Capítulo

4

Gestão de Chaves em Redes Quantum-Safe: QKD, KMS e Integração com Sistemas Clássicos

Adriano Maia (UFBA/QuIIN), Isys Sant'Anna (UFBA/QuIIN), Marcus Freire (UFBA/QuIIN), Thiago Mello (UFBA/QuIIN), Anderson Tomkelski (QuIIN), Gabriel Caldas (UFBA), João Souza (QuIIN), Ricardo Parizotto (UFFS), Bruno Santos (UFBA) e Maycon Peixoto (UFBA)

Abstract

As quantum communications advance, the standardization of key management has become a fundamental pillar for achieving global interoperability. This chapter analyzes the regulatory frameworks of ETSI ISG QKD and the ITU-T Y.3800 series, providing in-depth insights into the functional architecture, requirements, and operational procedures of Quantum Key Distribution Networks (QKDN). The study highlights the differences and complementarities between key delivery interfaces (REST API) and network infrastructure management. Furthermore, the chapter includes a practical section dedicated to simulating real-world scenarios using GNS3, demonstrating the configuration of IPsec security integrated with QKD systems. The chapter concludes with a synthesis of technological challenges and future trends in hybrid quantum security.

Resumo

Com o avanço das comunicações quânticas, a padronização do gerenciamento de chaves tornou-se um pilar fundamental para a interoperabilidade global. Este capítulo analisa os frameworks normativos do ETSI ISG QKD e da série ITU-T Y.3800, fornecendo uma visão ampla sobre a arquitetura funcional, requisitos e procedimentos operacionais das Redes de Distribuição de Chaves Quânticas (QKDN). O estudo destaca as diferenças e complementaridades entre as interfaces de entrega de chaves (REST API) e a gestão da infraestrutura de rede. A obra inclui ainda uma seção prática dedicada à simulação de cenários reais via GNS3, onde é demonstrada a configuração de segurança IPsec integrada a sistemas QKD. O capítulo encerra com uma síntese dos desafios tecnológicos e as tendências futuras para a segurança quântica híbrida.

4.1. Introdução

O avanço da computação quântica impõe novos desafios à segurança da informação, ao ameaçar sistemas criptográficos convencionais baseados em problemas matemáticos de difícil solução, como a fatoração de inteiros e o logaritmo discreto, tradicionalmente considerados intratáveis para a computação clássica [Ahmed et al. 2025, Easttom 2022, Nielsen and Chuang 2010]. Esse cenário evidencia a necessidade de mecanismos de proteção que não se fundamentem apenas em hipóteses de dificuldade computacional. Nesse sentido, a Distribuição Quântica de Chaves (do Inglês *Quantum Key Distribution (QKD)*) destaca-se como uma alternativa promissora para a segurança das comunicações, por basear sua proteção nas leis da mecânica quântica. Essa abordagem possibilita a geração e o compartilhamento de chaves criptográficas simétricas com segurança teoricamente incondicional, constituindo uma estratégia relevante para a proteção de dados sensíveis em cenários futuros marcados pela computação quântica [Gisin et al. 2002].

Embora a QKD ofereça garantias de segurança fundamentadas nas leis da física [Narroway 2025], sua aplicação em ambientes reais ainda esbarra em limitações tecnológicas e operacionais significativas. Entre os principais entraves, destacam-se as perdas em canais ópticos, que impõem restrições ao alcance da comunicação, as limitações na taxa de geração de chaves, a necessidade de canais clássicos autenticados e a dependência de nós confiáveis para viabilizar comunicações em longas distâncias. Além desses aspectos, sua integração com as infraestruturas de telecomunicações existentes demanda mecanismos eficientes de gerenciamento, armazenamento, sincronização e distribuição do material criptográfico. Como consequência, a QKD configura-se, essencialmente, como uma tecnologia de enlace ponto a ponto, o que exige arquiteturas de rede e soluções de gestão de chaves capazes de sustentar sua escalabilidade e favorecer sua adoção em larga escala [Dervisevic et al. 2025, Mehic et al. 2020].

Diante dessas demandas, este minicurso adota uma abordagem orientada à engenharia de redes e sistemas, com ênfase na gestão do ciclo de vida das chaves criptográficas e em sua integração com infraestruturas de segurança já consolidadas. Nessa perspectiva, são discutidas arquiteturas e iniciativas de padronização internacional, com destaque para as recomendações do *European Telecommunications Standards Institute (ETSI)* [ETSI 2019] e da *International Telecommunication Union – Telecommunication Standardization Sector (ITU-T)* [ITU-T 2019], bem como para os conceitos de *Quantum Key Distribution Networks (QKDN)* e *Key Management Systems (KMS)*. Tal abordagem permite compreender de que maneira chaves criptográficas geradas por sistemas QKD podem ser incorporadas ao plano de controle da segurança e empregadas de forma integrada a protocolos clássicos, como o IPsec.

Além da fundamentação teórica, este capítulo adota uma abordagem teórico-prática. Neste sentido, propomos uma interação em laboratório prático usando uma API REST baseada na especificação *ETSI Group Specification (ETSI GS)* QKD 014. Nesta atividade, você pode assumir o papel de *Secure Application Entitiess (SAEs)*, isto é, entidades de aplicação que consomem chaves criptográficas fornecidas pela infraestrutura de gerenciamento de chaves, abrangendo, na prática, o fluxo de solicitação, entrega e sincronização de chaves em ambientes híbridos clássico-quânticos. O laboratório inclui a implementação de uma *Key Management Entity (KME)* e a integração com uma VPN

IPsec em ambiente simulado, evidenciando a aplicação dos padrões internacionais na proteção de infraestruturas de rede. Dessa forma, pretende-se contribuir para a capacitação de estudantes, pesquisadores e profissionais no projeto, na implementação e na integração de soluções de segurança *Quantum-Safe*, promovendo o avanço das redes seguras de próxima geração.

Este capítulo está estruturado de maneira progressiva, da fundamentação teórica à experimentação prática de redes QKDN. Após a apresentação conceitual dos fundamentos do QKD e da necessidade estrutural do KMS, serão discutidos os conceitos de arquitetura e padronização, detalhando o modelo de referência da ITU-T e, logo após, a arquitetura e as interfaces de programação estabelecidas pela ETSI. Compreendida essa base de comunicação e interface, o texto aprofundará as questões de segurança e confiança do KMS, aspecto que garante a proteção e a integridade da infraestrutura. Para ilustrar os conceitos expostos, a teoria será conectada à prática por meio de uma simulação de cenário onde a segurança de uma VPN IPsec é reforçada por chaves quânticas em operação conforme com o padrão ETSI GS QKD 014, culminando em uma conclusão que aborda os desafios e o futuro da área. Essa organização foi adotada com o objetivo de explorar a essência do ecossistema QKDN, desde os fundamentos físicos até as interfaces de rede, possibilitando ao leitor condições de explorar com maior facilidade a implementação real e as futuras evoluções dessa tecnologia.

4.2. Do QKD ao Problema da Gestão de Chaves

A segurança das comunicações digitais modernas fundamenta-se historicamente no emprego de técnicas de criptografia simétrica e assimétrica [Mehic et al. 2020, Stallings 2017]. No escopo da criptografia simétrica, os processos de cifragem e decifragem exigem que a mesma chave seja mantida em estrito sigilo entre as partes comunicantes. Por outro lado, no paradigma de criptografia assimétrica (ou de chave pública), cada entidade gera um par de chaves correlacionadas matematicamente: uma pública, distribuída abertamente para o processo de cifragem, e uma privada, mantida em sigilo absoluto para a decifragem. Na prática, a criptografia simétrica é mais utilizada para cifragem, enquanto a assimétrica é utilizada para distribuir chaves para sistemas criptográficos simétricos [Gisin et al. 2002, Stallings 2017].

A resiliência da criptografia assimétrica, entretanto, baseia-se em premissas de complexidade computacional. Algoritmos amplamente adotados na proteção da Internet, como o Rivest-Shamir-Adleman (RSA) e a Elliptic-Curve Cryptography (ECC), fundamentam sua inviolabilidade na dificuldade prática de resolver problemas matemáticos de via única, notadamente a fatoração de grandes inteiros e o cálculo de logaritmos discretos. A validade desta abordagem, sob o ponto de vista da segurança prática que ela é capaz de proporcionar, baseia-se na hipótese de que a reversão de tais operações é intratável computacionalmente para a arquitetura dos processadores clássicos [Stallings 2017].

É precisamente a dependência da complexidade computacional que representa a principal ameaça contemporânea à segurança das redes. O avanço no desenvolvimento de computadores quânticos tolerantes a falhas desestabiliza essa premissa, uma vez que tais máquinas serão capazes de solucionar problemas de fatoração e de logaritmo discreto em tempo polinomial por meio da execução de algoritmos como o de

Shor [Sanz et al. 2025, Lai et al. 2023, Bhatia and Ramkumar 2020]. Por conseguinte, a infraestrutura assimétrica torna-se estruturalmente vulnerável, exigindo que a segurança de redes passe a adotar modelos imunes a esse novo vetor de ataque.

Em resposta a esse cenário, a distribuição de chaves quânticas consolida-se como uma alternativa eficaz para o estabelecimento seguro de material criptográfico [Lai et al. 2023]. Diferentemente dos criptossistemas clássicos, a QKD não pauta sua segurança pela complexidade matemática, mas sim pelas leis fundamentais da física [Elboukhari et al. 2010]. A imunidade do protocolo contra interceptações é assegurada pelo princípio da incerteza de Heisenberg e pelo teorema da não-clonagem [Sanz et al. 2025, Gisin et al. 2002]. Qualquer tentativa de medição não autorizada no canal quântico perturbará irreversivelmente o estado não ortogonal dos fótons transmitidos, induzindo um aumento na Taxa de Erro de Bits Quânticos (*Quantum Bits Error Rate (QBER)*), que será detectado pelas partes legítimas. Desta forma, a QKD extingue a incerteza probabilística da espionagem computacional quando avalia-se o ajuste do canal ao limite estatístico tolerável para a perda de bits quânticos (*qubit*) e torna-se possível classificar se a QBER corresponde a um provável produto das interferências eletromagnéticas naturais à transmissão dos fótons em canais físicos, ou se corresponde a uma provável espionagem [Lai et al. 2023].

4.2.1. O que o QKD resolve (e o que não resolve)

Sob a perspectiva da arquitetura de uma rede baseada em QKD, esta opera na chamada camada quântica [ITU-T 2019]. Contudo, a natureza do seu funcionamento permite classificá-la, por analogia ao modelo *Open System Interconnection (OSI)* [Day and Zimmermann 1984], como um protocolo de camadas física e de enlace, com a função específica de atuar como um mecanismo provável e fisicamente seguro para o estabelecimento de chaves [ITU-T 2019, Mehic et al. 2020]. O problema central que essa tecnologia soluciona é a distribuição de chaves por um canal interceptável.

A operação completa exige a coexistência de um canal quântico, responsável pela transmissão física dos qubits, e de um canal clássico, no qual ocorrem as fases análogas à camada clássica de enlace [ITU-T 2019]. A etapa de natureza física é a transmissão de fótons em um canal quântico de fibra óptica, transmissão essa que tem o seu insucesso intimamente associado às imperfeições do meio de propagação e às consequentes interferências eletromagnéticas que degradam os dados transmitidos e gera aumento na QBER [Bennett and Brassard 2014].

Para recuperar a integridade da informação, ainda com a parcela de dados corrompidos no processo físico, a processo de QKD demanda o uso do canal clássico em operação análoga à camada de enlace do modelo OSI [Mehic et al. 2020]. A QKD utiliza o canal público clássico para processar os dados brutos recebidos [ITU-T 2019, Gisin et al. 2002]. Essa fase de deputação engloba a reconciliação de bases incompatíveis (*sifting*), correção algorítmica de erros e amplificação de privacidade. Assim, consolida-se uma chave simétrica que pode ser classificada como segura, dada a impossibilidade física de espionagem não detectável, pronta para alimentar cifras como o *Advanced Encryption Standard (AES)* ou o *One-Time Pad (OTP)* [Gisin et al. 2002].

Contudo, é destacável a fragilidade da proposta perante a autenticação, visto

que o canal quântico garante o sigilo contra interceptações passivas, mas não dispõe nativamente de mecanismos que validem a identidade das partes em comunicação. A fase de reconciliação no canal clássico é vulnerável a ataques do tipo Homem no Meio (*Man-in-the-Middle (MitM)*) [Elboukhari et al. 2010], em que um adversário poderia se passar pelos usuários legítimos e estabelecer chaves independentes de origem e destino [Gisin et al. 2002]. Portanto, os protocolos de QKD requerem que as extremidades no canal clássico sejam autenticadas [Bennett and Brassard 2014]. Vale destacar que pelo produto do processo de distribuição das chaves, a adoção da QKD reintroduz a utilização de criptografia simétrica e as suas respectivas limitações de eficiência operacional.

Além das fragilidades na segurança das identidades e da ineficiência na gestão de chaves geradas, a QKD não fornece uma estrutura metodológica suficiente para um cenário prático de redes. Não há, por definição, a gestão do ciclo de vida das chaves geradas; não são impostas as políticas de acesso e as chaves não são formatadas nativamente para os padrões exigidos por protocolos como Internet Protocol Securiry (IPsec) ou *Transport Layer Security (TLS)* [ITU-T 2019, Gisin et al. 2002]. Somam-se a isso as limitações topológicas impostas pelo teorema da não-clonagem [Bennett and Brassard 2014], que impede a regeneração do sinal por amplificadores ópticos clássicos. A atenuação natural da fibra restringe o alcance a conexões ponto a ponto de distâncias limitadas [Mehic et al. 2020, Lai et al. 2023]. Escalar a rede para interligar múltiplos usuários exigiria uma infraestrutura de malha física completa, atualmente impraticável. A soma destas limitações evidencia que a QKD, isoladamente, é computacionalmente estéril para a prestação de serviços fim a fim, exigindo, obrigatoriamente, a sobreposição de uma infraestrutura clássica de orquestração.

4.2.2. Por que o KMS é necessário em sistemas QKD

A tecnologia QKD atua, por definição, com estruturas de enlaces ponto a ponto [Lai et al. 2023]. A expansão da escala de aplicação da tecnologia em redes de múltiplos nós é viabilizada pela arquitetura padronizada em um modelo de camadas lógicas independentes, as *Quantum Key Distribution Networks* [ITU-T 2019]. Essa arquitetura divide o sistema fundamentalmente em três camadas: a camada quântica, a camada de gerenciamento de chaves e as camadas de controle e gerenciamento [ITU-T 2019]. Embora a QKD, atuante na camada quântica, resolva o desafio da distribuição de chaves criptográficas seguras, esta tecnologia atua em níveis "distantes" das camadas de aplicação na rede do usuário [Mehic et al. 2020].

As aplicações nas redes dos usuários, sejam túneis IPsec, *Media Access Control Security (MACsec)* ou sistemas de criptografia simétrica, exigem chaves devidamente formatadas, exigência essa a que o fluxo de bits aleatórios brutos gerado via QKD não consegue atender de forma direta [Dervisevic et al. 2025]. O Sistema de Gerenciamento de Chaves é o sistema que atua na camada de gerenciamento de chaves de uma QKDN, responsável por entregar as chaves prontas às aplicações de rede do usuário, a partir do produto da camada quântica. Sua arquitetura, interfaces e modelos de operação serão detalhados na Seção 4.3.1.

A camada quântica fornece ao KMS cadeias de bits que são redimensionadas por meio de fatiamento ou agrupamento em blocos de tamanhos fixos exigidos pelas apli-

cações criptográficas da rede do usuário [Mehic et al. 2020]. Uma vez que os bits estão dimensionados no tamanho adequado, o KMS formata os blocos anexando-lhes cabeçalhos (*headers*) e rodapés (*footers*) lógicos com metadados úteis para a sincronização e rastreamento na rede [ITU-T 2020a]. Após a estruturação dos metadados, a cadeia de bits formatada é convertida usando codificadores padrão, como o *Base64* e envelopada em estruturas de dados legíveis pelas aplicações da rede clássica, como o formato *JavaScript Object Notation (JSON)* [ETSI 2019]. Por fim, a partir de um canal clássico de comunicação dedicado, o sistema comunica com o KMS vizinho na rede para sincronizar e autenticar as chaves formatadas, garantindo que o armazenamento de ambos os lados em comunicação possua o mesmo material redimensionado para que a chave possa estar disponível para consumo [ITU-T 2019].

Além da adaptação estrutural dos dados, a necessidade do KMS em redes quânticas fundamenta-se na superação das limitações inerentes às fragilidades das partículas quânticas em trânsito na camada física [Dervisevic et al. 2025]. O tratamento da instabilidade na geração de bits e a restrição de distância de transmissão de partículas são os pontos que sustentam a importância do sistema em uma QKDN.

Por definição, a taxa com que o meio físico de transmissão de *qubits* gera chaves é inconstante [Mehic et al. 2020]. Para evitar que as aplicação fiquem sem chaves criptográficas em momentos de execução, o KMS funciona como um estoque de chaves prontas para uso, privando o serviço de uma possível indisponibilidade por conta das oscilações físicas do hardware associado à QKD [ITU-T 2019].

O KMS também se mostra útil na superação de outro obstáculo na aplicação prática de QKDNs, que é a limitação da distância de fibra óptica, de no máximo 100 quilômetros [Mehic et al. 2020, Narroway 2025]. O KMS, propõe o tratamento desse gargalo a partir do revezamento de chaves (*key relay*) [ITU-T 2019]. Utilizando uma rede de nós intermediários, os sistemas KMS encaminham a chave nó a nó até o destino final [ITU-T 2019, Mehic et al. 2020], criptografando-a a cada salto entre nós. Desta forma, o KMS permite que aplicações em extremidades fisicamente distantes de uma rede compartilhem chaves simétricas mesmo sem uma conexão óptica direta, o que viabiliza, praticamente, uma estrutura QKDN [ITU 2023].

4.2.3. Visão geral do ciclo de vida de uma chave

A operação de uma rede QKDN e sua integração à camada de gerenciamento ocorrem ao longo do ciclo de vida do seu material criptográfico. Esse ciclo abrange a sequência de estágios que uma cadeia de bits percorre desde a sua geração física, passando pelo suprimento a uma aplicação na camada de serviço, até a sua exclusão [ITU-T 2019]. Em arquiteturas baseadas em nós confiáveis, o ciclo de vida da chave desenrola-se em um fluxo contínuo.

A geração da chave ocorre na camada quântica, onde os módulos transmissores (QKD-Tx) e receptores (QKD-Rx) executam protocolos físicos, como o BB84, ou protocolos de estados coerentes, e o processamento ocorre no canal clássico [Gisin et al. 2002]. O fluxo de bits resultante é transferido para a camada de gerenciamento, ingressando em repositórios lógicos temporários do KMS local, denominados *pickup stores* [Mehic et al. 2020, ITU-T 2019]. Para garantir a consistência, os gerenciadores de

nós adjacentes interagem por meio de canais clássicos autenticados para confirmar a exatidão e a paridade das sequências geradas. Validadas, as chaves recebem metadados para o rastreamento lógico, como identificadores únicos e *timestamps* e são promovidas para repositórios de longa permanência (*common stores*). Neste estágio, o KMS atua como um *buffer*, isolando a rede de dados das flutuações da geração óptica [Mehic et al. 2020, ITU-T 2019]. Em topologias em que as aplicações não possuem conectividade óptica direta entre si, o material entra em uma fase de revezamento. Orientados pela camada de controle da QKDN, os nós intermediários utilizam as chaves armazenadas localmente para cifrar e retransmitir a chave de serviço salto a salto. Esse processo assegura que o trânsito da chave até o destino ocorra sem que o conteúdo da chave transite em claro pela rede [ITU-T 2019].

Ao atingir os nós de borda ou quando o enlace direto é suficiente, inicia-se a fase de suprimento. Quando uma aplicação na camada de serviço, como instâncias de redes privadas virtuais, necessita de chaves, ela emite uma requisição ao KMS por meio de *Application Programming Interfaces (APIs)*. A chave e seus metadados cruzam a fronteira de demarcação de segurança (*security demarcation boundary*) que isola a QKDN da rede do usuário [ITU-T 2019]. Na rede clássica, o material quântico pode ser consumido nativamente ou injetado como uma chave simétrica, a ser mesclada a chaves derivadas de protocolos tradicionais, como IPsec, MACsec ou TLS. Essa abordagem híbrida eleva a segurança das sessões convencionais contra a decifragem quântica [Lai et al. 2023].

A etapa final do ciclo de vida é o descarte da chave. Assim que a chave é consumida pelas aplicações criptográficas ou o seu período de validade expira, as diretrizes da QKDN determinam que os bits sejam apagados dos *buffers* de armazenamento dos gerenciadores envolvidos [ITU-T 2019]. Essa destruição lógica impede a reutilização de chaves, mitigando ataques de análise estatística e preservando o sigilo adiante. Desse modo, garante-se que os dados cifrados no presente não possam ser expostos na hipótese de o hardware dos nós ser fisicamente comprometido no futuro [ITU-T 2019].

