TTC標準
Standard

JT-Y3808

量子鍵配送ネットワークとセキュアストレージネットワーク統合フレームワーク

Framework for integration of quantum key distribution network and secure storage network

第 1.0 版

2023 年 11 月 9 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

目　次

1　規定範囲 6
2　参考文献 6
3　定義 6
3.1　本標準以外で定義されている用語 6
3.2　本標準で定義された用語定義 7
4　略語と頭文字 7
5　表記法 7
6　はじめに 7
7　PKI 10
8　SSN 10
8.1　秘密分散 10
8.2　QKDNによってサポートされるプライベートチャネル 10
8.3　PKIによってサポートされる安全な運用 11
9　SSNの機能的要求条件 11
9.1　SSNユーザプレーン 11
9.2　SSN制御プレーン 11
9.3　SSNストレージプレーン 11
9.4　SSN管理プレーン 12
10　SSNの機能アーキテクチャモデル 12
10.1　SSAの機能 13
10.2　SSNコントローラの機能 13
10.3　SSNシェアホルダーの機能 14
10.4　SSN管理者の機能 14
11　参照点 14
11.1　SSAの参照点 14
11.2　SSNコントローラの参照点 14
11.3　SSNシェアホルダーの参照点 15
11.4　SSNマネージャの参照点 15
11.5　QKDNの参照点 15
11.6　PKIの参照点 15
12　動作手順 15
12.1　データ保存手順 15

12.2　データ取得手順 16
12.3　シェア更新手続 18
参考文献 20

＜参考＞

1. 国際勧告などとの関連

本標準は量子鍵配送ネットワークとセキュアストレージネットワーク統合フレームワークについて規定しており、2022年2月にITU-T SG13において発行されたITU-T勧告Y.3808に準拠している。

2. 上記勧告などに対する追加項目など

2.1 オプション選択項目

なし

2.2 ナショナルマター決定項目

なし

2.3 その他

なし

2.4 原勧告との章立て構成比較表

章立てに変更なし

3. 改版の履歴

版数	発行日	改版内容
第1版	2023年11月9日	制定

4. 工業所有権

本標準に関わる「工業所有権の実施の権利に係る確認書」の提出状況は、TTCホームページでご覧になれます。

5. その他

(1) 参照している勧告、標準など

ITU-T勧告	X.509, Y.3800, Y.3802
ISO/IEC標準	ISO/IEC 27040, ETSI GR QKD007

6. 標準作成部門

ネットワークビジョン専門委員会

1　規定範囲

標準Y.3808は、量子鍵配送ネットワーク(QKDN)とセキュアストレージネットワーク(SSN)を統合するためのフレームワークについて記述する。特に、本標準の範囲には以下が含まれる。

- SSNの概要
- SSNの機能要求条件
- SSNの機能アーキテクチャモデル
- 参照点
- 動作手順

2　参考文献

以下に列挙するITU-T勧告およびその他の参考文献は、この本文中の参照を通して、本標準を構成する規定を含む。発行時点では、示された版は有効であった。すべての勧告及び他の参考文献は改訂の対象である。したがって、本標準の利用者は、以下に列挙する勧告及び他の参考文献の最新版を適用する可能性を調査することが推奨される。現在有効なITU-T勧告のリストは定期的に発行されている。本標準が文献を参照することは、その文献がそれ単体で勧告となる地位をその文献に与えるものではない。

[ITU-T X.509]　ITU-T X.509(2016)、情報技術－開放型システム間相互接続－ディレクトリ：公開鍵及び属性認証フレームワーク

[ITU-T Y.3802]　ITU-T Y.3802(2020)、量子鍵配送ネットワークのアーキテクチャ

3　定義

3.1　本標準以外で定義されている用語

本標準は、本標準以外で定義された次の用語を使用する。

3.1.1　鍵マネージャ (KM) [b-ITU-T Y.3800]：鍵管理レイヤ内で鍵管理を実行する機能モジュールで、QKDノード内に配置される。

3.1.2　量子鍵配送(QKD) [b-ETSI GR QKD007]：量子情報理論に基づく情報理論的セキュリティを用いて対称暗号鍵を生成および配送する手順または方法。

