yang dibahas dalam dokumen ETSI GS QKD 015 ini.





BAB IV

STANDARITU-T



BAB IV

STANDAR ITU-T

Standar ITU-T Y.3800 *Overview On Supporting Quantum Key Distribution* memberikan gambaran umum tentang jaringan yang mendukung *Quantum Key Distribution* (QKD) [12]. Standar ini bertujuan untuk memberikan dukungan dalam perancangan, pengimplementasian, pengoperasian, dan pemeliharaan dalam penerapan QKD Network (QKDN), dari sisi teknologi yang terstandardisasi.

A. RUANG LINGKUP

Dokumen ini memberikan gambaran umum mengenai jaringan yang mendukung QKD dan membahas aspek-aspek jaringan untuk mengimplementasikan teknologi QKD.

Secara khusus, standar ini membahas hal-hal berikut:

- gambaran umum tentang teknologi QKD;
- kapabilitas jaringan untuk mendukung QKD;
- struktur konseptual dan fungsi dasar dari QKDN.

B. GAMBARAN UMUM TEKNOLOGI QKD

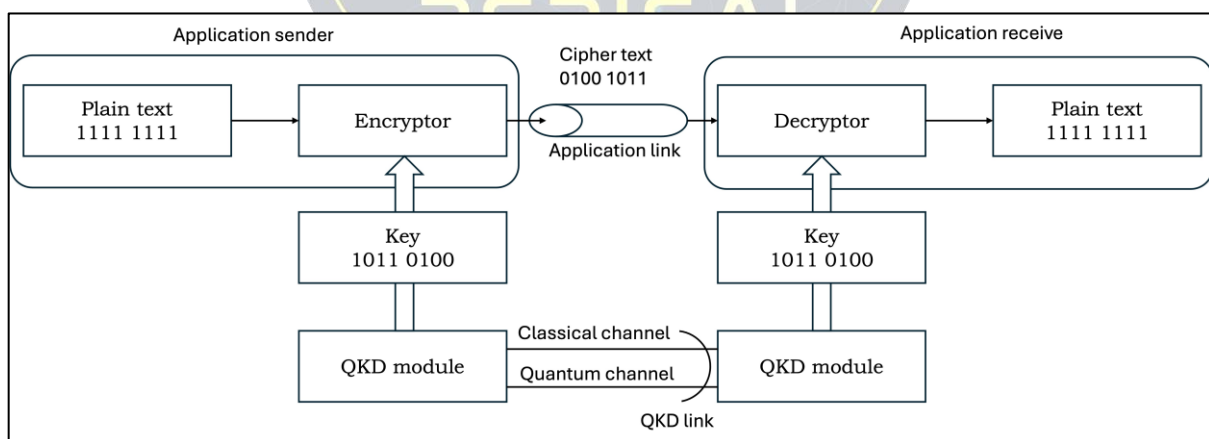
Protokol QKD memungkinkan pendistribusian deretan bit acak simetris sebagai kunci yang aman, yang keamanannya dapat dibuktikan bahkan terhadap penyadap dengan sumber daya komputasi yang tak terbatas, berdasarkan beberapa asumsi yang mendukung model pembuktian keamanannya. Jenis keamanan ini dikenal sebagai *information theoretic security*. Karena protokol QKD didasarkan pada hukum mekanika kuantum, maka aspek keamanan dalam implementasinya perlu diperhatikan.

Kunci yang dihasilkan oleh modul QKD yang mengimplementasikan protokol QKD dapat digunakan oleh berbagai aplikasi kriptografi yang memakai kunci simetris. Elemen dasar dari sistem QKD terdiri atas pemancar (QKD-Tx) dan penerima (QKD-Rx), yang masing-masing disebut sebagai modul QKD.