Diante da visão geral do ciclo de vida de uma chave em QKDNs, torna-se evidente a necessidade de mecanismos padronizados que assegurem a interoperabilidade, a entrega segura e o gerenciamento eficiente do material criptográfico. Nesse contexto, o ETSI, por meio do *Industry Specification Group on Quantum Key Distribution (ISG QKD)*, desempenha um papel fundamental na definição de interfaces e protocolos que viabilizam a integração da QKD com aplicações e infraestruturas de comunicação clássicas. Destacam-se, em particular, as especificações ETSI GS QKD 004 e ETSI GS QKD 014, que estabelecem, respectivamente, a interface entre sistemas de gerenciamento de chaves e aplicações e uma API baseada em REST para a entrega de chaves criptográficas. Essas normas fornecem os elementos necessários para a implementação de soluções interoperáveis e seguras, essenciais para a operacionalização de serviços baseados em QKD. Assim, as subseções a seguir apresentam uma análise detalhada dessas especificações, enfatizando suas funcionalidades, modelos operacionais e contribuições para a consolidação de redes quânticas seguras [Sáez et al. 2024, James et al. 2023].

4.3. Interfaces Padronizadas de KMS: ETSI ISG QKD

Esta seção apresenta a abordagem elaborada pela *Industry Specification Group* (ISG) da *European Telecommunications Standards Institute* (ETSI), que posiciona o KMS como serviço acessível via API, promovendo a separação entre a infraestrutura QKD e as aplicações. Introduz as entidades fundamentais do modelo ETSI: KME e SAE, detalha as especificações ETSI GS QKD 004, que definem a interface entre KMS e a aplicação, e ETSI GS QKD 014, que padroniza uma API REST para a entrega de chaves em modelo cliente-servidor. A seção conclui ao comparar as abordagens ITU-T (gestão como função de rede) e ETSI (gestão como serviço), destacando sua complementaridade.

4.3.1. Abordagem ETSI: KMS como serviço

A arquitetura da ETSI para distribuição quântica de chaves define o KMS como uma camada de abstração essencial localizada entre os módulos QKD físicos e as diversas aplicações de usuário [ETSI 2020].

Essa arquitetura é governada por uma visão *API-centric*: toda interação entre aplicações e o sistema de distribuição de chaves deve ocorrer exclusivamente por meio de APIs, independentemente do fabricante do hardware quântico ou do protocolo óptico utilizado. Essa escolha de projeto garante interoperabilidade entre equipamentos de diferentes fornecedores e desacopla o desenvolvimento de aplicações da evolução da infraestrutura física. A ETSI materializou essa visão em duas normas complementares: a ETSI GS QKD 004, orientada a fluxos contínuos de chaves, e a ETSI GS QKD 014, baseada em REST para entregas sob demanda, ambas detalhadas nas seções seguintes [ETSI 2020, ETSI 2019].

O papel fundamental do KMS é gerenciar a sincronização, o armazenamento e a exclusão de chaves, entregando-as sob demanda, como um serviço, para aplicações pares nos pontos terminais da comunicação [ETSI 2019]. Para isso, o modelo ETSI organiza a rede em duas entidades fundamentais com responsabilidades bem delimitadas: a *Key Management Entity* e a *Secure Application Entities*.

- A KME é responsável por gerenciar, armazenar e entregar chaves simétricas geradas pelos módulos QKD físicos conectados a ela. Em termos arquiteturais, a KME atua como intermediária entre o hardware quântico que produz o material criptográfico bruto por meio de protocolos como o BB84[1] e as aplicações que consomem esse material por meio de APIs padronizadas [ETSI 2020]. Do ponto de vista operacional, cada KME mantém um reservatório de chaves (*key pool*) sincronizado com a KME do nó par, garantindo que ambos os lados de uma comunicação segura disponham do mesmo material criptográfico sem que ele precise ser transmitido pela rede clássica. Uma KME pode servir simultaneamente múltiplas SAEs, controlando o acesso e evitando o reuso indevido de chaves já entregues [ETSI 2019]. Formalmente, uma KME é identificada por um `KME_ID` único na rede, e cada par

[1]O protocolo BB84, proposto por Bennett e Brassard em 1984, é o protocolo de distribuição quântica de chaves mais amplamente estudado e implementado. Ele utiliza propriedades de polarização de fótons para estabelecer uma chave secreta compartilhada entre duas partes, com segurança garantida pelas leis da mecânica quântica.

de KMEs que compartilha um enlace quântico estabelece entre si uma associação de chaves que serve de base para todas as requisições das aplicações conectadas a elas [ETSI 2019].

- A SAE é uma aplicação ou sistema que consome chaves criptográficas providas pela KME local. Exemplos típicos de SAEs incluem roteadores IPsec, servidores TLS, sistemas de criptografia de disco ou qualquer outro componente que necessite de material criptográfico de alta entropia para proteger suas comunicações [ETSI 2020]. A SAE não possui conhecimento direto sobre o funcionamento do hardware quântico, os protocolos de distribuição de chaves ou a topologia da rede. Ela interage exclusivamente com sua KME local por meio da API padronizada, tratando o sistema QKD como uma *caixa-preta* que entrega chaves sob demanda. Essa separação de responsabilidades é uma das principais vantagens arquiteturais do modelo ETSI: aplicações podem ser desenvolvidas e testadas de forma independente da infraestrutura quântica subjacente [ETSI 2020].

A interação entre KME e SAE é estruturada por meio de associações vínculos lógicos que identificam unicamente uma sessão de entrega de chaves entre um par de SAEs. O identificador dessas associações varia conforme a norma utilizada: na ETSI GS QKD 004, é denominado *Key Stream ID* (KSID); na ETSI GS QKD 014, cada chave individual recebe um *Key ID*. Ambos são implementados no formato UUID v4[2], garantindo unicidade sem necessidade de coordenação centralizada [ETSI 2020, ETSI 2019].

Vale destacar uma premissa arquitetural importante: O modelo de confiança do ETSI assume que a comunicação entre uma SAE e sua KME local ocorre dentro de um perímetro de segurança controlado tipicamente a mesma instalação física ou rede local protegida. A norma não define mecanismos de segurança para esse enlace local, delegando essa responsabilidade à infraestrutura de rede do operador [ETSI 2020, ETSI 2019]. Essa premissa é importante: ela significa que a segurança fim-a-fim do sistema QKD depende não apenas das propriedades quânticas do canal óptico, mas também da integridade física e lógica dos nós que compõem a rede.

Com as entidades e o modelo de confiança estabelecidos, é possível detalhar a primeira interface padronizada que governa sua interação: a norma ETSI GS QKD 004, que define o ciclo de vida completo de uma associação de chaves por meio de chamadas de função estruturadas.

4.3.2. ETSI GS QKD 004

A norma ETSI GS QKD 004 define a interface por meio da qual as aplicações interagem com o KMS para solicitar e consumir material criptográfico [ETSI 2020]. Como ilustrado na Figura 4.1, o KMS coordena a entrega de chaves simétricas idênticas em ambos os pontos terminais de uma sessão segura, abstraindo os aplicativos e toda a complexidade da camada quântica subjacente. Para isso, a norma estrutura essa interação em torno de três operações que definem o ciclo de vida completo de uma associação de chaves.

[2]UUID (*Universally Unique Identifier*) versão 4 é um identificador de 128 bits gerado aleatoriamente, padronizado pela RFC 4122. Sua probabilidade de colisão é suficientemente baixa para uso prático em sistemas distribuídos.

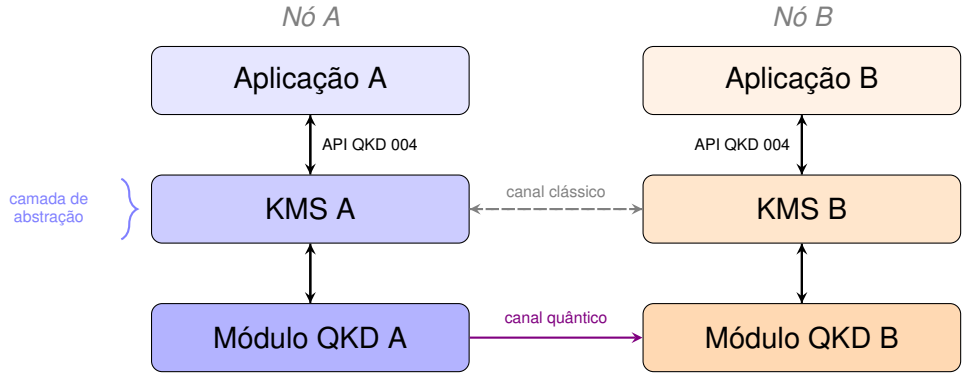

Figura 4.1. Arquitetura em camadas da norma ETSI GS QKD 004: o KMS atua como camada de abstração entre os módulos QKD físicos e as aplicações finais.

O ciclo se inicia com `OPEN_CONNECT`, que reserva uma associação identificada pelo KSID introduzido na seção anterior, um identificador que referencia o fluxo de bits sincronizados entre os pares, mas não contém nem permite derivar material criptográfico em si. Uma vez aberta a associação, `GET_KEY` permite que a aplicação recupere o material de chave correspondente: a sincronização entre os pares é garantida por um parâmetro de índice (*index*), que especifica a posição exata da chave a ser extraída no reservatório reservado, assegurando que ambos os lados obtenham o mesmo material. Por fim, `CLOSE` encerra a associação e descarta as chaves não utilizadas, seja ao término da sessão ou por expiração do tempo de vida definido, prevenindo o acúmulo de material criptográfico ocioso. A Figura 4.2 ilustra esse fluxo completo.

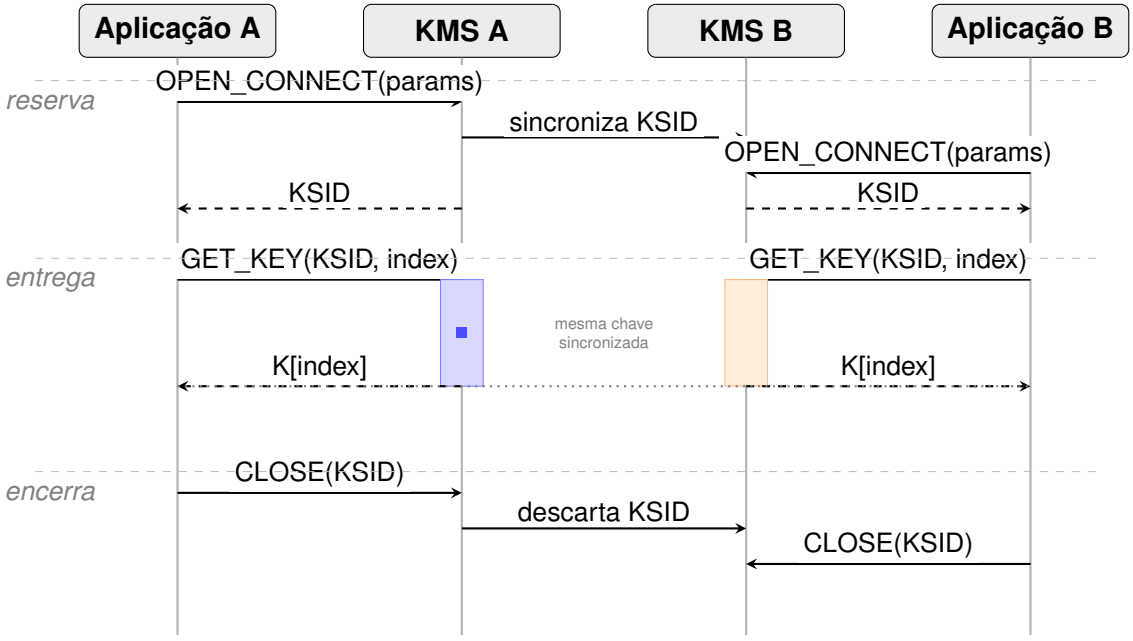

Figura 4.2. Diagrama de sequência da norma ETSI GS QKD 004: ciclo de vida completo de uma associação de chaves, desde a reserva via `OPEN_CONNECT` até o encerramento via `CLOSE`.

Aplicações distintas têm requisitos distintos de taxa, latência e janela de exposi-

ção criptográfica: um sistema de criptografia de enlaces de *backbone* exige altíssima taxa de bits e baixíssima variação temporal, enquanto uma aplicação de autenticação pontual pode tolerar taxas menores, desde que as chaves expirem rapidamente após o uso. Para acomodar essa diversidade, a norma prevê parâmetros de *Quality of Service (QoS)* negociados durante a chamada `OPEN_CONNECT`, organizados em dois grupos. O primeiro governa o desempenho: o tamanho do bloco de chave (*Key_chunk_size*), os limites de taxa de bits (*Max_bps* e *Min_bps*), a variação temporal na entrega (*Jitter*) e o nível de prioridade da requisição frente a outras em curso. O segundo governa o ciclo de vida do material criptográfico: o parâmetro Time to Live (TTL) determina por quanto tempo as chaves podem permanecer armazenadas na aplicação antes de serem descartadas, limitando a janela de exposição; os metadados complementares, como a idade da chave e o número de saltos percorridos na rede, fornecem dados de diagnóstico e estatísticas operacionais sobre a infraestrutura QKD subjacente [ETSI 2020].

A norma oferece, portanto, controle granular sobre todo o ciclo de vida das chaves e sobre os parâmetros de qualidade de serviço, mas pressupõe familiaridade com interfaces de baixo nível orientadas a chamadas de função. Para cenários que demandam uma integração mais ágil e acessível aos desenvolvedores de aplicações web, a ETSI propôs uma segunda interface, apresentada a seguir.

4.3.3. ETSI GS QKD 014: API REST para Entrega de Chaves

Diferente da abordagem orientada a fluxos contínuos da norma anterior, esta norma, ETSI GS QKD 014, define um protocolo de comunicação e formato de dados voltados à entrega de chaves por meio de uma interface REST, aproveitando convenções já consolidadas no desenvolvimento web [ETSI 2019]. Todas as interações utilizam HTTPS (TLS 1.2 ou superior), garantindo confidencialidade e integridade no transporte, e as requisições e respostas são codificadas em JSON, formato leve e amplamente suportado pelas principais linguagens e bibliotecas de programação. A API expõe três operações centrais: `Get status`, para verificar a disponibilidade de chaves no KME; `Get key`, para solicitar novas chaves; e `Get key with key IDs`, para recuperar chaves específicas a partir de seus identificadores.

O modelo de operação estrutura-se como um ciclo de requisição e resposta entre SAE e KME, com dois papéis complementares. A **Master SAE** é a aplicação que inicia a requisição de novas chaves à sua KME local e, além do material criptográfico, recebe os *Key IDs* associados a cada chave. A **Slave SAE**, após ser notificada do *Key ID* pela *Master SAE* por meio de um canal externo, utiliza esse identificador para solicitar a mesma chave à sua KME local, garantindo que ambos os lados compartilhem o mesmo material criptográfico sem que ele trafegue diretamente pela rede clássica. A Figura 4.3 ilustra o fluxo completo dessa troca, desde a solicitação inicial até a recuperação simétrica da chave.

Por adotar ferramentas familiares ao ecossistema web, a norma 014 apresenta uma barreira de entrada significativamente menor do que a 004. Enquanto a norma 004 pode ser implementada em C sem quaisquer dependências externas, a 014 se beneficia de *frameworks* de alto nível, acelerando a criação de protótipos e provas de conceito. Isso a torna especialmente adequada para ambientes de nuvem e aplicações que não exigem

o gerenciamento contínuo de fluxos de chaves, cenários em que entregas pontuais sob demanda por chamadas HTTP são suficientes. Seu objetivo central é, portanto, viabilizar a interoperabilidade entre equipamentos de diferentes fabricantes de forma simples e escalável, ampliando o ecossistema de adoção do QKD para além dos ambientes de telecomunicações tradicionais [ETSI 2019].

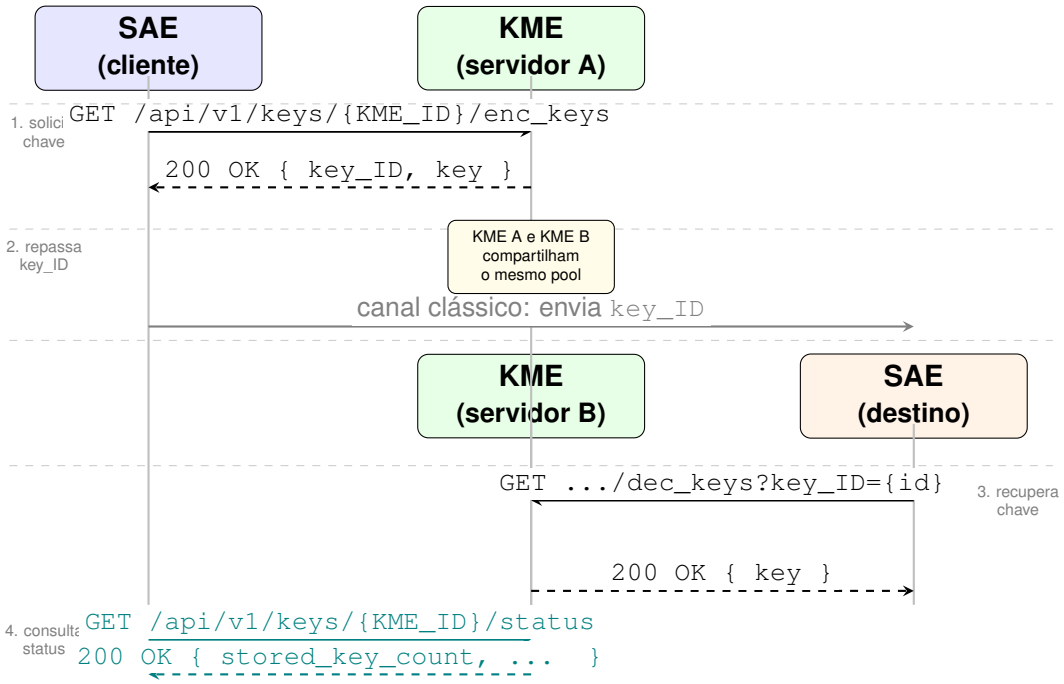

Figura 4.3. Fluxo de comunicação REST da norma ETSI GS QKD 014: a SAE cliente obtém a chave via `enc_keys`, repassa o `key_ID` pelo canal clássico e a SAE destino recupera a mesma chave via `dec_keys`.

A evolução da padronização da QKD evidencia uma abordagem complementar entre organismos internacionais distintos. Estudos recentes, como [Sáez et al. 2024], indicam que a ETSI tem desempenhado um papel fundamental na definição de interfaces, modelos de interoperabilidade e mecanismos de entrega de chaves para aplicações, promovendo a integração da QKD com infraestruturas criptográficas convencionais, como evidenciado nas especificações do ETSI ISG QKD e em análises sobre o estado da padronização da tecnologia. Em contrapartida, a ITU-T concentra-se na especificação de arquiteturas de rede, planos de controle e estruturas de gerenciamento capazes de sustentar a operação de redes QKDN em larga escala. Trabalhos como [James et al. 2023] sobre sistemas de gerenciamento de chaves em redes QKD reforçam essa distinção ao destacar a necessidade de arquiteturas escaláveis e alinhadas aos modelos da série ITU-T Y.3800 [ITU-T 2019]. Nesse contexto, a consolidação de um ecossistema global seguro depende da convergência entre essas iniciativas normativas, especialmente quanto à escalabilidade, à interoperabilidade e à gestão do material criptográfico. Assim, a próxima seção apresenta uma visão detalhada das recomendações da série ITU-T Y.3800, destacando seus modelos arquiteturais e mecanismos de controle e de gerenciamento para redes de distribuição quântica de chaves.

4.4. KMS em Redes QKD: Padronização pela Série ITU-T Y.3800

A evolução da QKD de enlaces ponto a ponto para infraestruturas de rede desloca o problema da segurança quântica do nível do enlace para o nível da arquitetura, da operação e da interoperabilidade [Sanz et al. 2025]. Quando a geração quântica de chaves precisa atender múltiplos nós, suportar retransmissão segura, integrar-se a aplicações criptográficas convencionais e operar de forma coordenada em ambientes heterogêneos, torna-se necessário definir modelos padronizados para funções, interfaces e responsabilidades ao longo da rede. Nesse contexto, a série ITU-T Y.3800 estabelece a base normativa para QKDNs, fornecendo uma visão geral da rede, requisitos funcionais, arquitetura funcional, mecanismos de gerenciamento de chaves e funções de controle e gerenciamento [ITU-T 2019, ITU-T 2020a, ITU-T 2020d, ITU-T 2020b].