3.1.3　QKD リンク[ITU-T Y.3800]：QKD を動作させるための 2 つの QKD モジュール間の通信リンク。

注：QKDリンクは、量子信号を送受信する量子チャネルと、同期と鍵蒸留のために情報を交換する古典チャネルから構成される。

3.1.4　QKD モジュール [b-ITU-T Y.3800]：暗号機能と、QKDプロトコル、同期、鍵生成のための蒸留などの量子光プロセスを実装するハードウェアおよびソフトウェアコンポーネントのセット。定められた暗号境界内に含まれる。

注： QKDモジュールは、QKDリンクに接続され、鍵を生成するエンドポイントモジュールとして動作する。QKD モジュールには 2 つのタイプ、すなわち送信器 (QKD-Tx) および受信器 (QKD- Rx) がある。

3.1.5　QKD ネットワーク (QKDN) [b-ITU-T Y.3800]： QKD リンクを介して接続された 2 以上の QKD ノードから構成するネットワーク。

注： QKD ネットワーク (QKDN) では、QKD リンクで直接接続されていないQKDノード間でも、鍵リレーによって鍵を共有できる。

3.1.6　QKDN コントローラ [b-ITU-T Y.3800]：QKDN を制御するために QKDN制御レイヤに位置する機能モジュール。

3.1.7　QKDN マネージャ [b-ITU-T Y.3800]：QKDN を監視および管理するために QKDN管理レイヤに位置する機能モジュール。

3.1.8　QKD ノード [b-ITU-T Y.3800]：許可されていない当事者による侵入および攻撃から保護されている1つ以上のQKDモジュールを含むノード。

注：QKDノードは、鍵マネージャ(KM)を含むことができる。

3.2　本標準で定義された用語定義

無し。

4　略語と頭文字

本標準は、以下の略語を使用する。

AES	Advanced Encryption Standard (高度暗号化標準)
CA	Certification Authority (認証局)
FCAPS	Fault, Configuration, Accounting, Performance and Security (障害、構成、課金、パフォーマンス、およびセキュリティ)
IPsec	Internet Protocol Security (インターネットプロトコルセキュリティ)
IT-secure	Information-Theoretically secure (情報理論的安全性)
KM	Key Manager (鍵マネージャ)
OTP	One-Time Pad (ワンタイムパッド)
PKI	Public Key Infrastructure (公開鍵基盤)
QKD	Quantum Key Distribution (量子鍵配送)
QKDN	Quantum Key Distribution Network (量子鍵配送ネットワーク)
SSA	Secure Storage Agent (セキュアストレージエージェント)
SSN	Secure Storage Network (セキュアストレージネットワーク)
TLS	Transport Layer Security (トランスポートレイヤセキュリティ)

5　表記法

本標準ではキーワード「が要求される」は、厳密に従わなければならず、この文書への適合性が主張される場合にはそこから逸脱することは許されない要求条件を示す。

キーワード「推奨される」は、推奨されるが絶対に必要ではない要求条件を示す。従って、この要求条件は、適合性を主張するために存在する必要はない。

6　はじめに

現在の通信ネットワークや暗号インフラに量子鍵配送ネットワーク(QKDN)を導入する目的は、暗号アプリケーションに安全性の高い対称鍵を提供することにより、セキュリティレベルを向上させることである。これらの既存のインフラにQKDNを導入することは、システムや要素に多大なオーバーヘッドコスト/影響を与える可能性がある。最悪の場合、QKDNが適切に設計、運用、または暗号アプリケーションとの連携が行われていないと、新たな脆弱性が発生する可能性もある。

QKDNをサポートするためには、さまざまな暗号方式を適切に組み合わせて使用する必要がある。信頼できるノードを介した鍵リレープロセス中に鍵の機密性を確保するために、情報理論的に安全な方式であるワンタイムパッド(OTP)暗号化を使用して、鍵の長期的な機密性を確保することが推奨される。公開鍵暗号やハッシュ関数などの暗号方式は、計算量的に安全であり、鍵の整合性を確保するために使用できる。つまり、