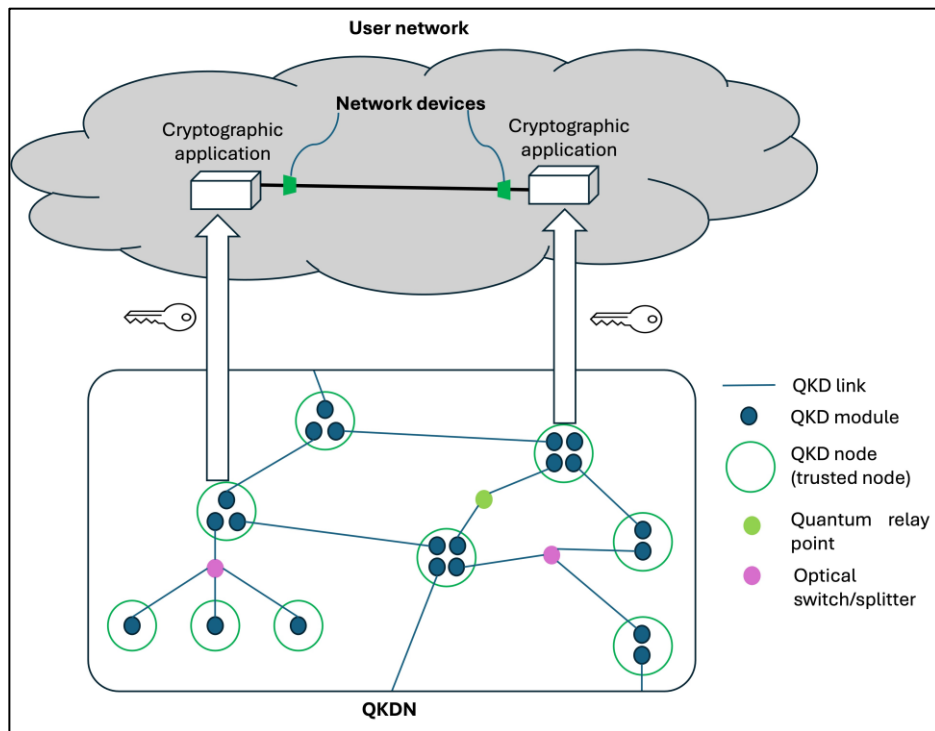
Sebuah QKD *link* menghubungkan modul-modul QKD, yang dapat melibatkan *quantum relay point*. Kunci dibagikan melalui QKD *link*. QKD *link* biasanya terdiri atas kanal kuantum dan kanal klasik. Kanal kuantum disediakan oleh sinyal kuantum, untuk mentransmisikan deretan bit acak. Kanal klasik digunakan untuk sinkronisasi dan pertukaran data antara modul QKD.

Gambar 4.1 mengilustrasikan contoh penerapan QKD untuk mengamankan sambungan aplikasi *point-to-point*. Modul QKD menghasilkan kunci dan menyediakannya untuk aplikasi. Sambungan aplikasi tempat data terenkripsi ditransmisikan dapat berupa saluran komunikasi apa pun dalam jaringan konvensional maupun jaringan masa depan. Oleh karena itu, QKD merupakan teknologi (dan layanan) tambahan bagi jaringan yang ada saat ini maupun yang akan datang.

Kondisi ini tidak berubah sekalipun QKD digunakan dalam bentuk jaringan. Protokol QKD dapat dibuktikan memiliki *information theoretical security* atau IT-secure, namun implementasi modul QKD tetap membutuhkan asumsi tambahan. Keamanan teoretis informasi pada QKD dijamin oleh hukum mekanika kuantum dan teori informasi kuantum.



Gambar 4.1 Contoh konfigurasi QKD
digambar ulang dari [12].



Gambar 4.2 Ilustrasi QKDN dan hubungannya dengan jaringan pengguna digambar ulang dari [12].

Gambar 4.2 menggambarkan sebuah QKDN serta hubungan logisnya dengan jaringan pengguna yang menerima pasokan kunci. Kunci dibagikan di antara node-node QKD, yaitu, node QKD berperan sebagai titik untuk berbagi kunci dan/atau sebagai titik relai kunci untuk memperluas jangkauan QKD. Sedangkan titik relai untuk saklar optik, *Measurement Device Independent* QKD (MDI-QKD), *Twin Field* (TF-QKD), atau pengulang kuantum disebut sebagai titik relai kuantum, yaitu titik relai untuk sinyal kuantum dan tidak harus dapat dipercaya.

Berkat titik-titik relai yang dipercaya (*trusted relay*: berbasis pembangkitan dan enkripsi ulang) maupun tidak dipercaya (*quantum relay*: berbasis *entanglement*, memori, dan *Bell state*) ini, kunci dapat dibagikan di antara node-node QKD mana pun dalam QKDN yang sama. Tidak ada kunci yang dihasilkan atau dibagikan di titik relai kuantum. Oleh karena itu, titik relai kuantum termasuk dalam *link* QKD dan dengan demikian memungkinkan jarak yang lebih jauh atau topologi yang lebih fleksibel untuk QKDN. Deskripsi teknis dari cara-cara ini berada di luar cakupan Standar ini.