A série ITU-T Y.3800 organiza a padronização de redes de distribuição quântica de chaves como um conjunto progressivo de recomendações voltadas à inserção da QKD em infraestruturas de telecomunicações. No âmbito da ITU-T, esse trabalho está associado ao *Study Group* 13 (SG13), responsável por estudos sobre arquiteturas de redes futuras, no qual a QKDN é tratada como um problema de rede que abrange estrutura conceitual, requisitos funcionais, arquitetura, gerenciamento de chaves e mecanismos de controle e gerenciamento [ITU-T 2019]. Embora outros grupos, como o SG11 e o SG17, também dialoguem com temas relevantes, tais como protocolos, sinalização, segurança e o panorama evolutivo da padronização, os documentos por eles produzidos excedem o escopo deste módulo. Nesse contexto, a série Y.3800, desenvolvida no ecossistema normativo do SG13, estabelece a base arquitetural principal para QKDN.

Assim, sua organização pode ser compreendida de forma hierárquica, como ilustrado na Figura 4.4. A recomendação ITU-T Y.3800[3] apresenta a visão geral das redes que suportam QKD e delimita aspectos como a estrutura conceitual, o modelo em camadas e as funções básicas. A Y.3801 especifica os requisitos funcionais da QKDN, a Y.3802 formaliza sua arquitetura funcional, a Y.3803 detalha o gerenciamento de chaves, considerado central para a operação significativa da rede, e a Y.3804 define as funções e os procedimentos de controle e gerenciamento da QKDN [ITU-T 2019, ITU-T 2020a, ITU-T 2020c, ITU-T 2020d, ITU-T 2020b]. Para fins de delimitação temática, este módulo concentra-se na base conceitual, funcional e operacional estabelecida por essas recomendações fundamentais.

4.4.1. Motivação para padronização de redes QKD

Apesar das garantias teóricas de segurança da QKD, sua implementação prática permanece condicionada por restrições físicas e imperfeições dos dispositivos. Em sistemas reais, perdas em canais ópticos, ruído de detecção, limitações de fontes e vulnerabilidades de implementação afetam a taxa de geração de chaves e restringem o alcance útil dos enlaces diretos. Como consequência, a operação de QKD em ampla escala não pode ser tratada apenas como um problema de prova de segurança do protocolo, mas também como um problema de arquitetura e operação de rede [Xu et al. 2020].

Essas limitações tornam insuficiente o modelo baseado exclusivamente em enlaces

[3]Doravante chamada apenas de Y.38XX.

Figura 4.4. Estrutura da série ITU-T Y.3800 para QKDNs, evidenciando a relação entre a visão geral (Y.3800), os requisitos funcionais (Y.3801), a arquitetura funcional (Y.3802), o gerenciamento de chaves (Y.3803) e os mecanismos de controle e gerenciamento da rede (Y.3804).

ponto a ponto [Narroway 2025, Ahmed et al. 2025]. Em enlaces isolados, a geração de chaves ocorre apenas entre nós diretamente conectados, o que restringe a conectividade, dificulta o atendimento a múltiplos usuários e reduz a flexibilidade operacional da infraestrutura. Além disso, a ausência prática de repetidores quânticos escaláveis faz com que, no estado atual da tecnologia, a expansão do alcance dependa de arquiteturas multi-nó com retransmissão por nós confiáveis, o que desloca o foco da simples geração de chaves para problemas de armazenamento, sincronização, retransmissão, roteamento e provisão de serviço [Cao et al. 2022, Mehic et al. 2020].

Nesse cenário, a evolução para redes QKD não responde apenas à necessidade de ampliar cobertura, mas também à necessidade de prover escalabilidade, robustez e continuidade operacional. Uma QKDN pode explorar caminhos alternativos para distribuição de chaves, suportar múltiplas aplicações e integrar diferentes tecnologias e equipamentos sob uma camada lógica comum de gerenciamento. Isso torna a padronização um requisito estrutural para garantir interoperabilidade, operação consistente e integração com redes de usuário. É nesse contexto que a série ITU-T Y.3800 se estabelece como framework normativo para QKDN, definindo estrutura conceitual, requisitos funcionais, arquitetura, gerenciamento de chaves e mecanismos de controle e gerenciamento da rede [ITU-T 2019, ITU-T 2020a, ITU-T 2020c, ITU-T 2020d, ITU-T 2020b].

4.4.2. Visão arquitetural das QKDN

A recomendação ITU-T Y.3800 estabelece a visão geral de redes que suportam QKD e delimita os aspectos necessários para sua implementação. Seu escopo abrange uma visão das tecnologias QKD, as capacidades de rede para seu suporte, a estrutura conceitual da QKDN e suas funções básicas [ITU-T 2019]. Com isso, a recomendação desloca a discussão da QKD do nível estrito do enlace físico para o nível da arquitetura de rede, no qual a geração quântica de chaves precisa ser articulada com funções de gerenciamento, controle e provisão de serviço.

A Y.3800 assume que a QKD é uma tecnologia adicional às redes de comunicação, e não um substituto completo da infraestrutura de telecomunicações. Em outras palavras, a QKDN não elimina a rede clássica, mas a complementa ao prover material criptográfico simétrico com garantias associadas à mecânica quântica. Essa formulação é importante porque situa a QKD no interior de uma arquitetura híbrida, na qual enlaces quânticos,

enlaces clássicos, funções de rede e aplicações criptográficas precisam operar de forma coordenada [ITU-T 2019].

Um modelo de comunicação elementar baseado em QKD conta com enlace ponto a ponto entre dois módulos QKD, como ilustrado na Figura 4.5. Esses módulos estão conectados por um canal quântico e por um canal clássico autenticado. Nesse arranjo, as chaves geradas são entregues localmente às aplicações criptográficas em cada extremidade. Embora esse modelo seja adequado para demonstrar o funcionamento da tecnologia, ele não atende às demandas de ambientes com múltiplos nós, usuários e requisitos de escalabilidade. É precisamente para superar essa limitação que a Y.3800 introduz o conceito de QKDN, definido como uma rede composta por dois ou mais nós QKD conectados por enlaces QKD, permitindo o compartilhamento de chaves entre nós arbitrários por meio de funções adicionais de gerenciamento e retransmissão [ITU-T 2019].

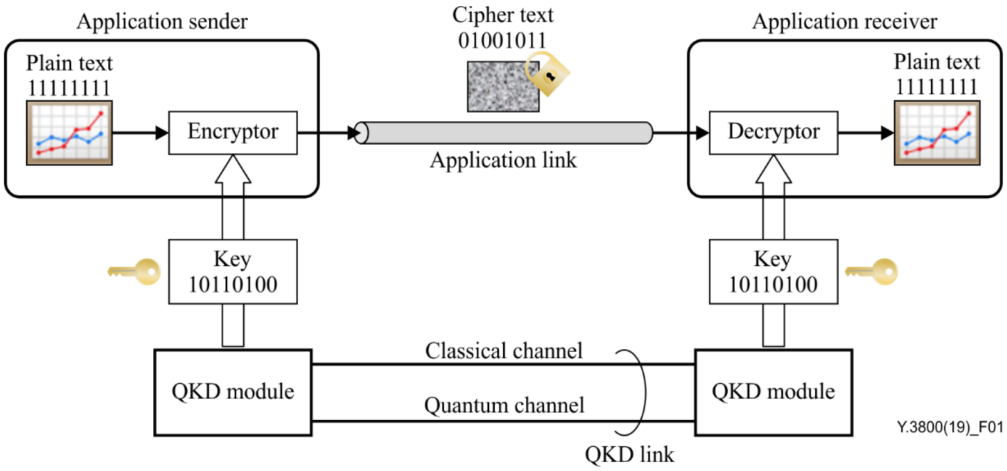

Figura 4.5. Exemplo de uso de QKD para proteção de um enlace de aplicação ponto a ponto.

Fonte: Figura 1 ITU-T Y.3800 [ITU-T 2019].

Um dos pontos centrais da Y.3800 é a distinção entre a QKDN e rede de usuário (*user network* na série). A QKDN tem por função produzir, armazenar, retransmitir e fornecer chaves. A rede do usuário, por sua vez, consome essas chaves em aplicações criptográficas, como cifragem, autenticação ou outros mecanismos de proteção. Essa separação é conceitualmente importante porque delimita duas responsabilidades distintas: a responsabilidade da infraestrutura QKDN sobre a gestão do material criptográfico e a responsabilidade da aplicação sobre o uso efetivo da chave recebida [ITU-T 2019].

A recomendação também introduz a noção de *security demarcation boundary*, isto é, uma fronteira de responsabilidade entre a QKDN e a rede do usuário. Essa fronteira é relevante porque ajuda a organizar interfaces de fornecimento de chaves, requisitos de autenticação e mecanismos de gerenciamento. Na prática, ela permite que desenvolvedores de aplicações tratem a chave como um recurso recebido da rede, sem necessidade de conhecer os detalhes internos do processo de geração e *relay* dentro da QKDN, ao mesmo tempo em que preserva a autonomia da infraestrutura QKDN quanto às suas políticas internas de armazenamento, ciclo de vida e retransmissão [ITU-T 2019].

A Y.3800 reconhece que a QKD é, por natureza, uma tecnologia ponto a ponto

sujeita a restrições físicas de alcance. Para ampliar a conectividade e a disponibilidade, a recomendação discute diferentes mecanismos de formação de rede, incluindo comutação ou divisão óptica, retransmissão por nós confiáveis (*trusted relaying*), retransmissão assistida por medição e, em uma perspectiva de longo prazo, redes totalmente quânticas com repetidores quânticos [ITU-T 2019]. No entanto, sob a perspectiva da implementação prática, a recomendação concentra sua análise em QKDNs baseadas em nós confiáveis.

Assim, os nós intermediários armazenam e retransmitem chaves entre nós adjacentes da rede, viabilizando o mecanismo de *key relay*, pelo qual chaves podem ser compartilhadas entre nós sem enlace QKD direto. Essa solução amplia o alcance e a flexibilidade topológica da rede, mas faz com que os nós intermediários passem a integrar seu domínio de confiança. Desse modo, a segurança do sistema deixa de depender apenas da integridade do enlace quântico e passa a exigir também a proteção física e lógica desses nós, o gerenciamento do ciclo de vida das chaves e a coordenação entre as funções de *relay* e *supply* [ITU-T 2019].

Uma das principais contribuições da recomendação ITU-T Y.3800 para a arquitetura de QKDN é a definição de um modelo em camadas e de um conjunto de funções básicas. A recomendação organiza as capacidades de rede necessárias ao suporte da QKD em uma estrutura conceitual composta pela camada quântica, pela camada de gerenciamento de chaves, pela camada de controle da QKDN e pela camada de gerenciamento da QKDN, além de sua relação com a camada de serviço e com a rede do usuário [ITU-T 2019].

Ainda seguindo a recomendação, a QKDN, no nível das funções básicas, deve distribuir suas principais capacidades entre as diferentes camadas. À camada quântica cabem a geração de chaves e a operação dos módulos QKD e seus enlaces. À camada de gerenciamento de chaves são atribuídas funções como redimensionamento, reformatação com metadados, armazenamento, *relay*, sincronização, autenticação e fornecimento de chaves às aplicações criptográficas. A camada de controle, por sua vez, compreende o controle de rotas de *relay*, a reconfiguração diante de falhas ou tentativas de interceptação, o controle de módulos e enlaces, além de funções de autenticação, autorização e aplicação de políticas de QoS. Por fim, a camada de gerenciamento abrange funções de monitoramento global, suporte a FCAPS (*Fault, Configuration, Accounting, Performance and Security*), gerenciamento do ciclo de vida das chaves e suporte aos mecanismos de autenticação e autorização [ITU-T 2019]. Essa decomposição é fundamental por antecipar, em nível conceitual, aspectos que serão posteriormente refinados nas recomendações subsequentes.

Em síntese, a Y.3800 fornece a moldura arquitetural. Define-se o problema de rede que a QKDN pretende resolver, delimita a relação entre infraestrutura quântica e aplicações, explicita a necessidade de *trusted nodes* e de *key relay* e estabelece a estrutura em camadas sobre a qual se apoiam os requisitos funcionais da Y.3801 e a arquitetura funcional formalizada em Y.3802.

4.4.3. Requisitos funcionais da QKDN

A recomendação ITU-T Y.3801 tem por objetivo especificar os requisitos funcionais de uma QKDN. Seu escopo abrange quatro camadas de requisitos (Figura 4.6), correspondentes à camada quântica, à camada de gerenciamento de chaves, à camada de controle

da QKDN e à camada de gerenciamento da QKDN [ITU-T 2020a]. Enquanto a Y.3800 define a estrutura conceitual e as funções básicas da arquitetura, a Y.3801 detalha os requisitos mínimos que devem ser atendidos para assegurar o funcionamento coerente da rede.

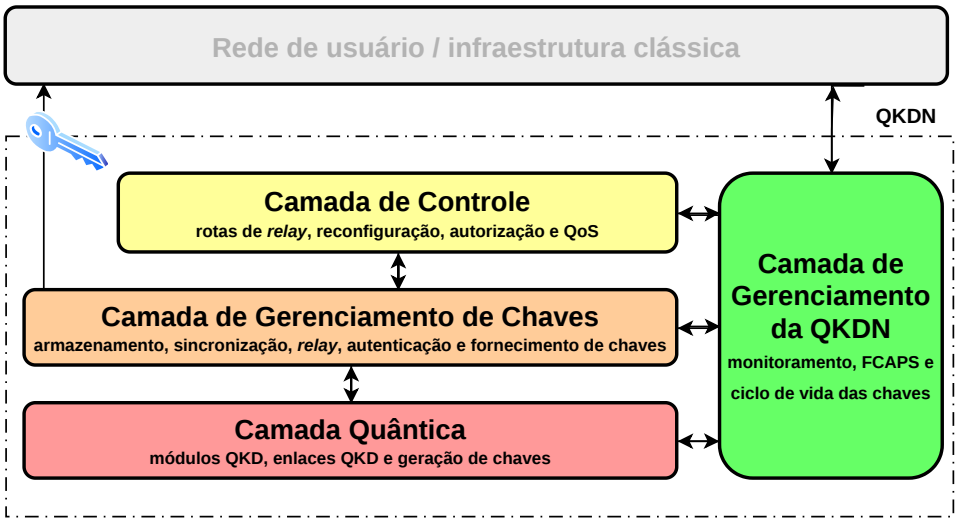

Figura 4.6. Arquitetura funcional em camadas de uma QKDN, com base na ITU-T Y.3802.

Requisitos da camada quântica: Na camada quântica, a Y.3801 estabelece que os protocolos QKD adotados devem ser comprovadamente seguros no modelo considerado e aptos a viabilizar o estabelecimento de chaves com segurança teórica da informação. Para isso, o módulo QKD deve implementar as funções necessárias à execução de um ou mais protocolos QKD com o módulo correspondente conectado por um enlace QKD, incluindo, entre outras, geração de números aleatórios, comunicação quântica, destilação de chaves e sincronização do canal [ITU-T 2020a]. A recomendação também determina que esse módulo esteja contido em um limite criptográfico bem definido, uma vez que a segurança da camada quântica depende não apenas do protocolo em abstrato, mas também da delimitação do domínio em que seus componentes e processos relevantes permanecem protegidos. Além disso, os pares de módulos QKD devem transferir as chaves geradas aos respectivos *Key Managers* (KM) por meio de interfaces apropriadas, bem como disponibilizar informações de estado, falha e desempenho às camadas superiores de controle e gerenciamento [ITU-T 2020a]. Assim, a camada quântica não se configura como um subsistema isolado, mas como um componente integrado à arquitetura da QKDN, cuja operação deve fornecer visibilidade suficiente para que a rede reaja adequadamente a degradações, falhas e eventos de segurança.

Requisitos da camada de gerenciamento de chaves: Na camada de gerenciamento de chaves, a Y.3801 estabelece os requisitos que permitem transformar as chaves geradas na camada quântica em recursos efetivamente utilizáveis por aplicações criptográficas. Nesse contexto, o *Key Manager* (KM) deve ser capaz de receber chaves dos módulos

QKD, armazená-las de forma segura quando necessário e formatá-las conforme as exigências de uso interno, de *relay* ou de *supply* [ITU-T 2020a]. A recomendação também prevê, de forma preferencial, compatibilidade com diferentes tipos de módulos QKD, favorecendo a interoperabilidade entre implementações heterogêneas. Além disso, o Key Manager (KM) deve disponibilizar informações de gerenciamento às funções de controle e gerenciamento da QKDN, bem como dados de falha e desempenho relativos a si próprio e aos enlaces de gerenciamento. Também se recomenda que suporte funções como *key relay*, *key supply* e gerenciamento do ciclo de vida das chaves [ITU-T 2020a]. Em conjunto, esses requisitos evidenciam que o KM não se limita a atuar como um repositório local, mas desempenha um papel central na articulação entre geração, armazenamento, rastreabilidade, sincronização e provisão do material criptográfico ao longo da rede.

Requisitos da camada de controle: Na Y.3801, a camada de controle deve coordenar os recursos da rede de modo a assegurar uma operação segura, estável, eficiente e robusta. Entre seus principais requisitos, destacam-se a capacidade de provisionar e controlar rotas de *relay* entre os extremos que demandam chaves, rerotear essas rotas de acordo com o estado da camada quântica e da camada de gerenciamento de chaves, controlar a configuração de módulos e enlaces e aplicar, quando pertinente, políticas de QoS e de cobrança [ITU-T 2020a]. Exigem-se mecanismos de autenticação e autorização para os elementos da rede, aspecto particularmente relevante em QKDNs baseadas em nós confiáveis, nas quais o domínio de confiança da arquitetura depende do controle consistente de identidades, papéis e permissões dos componentes sob gerenciamento do sistema.

Requisitos da camada de gerenciamento: Na camada de gerenciamento, a Y.3801 define requisitos voltados ao suporte das funções clássicas de operação de rede, com ênfase em falhas, configuração, contabilidade, desempenho e segurança. Nesse contexto, a recomendação estabelece que o gerenciador da QKDN deve ser capaz de realizar o monitoramento de falhas, a coleta e a análise de dados de desempenho, a provisão e a configuração de recursos, bem como o gerenciamento de informações de segurança relevantes para a operação da rede [ITU-T 2020a]. Além disso, atribui a essa camada o suporte ao gerenciamento do ciclo de vida das chaves e à coordenação com a camada de controle. Em conjunto, esses requisitos reforçam que a QKDN é concebida, no âmbito da série Y.3800, como uma infraestrutura de telecomunicações em sentido pleno, na qual as chaves constituem o recurso central, mas sua utilidade depende diretamente de mecanismos explícitos de observabilidade, controle, manutenção e governança operacional.

Uma das principais contribuições da Y.3801 é transformar a decomposição conceitual da Y.3800 em um conjunto de exigências funcionais que orientam a implementação de rede. A recomendação não define ainda a arquitetura funcional detalhada de cada entidade, mas prepara o terreno para isso ao explicitar o que cada camada precisa fazer para que a QKDN seja operacionalmente viável. Desse modo, a Y.3801 funciona como elo normativo entre a visão arquitetural geral da Y.3800 e a formalização da arquitetura funcional apresentada em Y.3802.

4.4.4. Arquitetura funcional da QKDN

A recomendação ITU-T Y.3802 formaliza a arquitetura funcional das redes de distribuição de chaves quânticas. Seu escopo abrange o modelo funcional da QKDN, os elementos funcionais de cada camada, os pontos de referência entre entidades, as configurações arquiteturais possíveis e os procedimentos operacionais básicos da rede [ITU-T 2020c]. Em relação à Y.3800, que define a visão geral e a estrutura conceitual da QKDN, e à Y.3801, que explicita os requisitos funcionais por camada, a Y.3802 representa a etapa em que a rede passa a ser descrita em termos de entidades funcionais, interfaces e modos de organização arquitetural.

Do ponto de vista da engenharia de redes, a importância da Y.3802 reside em transformar a QKDN em um modelo sistemático de composição funcional. Em vez de tratar a QKD apenas como um conjunto de enlaces quânticos e dispositivos especializados, a recomendação organiza a rede em camadas articuladas, cada uma com funções próprias e interfaces explícitas. Com isso, a distribuição quântica de chaves deixa de ser vista apenas como processo físico de geração de material criptográfico e passa a ser tratada como um serviço de rede sustentado por mecanismos de gerenciamento, controle e integração com aplicações [ITU-T 2020c].

A Y.3802 estabelece um modelo funcional organizado em seis camadas: camada quântica, camada de gerenciamento de chaves, camada de controle da QKDN, camada de gerenciamento da QKDN, camada de serviço e camada de gerenciamento da rede do usuário [ITU-T 2020c]. Essa organização preserva a coerência com a estrutura conceitual proposta na Y.3800, mas a aprofunda ao explicitar entidades funcionais, subfunções internas e pontos de referência para a troca de informações entre os diferentes componentes da arquitetura. Nesse modelo, a camada quântica reúne os módulos QKD e os enlaces QKD responsáveis pela geração de chaves; a camada de gerenciamento de chaves encarrega-se de recebê-las, tratá-las, armazená-las, retransmiti-las e fornecê-las às aplicações; a camada de controle coordena os recursos da rede, as rotas de *relay* e os mecanismos de reconfiguração operacional; e a camada de gerenciamento provê supervisão global, coleta de informações operacionais e suporte às funções de controle. Complementarmente, a camada de serviço abriga as aplicações criptográficas que consomem as chaves disponibilizadas pela QKDN, enquanto a camada de gerenciamento da rede do usuário representa a interface com o ambiente administrativo e operacional da rede na qual essas aplicações se inserem [ITU-T 2020c].