鍵が変更されないことを保証する。これらの方式は、QKDN内の機能要素の認証とアクセス制御を実現するためにも重要な役割を果たす。QKDN内の制御および管理情報は、公開鍵暗号(特に認証と鍵交換のため)と高度暗号化標準(AES)などの対称暗号(特にデータ暗号化のため)の組み合わせによって保護される必要がある。これらの暗号技術の暗号スイートは、公開鍵基盤(PKI)に基づいて、インターネットプロトコルセキュリティ(IPsec)とトランスポートレイヤセキュリティ(TLS)に実装されている。したがって、QKDNを構築することは、量子鍵配送(QKD)技術と既存の安全なネットワークインフラストラクチャの統合を意味する。

QKDNによって提供される鍵は、伝送中の機密性の高い高価値データを暗号化するために使用することができる。QKDN自体はデータストレージの機密性を保護することはできないが、ストレージネットワークのセキュリティを強化するために使用することができる。実際、今日デジタルデータはデータセンターに永遠に保存されており、データは悪意のある攻撃の標的にされやすく、自然災害などの悪意のない事件によって脅かされることさえある。ストレージネットワーク内の重要なデータを長期的に保護するには、QKDNを使用する必要があり、オーバーヘッドコストに値するはずである。セキュアストレージネットワーク(SSN)は、複数のデータサーバで構成され、秘密分散方式によってサポートされている。Shamirしきい値方式などのいくつかの秘密分散方式は、破損したサーバの数が特定のしきい値未満であり、データ共有が高度にプライベートなチャネルを介して交換される場合に、ストレージの情報理論的機密性を保証する。これらの高度にプライベートなチャネルは、QKDNによって提供される鍵を使用したOTP暗号化を使用することによって実現できる。SSNにおける認証、アクセス制御、完全性保護を実現するために、PKIは重要な役割を果たす。