Hal-hal yang perlu dipertimbangkan dalam desain QKDN adalah:

1. Keamanan

- Penyediaan bukti keamanan protokol QKD yang ketat;
- Penyediaan sertifikasi keamanan atas implementasi QKD;
- Penyediaan langkah-langkah penanggulangan yang efektif terhadap ancaman-ancaman yang diketahui pada lapisan kuantum;
- Dukungan untuk peningkatan keamanan yang efektif pada node yang dipercaya;
- Dukungan untuk pembentukan kunci yang aman secara IT antara dua pihak jarak jauh yang terhubung ke QKDN.

2. Skalabilitas

- Dukungan untuk ekspansi jaringan yang fleksibel dan ekonomis sesuai dengan pertumbuhan layanan;
- Dukungan untuk topologi jaringan yang fleksibel demi cakupan wilayah yang luas;
- Dukungan untuk QKD satu-ke-banyak yang efisien pada jaringan akses.

3. Stabilitas

- Dukungan untuk desain, penyebaran, dan operasi QKDN yang stabil.

4. Efisiensi

- Dukungan untuk skema penyediaan dan relai kunci yang efisien;
- Penyediaan *throughput* kunci aman yang tinggi dan latensi rendah untuk memenuhi berbagai kebutuhan aplikasi keamanan.

5. Berorientasi Aplikasi

- Dukungan terhadap berbagai kebutuhan modul, pengguna, dan aplikasi;
- Penyediaan antarmuka pemrograman aplikasi (API) yang ramah bagi pengembang untuk kapabilitas QKDN;
- Memfasilitasi integrasi dengan berbagai protokol dan aplikasi TIK.

6. Ketangguhan

- Deteksi dan pemulihan kesalahan secara cepat ketika beberapa node atau *link* gagal, untuk memastikan keberlangsungan layanan.

7. Kemampuan Integrasi

- Dukungan terhadap kemampuan integrasi untuk berbagai jenis teknologi QKD.

8. Interoperabilitas

- Dukungan untuk interoperabilitas multi-vendor baik untuk modul QKD maupun modul jaringan.

9. Kemampuan Migrasi

- Dukungan terhadap kemampuan migrasi dan kelincahan kriptografi (*crypto-agility*) untuk teknologi, modul, dan implementasi QKD.

10. Kemampuan Manajemen

- Dukungan terhadap kemampuan manajemen untuk modul dalam QKDN, konfigurasi jaringan, operasi, pemantauan, perubahan, dan peningkatan QKDN.

C. KAPABILITAS JARINGAN UNTUK MENDUKUNG QKD

Sebuah QKDN harus memiliki kapabilitas-kapabilitas berikut:

1. QKDN memiliki kapabilitas untuk menyediakan kunci yang diminta kepada aplikasi kriptografi sesuai dengan spesifikasi ketersediaan dan keandalan layanan yang telah disepakati dari QKDN.
2. QKDN memiliki kapabilitas untuk mendukung keamanan dan perlindungan, termasuk mempertimbangkan kerahasiaan, integritas, keaslian, non-repudiasi, ketersediaan, dan keterlacakan.
3. QKDN memiliki kapabilitas untuk bekerja sama dengan jaringan pengguna, baik melalui manajemen yang terintegrasi maupun yang independen.
4. QKDN memiliki kapabilitas manajemen kunci.

5. QKDN yang menawarkan fungsi relai kunci harus mampu menggunakan enkripsi yang sangat aman, dengan *One-Time Pad* (OTP) direkomendasikan untuk merelai kunci.
6. QKDN memiliki kapabilitas untuk menyediakan kunci bersama bagi berbagai aplikasi terminal, selain aplikasi titik-ke-titik (P-to-P).
7. QKDN memiliki kapabilitas pengendalian dan manajemen jaringan.
8. QKDN memiliki kapabilitas untuk menyertakan antarmuka antara jaringan pengguna dan QKDN guna menyediakan kunci dalam format kunci yang sesuai untuk berbagai aplikasi.
9. QKDN memiliki kapabilitas untuk menerima permintaan kunci dari aplikasi kriptografi dalam jaringan pengguna dan menerapkan kebijakan manajemen kunci seperti menghapus atau menyimpan kunci setelah kunci disediakan.
10. QKDN memiliki kapabilitas untuk menyediakan kunci dalam format yang dipilih oleh aplikasi kriptografi dari berbagai format yang ditawarkan oleh antarmuka antara jaringan pengguna dan QKDN.
11. QKDN memiliki kapabilitas untuk menggunakan saluran serat optik atau saluran optik ruang bebas langsung untuk jaringan saluran kuantum.
12. QKDN memiliki kapabilitas untuk menggunakan saluran yang terautentikasi untuk komunikasi klasik.
13. QKDN memiliki kapabilitas untuk secara otomatis mengautentikasi dan mengoperasikan node-node QKD yang mengalami *reboot*.
14. QKDN memiliki kapabilitas untuk mengelola QoS dengan mempertimbangkan permintaan dari jaringan pengguna.