A Figura 4.6 evidencia que a arquitetura funcional da QKDN vai além de uma cadeia linear entre a geração e o consumo de chaves. Em vez disso, ela se organiza como uma infraestrutura em que o material criptográfico circula entre funções especializadas, acompanhado por informações de estado e desempenho, e cuja operação depende de mecanismos de controle e gerenciamento capazes de assegurar disponibilidade, rastreabilidade e coerência operacional. A separação em camadas é particularmente relevante nesse contexto, pois permite integrar a QKDN a redes clássicas preservando a distinção entre, de um lado, os processos físicos associados à QKD e, de outro, as funções de rede voltadas ao *relay*, ao *supply*, à supervisão e à coordenação do sistema.

Elementos funcionais da camada quântica: Na camada quântica, a Y.3802 descreve o módulo QKD como uma entidade composta por um conjunto de funções responsáveis tanto pela execução do protocolo quanto pela operação do enlace quântico. Entre elas, incluem-se a função de comunicação quântica, encarregada de preparar, transmitir e medir sinais quânticos; a função de sincronização do canal quântico; a função de destilação de chaves, que compreende etapas como *sifting*, estimação de parâmetros, correção de erros e amplificação de privacidade; a função de fornecimento de chaves QKD; a função de geração de números aleatórios; e a função de controle e gerenciamento do próprio módulo [ITU-T 2020c].

Essa decomposição é relevante porque explicita que a geração de chaves não é uma operação monolítica. No interior da camada quântica, a obtenção de material criptográfico seguro depende de subfunções com papéis distintos, cada uma sujeita a requisitos próprios de sincronização, processamento e monitoramento. Além disso, a recomendação admite funções opcionais, como multiplexação de canais, comutação ou divisão óptica e pontos de *relay* quântico, o que mostra que a camada quântica pode assumir diferentes formas de implementação sem abandonar a arquitetura funcional geral [ITU-T 2020c].

Elementos funcionais da camada de gerenciamento de chaves: A camada de gerenciamento de chaves ocupa posição central na Y.3802. Assim, o Key Manager deixa de ser tratado como caixa lógica única e passa a ser decomposto em duas entidades funcionais: a *Key Management Agent (KMA)* e a *Key Supply Agent (KSA)* [ITU-T 2020c]. Essa distinção tem impacto arquitetural, pois organiza de forma clara a trajetória da chave entre a camada quântica e a aplicação consumidora.

A KMA é responsável por adquirir chaves dos módulos QKD, sincronizá-las, redimensioná-las, reformatá-las com metadados, armazená-las e retransmiti-las por enlaces apropriados. Nessa entidade se concentram, portanto, as funções associadas à gestão interna do material criptográfico na QKDN. A KSA, por sua vez, atua entre a KMA e a aplicação criptográfica. Sua função é sincronizar e autenticar as chaves compartilhadas entre as extremidades e fornecê-las sob demanda às aplicações por meio da interface apropriada [ITU-T 2020c]. A recomendação também prevê, de forma opcional, a função de combinação de chaves, relevante em cenários híbridos em que a QKD pode ser associada a outros métodos de troca ou derivação de chaves.

Essa decomposição confirma que o gerenciamento de chaves é o elo estrutural entre produção quântica e provisão de serviço. Em termos de arquitetura, a QKDN só se torna operacionalmente útil porque existe uma camada dedicada a transformar sequências simétricas produzidas por módulos QKD em chaves utilizáveis por aplicações distribuídas, sob políticas de armazenamento, identificação, sincronização, *relay* e *supply*.

Elementos funcionais das camadas de controle e de gerenciamento: Na camada de controle, a Y.3802 especifica funções como controle de sessão, controle de roteamento, controle de configuração, controle baseado em políticas, controle de acesso e controle e gerenciamento do próprio controlador [ITU-T 2020c]. Em conjunto, essas funções permitem coordenar o estabelecimento dos fluxos de chaves na rede, definir rotas de *relay*

entre nós, reagir a falhas e administrar recursos de modo compatível com requisitos de QoS e de segurança.

Na camada de gerenciamento, a recomendação organiza as funções segundo o modelo FCAPS, contemplando o gerenciamento de falhas, a configuração, a contabilidade, o desempenho e a segurança [ITU-T 2020c]. Além disso, essa camada desempenha um papel transversal de suporte à operação da QKDN, incluindo o acompanhamento de seu estado global, o registro de informações de desempenho, o apoio às decisões da camada de controle e o suporte ao gerenciamento do ciclo de vida das chaves. Em conjunto, as camadas de controle e gerenciamento conferem à QKDN características de infraestrutura de telecomunicações, e não apenas de um arranjo local de dispositivos quânticos.

Pontos de referência: Na Y.3802, a interação entre as diferentes entidades funcionais da QKDN é descrita por meio de pontos de referência. Em termos arquiteturais, um ponto de referência corresponde a uma interface funcional que delimita onde e como ocorre a troca de informações entre dois componentes do sistema. Com base nesse conceito, a recomendação especifica pontos de referência nos módulos QKD, no KM, no controlador da QKDN, no gerenciador da QKDN, no gerenciamento da rede do usuário e nas aplicações criptográficas [ITU-T 2020c]. Esses pontos de referência representam, portanto, interfaces padronizadas para a troca de informações de sincronização, gerenciamento, controle, autenticação e fornecimento de chaves.

Para o propósito deste capítulo, o ponto mais importante não é a listagem exaustiva de todos os identificadores, mas a compreensão de seu papel arquitetural. Ao explicitar interfaces funcionais, a Y.3802 estabelece as condições para interoperabilidade entre componentes, separação de responsabilidades entre camadas e integração entre a infraestrutura QKDN e a rede do usuário. Em particular, a interface entre a KSA e a aplicação criptográfica é a materialização arquitetural do momento em que a chave deixa de estar sob responsabilidade exclusiva do gerenciamento interno da QKDN e passa a ser consumida como recurso de serviço.

4.4.5. Configurações arquiteturais da QKDN

Além do modelo funcional geral, a Y.3802 descreve quatro configurações arquiteturais possíveis para a QKDN. Essas configurações evidenciam que a arquitetura funcional pode ser concretizada de diferentes formas, com distintos níveis de centralização e formas de distribuição das funções entre os nós da rede [ITU-T 2020c]. Embora tais variações não modifiquem a lógica fundamental da arquitetura, elas influenciam diretamente a maneira como as funções de controle, *relay* e coordenação são organizadas e executadas no ambiente de rede.

Configuração 1 – QKDN distribuída: Nesta configuração, conforme apresentada da Figura 4.7, a QKDN adota uma organização distribuída, na qual cada nó do tipo 1 incorpora módulos QKD, um KM e um controlador da QKDN. Nesse arranjo, as funções de controle são executadas localmente, sem a necessidade de um controlador centralizado [ITU-T 2020c]. Essa configuração tende a favorecer maior autonomia operacional dos nós e maior resiliência à indisponibilidade de uma entidade central, mas também am-

plia a complexidade funcional de cada elemento da rede. Sob a perspectiva arquitetural, trata-se de uma alternativa adequada para cenários em que se busca reduzir dependências centralizadas e em que os nós dispõem de capacidade suficiente para executar localmente funções de controle, roteamento de *relay* e reconfiguração. Em contrapartida, em redes mais extensas ou com topologias mais dinâmicas, essa abordagem pode tornar mais complexa a coordenação global das decisões operacionais.

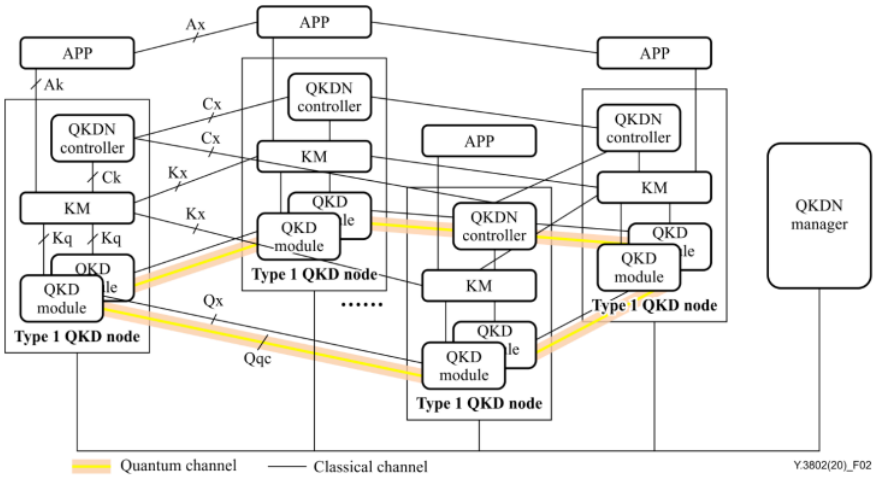

Figura 4.7. Configuração 1 da Y.3802, correspondente a uma QKDN distribuída, na qual cada nó integra módulos QKD, gerenciamento de chaves e funções de controle.

Fonte: Figura 2 ITU-T Y.3802 [ITU-T 2020c].

Configuração 2 – QKDN centralizada: já nesta configuração descrita pela Y.3802, as funções de controle são concentradas em um ou mais controladores da QKDN. A Figura 4.8 apresenta a configuração. Nesse arranjo, os nós do tipo 2 passam a abrigar apenas os módulos QKD e o KM, enquanto o controlador é tratado como uma entidade funcional separada na arquitetura [ITU-T 2020c]. Essa organização busca tornar o controle da rede mais eficiente ao deslocar decisões de roteamento, reconfiguração e aplicação de políticas para uma entidade com visão mais ampla da topologia e do estado global da QKDN. Como resultado, os nós tendem a se tornar funcionalmente mais simples, e a coordenação de *relay* e o uso global dos recursos da rede podem ser conduzidos de forma mais consistente, especialmente em cenários de maior porte. Em contrapartida, essa configuração aumenta a relevância da disponibilidade, da robustez e da proteção da entidade central de controle.

Configuração 3 – QKDN centralizada com nós hierárquicos: Na terceira configuração, a Y.3802 apresenta um modelo centralizado organizado hierarquicamente dos nós da QKDN, como apresentado da Figura 4.9. Para isso, a arquitetura passa a distinguir três tipos de nós conforme sua função predominante: *QKDN user node*, *QKDN access node* e *QKDN relay node* [ITU-T 2020c]. Essa diferenciação funcional é particularmente adequada a redes de maior escala e com cobertura geográfica mais ampla, nas quais os papéis de acesso, agregação e retransmissão tendem a se tornar mais especializados. Nesse arranjo, os nós de usuário conectam-se à rede para consumir o serviço de chaves, os nós de

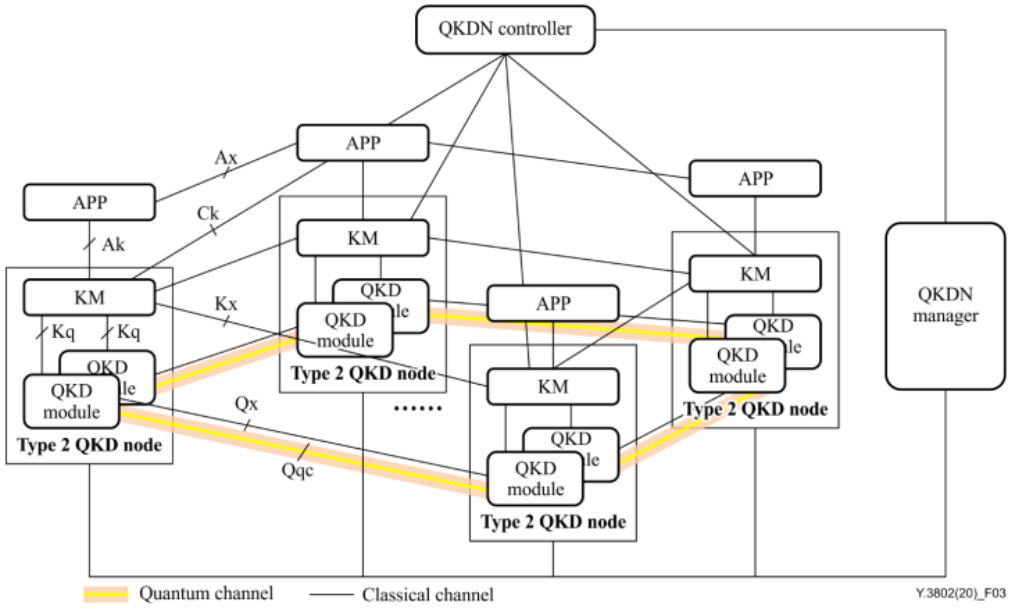

Figura 4.8. Configuração 2 da Y.3802, correspondente a uma QKDN centralizada, na qual as funções de controle são deslocadas para um ou mais controladores dedicados.

Fonte: Figura 3 ITU-T Y.3802 [ITU-T 2020c].

acesso atuam como pontos de entrada e agregação, e os nós de *relay* assumem papel mais direto na retransmissão de chaves entre diferentes segmentos da QKDN. Como resultado, a arquitetura torna-se mais compatível com cenários de implantação em larga escala, nos quais diferentes porções da rede exercem funções distintas e complementares.

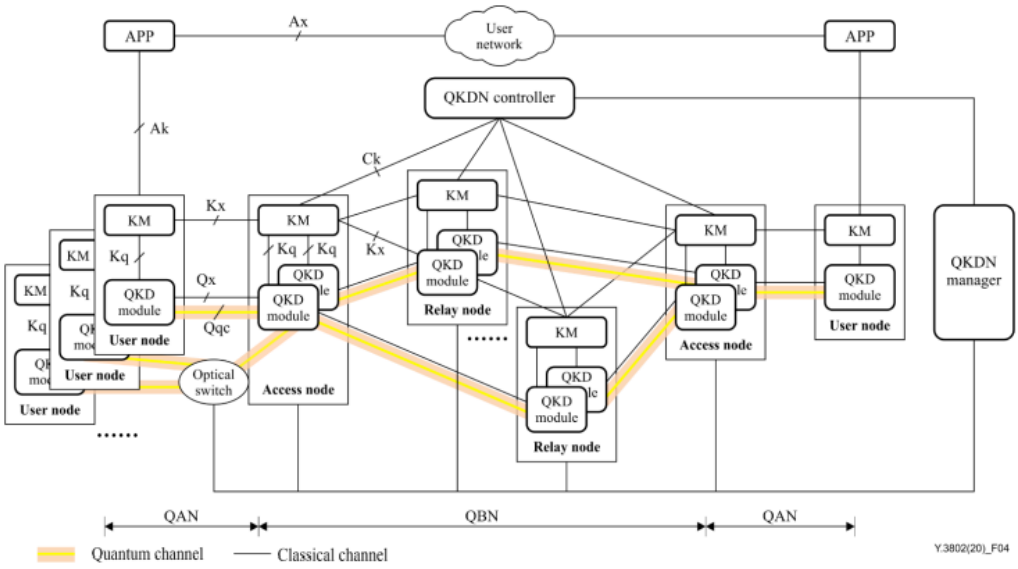

Figura 4.9. Configuração 3 da Y.3802, correspondente a uma QKDN centralizada com nós hierárquicos, distinguindo nós de usuário, de acesso e de *relay*.

Fonte: Figura 4 ITU-T Y.3802 [ITU-T 2020c].

Configuração 4 – QKDN centralizada com *relay* de chaves centralizado: Na quarta configuração, apresentada na Figura 4.10, a Y.3802 amplia o grau de centralização da arquitetura ao concentrar também a função de *relay* de chaves em uma entidade central, em vez de distribuí-la entre os nós da rede [ITU-T 2020c]. Com isso, torna-se mais nítida a separação entre as funções de geração de chaves, de gerenciamento local e de coordenação do *relay*. Essa organização pode ser especialmente vantajosa em cenários que exigem um controle global mais rigoroso do fluxo de chaves, seja para otimizar o uso de recursos, seja para aplicar políticas unificadas de *relay* ou reduzir a complexidade funcional dos nós. Em contrapartida, essa configuração aumenta a dependência de componentes centrais da arquitetura e, por isso, exige mecanismos mais robustos de gerenciamento, de proteção operacional e de tolerância a falhas.

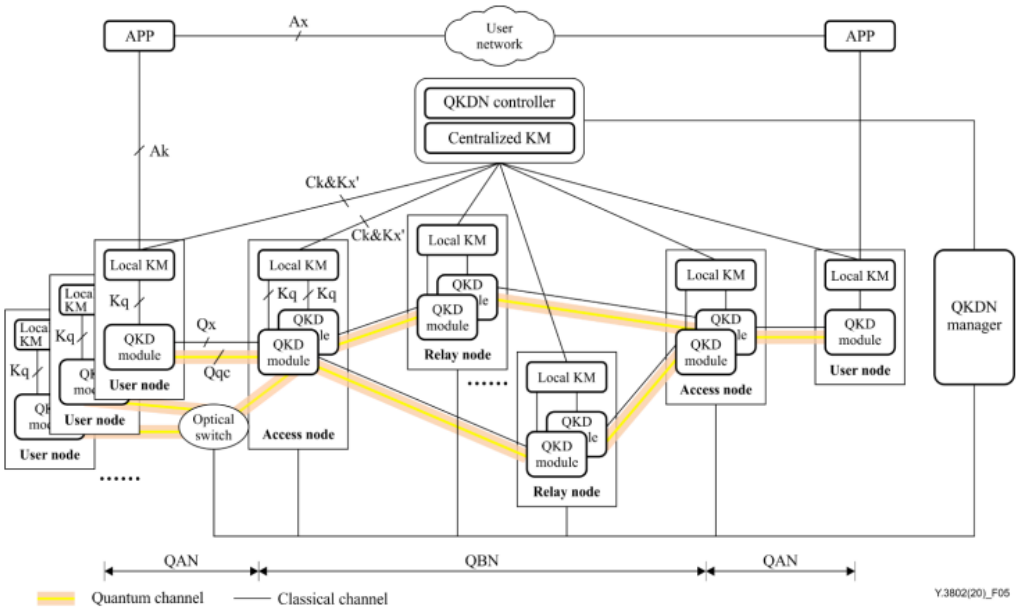

Figura 4.10. Configuração 4 da Y.3802, correspondente a uma QKDN centralizada com *relay* de chaves centralizado, na qual a coordenação do *relay* é concentrada em entidade dedicada.

Fonte: Figura 5 ITU-T Y.3802 [ITU-T 2020c].

4.4.6. Procedimentos operacionais básicos

A Y.3802 não se restringe à descrição estática dos componentes da QKDN. A recomendação também especifica procedimentos operacionais fundamentais para o funcionamento da rede, incluindo provisão de serviço e inicialização do sistema, geração de chaves, requisição e fornecimento de chaves, *relay* de chaves e reroteamento de *relay* [ITU-T 2020c]. Esse aspecto é particularmente relevante porque evidencia que a arquitetura funcional não deve ser compreendida apenas como um conjunto de entidades e interfaces, mas como um modelo normativo de operação, no qual o comportamento dinâmico da rede também é explicitamente previsto.

No procedimento de provisão e inicialização, a arquitetura prepara as entidades e os recursos necessários ao funcionamento da QKDN. Em seguida, no procedimento de geração de chaves, os módulos QKD produzem o material criptográfico e o transferem à

camada de gerenciamento de chaves. Já no procedimento de requisição e fornecimento, as aplicações criptográficas solicitam chaves e as recebem por meio das funções apropriadas da camada de *supply*. No procedimento de *relay*, por sua vez, a arquitetura viabiliza o compartilhamento de chaves entre nós que não possuem enlace direto. Por fim, no procedimento de reroteamento, a camada de controle ajusta os caminhos de *relay* diante de falhas, degradação de desempenho ou indisponibilidade de recursos, de modo a contornar enlaces ou nós problemáticos [ITU-T 2020c].

A contribuição central da Y.3802 é tornar explícito como a QKDN deve ser organizada para operar como rede. A recomendação transforma a estrutura conceitual da Y.3800 e os requisitos funcionais da Y.3801 em um arranjo coerente de camadas, entidades, interfaces, configurações e procedimentos. Nesse arranjo, o gerenciamento de chaves aparece como função estrutural, não apenas operacional, porque é ele que conecta a geração quântica de chaves ao *relay* entre nós, ao fornecimento para aplicações e à coordenação com as camadas de controle e gerenciamento. É por isso que a Y.3802 ocupa posição central na série: ela é a recomendação em que a QKDN passa a existir, de fato, como arquitetura funcional padronizada.