QKDNとPKIおよびSSNの統合の概念を図1に示す。これは、QKDNと安全なネットワークインフラストラクチャの統合の典型的な例である。

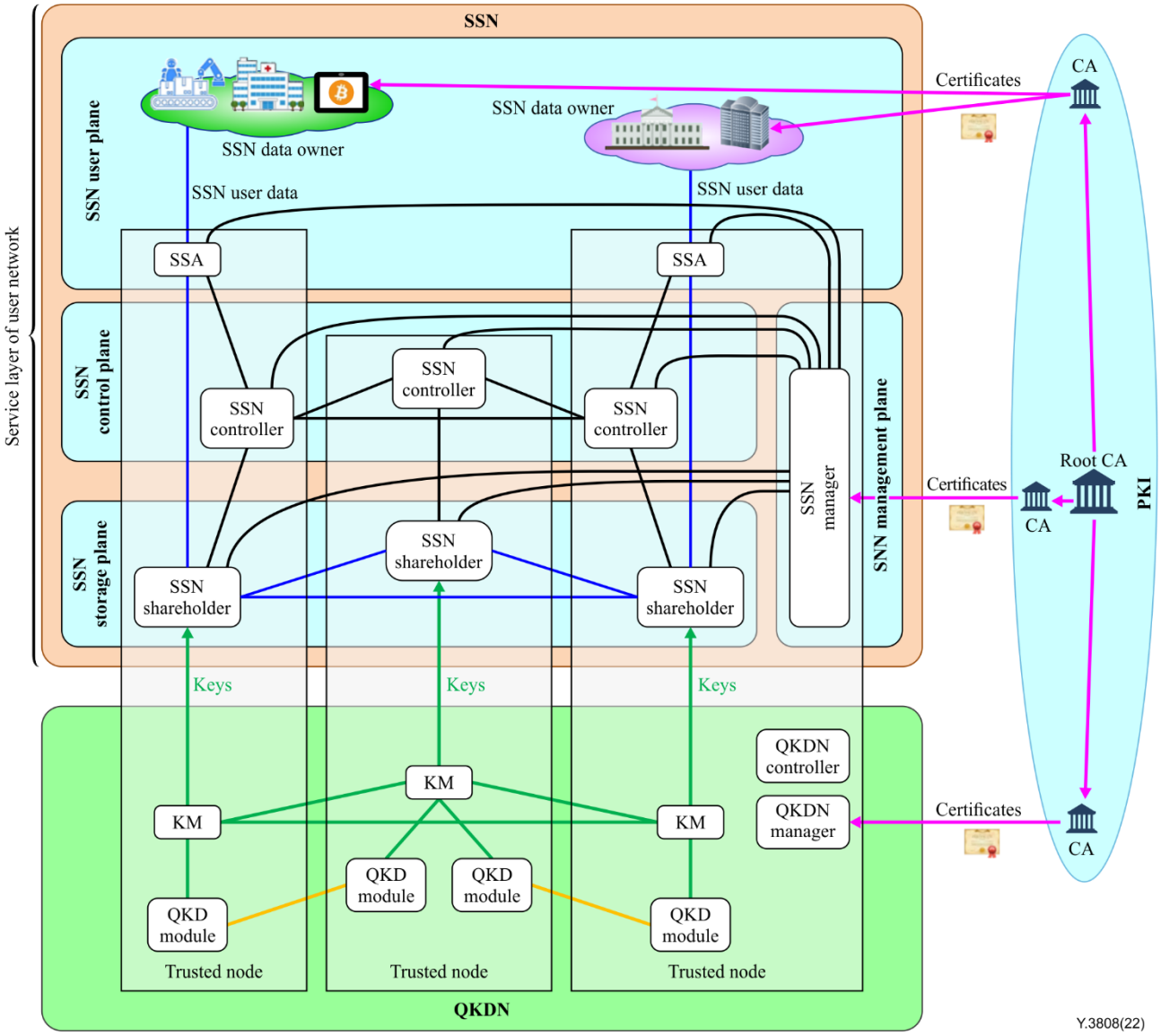

図1 QKDNとPKIおよびSSN統合の概念図

図1のSSNには、以下の機能要素が含まれている:

- セキュアストレージエージェント(SSA):オリジナルデータからシェアを作成し、シェアからオリジナルデータを再構築する機能要素。
- SSNコントローラ:秘密分散プロセスを制御する機能要素。すなわち、オリジナルデータを受信し、データを適切に暗号化し(例えば、秘密分散プロトコルによってデータをシェアに変換する)、SSNシェアホルダーのための通信を制御する。

注:SSNコントローラは、例えば、SDNコントローラが両方のネットワークを制御する場合、QKDNコントローラと通信することができる。

- SSNマネージャ:SSNの障害、構成、アカウンティング、パフォーマンス、およびセキュリティ(FCAPS)機能を管理する機能要素。
- SSNシェアホルダー:シェアの処理、交換、更新、保管を行う機能的要素。
- SSNシェアホルダーリンク:SSAとSSNシェアホルダー間およびSSNシェアホルダー間の通信リンク。SSNシェアホルダーリンクは、図1に青色で示されている。これらのリンクは、OTP暗号などの安全性

の高い暗号化を使用してシェアを送信する。

- SSN制御リンク：SSNコントローラ間およびSSNコントローラとSSNシェアホルダー間の通信リンク。SSN制御リンクは、図1に黒で示されている。これらのリンクは、SSNコントローラとSSNシェアホルダー間の制御および管理情報を送信する。

7 PKI

Public Key Infrastructure (PKI；公開鍵基盤) は、デジタル証明書の発行、失効、および検証をサポートするために確立されたインフラストラクチャである。PKIのフレームワークは、[ITU-T X.509]で規定されている。この勧告は、非対称暗号技術の基本概念と公開鍵証明書のデータタイプを規定している。PKIのCertification Authority (CA；認証局) は、証明書を発行する機能コンポーネントである。CAは、トラストチェーンを構築するためにツリー構造を形成する。ツリーの最上位にあるCAはルートCAと呼ばれ、トラストアンカーになる場合がある。SSNマネージャはPKIから証明書を受信し、SSNマネージャがSSN内のルートCAになることができる。SSNマネージャ内のルートCAは、SSA、SSNコントローラ、SSNシェアホルダーなどのSSN内の機能コンポーネントにある次のCAに対して証明書を発行する。証明書を受信する機能コンポーネントは、公開鍵内のデジタル署名の検証に証明書を使用できる。CAが提供するデジタル証明書は、SSN内のエンティティおよびメッセージの認証にも使用できる。

8 SSN

SSNは、サービスレイヤにおける代表的なユースケースの1つである。この章では、秘密分散、プライベートチャネル、PKIなどを含む、安全なストレージネットワークの基本概念と基盤となる技術をレビューする。特に、長期的なセキュリティに注意が払われる。ストレージセキュリティの技術要件とガイダンスは、[b-ISO/IEC 27040]で検討されている。