Sedangkan kapabilitas yang harus dimiliki oleh jaringan pengguna adalah:

1. Jaringan pengguna memiliki kapabilitas untuk memungkinkan permintaan kunci dari aplikasi kriptografi ke QKDN dan menerima kunci sebagai respons.
2. Jaringan pengguna memiliki kapabilitas untuk meminta kunci dengan informasi yang diperlukan (misalnya informasi tentang panjang kunci).

3. Jaringan pengguna memiliki kapabilitas untuk menyediakan informasi yang diperlukan untuk manajemen dan pengendalian QKDN melalui antarmuka yang relevan.
4. Jaringan pengguna memiliki kapabilitas untuk meminta kebutuhan QoS kepada QKDN.

D. STRUKTUR KONSEPTUAL DAN FUNGSI DASAR

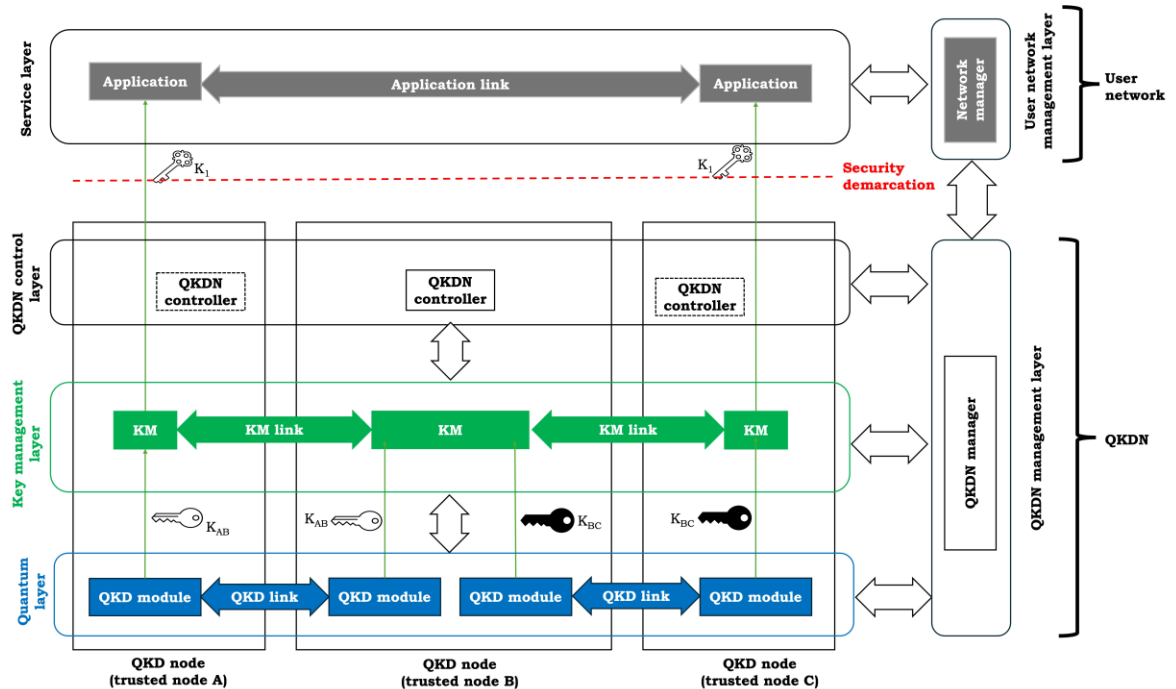
Struktur Konseptual QKDN dan Jaringan Pengguna

Tujuan utama dari QKDN adalah untuk meningkatkan keamanan komunikasi. Salah satu pendekatan utama untuk mencapai tujuan ini adalah dengan menggabungkan QKD *link* melalui node QKD untuk membagikan kunci secara aman antara node-node QKD meskipun tidak terhubung secara langsung melalui QKD *link*, dan untuk menyediakan kunci tersebut ke aplikasi kriptografi dalam jaringan pengguna.

Untuk mewujudkan tujuan berbagi kunci yang aman secara teknologi informasi (IT-secure), kunci harus diteruskan dari satu node ke node lainnya menggunakan kunci masing-masing, hingga sampai ke node tujuan. Kunci-kunci tersebut kemudian harus disimpan di node-node QKD, digunakan untuk *relay* kunci saat dibutuhkan, dan disediakan untuk aplikasi kriptografi. Seluruh operasi ini disebut sebagai manajemen kunci. Merupakan asumsi penting dalam QKDN bahwa node QKD adalah node yang dipercaya, dalam arti bahwa ia aman dari penyusupan dan serangan oleh pihak yang tidak berwenang.