4.4.7. Gerenciamento de chaves na QKDN

A recomendação ITU-T Y.3803 especifica o gerenciamento de chaves em redes de distribuição de chaves quânticas. Seu escopo cobre a visão geral do gerenciamento de chaves, os elementos funcionais associados a essa atividade, as operações de gerenciamento e os formatos de chave utilizados na QKDN [ITU-T 2020d]. No encadeamento da série Y.3800, essa recomendação ocupa posição central porque traduz, em termos operacionais, a função que conecta a geração quântica de chaves ao seu uso por aplicações criptográficas em rede.

A própria Y.3803 afirma que o gerenciamento de chaves é a questão de maior prioridade para a operação eficiente e segura de uma QKDN, pois, sem ele, a maior parte das operações e serviços significativos da rede não pode ser realizada [ITU-T 2020d]. Essa observação é arquiteturalmente relevante. A utilidade prática da QKD em rede não decorre apenas da capacidade de módulos QKD produzirem cadeias simétricas de bits, mas da capacidade da rede de receber esse material, tratá-lo, armazená-lo, retransmiti-lo entre nós, sincronizá-lo entre extremidades e fornecê-lo de forma confiável às aplicações. Nesse sentido, a Y.3803 é a recomendação em que o KMS aparece de forma mais explícita como função estruturante da QKDN.

Modelo funcional interno da camada de gerenciamento de chaves: A Y.3803 não trata o *Key Manager* como uma entidade monolítica. Antes de detalhar operações como armazenamento, *relay* e fornecimento de chaves, a recomendação propõe uma decomposição funcional da camada de gerenciamento de chaves, ilustrada na Figura 4.11. Essa decomposição, alinhada à arquitetura funcional definida na Y.3802, torna explícita a separação entre três conjuntos de responsabilidades no interior do KM: as funções voltadas à gestão interna do material criptográfico, incluindo recebimento, organização, armazenamento e controle do ciclo de vida das chaves; as funções responsáveis pelo fornecimento de chaves às aplicações criptográficas; e as funções de comunicação do KM com as cama-

das de controle e de gerenciamento da QKDN, por meio das quais circulam informações operacionais, de coordenação e de supervisão [ITU-T 2020c, ITU-T 2020d].

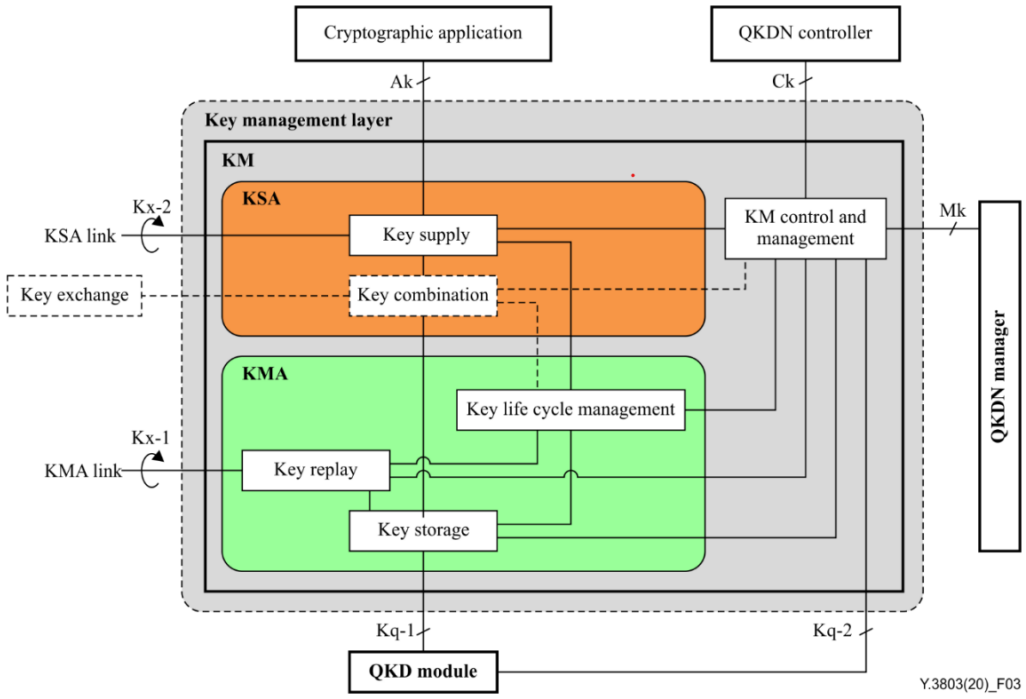

Figura 4.11. Modelo funcional da camada de gerenciamento de chaves na QKDN, com destaque para a decomposição do KM em KMA, KSA, função de controle e gerenciamento do KM, enlaces KMA/KSA e a fronteira de demarcação de segurança entre o KSA e a aplicação criptográfica.

Fonte: Figura 3 ITU-T Y.3803 [ITU-T 2020d].

Segundo a Y.3803, é conveniente identificar dois elementos funcionais no interior do KM: o *Key Management Agent* e o *Key Supply Agent* [ITU-T 2020d]. O KMA é responsável pela gestão interna das chaves no âmbito da QKDN. Para isso, recebe as chaves provenientes dos módulos QKD, participa da interconexão entre os nós da rede por meio de *key relay* e executa funções de armazenamento, retransmissão e gerenciamento do ciclo de vida das chaves. Assim, é no KMA que a chave deixa de ser tratada apenas como resultado do processo quântico de geração e passa a constituir um recurso gerenciado pela infraestrutura de rede [ITU-T 2020d].

O KSA, por sua vez, localiza-se entre o KMA e a aplicação criptográfica e realiza a função de *key supply*. A recomendação o descreve como a entidade que abriga interfaces para diferentes aplicações criptográficas e que pode, opcionalmente, incluir a função de *key combination*, na qual uma chave vinda do KMA é associada a outra chave proveniente de método externo de troca, preservando o nível de segurança da chave de entrada proveniente do KMA [ITU-T 2020d]. Essa possibilidade é relevante em cenários híbridos de integração entre QKD e outros mecanismos de distribuição de chaves.

Além das funções desempenhadas por KMA e KSA, o KM também incorpora a função de *KM Control and Management*, responsável pela articulação da camada de gerenciamento de chaves com os demais componentes da arquitetura da QKDN. Segundo a Y.3803, essa função estabelece a comunicação do KM com os módulos QKD, com o

controlador da QKDN e com o gerenciador da rede [ITU-T 2020d]. Sua relevância decorre do fato de que o gerenciamento de chaves não ocorre de forma isolada: ele depende do recebimento de informações da camada quântica, da disponibilização de informações operacionais às camadas superiores e da cooperação com funções de controle e gerenciamento associadas às decisões de *relay*, rerroteamento e supervisão da rede.

A norma Y.3803 também refina a noção de enlace do KM. Em vez de um único *KM link* indiferenciado, a recomendação estabelece que esse enlace é composto por um *KMA link* e um *KSA link* [ITU-T 2020d]. O KMA link conecta KMAs para realizar *relay* e outras comunicações de gerenciamento. O *KSA link* conecta KSAs para sincronização e verificação de integridade antes do fornecimento da chave à aplicação. Essa separação ajuda a distinguir o domínio do gerenciamento interno do material criptográfico do domínio de sua preparação final para consumo no plano de serviço.

A Figura 4.11 também destaca um aspecto arquitetural fundamental: a *security demarcation boundary* estabelecida entre o KSA e a aplicação criptográfica. Essa fronteira define o ponto em que a responsabilidade pela chave deixa de pertencer à infraestrutura da QKDN e passa a ser atribuída à aplicação que a utiliza [ITU-T 2020d]. Até esse limite, a chave permanece sujeita às políticas de armazenamento, sincronização, rastreabilidade e eliminação estabelecidas pelo gerenciamento da QKDN. A partir do *key supply*, entretanto, seu uso passa a ser regido pela lógica operacional da aplicação consumidora.

4.4.8. Operações de gerenciamento de chaves

Uma vez definido o modelo funcional interno do KM, a norma Y.3803 passa a descrever as operações que compõem o gerenciamento de chaves. A recomendação organiza essas operações em torno da trajetória da chave desde sua geração na camada quântica até seu uso pela aplicação criptográfica, abrangendo aquisição, autenticação, armazenamento, *relay*, fornecimento, reroteamento e gerenciamento do ciclo de vida [ITU-T 2020d]. A Figura 4.12 sintetiza as principais operações de gerenciamento e as interações entre KMA, KSA, os módulos QKD, o controlador, o gerenciador da rede e a aplicação criptográfica. Essa sequência de operações transforma o modelo funcional da Figura 4.11 em um fluxo operacional de rede.

Aquisição, autenticação, armazenamento, formatação e metadados: A Y.3803 trata a aquisição e o armazenamento de chaves como um processo estruturado, e não como simples gravação local de sequências de bits. Na camada quântica, cada par de módulos QKD gera uma *QKD-key*, entendida como a sequência simétrica de bits antes de qualquer redimensionamento ou formatação no *Key Manager*. Como diferentes pares de módulos QKD podem empregar protocolos distintos e produzir unidades de chave com comprimentos diferentes, a recomendação estabelece que, já no módulo QKD, os metadados sejam anexados à *QKD-key*, formando um *key file*, que é então transferido ao KMA correspondente [ITU-T 2020d].

No KMA, a primeira etapa é receber os *QKD-key files* do ponto de referência *Kq-1*. Como os comprimentos dessas chaves podem variar, a Y.3803 recomenda que o KMA padronize as *QKD-keys*, combinando ou dividindo os bit *strings* em chaves de comprimento unitário prescrito, adequado à política interna de gerenciamento e ao uso posterior

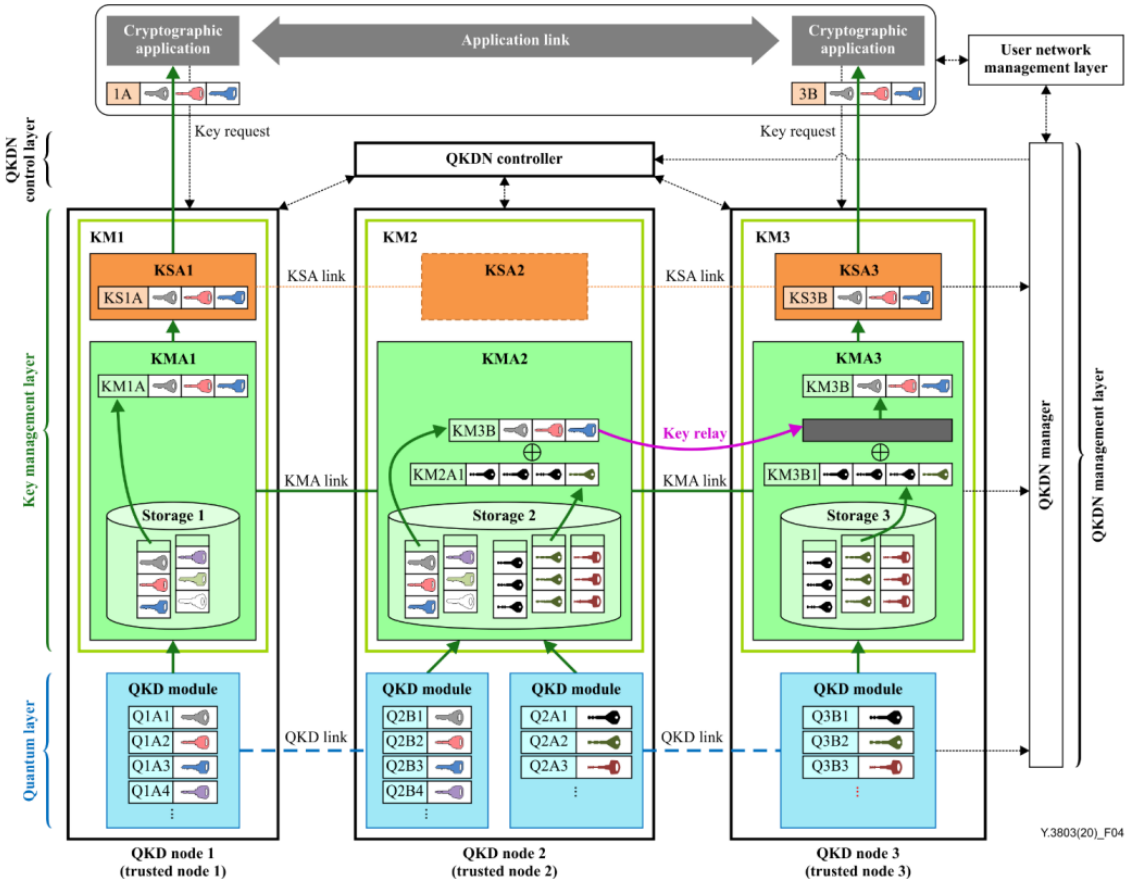

Figura 4.12. Principais operações de gerenciamento de chaves em uma QKDN. A figura ilustra o percurso da chave desde sua geração na camada quântica, passando pela aquisição pelo KMA, pelas funções de *relay* e sincronização, até sua entrega (*key supply*), em articulação com funções de controle e gerenciamento da rede.

Fonte: Figura 4 ITU-T Y.3803 [ITU-T 2020d].

na rede. Antes do armazenamento definitivo, essas chaves formatadas são mantidas temporariamente em um *buffer* [ITU-T 2020d]. Esse detalhe é importante, pois mostra que a formatação não é uma operação opcional, mas parte constitutiva da transição da chave do domínio de geração quântica para o domínio de gerenciamento de rede.

A recomendação também exige que o armazenamento definitivo seja precedido da verificação da identidade da chave entre os KMAs correspondentes. Assim, os KMAs autenticam-se mutuamente por meio do *KMA link*, e um deles envia ao outro uma requisição de autenticação contendo o identificador da *QKD-key* e um valor de verificação, como um *hash* criptográfico ou um *message authentication code*. O KMA par, então, realiza sincronização em posição de bits e autenticação do conteúdo armazenado em *buffer*, comparando o valor recebido com o calculado localmente. Se os valores coincidirem, as chaves *buffered* são finalmente armazenadas como *KMA-key*, acompanhadas de metadados no diretório de armazenamento; caso contrário, o material é abortado [ITU-T 2020d].

Esse ponto é central para compreender a diferença entre *QKD-key* e *KMA-key*. A primeira corresponde ao material oriundo diretamente dos módulos QKD. A segunda

corresponde à chave já admitida no domínio de gerenciamento do KMA, após recepção, reformatação, sincronização e autenticação. Portanto, o KMA não apenas guarda a chave, mas a transforma em um objeto gerenciável pela arquitetura da QKDN [ITU-T 2020d].

A Y.3803 também formaliza a noção de *key file* como o conjunto lógico composto por dados-chave e metadados. Essa estrutura é necessária para manter a interconectividade e a expansibilidade na QKDN, pois os metadados não servem apenas para identificação local. Eles também sustentam comunicações entre KMAs, KSAs, aplicações criptográficas, controlador e gerenciador da rede [ITU-T 2020d]. Para a *QKD-key*, a recomendação inclui, como metadados básicos, o identificador da chave, além de campos opcionais, como o comprimento, o identificador do módulo QKD, o identificador do módulo correspondente, o *timestamp* de geração e o *hash* da chave. Para a *KMA-key*, são previstos, entre outros, identificador único na QKDN, comprimento, tipo da chave, identificador do KMA, identificador do KMA correspondente, *timestamp* de geração, referência ao módulo QKD de origem e *hash* da chave [ITU-T 2020d].

Do ponto de vista arquitetural, isso significa que o armazenamento de chaves na Y.3803 é inseparável da formatação e dos metadados. A chave não é mantida apenas como sequência de bits secretos, mas também como entidade identificável, sincronizável e rastreável, apta a participar de operações posteriores de *relay*, *supply* e de gerenciamento do ciclo de vida. É essa estrutura que permite ao KMS operar de forma interoperável, auditar a trajetória da chave e oferecer suporte às camadas de controle e gerenciamento da QKDN.

Relay entre KMAs: Quando dois nós não possuem enlace QKD direto, a QKDN depende do *key relay* para permitir o compartilhamento de chaves entre extremos arbitrários. A Y.3803 trata essa operação como função central do KMA, realizada por meio de KMA links entre nós confiáveis [ITU-T 2020d]. Do ponto de vista arquitetural, isso significa que o KMA não apenas armazena chaves localmente, mas também participa da extensão lógica da rede ao retransmitir material criptográfico entre segmentos distintos da QKDN.

O *relay* também evidencia a interdependência entre Y.3803 e Y.3804. Embora o conteúdo criptográfico permaneça sob responsabilidade do gerenciamento de chaves, a viabilidade do *relay* depende do suporte do controlador da QKDN para a definição e a manutenção das rotas apropriadas. Assim, a Y.3803 trata o *relay* como uma operação de gerenciamento de chaves, mas essa operação é sustentada por decisões de controle e de gerenciamento de rede [ITU-T 2020d, ITU-T 2020b]. Essas decisões podem incluir o re-roteamento do *relay* entre KMAs quando a rota inicialmente escolhida deixa de ser operacionalmente adequada. A recomendação indica que isso pode ocorrer, por exemplo, quando a quantidade de chaves disponíveis em um nó intermediário fica abaixo de um limiar, quando há falha em KM ou em *KMA link*, ou quando um aumento de QBER em determinado enlace QKD reduz ou impede a geração de chaves necessárias para sustentar a rota em uso [ITU-T 2020d]. Nesses casos, a camada de gerenciamento de chaves precisa cooperar com o controlador e com o gerenciamento da QKDN para reconfigurar o caminho lógico do *relay* e preservar a continuidade do serviço de chaves.

Fornecimento e ciclo de vida de chaves: Se, por um lado, o *relay* amplia a conectividade da QKDN, por outro, o *key supply* materializa sua utilidade como serviço. A recomendação define essa operação como a entrega da chave à aplicação criptográfica por meio do KSA [ITU-T 2020d]. Para isso, o KSA sincroniza as chaves entre as extremidades, verifica a integridade via *KSA link* e então as fornece à aplicação pela interface apropriada. É nesse ponto que a QKDN se apresenta ao plano de serviço não mais como rede interna de gerenciamento, mas como provedora de recurso criptográfico utilizável por protocolos, sistemas e aplicações.

Por fim, a recomendação integra todas essas operações ao conceito de ciclo de vida da chave. O *Key Life Cycle* é definido como a sequência de etapas que a chave percorre desde sua recepção pelo KM, passando por armazenamento, formatação, *relay*, sincronização, autenticação e *supply*, até sua eliminação ou preservação conforme a política vigente [ITU-T 2020d]. Essa formulação reforça que o gerenciamento de chaves em uma QKDN não é apenas manipulação pontual de bit strings, mas governança contínua de um recurso criptográfico distribuído.

Síntese da contribuição da Y.3803: A organização da subseção em dois níveis, modelo funcional e operações, reflete a própria lógica da Y.3803. Primeiro, a recomendação mostra como o KM é decomposto em KMA, KSA, função de controle e enlaces específicos. Depois, mostra como esses elementos executam aquisição, armazenamento, *relay*, *supply*, rerroteamento e gerenciamento do ciclo de vida [ITU-T 2020d]. Essa sequência é importante porque permite compreender por que o KMS não deve ser interpretado como um simples repositório de chaves, mas como uma função estrutural da rede, responsável por transformar a geração quântica de bits em provisão segura, rastreável e interoperável de chaves para aplicações distribuídas.

4.4.9. Controle e gerenciamento da QKDN:

A recomendação ITU-T Y.3804 especifica as funções e os procedimentos de controle e gerenciamento das redes de distribuição de chaves quânticas. Seu escopo cobre os elementos funcionais de controle, gerenciamento e orquestração da QKDN, as funções associadas a esses elementos e os procedimentos necessários para sustentar a operação da rede [ITU-T 2020b]. No encadeamento da série Y.3800, essa recomendação complementa a arquitetura funcional definida em Y.3802 ao explicitar como a rede deve ser supervisionada, coordenada e mantida em operação diante de falhas, degradação de desempenho, variações de disponibilidade e requisitos de segurança.

Do ponto de vista arquitetural, a Y.3804 é importante porque consolida a QKDN como uma infraestrutura de telecomunicações gerenciável. Se a Y.3803 mostra como o material criptográfico é armazenado, sincronizado, retransmitido e fornecido às aplicações, a Y.3804 mostra como a rede que sustenta essas operações é controlada e gerenciada como um todo. Portanto, a recomendação desloca a discussão do domínio do fluxo de chaves para o domínio da governança operacional da infraestrutura que produz, distribui e entrega essas chaves.