8.1 秘密分散

秘密分散は、ストレージ、可用性、および機能の機密性を実現する。秘密分散は、多項式を使用してオリジナルデータから新しい複数のデータシェアが作成され、複数のデータサーバ (シェアホルダー) に保存される。Shamirの(k, n)しきい値スキーム[b-Shamir]は、n個のシェアホルダーを使用し、少なくともk(≤n)のシェアを収集することによって元のデータを復元する。k-1以下のシェアでは、無制限の計算能力を使用しても元のデータを再構築することはできない。破損したシェアホルダーの数がk未満で、シェアがプライベートチャネルを通じて交換される場合、Shamirの(k, n)しきい値スキームは、ストレージの情報理論的な機密性を保証する。つまり、機密性を実現する。シェアは追加および乗算することができる。これは、完全な同形性-機能-を満たすことができることを意味する。n-kまでのシェアが失われても、元のデータは残りのk個のシェアを使用して再構築でき、可用性が提供される。

XORベースの秘密分散方式は、別の秘密分散方式として研究されてきた。XORベースの秘密分散方式は、排他的論理和(XOR)演算のみで分散と再構成を行うため、分散と再構成の高速処理が可能である。

しかし、これらのスキームは完全性を保護することができない。プライベートチャネルもまた、データ伝送の機密性を保護するために何らかの形で実装されるべきであり、これはもう一つの重要な機密性要求条件である。

8.2 QKDNによってサポートされるプライベートチャネル

秘密分散方式自体は数学的アルゴリズムであり、リモートストレージに安全にシェアを送信する(すなわち、送信の秘密性を確保する)解決策を提供しない。データ伝送の秘匿性を実現するQKDNと組み合わせることで、秘密分散方式をプロトコルレベルで情報理論的に安全なSSNに用いることができる。SSAはオリジナルデータ

からシェアを作成し、SSNシェアホルダーに送信する。SSNシェアホルダーはSSNシェアホルダーリンクを通じてシェアを交換する。シェアを送信するこれらのリンクは、QKDNが提供する鍵による暗号化によって保護されたプライベートチャネルである。

8.3　PKIによってサポートされる安全な運用

QKDや秘密分散は、データの機密性や可用性を実現することはできるが、保存されたデータの破損を長期的に防ぐことはできない。そのため、システムにデジタル署名などのセキュリティ技術を導入する必要がある。これらの機能は、図1のPKIのCAで実行される。整合性保護のためには、一定期間の短期的なセキュリティを確保すれば十分であることに注意すべきである。タイムスタンプチェーンは、元のデータのデジタル署名の有効性を任意の期間延長するために使用される。例えば、Pedersenコミットメント方式を採用すると、オリジナルデータへのコミットメントはタイムスタンプされてシェアされる。この方式は、理論的にはオリジナルデータ情報の機密性を保護できるが、データの正確性は必然的に計算量的である。したがって、コミットメントとタイムスタンプは定期的に更新される。これにより、整合性保護を長期的に実現できる。

9　SSNの機能的要求条件

9.1　SSNユーザプレーン

SSAは、次の要求条件を満たす必要がある。

- Req_SSN_A 1　SSAは、データオーナからオリジナルデータを受信することが要求される。
- Req_SSN_A 2　SSAは、オリジナルデータのシェアを作成することが要求される。
- Req_SSN_A 3　SSAは、SSNシェアホルダーにシェアを送付することが要求される。
- Req_SSN_A 4　データオーナがオリジナルデータの復元を要求した場合、SSAはシェアからオリジナルデータを再構築することが要求される。

9.2　SSN制御プレーン

SSNコントローラは、次の要求条件を満たす必要がある。

- Req_SSN_C 1　SSNコントローラは、SSNシェアホルダーへシェアの分配を制御することが要求される。
- Req_SSN_C 2　SSNコントローラは、オリジナルデータを再構築するために、SSNシェアホルダーからのシェアの収集を制御することが要求される。
- Req_SSN_C 3　SSNシェアに障害が発生した場合、SSNコントローラはシェアの再共有を制御することが要求される。
- Req_SSN_C 4　SSNコントローラは、CAから証明書を受信し、セキュリティ機能に使用することが要求される。
- Req_SSN_C 5　SSNコントローラは、SSNコントローラ間の制御および管理情報を暗号化することが要求される。
- Req_SSN_C 6　SSNコントローラは、SSNシェアホルダーの構成を管理することが要求される。