Gambar 3 menggambarkan struktur konseptual dari QKDN dan jaringan pengguna. Di setiap node QKD terdapat tidak hanya modul QKD tetapi juga KM. Sepasang modul QKD dihubungkan oleh sebuah QKD *link*, dan pasangan-pasangan serta *links* ini digabungkan melalui node QKD. KM ini saling terhubung oleh KM *links* dan menyediakan fungsi manajemen kunci, termasuk kemampuan untuk *me-relay* kunci. Modul QKD, QKD *link*, KM, dan KM *link* dikendalikan oleh pengendali QKDN (QKDN controller). Rute *relay* kunci juga dapat dikendalikan oleh pengendali

QKDN. Kunci-kunci disediakan dari KM ke para pengguna, dan digunakan untuk aplikasi kriptografi dalam jaringan pengguna. Fungsi penyediaan kunci juga termasuk dalam KM. Manajer QKDN biasanya memantau dan mengelola keseluruhan QKDN.



Gambar 4.3 Ilustrasi struktur QKDN dan jaringan pengguna digambar ulang dari [12].

Dalam Gambar 4.3, kotak persegi panjang dan panah masing-masing mewakili entitas dan *link*. Modul QKD dan QKD *link* yang membawa sinyal kuantum berada dalam lapisan kuantum. KM, KM *link*, dan jalur antarmuka yang diwakili oleh panah vertikal yang terhubung ke KM membawa kunci-kunci yang memiliki perhatian keamanan khusus. Panah antara lapisan-lapisan menunjukkan bahwa entitas fungsional dalam lapisan terkait atau dalam node QKD saling bertukar informasi klasik yang dibutuhkan untuk operasi QKD, seperti status QKD *link* dan sinyal kontrol. *Link* horizontal antara elemen dalam node QKD pada lapisan kuantum dan lapisan manajemen kunci menggunakan QKD *link* dan KM *link* masing-masing, dan harus dicirikan lebih lanjut untuk keperluan desain dan operasi QKDN. Kanal kuantum pada QKD *link* dalam implementasinya adalah *link* fisik, yang digunakan untuk

mengoperasikan protokol QKD berdasarkan hukum mekanika kuantum.

Layers pada QKDN dan Jaringan Pengguna

1. Lapisan Kuantum (*Quantum Layer*)

Pada lapisan ini, setiap pasangan modul QKD yang terhubung oleh QKD *link* menghasilkan *string* bit acak simetris dengan caranya masing-masing. Setiap modul QKD mengirimkan *string* bit acak tersebut ke KM yang berada di node QKD yang sama. Setiap modul QKD juga mengirimkan parameter QKD *link* (misalnya, QBER dan lain-lain) kepada manajer QKDN. Pasangan modul QKD yang terhubung oleh QKD *link* dihubungkan melalui node QKD.

2. Lapisan Manajemen Kunci (*Key Management Layer*)

Lapisan ini mencakup KM dan KM *link*. Setiap KM berada di dalam node QKD. KM bertugas untuk menjalankan fungsi manajemen kunci. KM ini saling terhubung melalui KM *link*. KM menerima *string* bit acak dari modul QKD yang berada dalam node QKD yang sama, lalu mensinkronkan dan memformat ulang bit-bit tersebut dan menyimpannya sebagai kunci di dalam penyimpanan.

Antarmuka untuk berbagai aplikasi kriptografi telah terpasang dalam KM. KM menerima permintaan kunci dari aplikasi kriptografi, mengambil sejumlah kunci yang dibutuhkan dari penyimpanan, mensinkronkan dan mengautentikasi kunci tersebut melalui KM *link*, lalu menyediakannya dalam format yang sesuai untuk aplikasi kriptografi.

KM kemudian meminta pengendali QKDN (*QKDN controller*) untuk menentukan rute relai yang tepat. Atas kendali dari *QKDN controller*, setiap KM merelai kunci melalui KM *link*, dengan kunci lain dalam KM lain dalam enkripsi yang sangat aman (misalnya, dengan OTP). Dengan demikian, kunci-kunci ditransfer dan akhirnya disediakan ke aplikasi kriptografi. Setelah kunci diberikan ke aplikasi

kriptografi, KM harus menerapkan kebijakan manajemen kunci, seperti menghapus atau menyimpan kunci tersebut.