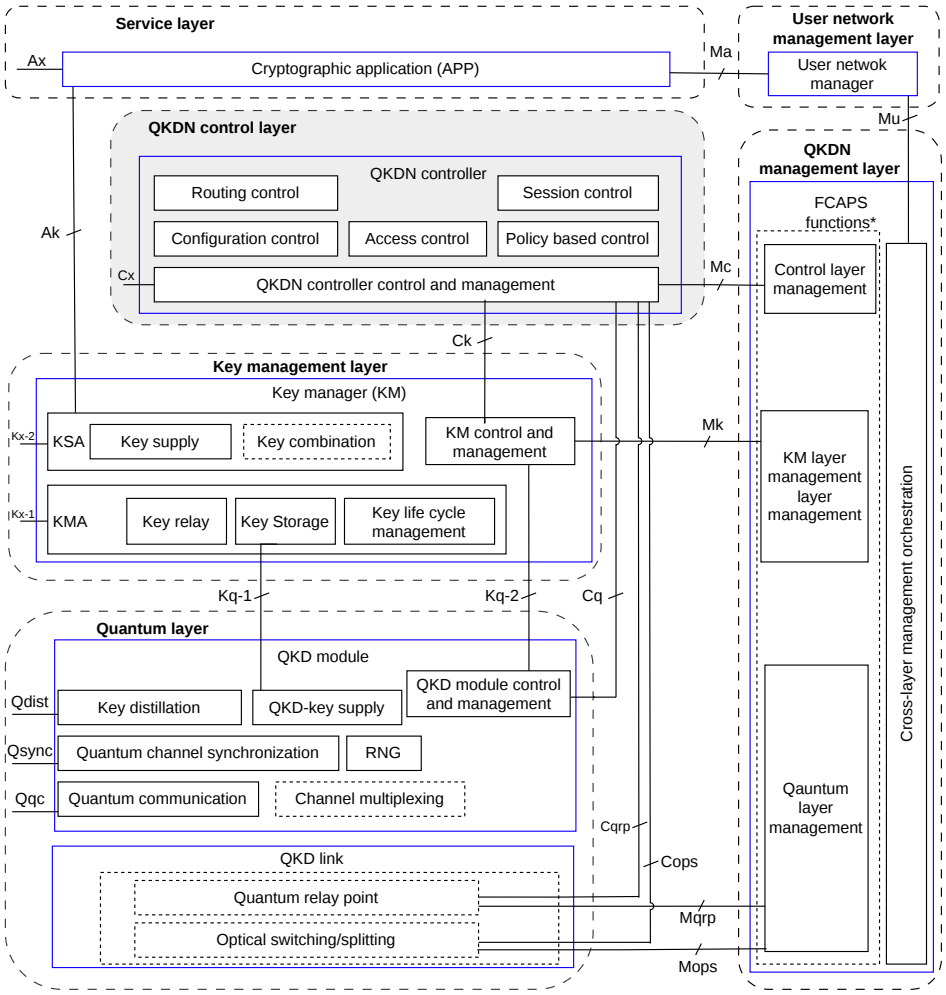

Figura 4.13. Elementos funcionais e pontos de referência relevantes para o controle e o gerenciamento da QKDN.

Fonte: Figura 1 ITU-T Y.3804 [ITU-T 2020b].

Arquitetura funcional de controle e gerenciamento: A Y.3804 organiza o problema em torno de duas esferas funcionais: a camada de controle da QKDN e a camada de gerenciamento da QKDN [ITU-T 2020b]. A camada de controle atua sobre os recursos da rede para garantir operação segura, estável, eficiente e robusta. A camada de gerenciamento, por sua vez, supervisiona a rede como um todo, coleta informações de múltiplas camadas, sustenta decisões operacionais e provê mecanismos de orquestração entre diferentes domínios funcionais.

A Figura 4.13 deve ser posicionada nesta subseção, pois sintetiza os elementos funcionais e os pontos de referência mais relevantes para o controle e o gerenciamento da QKDN. Em especial, ela evidencia que a recomendação não trata apenas de monitoramento passivo, mas de uma estrutura explícita de interação entre controlador, gerenciador, camada quântica, camada de gerenciamento de chaves e rede do usuário.

A recomendação define, para fins de controle, pontos de referência como *Cx*, *Ck*,

Cq, *Cops* e *Cqrp*, empregados na comunicação entre o controlador da QKDN e os componentes sob controle. Para fins de gerenciamento, define pontos de referência como *Mq*, *Mqrp*, *Mops*, *Mk*, *Mc*, *Mx* e *Mu*, empregados na comunicação entre o gerenciador da QKDN e os elementos sob gerenciamento [ITU-T 2020b]. Essa explicitação de interfaces é importante porque transforma o controle e o gerenciamento em funções arquiteturalmente observáveis, integráveis e interoperáveis.

Funções da camada de controle: A Y.3804 atribui à camada de controle cinco funções principais: controle de roteamento, controle de configuração, controle baseado em políticas, controle de acesso e controle de sessão [ITU-T 2020b]. Em conjunto, essas funções permitem que a rede ajuste dinamicamente o uso de recursos e mantenha a continuidade do serviço de chaves.

A função de roteamento é especialmente relevante em QKDNs baseadas em *trusted nodes*, pois é responsável por provisionar rotas apropriadas de *key relay* entre os extremos e por rerroteá-las quando a camada quântica ou a camada de gerenciamento de chaves indica degradação ou indisponibilidade [ITU-T 2020b]. Para isso, o controlador mantém informações de endereçamento de nós, identifica KMs envolvidos, consulta o consumo e o estoque residual de chaves, recebe parâmetros dos enlaces QKD e combina essas informações com a topologia global da rede. O resultado é uma decisão de *relay* que não depende apenas da conectividade física, mas também da disponibilidade efetiva de recursos criptográficos ao longo do caminho.

A função de configuração controla o estado de módulos e enlaces, incluindo a ativação, a desativação, a reserva e a reconfiguração. A recomendação relaciona esse ponto a situações em que falhas ou alterações de condição, como o aumento de QBER ou a perda de enlace, exigem a recomposição da infraestrutura operacional [ITU-T 2020b]. A função baseada em políticas, por sua vez, associa o uso da rede a critérios como QoS, prioridades e cobrança. Já a função de controle de acesso estabelece mecanismos de autenticação e autorização para componentes da rede, o que é especialmente importante em uma arquitetura cujo domínio de confiança depende de uma coordenação rigorosa entre nós, módulos QKD, KMs e aplicações. Por fim, a função de controle de sessão apoia o estabelecimento de fluxos de *relay* e de *supply*, articulando-se ao gerenciamento de chaves e às políticas da rede [ITU-T 2020b].

Um ponto conceitualmente importante da recomendação é a afirmação explícita de que o controlador da QKDN **não lida diretamente com as chaves**. As chaves são fornecidas do KM à aplicação criptográfica, enquanto o controlador estabelece as condições para que o *relay* e o *supply* ocorram de forma contínua e com coerência operacional [ITU-T 2020b]. Essa distinção preserva a separação arquitetural entre o domínio do material criptográfico e o da coordenação da rede.

Funções da camada de gerenciamento: Na camada de gerenciamento, a Y.3804 estrutura as funções segundo a lógica FCAPS, cobrindo falhas, configuração, contabilidade, desempenho e segurança [ITU-T 2020b]. Isso coloca a QKDN em continuidade com modelos já consolidados de gestão de redes de telecomunicações, mas adaptando-os às

especificidades da distribuição quântica de chaves.

No gerenciamento de falhas, o sistema monitora eventos e apoia diagnósticos e ações corretivas relacionados a módulos QKD, enlaces QKD, KMs e enlaces de gerenciamento. No gerenciamento de configuração, mantém a topologia, o inventário de recursos e os estados operacionais. No gerenciamento de contabilidade, mede o uso de recursos e apoia políticas de cobrança. No gerenciamento de desempenho, coleta e analisa dados operacionais da rede. No gerenciamento de segurança, reúne informações relacionadas a eventos, registros, rastros de auditoria e suporte ao ciclo de vida das chaves [ITU-T 2020b].

A recomendação também explicita as funções específicas de cada camada. O gerenciamento da camada quântica acompanha, por exemplo, parâmetros de desempenho e detecção de tentativas de ataque ao canal quântico. O gerenciamento da camada de chaves acompanha o estoque e a disponibilidade de chaves para *relay* e *supply*. O gerenciamento da camada de controle apoia o controlador nas decisões de roteamento e de rerroteamento. Essa separação é importante porque evidencia que a camada de gerenciamento não atua como uma entidade abstrata única, mas como um mecanismo de supervisão articulado às necessidades específicas de cada camada da QKDN [ITU-T 2020b].

Orquestração entre camadas: Um aspecto relevante da Y.3804 é a introdução explícita de funções de orquestração entre camadas, reunidas sob a lógica de *cross-layer management and orchestration (XLMO)* [ITU-T 2020b]. Essa função coordena informações e ações entre a camada quântica, a camada de gerenciamento de chaves e a camada de controle, além de interagir com sistemas externos de gerenciamento, especialmente o gerenciamento da rede do usuário.

Essa orquestração é importante porque a QKDN não opera como um conjunto de camadas independentes. Um aumento de QBER na camada quântica pode exigir reroteamento decidido pelo controlador. A redução do estoque de chaves em nós intermediários pode afetar a viabilidade de determinadas rotas de *relay*. Uma mudança na política de serviço ou na prioridade de aplicação pode afetar as decisões de *supply*. Em todos esses casos, a operação coerente da rede depende de coordenação transversal. A XLMO formaliza exatamente essa necessidade, transformando-a em uma função arquitetural explícita [ITU-T 2020b].

Além de definir funções de controle e gerenciamento, a ITU-T Y.3804 explicita procedimentos operacionais que mostram como essas funções interagem em situações concretas de operação da QKDN, incluindo falhas, configuração, desempenho, segurança, *key relay* e reroteamento de *key relay* [ITU-T 2020b]. No contexto deste capítulo, os procedimentos de *relay* e de reroteamento são relevantes porque evidenciam, de forma dinâmica, a divisão de responsabilidades entre a camada de gerenciamento de chaves e as camadas de controle e de gerenciamento da rede.

O ponto de partida desses procedimentos é a separação arquitetural já estabelecida nas recomendações anteriores. A Y.3802 indica que o *Key Manager* executa o *relay* quando necessário, mas pode depender do controlador da QKDN para obter a rota apropriada [ITU-T 2020c]. A Y.3803, por sua vez, esclarece que a continuidade do *relay* de-

pende do estado das chaves disponíveis nos nós intermediários e das condições da camada quântica, como alarmes e degradação associados ao aumento de QBER [ITU-T 2020d]. A Y.3804 formaliza essa dinâmica e mostra, passo a passo, como a rede transforma estado operacional em ação de controle.

Procedimento de *key relay*: O procedimento de *key relay* definido na Y.3804, ilustrado na Figura 4.14, descreve o fluxo pelo qual um KM obtém, por meio do controlador da QKDN, a rota lógica necessária para compartilhar chaves com outro KM não adjacente [ITU-T 2020b]. O procedimento começa quando um KM solicita uma rota de *relay* à função de controle de sessão (*session control function*) do controlador da QKDN. Essa escolha é significativa porque mostra que o *relay* não é tratado apenas como uma decisão de roteamento isolada, mas como parte do gerenciamento de uma sessão lógica de compartilhamento de chaves entre um nó de origem e um nó de destino.

Recebida a solicitação, a função de controle de sessão verifica inicialmente se já existe uma sessão estabelecida entre o nó QKD de origem e o nó QKD de destino. Caso essa sessão ainda não exista, a função de controle de sessão consulta a função de controle de roteamento (*routing control function*) para determinar uma rota adequada para *relay*. Em seguida, a função de roteamento consulta a função de controle de configuração (*configuration control function*), da qual obtém as informações de configuração da rede necessárias para avaliar os caminhos possíveis. Com base nessas informações, a função de roteamento calcula uma rota ótima para o *relay* e a devolve à função de controle de sessão, que então a repassa ao KM solicitante [ITU-T 2020b].

Do ponto de vista funcional, esse procedimento evidencia três aspectos centrais. Primeiro, a decisão de *relay* não é tomada localmente pelo KM com base apenas na conectividade imediata, mas depende de uma visão lógica da rede mediada pelo controlador. Segundo, a determinação da rota não se reduz a um problema abstrato de grafo, pois depende de informações sobre a configuração efetiva da infraestrutura. Terceiro, o resultado do procedimento não é a própria chave, mas sim a informação de rota que habilita a camada de gerenciamento de chaves a executar o *relay*. Em outras palavras, o controlador não manipula diretamente o material criptográfico, mas fornece ao KM as condições operacionais para que o *relay* ocorra de forma coerente com o estado da rede.

Essa leitura é compatível com a descrição geral da função de roteamento na própria Y.3804, segundo a qual o controlador deve gerenciar a tabela de rotas, adquirir informações sobre o consumo de chaves, o estoque residual nos KMs, os parâmetros dos enlaces QKD e a topologia da rede, e então provisionar uma rota apropriada entre os KMs extremos [ITU-T 2020b]. A Figura 4.14 traduz essa função em um encadeamento operacional mais concreto.

Procedimento de rerroteamento de *key relay*: Se o procedimento anterior trata da provisão inicial de uma rota de *relay*, o procedimento de rerroteamento, ilustrado na Figura 4.15, trata da adaptação dessa rota quando a continuidade do serviço de chaves está ameaçada [ITU-T 2020b]. Aqui, a ênfase da recomendação desloca-se da simples decisão de caminho para a cooperação entre gerenciamento e controle diante de mudanças de

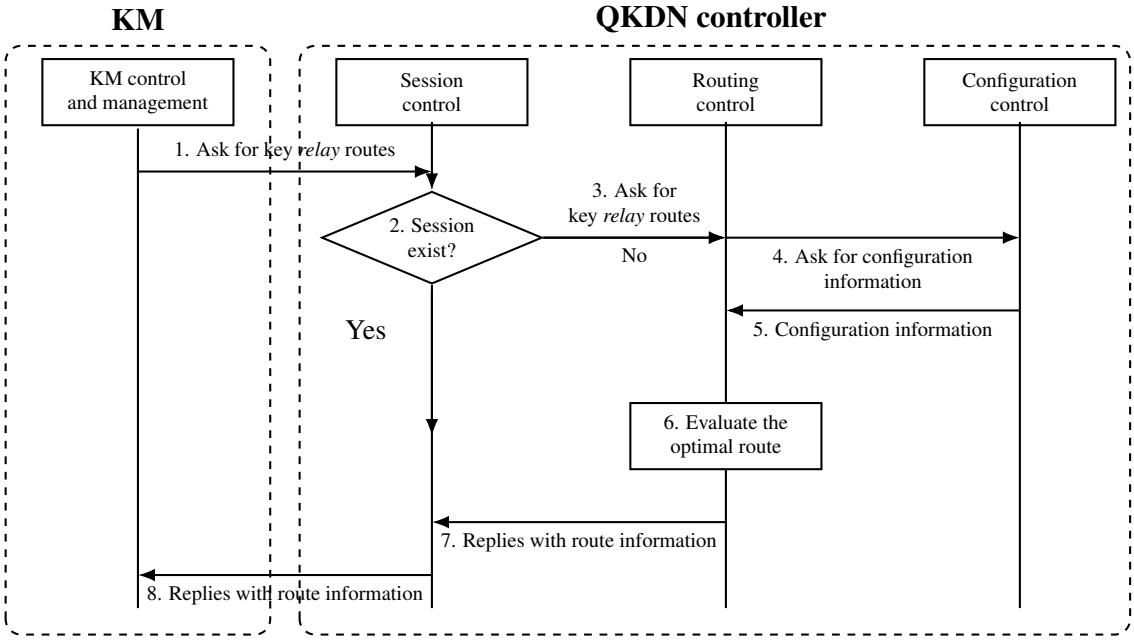

Figura 4.14. Procedimento de *key relay* em uma QKDN, adaptado da Figure 14 da ITU-T Y.3804. A figura mostra como a requisição de *relay* parte do KM, é tratada pelas funções de sessão, roteamento e configuração do controlador da QKDN, e retorna ao KM como informação de rota para execução do *relay*.

estado na rede.

Segundo a Y.3804, o processo começa quando a função de gerenciamento da camada de controle da QKDN (*QKDN Control Layer Management*, QCLM) recebe, do controlador e de suas funções de controle e gerenciamento, uma requisição de informações de suporte para roteamento ou rerroteamento de *relay*. A QCLM, então, solicita à função de orquestração e gerenciamento entre camadas (*Cross-Layer Management and Orchestration*, XLMO) informações sobre a topologia da rede. A XLMO devolve essas informações à QCLM, que passa a analisar a topologia e a selecionar as informações de *relay* e de suporte compatíveis com a situação observada. Por fim, a QCLM envia ao controlador da QKDN o conjunto de informações resultante, permitindo que este execute ações de roteamento ou rerroteamento do *relay* [ITU-T 2020b].

Esse procedimento é arquiteturalmente importante porque evidencia que o rerroteamento não é apresentado como uma reação puramente local do controlador. Ao contrário, a decisão depende de suporte explícito da camada de gerenciamento, especialmente da correlação entre informações topológicas e de estado realizada pela XLMO e processada pela QCLM. Assim, o rerroteamento aparece como produto da coordenação entre camadas, e não apenas como uma atualização da tabela de rotas.

A motivação desse procedimento torna-se mais evidente quando analisado em conjunto com as Recomendações Y.3803 e Y.3804. A Y.3803 indica que o rerroteamento do *relay* pode ser necessário quando o número de chaves disponíveis em nós intermediários cai abaixo de um determinado limiar, quando ocorrem falhas em KM ou no enlace de gerenciamento, ou ainda quando um QBER elevado compromete ou reduz a geração de chaves em um enlace QKD [ITU-T 2020d]. Em consonância com isso, a Y.3804, ao

descrever a função de roteamento, destaca que o rerroteamento pode ser acionado em dois conjuntos mais amplos de situações: aquelas associadas à camada de gerenciamento de chaves, como esgotamento de estoque ou falhas em KM/KM link, e aquelas relacionadas à camada quântica, como aumento do QBER ou falha de um módulo QKD [ITU-T 2020b]. Nesse sentido, o procedimento apresentado na Figura 4.15 explicita como essas informações são encaminhadas ao plano de gerenciamento e, posteriormente, retornam ao controlador como subsídio para a decisão sobre uma nova rota.

Em termos operacionais, o procedimento de rerroteamento aponta que a disponibilidade de serviço em uma QKDN depende de monitoramento contínuo e de uma cadeia de decisão que articula quatro níveis: (i) os elementos que detectam degradação ou falha; (ii) o gerenciamento por camada, que consolida essas informações; (iii) a orquestração entre camadas, que correlaciona topologia e estado global; e (iv) o controlador, que transforma esse suporte em ação sobre as rotas de *relay*. O serviço de chaves, portanto, não depende apenas da existência física de enlaces QKD, mas também da capacidade da rede de reconfigurar, de forma lógica, o uso desses recursos frente a eventos operacionais.

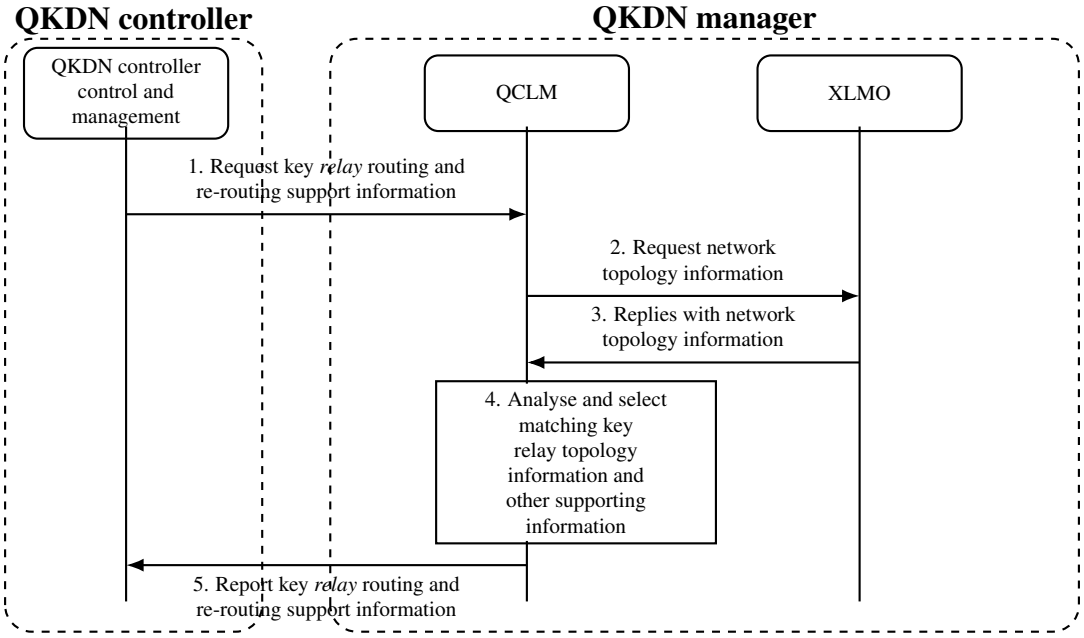

Figura 4.15. Procedimento de rerroteamento de *key relay* em uma QKDN, adaptado da Figure 15 da ITU-T Y.3804. A figura mostra como a QCLM e a XLMO fornecem ao controlador da QKDN o suporte topológico e operacional necessário para reconfiguração da rota de *relay*.