9.3　SSNストレージプレーン

SSNシェアホルダーは、次の要求条件を満たす必要がある。

- Req_SSN_S 1　SSNシェアホルダーは、SSAからシェアを受け取ることが要求される。

- Req_SSN_S 2　SSNシェアホルダーは、シェアを処理する能力を持つことが要求される。
- Req_SSN_S 3　SSNシェアホルダーは、SSNコントローラの制御下で、OTP暗号化などのITセキュア暗号化を使用してシェアを他のSSNシェアホルダーに送信し、保存することが要求される。
- Req_SSN_S 4　SSNシェアホルダーは、長期的な完全性を確保するためにシェアを更新することが推奨される。
- Req_SSN_S 5　SSNシェアホルダーは、オリジナルデータが要求されたときに、OTP暗号化などのITセキュア暗号化を使用してシェアをSSAに送信することが要求される。
- Req_SSN_S 6　SSNシェアホルダーに障害が発生した場合、SSNコントローラはシェアの再共有を実行することが要求される。

9.4　SSN管理プレーン

SSNマネージャは、次の要求条件を満たす必要がある。

- Req_SSN_M 1　SSNマネージャは、SSNコントロールプレーンおよびSSNストレージプレーンのFCAPS管理を提供することが要求される。

10　SSNの機能アーキテクチャモデル

図2は、SSNの機能アーキテクチャーモデルを示している。

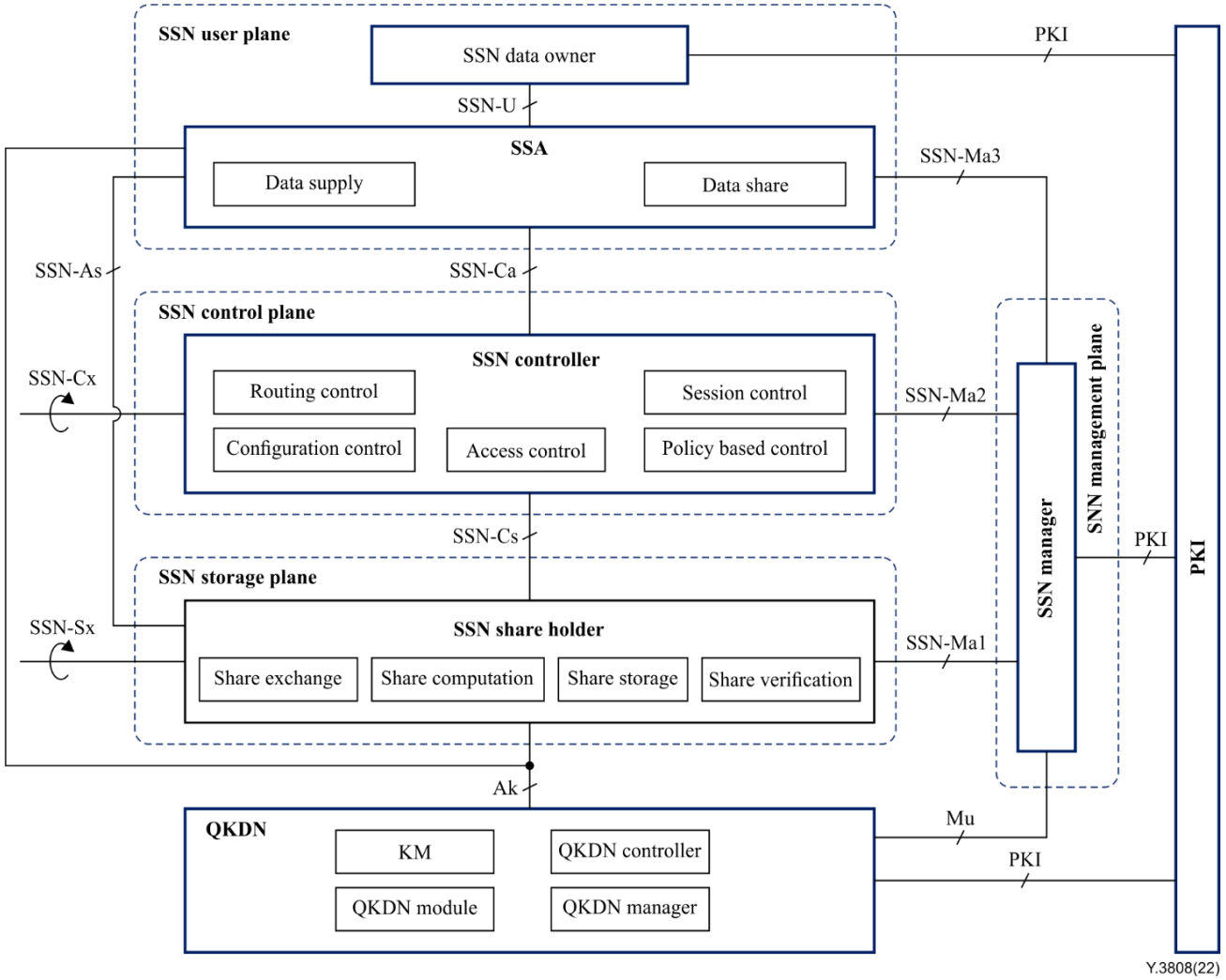

図2：SSNの機能アーキテクチャモデル

10.1　SSAの機能

SSNユーザープレーンでは、SSAがシェアを作成し、オリジナルデータを再構築する。以下の機能要素で構成されている。

- データ供給機能：データオーナからオリジナルデータを受け取り、安全性の高い暗号化(OTP暗号化の使用を推奨)でオリジナルデータをデータオーナに送信する。
- データ共有機能：オリジナルデータのシェアを作成し、シェアからオリジナルデータを再構築することをサポートする。

10.2　SSNコントローラの機能