Dalam Gambar 4.3, relai kunci untuk membagikan kunci K1 antara node terpercaya A dan C melalui node B dicontohkan. Kunci K1 dapat berupa (1) kunci KAB yang dihasilkan antara node A dan B, atau (2) *string* bit acak, misalnya KRN, yang dihasilkan secara lokal di node A.

Dalam skenario 1, KAB direlai dari node B ke C melalui enkripsi OTP menggunakan kunci KBC.

Dalam skenario 2, KRN dikirim dari node A ke B melalui OTP dengan kunci KAB, didekripsi di node B, kemudian dienkripsi lagi dengan OTP menggunakan kunci KBC, lalu dikirim dari B ke C dan akhirnya didekripsi di C.

Dengan demikian, kunci K1 (= KAB atau KRN) dapat dibagikan antara node A dan C. KM juga dapat memiliki akses ke modul QKD dan QKD *link* untuk aktivasi, deaktivasi, pengaturan parameter, dan kalibrasi. KM menjalankan manajemen siklus hidup kunci (*key lifecycle management*).

3. Lapisan Kontrol QKDN (*QKDN Control Layer*)

Fungsi kontrol QKDN disediakan oleh pengendali QKDN (*QKDN controllers*). Fungsi-fungsi ini meliputi:

- Kontrol perutean untuk relai kunci
- Kontrol QKD *link* dan KM *link*
- Kontrol sesi untuk layanan QKD
- Kontrol autentikasi dan otorisasi
- Kontrol kebijakan kualitas layanan (QoS) dan kebijakan biaya (*charging policy*)

4. Lapisan Manajemen QKDN (*QKDN Management Layer*)

Manajer QKDN yang berada di lapisan ini memantau dan mengelola seluruh QKDN. Tugas-tugasnya meliputi:

- Manajemen gangguan (*fault*)
- Manajemen konfigurasi
- Manajemen akuntansi
- Manajemen kinerja
- Manajemen keamanan
- Manajer QKDN mengumpulkan informasi tentang kinerja modul QKD dan QKD *link* (termasuk titik relai kuantum) di lapisan kuantum, serta informasi manajemen kunci di lapisan manajemen kunci, untuk memantau kedua lapisan tersebut.

5. Lapisan Layanan (*Service Layer*)

Aplikasi kriptografi berada di lapisan ini, diberi pasokan kunci dari QKDN dan melakukan komunikasi yang aman melalui *link* aplikasi.

6. Lapisan Manajemen Jaringan Pengguna (*User Network Management Layer*)

Fungsi-fungsi dalam lapisan ini menjalankan manajemen dan orkestrasi sumber daya yang divirtualisasi maupun tidak divirtualisasi dalam jaringan pengguna.

Fungsi Dasar pada QKDN

Fungsi dasar pada QKDN adalah sebagai berikut:

1. Pembangkitan Kunci Kuantum (*Quantum Key Generation*)

QKD melaksanakan tugas-tugas berikut:

- Autentikasi modul QKD melalui kanal klasik;
- Pembuatan kunci oleh masing-masing modul QKD;
- Pengiriman pasangan kunci ke pasangan KM yang sesuai (misalnya, mendorong kunci dari modul QKD ke KM, atau KM mengambil kunci dari modul QKD) seperti digambarkan dalam Gambar 3.

2. Manajemen Kunci (*Key Management*)

Manajemen kunci melaksanakan tugas-tugas berikut:

- Penyesuaian ukuran kunci (*key re-size*), reformat kunci dengan metadata (*header* dan *footer* yang diperlukan seperti ID kunci, tanggal pembuatan, panjang kunci, dll.), dan penyimpanan kunci;
- Pengambilan parameter QKD *link*, yang dapat mencakup QBER, laju kunci (*key rate*), status *link*, dll.; parameter-parameter ini tergantung pada protokol QKD dan implementasinya;
- Relai kunci yang aman secara teknologi informasi (*IT-secure*) antar KM melalui KM *link*, misalnya dengan enkripsi OTP menggunakan kunci lain yang dihasilkan pada QKD *link* tetangga atau yang telah direlai sebelumnya;
- Sinkronisasi dan autentikasi kunci melalui KM *link*;
- Penyediaan kunci ke aplikasi kriptografi di jaringan pengguna;
- Manajemen siklus hidup kunci, termasuk ID kunci, ID modul QKD, tanggal pembuatan kunci, nama aplikasi kriptografi yang menerima kunci, tanggal penyediaan kunci, dan lain-lain.