Interpretação conjunta dos dois procedimentos: As Figuras 4.14 e 4.15 devem ser lidas em conjunto. A primeira descreve a lógica de provisão inicial de uma rota de *relay*: uma solicitação parte do KM, percorre as funções de sessão, roteamento e configuração do controlador, e retorna ao KM como informação de rota. A segunda descreve a lógica de adaptação dessa rota quando o estado da rede torna necessário alterar o caminho previamente adotado: a demanda de suporte sobe da camada de controle ao gerenciamento por camada e à orquestração entre camadas, e então retorna ao controlador como base para

uma nova decisão de *relay* [ITU-T 2020b].

Em termos de controle e gerenciamento, essa distinção mostra-se bastante nítida. O *key relay* refere-se ao estabelecimento de um caminho lógico para o compartilhamento de chaves entre KMs não adjacentes, enquanto o *key relay rerouting* diz respeito à preservação desse serviço quando as condições operacionais deixam de sustentar a rota originalmente utilizada. Assim, o primeiro está associado à provisão do serviço, ao passo que o segundo se relaciona à sua resiliência. Em ambos os casos, a arquitetura padronizada da série Y.3800 mantém a mesma lógica de separação funcional: o material criptográfico permanece sob responsabilidade do gerenciamento de chaves, enquanto o controlador e as funções de gerenciamento da rede fornecem as condições estruturais

***Síntese da contribuição da Y.3804*:** A Y.3804 completa a base arquitetural da série Y.3800 ao demonstrar como a QKDN deve ser controlada, monitorada e orquestrada em operação. Se a Y.3803 torna o gerenciamento de chaves explicitamente central para a utilidade da rede, a Y.3804 mostra como essa utilidade depende de mecanismos de coordenação da infraestrutura: roteamento, reroteamento, controle de acesso, aplicação de políticas, supervisão FCAPS e articulação entre camadas [ITU-T 2020b].

Para este capítulo, a contribuição principal é tornar visível que uma QKDN não pode ser concebida apenas como um conjunto de módulos QKD e KMs. A rede também exige uma malha de controle e gerenciamento que acompanhe o estado da camada quântica, a disponibilidade do material criptográfico, a topologia operacional e as demandas das aplicações. É essa combinação entre geração quântica, gerenciamento de chaves e governança operacional da infraestrutura que transforma a QKD em um serviço de rede sustentado efetivamente.

4.4.10. Casos de uso representativos

O ITU-T Y Suppl. 80 é um documento complementar, de caráter informativo, da série Y.3800, que reúne casos de uso de QKDN no contexto das tecnologias de rede tratadas pelo SG13[4]. Esses casos são organizados em seis grandes grupos: combinação de QKD com primitivas criptográficas, integração com protocolos TCP/IP, implementação em diferentes topologias de rede, uso com distintas categorias de dispositivos, integração em diferentes tipos de rede e aplicação em setores verticais [ITU 2023]. Seu propósito é evidenciar que a arquitetura padronizada proposta pela ITU-T foi concebida para dar suporte a cenários concretos de integração com protocolos, topologias e serviços de rede. Em todos esses contextos, a existência de um sistema de gerenciamento de chaves funcionalmente bem definido constitui um requisito essencial para que a QKD possa ser oferecida como um serviço de rede interoperável e escalável.

Entre esses grupos, três são particularmente relevantes para a discussão de KMS e arquitetura de rede. O primeiro é a integração com protocolos TCP/IP, na qual o suplemento aponta o uso de QKD em camadas distintas da pilha, incluindo PPP e MACsec na camada de enlace, IPsec na camada de rede, TLS na camada de transporte e aplicações

[4]SG13 (*Study Group 13*) da ITU-T é responsável por estudos sobre arquitetura e serviços de redes futuras.

de camada superior. O segundo é o grupo de topologias de rede, que inclui explicitamente redes metropolitanas, *backbones* interurbanos e redes satélite-solo, o que evidencia que a QKDN deve ser tratada como infraestrutura de rede e não apenas como um enlace isolado. O terceiro é a integração em diferentes formas de rede, incluindo 4G/5G, Software Defined Networking (SDN)/Network Functions Virtualization (NFV), computação em nuvem, *blockchain* e outras arquiteturas futuras, o que reforça a necessidade de interfaces padronizadas de gerenciamento, controle e provisão de chaves [ITU 2023].

Entre as topologias destacadas no ITU-T Y Suppl. 80, a rede metropolitana de acesso ocupa posição relevante por representar um cenário de implantação próximo das infraestruturas urbanas de telecomunicações. O suplemento descreve esse caso de uso como uma rede de alta segurança para comunicações entre diferentes unidades ou escritórios em uma área metropolitana, tipicamente da ordem de 100 km de diâmetro, interconectada por enlaces ópticos dedicados para comunicação clássica e QKD. Nesse arranjo, as chaves geradas podem ser utilizadas tanto em mecanismos de autenticação quanto em primitivas de cifra, e, quando necessário, a conectividade, a disponibilidade e a largura de banda podem ser ampliadas com soluções baseadas em repetição confiável [ITU 2023].

Um exemplo representativo desse tipo de implantação é a *Madrid Quantum Network*. Trata-se de uma rede metropolitana baseada em fibra óptica, composta por 12 nós distribuídos entre centros de pesquisa, empresas e universidades, e integrada à infraestrutura de telecomunicações da Telefónica e da RediMadrid [García Cid et al. 2021]. Segundo os resultados reportados, o maior enlace da rede possui aproximadamente 55 km, a taxa máxima de geração de chaves atinge 70 kbps em alguns trechos e as perdas variam de cerca de 0,20 dB/km a 1,1 dB/km em segmentos mais degradados da região central urbana [García Cid et al. 2021]. Do ponto de vista arquitetural, a rede de Madri se destaca por adotar o paradigma de *SDN*, empregar uma camada de abstração denominada *Quantum Abstraction Interface (QuAI)* para integrar dispositivos de diferentes fabricantes e permitir a coexistência de canais quânticos e clássicos sobre a mesma infraestrutura [García Cid et al. 2021]. Em conjunto, essas características fazem dela um exemplo relevante de rede metropolitana orientada não apenas à conectividade, mas também à interoperabilidade e à orquestração de serviços.

Além da infraestrutura, a rede de Madri é relevante por já ter sido usada como base para diferentes cenários de aplicação. O próprio estudo relata a implementação ou a preparação de casos de uso associados à NFV baseada em QKD, IPsec e mecanismos de *Ordered Proof of Transit (OPoT)*, o que a aproxima diretamente das classes de uso discutidas no Y Suppl. 80, em especial aquelas relativas à integração com TCP/IP e a formas de rede como SDN/NFV [García Cid et al. 2021, ITU 2023]. Por essa razão, a rede de Madri é um bom exemplo para este capítulo: ela mostra que a QKDN metropolitana não precisa ser entendida apenas como um experimento físico de distribuição de chaves, mas também como uma plataforma de integração com serviços de rede existentes.

Outro exemplo é a *Rio Quantum Network*, que representa uma abordagem metropolitana ainda em construção, com forte ênfase em flexibilidade topológica e na adoção de protocolos que dispensam nós confiáveis na forma tradicional. O projeto conecta instituições de pesquisa no estado do Rio de Janeiro por meio de fibras ópticas da Rede Rio/FAPERJ e de um enlace em espaço livre de 7 km entre o CBPF e a UFF, com base em

uma implementação em laço Sagnac do protocolo TF-MDI-QKD [Temporão et al. 2024]. A rede é reconfigurável, permite que diferentes instituições assumam os papéis de Alice e Bob e concentra em Charlie a maior parte do hardware quântico, o que a torna um caso particularmente interessante para a discussão de redes metropolitanas orientadas a MDI-QKD e de integração híbrida entre fibra óptica e espaço livre [Temporão et al. 2024].

Em outra direção, o *Boston-Area Quantum Network* (BARQNET) configura-se como um *testbed* metropolitano voltado menos à provisão imediata de serviços de chaves e mais à caracterização de enlaces e à integração de componentes para futuras demonstrações de redes quânticas. O sistema conecta o MIT Lincoln Laboratory, o MIT e Harvard por meio de enlaces de fibra comerciais, em uma topologia de três nós, com cerca de 50 km de extensão entre as extremidades e diferentes configurações de operação, incluindo modo diferencial, ida e volta e arranjo de três nós [Bersin et al. 2024]. Seu interesse, no contexto desta discussão, reside em evidenciar que redes metropolitanas também podem atuar como ambientes de validação experimental para aspectos como sincronização, ruído de fase, ruído de polarização e protocolos de distribuição de qubits, complementando, assim, a perspectiva mais diretamente orientada a QKDN observada nos casos de Madri e Rio [Bersin et al. 2024].

Em síntese, as redes metropolitanas mostram por que a QKD precisa ser tratada em nível de arquitetura de rede. Elas exigem integração entre enlaces quânticos e infraestrutura clássica, mecanismos de gerenciamento de chaves, coordenação operacional e, em muitos casos, flexibilidade para acomodar heterogeneidade de dispositivos e múltiplos serviços. Nesse conjunto, a rede de Madri se destaca como referência particularmente útil para este capítulo por combinar escala metropolitana, integração com infraestrutura real de telecomunicações, heterogeneidade tecnológica e alinhamento com casos de uso próximos aos discutidos no ITU-T Y Suppl. 80.

4.5. Comparativo entre ITU-T e ETSI

Nesta subseção, apresenta-se uma análise comparativa entre os *frameworks* normativos desenvolvidos pela ETSI (Seção 4.3.1) e pela ITU-T (Seção 4.4), ambos centrais para a padronização das redes de QKD. Embora compartilhem o propósito de favorecer a interoperabilidade, a segurança e a escalabilidade, essas organizações adotam perspectivas arquiteturais distintas, porém complementares. A ETSI dedica-se principalmente à definição de interfaces e mecanismos de entrega de chaves voltados à integração com aplicações e sistemas clássicos, ao passo que a ITU-T propõe modelos arquiteturais, funcionais e de gerenciamento orientados à operação de redes QKDN em larga escala. Nesse contexto, a comparação entre essas abordagens contribui para compreender como a padronização internacional da QKD vem sendo estruturada de forma coordenada, em camadas e com foco na interoperabilidade.

4.5.1. Perspectivas Arquiteturais Distintas

A principal distinção entre as abordagens reside no *ponto de vista* adotado por cada organismo. A ITU-T, por meio da série Y.3800, enxerga o gerenciamento de chaves como uma **função intrínseca da rede**: a arquitetura em camadas funcionais, quântica, de chaves e de serviços, foi concebida para garantir que a infraestrutura física seja capaz de gerar, ro-

tear e controlar chaves em cenários de múltiplos nós, com controle de recursos e garantias de tráfego quântico.

A ETSI, por outro lado, adota a perspectiva de quem *consome* a infraestrutura. Seu KMS é projetado como uma camada de abstração entre os módulos QKD e as aplicações, oferecendo uma interface padronizada que oculta a complexidade do hardware quântico subjacente: a rede quântica é tratada como um "provedor de chaves", e as aplicações interagem com ela por meio de contratos de serviço bem definidos, seja via chamadas de função (ETSI GS QKD 004) ou via API REST (ETSI GS QKD 014). A distinção central entre os dois *frameworks* é, portanto, de perspectiva a ITU-T define *como* a rede gera e roteia chaves internamente; a ETSI define *como* as aplicações as solicitam e consomem.

4.5.2. Complementaridade dos Modelos

Longe de serem concorrentes, os dois modelos foram concebidos para atuar em camadas distintas da mesma pilha tecnológica, o que os torna **naturalmente complementares**. Uma rede QKD de produção pode, por exemplo, empregar a arquitetura ITU-T para gerenciar toda a lógica interna de seus nós, roteamento de chaves, controle de enlaces quânticos e balanceamento de carga, e, simultaneamente, expor interfaces ETSI nos pontos terminais da rede, permitindo que usuários finais, como roteadores IPsec ou servidores TLS, obtenham suas chaves de forma padronizada e transparente.

Essa complementaridade fica ainda mais evidente quando se considera a relação entre as próprias normas ETSI. A norma ETSI GS QKD 014, que define a API REST de alto nível (discutida na Seção 4.3.3), pode ser implementada *sobre* a norma ETSI GS QKD 004 (Seção 4.3.2): nesse arranjo, a interface REST recebe as requisições das aplicações, as traduz para as chamadas de função da 004 (`OPEN_CONNECT`, `GET_KEY`, etc.) e retorna os resultados no formato JSON esperado pelo cliente. O resultado é uma pilha coerente que unifica gestão de baixo nível e entrega de alto nível em uma única solução integrada, conforme ilustrado na Figura 4.16.

4.5.3. Integração com Protocolos de Segurança Existentes

Um aspecto frequentemente subestimado é a forma como as chaves distribuídas por essa pilha integrada se conectam aos protocolos de segurança já amplamente implementados nas redes convencionais. Protocolos como o **SKIP** (*Simple Key Infrastructure Protocol*) foram projetados exatamente para preencher essa lacuna: atuam como uma camada de adaptação capaz de injetar material criptográfico gerado por QKD em mecanismos de segurança consolidados, como o **IKEv2**, protocolo de troca de chaves utilizado em túneis IPsec [Dervisevic et al. 2025].

Essa integração é relevante porque permite que organizações adotem QKD de forma incremental, sem a necessidade de substituir toda a infraestrutura de segurança existente. O *Key Provider*, seja ele gerenciado conforme a arquitetura ITU-T, a norma ETSI 004 ou a norma ETSI 014, sincroniza o material criptográfico e o disponibiliza aos protocolos tradicionais, que passam a beneficiar-se da segurança incondicional da distribuição quântica de chaves, sem qualquer alteração em sua lógica interna.

4.5.4. Resumo Comparativo

A Tabela 4.1 sintetiza os principais pontos de distinção e complementaridade entre os dois *frameworks*, servindo como referência rápida para os conceitos discutidos ao longo deste capítulo.

Tabela 4.1. Comparação entre os *frameworks* ITU-T e ETSI para redes QKD.

Critério	ITU-T (Série Y.3800)	ETSI (GS QKD 004/014)
Foco principal	Infraestrutura e operação da rede	Entrega de chaves às aplicações
Perspectiva	Provedor de rede	Consumidor / desenvolvedor de aplicações
Modelo de gestão	Função intrínseca da rede (camadas funcionais)	Serviço acessível por API (KMS)
Interface de acesso	Interna à rede	Chamadas de função (004) ou REST/HTTPS (014)
Escalabilidade	Redes de múltiplos nós e roteamento quântico	Alta escalabilidade via APIs web padronizadas
Integração	Controle de recursos e enlaces quânticos	Integração com IPsec, TLS e protocolos legados
Relação mútua	Define *como* as chaves são geradas e roteadas	Define *como* as chaves são consumidas

A análise comparativa revela que a padronização internacional de QKD está sendo construída de forma estratificada e colaborativa. Não há sobreposição de escopo: cada organismo contribui com aquilo que conhece melhor, a ITU-T com sua tradição em arquiteturas de rede de telecomunicações, e a ETSI com sua expertise em interfaces de aplicação e ambientes de desenvolvimento web.

Para o profissional ou pesquisador que deseja implementar uma solução QKD real, a mensagem prática é clara: compreender ambos os *frameworks* não é opcional. A escolha de um deles em detrimento do outro não é uma decisão de arquitetura, mas sim um equívoco conceitual. Uma implantação robusta e interoperável demandará, invariavelmente, elementos de ambos os mundos.

4.6. Segurança do KMS e Avaliação de Confiança

Esta seção analisa os aspectos de segurança relacionados à gestão de chaves em redes QKD, com base nas normas ETSI GS QKD004 [ETSI 2020] e 014 [ETSI 2019] e no protocolo SKIP [Singh et al. 2025]. A discussão está organizada em três eixos complementares: as ameaças inerentes à arquitetura de nós confiáveis, os mecanismos de padronização e certificação de segurança, e a integração do KMS em ambientes híbridos que combinam QKD com criptografia clássica e pós-quântica.

4.6.1. Ameaças Específicas à Gestão de Chaves

As normas analisadas não apresentam uma taxonomia formal de ameaças, mas delineiam um modelo de segurança baseado em **nós confiáveis** e **perímetros controlados**, do qual

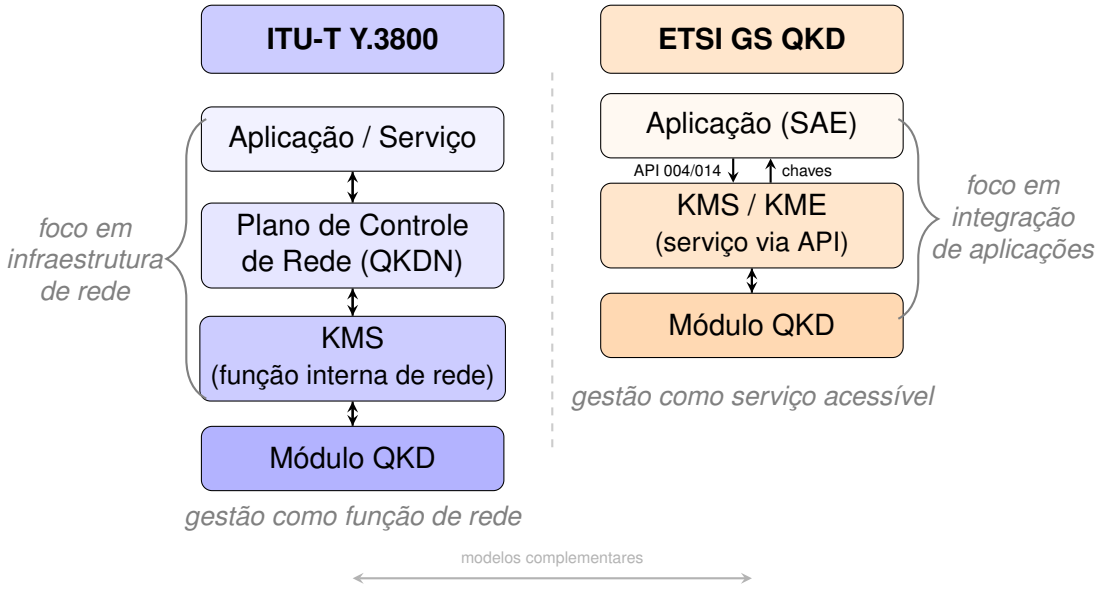

Figura 4.16. Comparação entre os modelos ITU-T e ETSI para gestão de chaves QKD: o ITU-T trata o KMS como função interna de rede, enquanto o ETSI o expõe como serviço acessível por API, tornando os modelos complementares.

decorrem três categorias principais de risco. Compreendê-las é essencial para avaliar a segurança prática de implantações QKD.

Comprometimento de nós confiáveis. A arquitetura ETSI assume que cada Nó Confiável (*Trusted Node*) é um ponto intermediário da rede responsável por armazenar e retransmitir chaves entre enlaces quânticos e é operado e gerenciado de forma segura dentro de um limite fisicamente controlado [ETSI 2020, ETSI 2019]. Essa premissa é, ao mesmo tempo, uma força e uma fragilidade do modelo: se um nó for comprometido, o sigilo das chaves que passaram por ele não pode mais ser garantido. O protocolo SKIP acrescenta uma dimensão adicional a esse risco ao apontar que o uso de identificadores persistentes de sessão pode vazar informações sobre a topologia da rede, facilitando *comprometimentos laterais*, situações em que um adversário, ao observar padrões de tráfego, identifica novos pontos vulneráveis de inserção na rede [Singh et al. 2025].

Segurança do perímetro. Tanto a ETSI GS QKD004 quanto a 014 assumem que a comunicação entre a aplicação consumidora de chaves (SAE) e o gerenciador de chaves (KME/KMS) ocorre dentro de um **perímetro de segurança local**, cuja integridade é pré-requisito para o funcionamento correto do protocolo [ETSI 2020, ETSI 2019]. Em termos práticos, isso significa que, embora a norma exija proteção lógica via HTTPS/TLS, ela pressupõe que essa comunicação ocorra dentro de um perímetro em que controles físicos e de acesso garantam a integridade dos terminais entre a SAE e o KME: essa proteção é responsabilidade da infraestrutura de rede local, tipicamente assegurada por controles físicos e de acesso lógico.