SSNコントロールプレーンでは、SSNコントローラがSSNストレージプレーンの機能を制御する。以下の機能要素で構成されている。

- セッション制御機能：SSNシェアホルダー間、SSNコントローラーとSSNシェアホルダー間、およびSSAとSSNシェアホルダー間のセッション手順の制御をサポートする。
- ルーティング制御機能：SSNシェアホルダー間の適切な分散ルートを規定し、SSNシェアホルダーリンクの障害、パフォーマンス、および/または可用性ステータスに応じてシェアの再共有ルーティングを

実行し、秘密分散の継続を保証する。

- 構成制御機能：SSNシェアホルダー、SSNコントローラー、SSNシェアホルダーリンク、SSNコントロールリンク、およびこれらのコンポーネントの状態(サービス中、サービス停止、スタンバイ、予約など)に関する構成情報の取得を実行する。障害診断の結果を含むアラームが通知された場合、SSNシェアホルダーとSSNシェアホルダーリンクの再構成を実行する。
- ポリシーベースの制御機能：SSNデータオーナのサービス品質(QoS)と課金ポリシーに基づいてSSNリソースを制御する。
- アクセス制御機能：SSNコントローラによる制御およびサポートの下にある機能および機能要素の要求されたアイデンティティを検証し(すなわち、認証)、実施されたポリシーに基づくアクセス権によって事前に認可された活動または役割に制限する(すなわち、認可)機能を提供する。

10.3 SSNシェアホルダーの機能

SSNストレージプレーンでは、SSNシェアホルダーが他のシェアホルダーとシェアを交換し保管する。以下の機能要素で構成されている。

- シェア交換機能：SSAからシェアを受領し、安全性の高い暗号(OTP暗号の使用が推奨される)を用いて他のSSNシェアホルダーとシェアを交換する。更新のためのシェアを適切かつ適時に交換する。
- シェア計算機能：乱数と秘密分散スキームを使用してシェアの計算を実行する。
- シェアストレージ機能：シェアを安全に保存する。
- シェア検証機能：シェアの更新やシェアからオリジナルデータの再構築などの場合に、証明書を使用してシェアの完全性を検証する。