3. Kontrol QKDN (*QKDN Control*)

Kontrol QKDN melaksanakan tugas-tugas berikut:

- Pengendalian rute relai kunci, termasuk pengalihan rute (*rerouting*) antara dua titik akhir aplikasi kriptografi yang memerlukan kunci;
- Pengendalian relai kunci berdasarkan permintaan dari lapisan layanan, dan status lapisan manajemen kunci dan lapisan kuantum;
- Pengendalian rekonfigurasi QKD *link* jika terjadi kegagalan atau penyadapan;
- Pengendalian KM dan KM *link*;
- Pengendalian modul QKD dan QKD *link*;
- Kontrol autentikasi dan otorisasi;
- Kontrol kebijakan QoS dan biaya (*charging policy*).

4. Manajemen QKDN (QKDN *Management*)

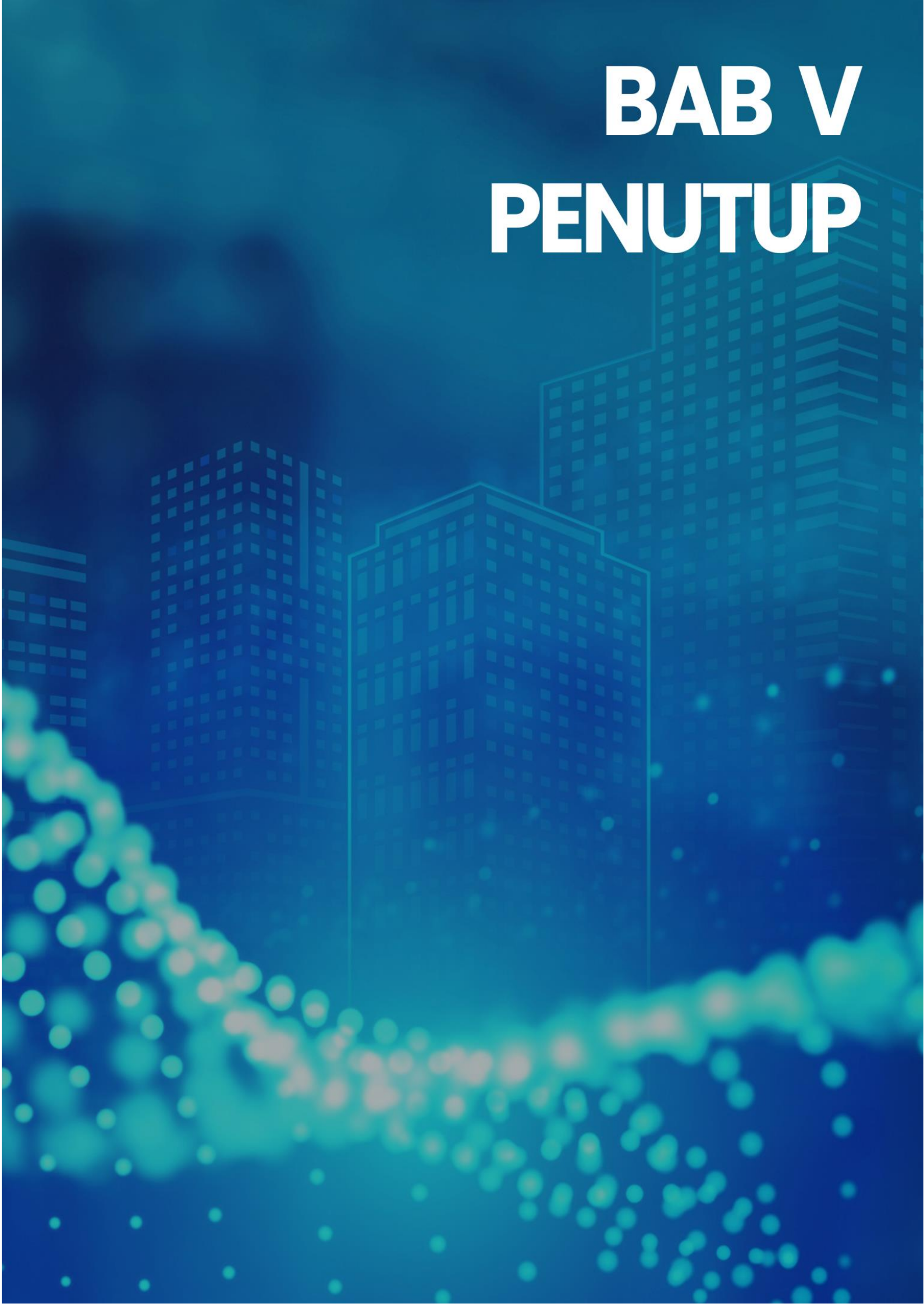
Manajemen QKDN melaksanakan tugas-tugas berikut:

- Mendukung manajemen gangguan, manajemen akuntansi, manajemen konfigurasi, manajemen kinerja, dan manajemen keamanan;
- Memantau status keseluruhan QKDN;
- Mendukung manajemen siklus hidup kunci di KM;
- Manajemen autentikasi dan otorisasi, misal manajemen identifikasi dan pendaftaran modul-modul dalam QKDN, serta hak aksesnya;
- Manajemen QoS dan manajemen biaya.