Proteção física e lógica. O SKIP destaca a importância de **co-localizar** o *Key Provider* e o encriptador ou, idealmente, executá-los no mesmo dispositivo físico como medida para reduzir a superfície de ataque no enlace entre esses dois componentes [Singh et al. 2025]. A intuição por trás dessa recomendação é basicamente: quanto

menor o caminho percorrido pela chave entre sua origem e seu uso, menor a janela de oportunidade para um adversário interceptá-la ou adulterá-la.

4.6.2. Padronização de Segurança

A segurança de um sistema QKD não depende apenas de sua implementação correta, mas também de sua capacidade de ser avaliada e certificada por terceiros de forma independente. Nesse sentido, a norma ETSI GS QKD 004 foi projetada com um *footprint* reduzido, isto é, com uma superfície de API deliberadamente pequena e bem delimitada, o que simplifica o escopo de uma auditoria formal de segurança e facilita processos de certificação [ETSI 2020]. Em termos práticos, uma API com menos funções e estados possíveis é mais fácil de verificar formalmente e menos propensa a vulnerabilidades introduzidas por complexidade desnecessária.

Complementarmente, o anexo bibliográfico da norma 004 refere-se ao *National Institute of Standards and Technology (NIST) Special Publications* 800-53 [ETSI 2020], um catálogo amplamente adotado de controles de segurança e privacidade para sistemas de informação, desenvolvido pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos. Essa referência sinaliza a intenção de alinhamento com *frameworks* de conformidade já estabelecidos, facilitando a adoção de QKD em organizações que já operam sob esses regimes regulatórios.

4.6.3. KMS em um Contexto Híbrido (QKD + Criptografia Clássica)

Este é, sem dúvida, um dos aspectos mais estratégicos da gestão de chaves em redes QKD, e também o mais detalhado nas fontes analisadas especialmente no protocolo SKIP [Singh et al. 2025]. A questão central é: como integrar a segurança incondicional fornecida pelo QKD à infraestrutura criptográfica clássica já amplamente implantada? A resposta é apresentada em três camadas complementares.

QKD como fonte de entropia (QRNG). O protocolo SKIP define explicitamente um método denominado `GetEntropy`, que permite ao *Key Provider* fornecer uma cadeia de bits verdadeiramente aleatórios gerados por processos quânticos para consumo interno dos encriptadores [Singh et al. 2025]. O encriptador pode solicitar tamanhos específicos de entropia via API, tornando o hardware quântico uma fonte de aleatoriedade certificável para sistemas clássicos. Isso é relevante porque a qualidade da aleatoriedade é um dos fatores mais críticos para a segurança de qualquer sistema criptográfico: geradores pseudoaleatórios clássicos podem apresentar padrões exploráveis por adversários suficientemente poderosos.

KMS como ponto de convergência com a Criptografia Pós-Quântica (PQC). O SKIP é apresentado como um protocolo de integração: o *Key Provider* pode utilizar tanto QKD quanto algoritmos de criptografia pós-quântica como os padronizados recentemente pelo NIST, como CRYSTALS-Kyber como fonte de material criptográfico, de forma completamente transparente para o encriptador [Singh et al. 2025]. Essa característica posiciona o KMS como um ponto de convergência natural entre os dois paradigmas de segurança quântica, permitindo que organizações adotem gradualmente as tecnologias mais adequadas ao seu contexto sem alterar a lógica dos sistemas que as consomem.

Defesa em profundidade. A abordagem mais poderosa descrita nas fontes

combina QKD e criptografia clássica em uma estratégia de **defesa em profundidade** (*defense-in-depth*): chaves fornecidas pelo KMS são injetadas no processo de derivação de chaves de protocolos consolidados, como IKEv2 (usado em túneis IPsec) e TLS [Singh et al. 2025, ETSI 2020]. Essas chaves pré-compartilhadas são resistentes ao algoritmo de Grover[5], reduzindo efetivamente pela metade o comprimento de bit da segurança de cifras simétricas. Uma chave AES-256, por exemplo, oferece segurança equivalente a 128 bits contra um adversário com computador quântico.O principal algoritmo quântico que ameaça cifras simétricas é integrado ao material de chaveamento já existente, sem exigir a substituição imediata de toda a infraestrutura. O resultado é um sistema que permanece seguro mesmo diante de adversários equipados com computadores quânticos, ao mesmo tempo em que preserva a compatibilidade com os protocolos e os equipamentos já implantados.

Em síntese, os três eixos discutidos nesta seção revelam uma visão de segurança madura e estratificada: as normas reconhecem os limites físicos e arquiteturais do modelo de nós confiáveis, buscam facilitar a certificação formal por meio de APIs enxutas e posicionam o KMS não como substituto da criptografia clássica, mas como uma camada adicional de segurança que fortalece e complementa a infraestrutura existente.

4.7. Laboratório prático em GNS3 para criação de tunel IPsec, conforme ETSI GS QKD 014

Este módulo apresenta a implementação prática de uma infraestrutura de rede *Quantum-Safe* em ambiente de simulação, focando na integração entre um KME e sistemas de rede clássicos para o estabelecimento de túneis seguros. O objetivo final é alcançar um laboratório com uma configuração como a mostrada na figura 4.17.

4.7.1. Visão Geral e Tecnologias Utilizadas

O laboratório simula um cenário onde a segurança de uma VPN IPsec é reforçada por chaves quânticas distribuídas via API REST. As principais tecnologias empregadas incluem:

- **GNS3:** Plataforma de simulação para a orquestração da topologia de rede.
- **MikroTik RouterOS (v7.22+):** Atua como o elemento de rede (*Secure Application Entity* - SAE), possuindo suporte nativo ao protocolo QKD para consumo de chaves externas.
- **Docker:** Utilizado para instanciar a KME de forma isolada e portável.
- **Python/Flask:** Linguagem e *framework* utilizados para desenvolver a lógica da KME, implementando a norma **ETSI GS QKD 014** para a entrega de chaves.
- **SQLite:** Base de dados leve para a persistência e sincronização do material criptográfico gerado.

[5]O algoritmo de Grover, proposto em 1996, é um algoritmo quântico capaz de realizar buscas em espaços não estruturados com complexidade $O(\sqrt{N})$.

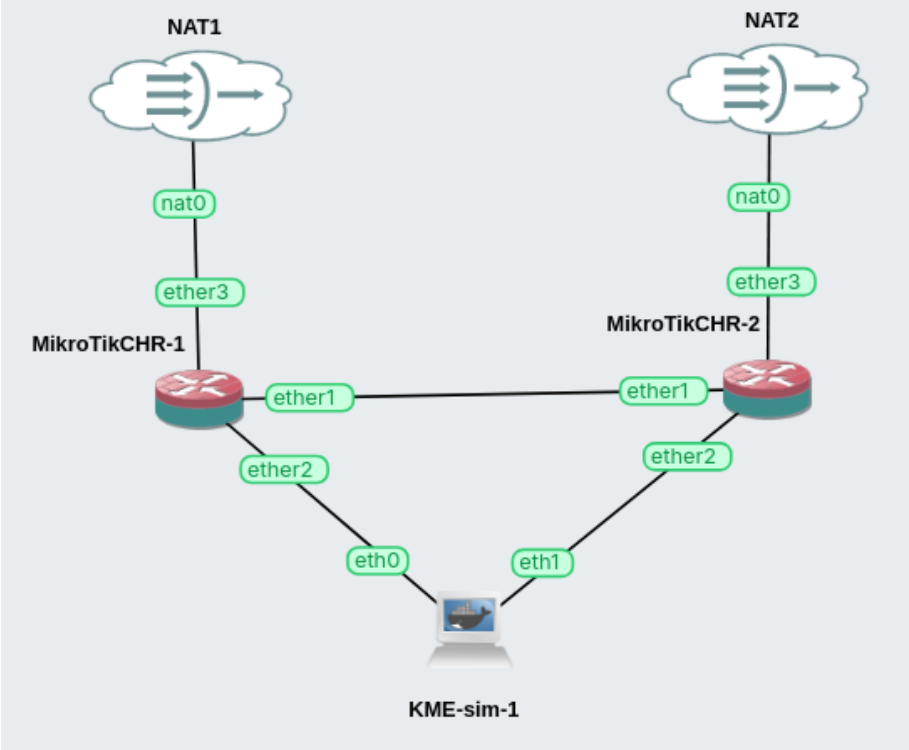

Figura 4.17. Imagem da simulação final no GNS3.

4.7.2. Topologia de Rede

A topologia é composta por três núcleos principais interconectados em um ambiente isolado:

- **Backbone Clássico:** Dois roteadores MikroTik (CHR-1 e CHR-2) conectados por um enlace ponto-a-ponto (sub-rede `10.0.0.0/30`).
- **Rede de Gerenciamento (KME-LAN):** Uma infraestrutura centralizada onde o servidor KME reside, acessível por ambos os roteadores através de interfaces dedicadas em suas respectivas LANs (`172.16.1.0/24` e `172.16.2.0/24`).
- **Plano de Dados:** Onde o tráfego do usuário é cifrado via IPsec utilizando a entropia fornecida pela KME.

4.7.3. Decisões Arquiteturais

O *design* do laboratório reflete escolhas estratégicas para garantir a segurança e a conformidade com padrões internacionais:

1. **Centralização da KME:** Diferente de modelos puramente descentralizados, utiliza-se uma KME central com interfaces múltiplas para simplificar a sincronização de chaves em ambiente de teste, atuando como o *middleware* entre a geração de entropia e o consumo.

2. **Autenticação via mTLS:** O acesso à API de chaves é protegido por TLS Mútuo (mTLS), garantindo que apenas roteadores autorizados (SAEs) possam solicitar material criptográfico.

3. **Separação de Planos:** O plano de gerenciamento de chaves (REST/HTTPS) é logicamente separado do plano de dados (IPsec), seguindo as recomendações de demarcação de segurança da série ITU-T Y.3800.

4. **Consumo Híbrido:** O sistema é configurado para que o IPsec utilize as chaves da KME como material primário, provendo o *Forward Secrecy* contra ameaças quânticas (ataques do tipo *Harvest Now, Decrypt Later*).

4.7.4. Fluxo de Operação

O funcionamento do laboratório segue o ciclo de vida da chave: a KME gera e armazena chaves sob demanda no SQLite; os roteadores MikroTik, agindo como clientes mTLS, solicitam essas chaves via `GET requests` na porta `8020`; por fim, o subsistema IPsec do RouterOS utiliza o `key_id` recebido para sincronizar a cifragem do túnel entre as duas pontas.

4.7.5. Artefatos

A implementação do laboratório, assim como um tutorial detalhado pode ser encontrado no seguinte repositório: `https://github.com/QuIIN-Quantum-Industrial-Innovation/lab_mc_sbrc_26`.

4.8. Encerramento, Desafios e Caminhos Futuros:

A jornada percorrida neste texto demonstrou que a segurança *Quantum-Safe* não é apenas uma aspiração teórica, mas uma realidade tecnológica em plena fase de padronização e implementação prática. A transição da criptografia clássica para modelos resilientes à computação quântica exige uma compreensão profunda da integração entre as leis da física e a engenharia de redes.

4.8.1. Síntese dos Conceitos Fundamentais

Um dos componentes centrais nessa arquitetura é o **KMS (Key Management System)**, que atua como o elemento de software vital para superar as limitações da camada física do QKD, restrita por distâncias e topologias ponto-a-ponto. O KMS transforma o fluxo bruto de material criptográfico em um recurso gerenciável, permitindo o armazenamento, o roteamento e a entrega eficiente de chaves para as aplicações finais.

Essa operacionalização é sustentada por uma dualidade de padronização complementar: enquanto a abordagem **ETSI ISG QKD** foca na *interface de serviço*, definindo como as aplicações consomem chaves via APIs (como a REST API na GS QKD 014) para garantir a interoperabilidade entre encriptadores e gerenciadores, a abordagem **ITU-T Série Y.3800** concentra-se na *arquitetura de rede*. Esta última define a interação entre os planos quântico, de chave, de controle e de gerenciamento para formar uma **QKDN** (*Quantum Key Distribution Network*) escalável e de múltiplos saltos.

O sucesso desse modelo reside no desacoplamento funcional, que separa a geração da chave na camada quântica de seu gerenciamento na camada de chaves, permitindo que a infraestrutura de segurança evolua independentemente do hardware. Além disso, a síntese prática demonstra que o QKD não substitui a criptografia clássica, mas a fortalece através de uma estratégia de defesa em profundidade. A integração com protocolos consolidados, como o **IPsec**, ilustra esse modelo de segurança híbrida, onde a segurança teórica da informação provida pelo QKD protege a negociação de chaves em canais clássicos. Por fim, a viabilidade técnica foi validada através de simulações no **GNS3**, comprovando que o uso de normas abertas já permite a construção de redes seguras com ferramentas de mercado, reduzindo as barreiras para administradores de redes tradicionais.

4.8.2. Desafios Tecnológicos e Operacionais

Apesar dos avanços, a implementação em larga escala enfrenta desafios significativos, especialmente no que tange à escalabilidade e à carga administrativa. A instalação manual de chaves pré-compartilhadas (PSKs) apresenta um gargalo, visto que o esforço administrativo cresce de forma quadrática com o aumento de nós, exigindo a transição para métodos de provisionamento dinâmico. Enquanto o modelo ETSI foca na entrega, o modelo **Y.38XX** destaca a complexidade de gerenciar o ciclo de vida das chaves em redes *multi-hop*, o que demanda automação robusta.

Somam-se a isso os obstáculos de interoperabilidade entre equipamentos de diferentes fabricantes, motivando a busca por APIs padronizadas. No nível físico e logístico, a segurança do "último salto" entre o Provedor de Chaves (KP) e o encriptador permanece crítica, recomendando-se a co-localização física ou a integração em um mesmo dispositivo para mitigar ataques. Há também a dependência de perímetros de segurança locais para as interfaces de aplicação, um desafio constante em redes distribuídas. Por fim, os desenvolvedores enfrentam um *trade-off* entre complexidade e analisabilidade: a norma ETSI 014 oferece simplicidade via integração *web*, mas exige bibliotecas HTTPS/JSON complexas, enquanto a ETSI 004, embora mais árdua, permite implementação em C puro, facilitando auditorias e certificações de segurança.

4.8.3. Caminhos Futuros e Tendências

O futuro da segurança quântica aponta para a agilidade criptográfica e a modularidade, permitindo que Provedores de Chaves sejam atualizados ou substituídos sem a necessidade de reconfigurar os encriptadores. A tendência de convergência sugere o uso de chaves quânticas para reforçar protocolos como IKEv2 e TLS, combinando a robustez do QKD com a flexibilidade da criptografia pós-quântica (PQC) em uma estratégia híbrida.

A expansão do uso dessas chaves em protocolos de mercado, como **MACsec** e **IPsec**, será facilitada por protocolos de integração como o **SKIP**, automatizando o ciclo de vida do material criptográfico. Paralelamente, o desenvolvimento de APIs REST leves visa democratizar o acesso à tecnologia, permitindo que o QKD seja consumido como um serviço de nuvem (*as-a-service*). Em arquiteturas mais complexas, a integração de servidores de chaves com controladores de Redes Definidas por Software (**SDN**) será essencial para otimizar a descoberta de aplicações e o roteamento de chaves. Por fim, observa-se uma tendência de integração com sistemas legados, onde o QKD passa a servir

como fonte adicional de entropia para sistemas de gerenciamento convencionais, como o padrão **KMIP da OASIS**.

Referências

[ITU 2023] (2023). Supplement 80 to itu-t y-series recommendations: Itu-t y.3800 series – quantum key distribution networks use cases. Technical report, ITU-T.

[Ahmed et al. 2025] Ahmed, N., Zhang, L., and Gangopadhyay, A. (2025). A survey of post-quantum cryptography support in cryptographic libraries. In *2025 IEEE International Conference on Quantum Computing and Engineering (QCE)*, volume 1, pages 906–917. IEEE.

[Bennett and Brassard 2014] Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[Bersin et al. 2024] Bersin, E., Grein, M., Sutula, M., Murphy, R., Huan, Y. Q., Stevens, M., Suleymanzade, A., Lee, C., Riedinger, R., Starling, D. J., et al. (2024). Development of a boston-area 50-km fiber quantum network testbed. *Physical Review Applied*, 21(1):014024.

[Bhatia and Ramkumar 2020] Bhatia, V. and Ramkumar, K. R. (2020). An efficient quantum computing technique for cracking rsa using shor's algorithm. In *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, pages 89–94.

[Cao et al. 2022] Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., and Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials*, 24(2):839–894.

[Day and Zimmermann 1984] Day, J. and Zimmermann, H. (1984). The osi reference model. *Proceedings of the IEEE*, 71:1334 – 1340.

[Dervisevic et al. 2025] Dervisevic, E., Tankovic, A., Fazel, E., Kompella, R., Fazio, P., Voznak, M., and Mehic, M. (2025). Quantum key distribution networks - key management: A survey. *ACM Comput. Surv.*, 57(10).

[Easttom 2022] Easttom, C. (2022). *Quantum Computing and Cryptography*, pages 397–407. Springer International Publishing, Cham.

[Elboukhari et al. 2010] Elboukhari, M., Azizi, M., and Azizi, A. (2010). Quantum key distribution protocols: A survey. *International Journal of Universal Computer Sciences*, 1(2):59–67.

[ETSI 2019] ETSI (2019). Quantum key distribution (qkd); protocol and data format of rest-based key delivery api. Technical Specification TS 102 014, ETSI. Version 1.1.1, Released: February 2019.

[ETSI 2020] ETSI (2020). Quantum key distribution (qkd); application interface. Technical Specification TS 102 004, ETSI. Version 2.1.1 , Released: August 2020.

[García Cid et al. 2021] García Cid, M. I., Ortiz Martín, L., and Martín Ayuso, V. (2021). Madrid quantum network: A first step to quantum internet. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, pages 1–7.

[Gisin et al. 2002] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195.

[ITU-T 2019] ITU-T (2019). Overview on Quantum Key Distribution Networks. Technical Report Recommendation ITU-T Y.3800, International Telecommunication Union. Accessed: 2026-03-08.

[ITU-T 2020a] ITU-T (2020a). Functional Requirements for Quantum Key Distribution Networks. Technical Report Recommendation ITU-T Y.3801, International Telecommunication Union. Accessed: 2026-03-08.

[ITU-T 2020b] ITU-T (2020b). Quantum Key Distribution Networks – Control and Management. Technical Report Recommendation ITU-T Y.3804, International Telecommunication Union. Accessed: 2026-03-08.

[ITU-T 2020c] ITU-T (2020c). Quantum Key Distribution Networks – Functional Architecture. Technical Report Recommendation ITU-T Y.3802, International Telecommunication Union. Accessed: 2026-03-08.

[ITU-T 2020d] ITU-T (2020d). Quantum Key Distribution Networks – Key Management. Technical Report Recommendation ITU-T Y.3803, International Telecommunication Union. Accessed: 2026-03-08.

[James et al. 2023] James, P., Laschet, S., Ramacher, S., and Torresetti, L. (2023). Key management systems for large-scale quantum key distribution networks. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*, pages 1–9.

[Lai et al. 2023] Lai, J., Yao, F., Wang, J., Zhang, M., Li, F., Zhao, W., and Zhang, H. (2023). Application and development of qkd-based quantum secure communication. *Entropy*, 25(4):1–18.

[Mehic et al. 2020] Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C., and Voznak, M. (2020). Quantum key distribution: A networking perspective. *ACM Computing Surveys (CSUR)*, 53(5):1–41.

[Narroway 2025] Narroway, e. a. (2025). Towards Global Quantum Key Distribution. *Nature Reviews Physics*.

[Nielsen and Chuang 2010] Nielsen, M. A. and Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge ; New York, 10th anniversary ed edition.

[Sáez et al. 2024] Sáez, J. M., Perales, A. P., Palancar, R. C., Lopez, D. R., Chavarria, J. F., Ayuso, V. M., and Mendez, J. P. B. (2024). Current status, gaps, and future directions in quantum key distribution standards: Implications for industry. In *2024 international conference on Quantum Communications, Networking, and Computing (QCNC)*, pages 341–345. IEEE.

[Sanz et al. 2025] Sanz, A., Atutxa, A., Franco, D., Astorga, J., Jacob, E., and López, D. (2025). Toward quantum-safe scalable networks: an open, standards-aware key management framework. *IEEE Network*.

[Singh et al. 2025] Singh, R., Hill, C., Kawaguchi, S., and Lupo, J. (2025). Secure Key Integration Protocol (SKIP). Internet-Draft draft-cisco-skip-02, Internet Engineering Task Force. Work in Progress.

[Stallings 2017] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Prentice Hall, Upper Saddle River, NJ, 7th edition.

[Temporão et al. 2024] Temporão, G. P., de Melo, F. R. B., and Khoury, A. Z. (2024). The rio quantum network: a reconfigurable hybrid multi-user metropolitan quantum key distribution network. In *Workshop de Redes Quânticas*, pages 19–24. SBC.

[Xu et al. 2020] Xu, F., Ma, X., Zhang, Q., Lo, H.-K., and Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. *Reviews of modern physics*, 92(2):025002.