BAB V

PENUTUP



BAB V

PENUTUP

Dokumen ini disusun sebagai pengantar terhadap berbagai standar internasional yang berkaitan dengan teknologi QKD, khususnya yang diterbitkan oleh ISO/IEC, ETSI, dan ITU-T. Melalui pembahasan mengenai persyaratan keamanan, metode evaluasi dan pengujian, spesifikasi teknis, serta parameter sistem QKD, dokumen ini diharapkan memberikan pemahaman awal yang utuh bagi para pemangku kepentingan dalam mengadopsi dan mengimplementasikan QKD secara tepat dan sesuai standar internasional.

Dengan memahami cakupan dan karakteristik dari masing-masing standar, pembaca diharapkan dapat merumuskan strategi pengembangan, kebijakan, serta mekanisme evaluasi sistem QKD secara terarah dan terukur. Selain itu, dokumen ini juga dapat dijadikan acuan dalam harmonisasi kebijakan nasional terhadap dinamika dan arah perkembangan standar internasional.

Dokumen ini diharapkan dapat menjadi referensi awal dalam penyusunan kebijakan teknis dan strategis nasional, serta mendorong terbentuknya ekosistem kriptografi kuantum yang andal, aman, dan terintegrasi. Hal ini merupakan bagian dari komitmen nasional dalam membangun sistem keamanan informasi yang kuat, adaptif, dan berkelanjutan. Selain itu, pemahaman terhadap standar internasional juga menjadi kunci bagi Indonesia untuk berpartisipasi aktif dalam forum internasional, serta memastikan kesiapan nasional menghadapi tantangan dan peluang di era perkembangan teknologi kuantum.

DAFTAR REFERENSI

- [1] ISO, A. ISO/IEC 23837-1:2023 Information security — Security requirements, test and evaluation methods for quantum key distribution Part 1: Requirements, ISO, 2023.
- [2] ISO, B. ISO/IEC 23837-2:2023 Information security — Security requirements, test and evaluation methods for quantum key distribution Part 2: Evaluation and testing methods, ISO, 2023.
- [3] ETSI, “Quantum Key Distribution (QKD); Vocabulary,” ETSI Industry Specification Group (ISG), Prancis, 2018.
- [4] ETSI, “ETSI GS QKD 002 V.1.1.1 Quantum Key Distribution (QKD): Use Cases,” 2010. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/qkd/001_099/002/01.01.01_60/gs_qkd002v010101p.pdf. [Diakses 2025].
- [5] ETSI, “ETSI GS QKD 005 V1.1.1 Quantum Key Distribution (QKD): Security Proofs,” 2010. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/qkd/001_099/005/01.01.01_60/gs_qkd005v010101p.pdf. [Diakses 2025].
- [6] ETSI, “ETSI GS QKD 008 V1.1.1 Quantum Key Distribution (QKD): QKD Module Security Specification,” 2010. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/qkd/001_099/008/01.01.01_60/gs_qkd008v010101p.pdf. [Diakses 2025].
- [7] ETSI, “ETSI GS QKD 012 V1.1.1 Quantum Key Distribution (QKD): Device and Communication Channel Parameters for QKD Deployment,” 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/012/01.01.01_60/gs_qkd012v010101p.pdf. [Diakses 2025].
- [8] ETSI, “ETSI GK QKD 016 V.1.1.1 Quantum Key Distribution (QKD): Common Criteria Protection Profile – Pair of Prepare and Measure Quantum Key Distribution Modules,” 2023. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf. [Diakses 2025].
- [9] ETSI, “ETSI GS QKD 016 V2.1.1 Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules,” 2024. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/02.01.01_60/gs_QKD016v020101p.pdf. [Diakses 2025].

- [10] ETSI, “ETSI GR QKD 003 V2.1.1 Quantum Key Distribution (QKD): Components and Internal Interfaces,” 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_gr/QKD/001_099/003/02.01.01_60/gr_qkd003v020101p.pdf. [Diakses 2025].
- [11] ETSI, ETSI GS QKD 015 V2.1.1 Quantum Key Distribution (QKD); Control Interface for Software Defined Networks, France: ETSI, 2022.
- [12] ITU-T, ITU-T Y.3800 Overview on networks supporting quantum key distribution, ITU, 2019.





**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