10.4 SSN管理者の機能

SSN管理プレーンでは、SSNマネージャがSSA、SSNコントローラ、およびSSNシェアホルダーのFCAPS機能をサポートする。

11 参照点

11.1 SSAの参照点

次の参照点は、SSAとの接続に関連する。

- SSN-U：SSNデータオーナとSSAを接続する参照点。SSNユーザーデータを送信する。
- SSN-As：SSAとSSNシェアホルダーを接続する参照点。SSAからSSNシェアホルダーにシェアを送信し、SSNシェアホルダーからSSAにシェアを供給する。

11.2 SSNコントローラの参照点

次の参照点は、SSNコントローラとの接続に関連する。

- SSN-Ca：SSAとSSNコントローラを接続する参照点。SSNコントローラからSSAへ制御情報を通信する。
- SSN-Cs：SSNコントローラとSSNシェアホルダーを接続する参照点。SSNコントローラからSSNシェアホルダーへ制御情報を通信する。
- SSN-Cx：2台のSSNコントローラを接続する参照点。2台のSSNコントローラ間で制御情報を相互に通信する。

11.3　SSNシェアホルダーの参照点

以下の参照点は、SSNシェアホルダーとの接続に関連する。

- SSN-Sx：SSNシェアホルダーと他のSSNシェアホルダーを接続する参照点。他のSSNシェアホルダーとのシェアを交換する。

11.4　SSNマネージャの参照点

次の参照点は、SSNマネージャとの接続に関連する。

- SSN-Ma1：SSNマネージャとSSNシェアホルダーを接続する参照点。SSNマネージャからSSNシェアホルダーへ管理情報を通信する。
- SSN-Ma2：SSNマネージャとSSNコントローラを接続する参照点。SSNマネージャからSSNコントローラへ管理情報を通信する。
- SSN-Ma3：SSNマネージャとSSAを接続する参照点。SSNマネージャからSSAへ管理情報を通信する。

11.5　QKDNの参照点

AkとMuの参照点は[ITU-T Y.3802]で定義されている。

11.6　PKIの参照点

PKIの参照点は、PKIとSSNデータオーナ、SSNマネージャ、QKDNを接続する。PKIは、SSNとQKDNにデジタル証明書を提供する。公開鍵証明書のデータ形式は、[ITU-T X.509]で規定されている。

12　動作手順

この章は、SSNの基本的な動作手順を構成するものであり、各手順の詳細は、SSNの実施状況に応じて構成され、及び/又は変更されることが想定される。

12.1　データ保存手順

データ保存手順を図3に示し、その概要を以下に示す。

1) SSNデータオーナは、データ保存要求をSSAに送信する。
2) SSNデータオーナとSSAはQKDNに鍵を要求し、QKDNはそれらに鍵を提供する。
3) SSNデータオーナは、QKDNが提供した鍵を使用して、OTP暗号化を使用しオリジナルデータをSSAに送信する。
4) SSAは、オリジナルデータからシェアを作成する。
5) SSAは、SSNシェアホルダーにシェア保管要求を送信する。
6) SSAとSSNシェアホルダーが同じトラステッドノードに収容されていない場合、SSAとSSNシェアホルダーはQKDNに鍵を要求し、QKDNはそれらに鍵を提供する。
7) SSAは、OTP暗号化を使用してSSNシェアホルダーにシェアを送信する。SSAとSSNシェアホルダーが同じトラステッドノードに収容されている場合、シェアを送信するためにOTP暗号化は必要としない。
8) SSAがSSNシェアホルダーへのシェアの送信を完了すると、SSAはSSNデータオーナにデータの保存を報告する。
9) SSNシェアホルダーがSSAからシェアを受領した場合、SSAはシェアの一部を保管し、残りのシェアを

他のSSNシェアホルダーに交換するためにSSNコントローラーにルート情報を要求する。

10) SSNシェアホルダーは、SSNコントローラが提供したルート情報に従って、他のSSNシェアホルダーにシェア交換要求を送信する。

11) SSNシェアホルダーと他のSSNシェアホルダーは、QKDNに鍵を要求し、QKDNはそれらに鍵を提供する。

12) SSNシェアホルダーと他のSSNシェアホルダーは、残りのシェアをOTP暗号化し交換する。

13) 他のSSNシェアホルダーは残りのシェアを保管する。

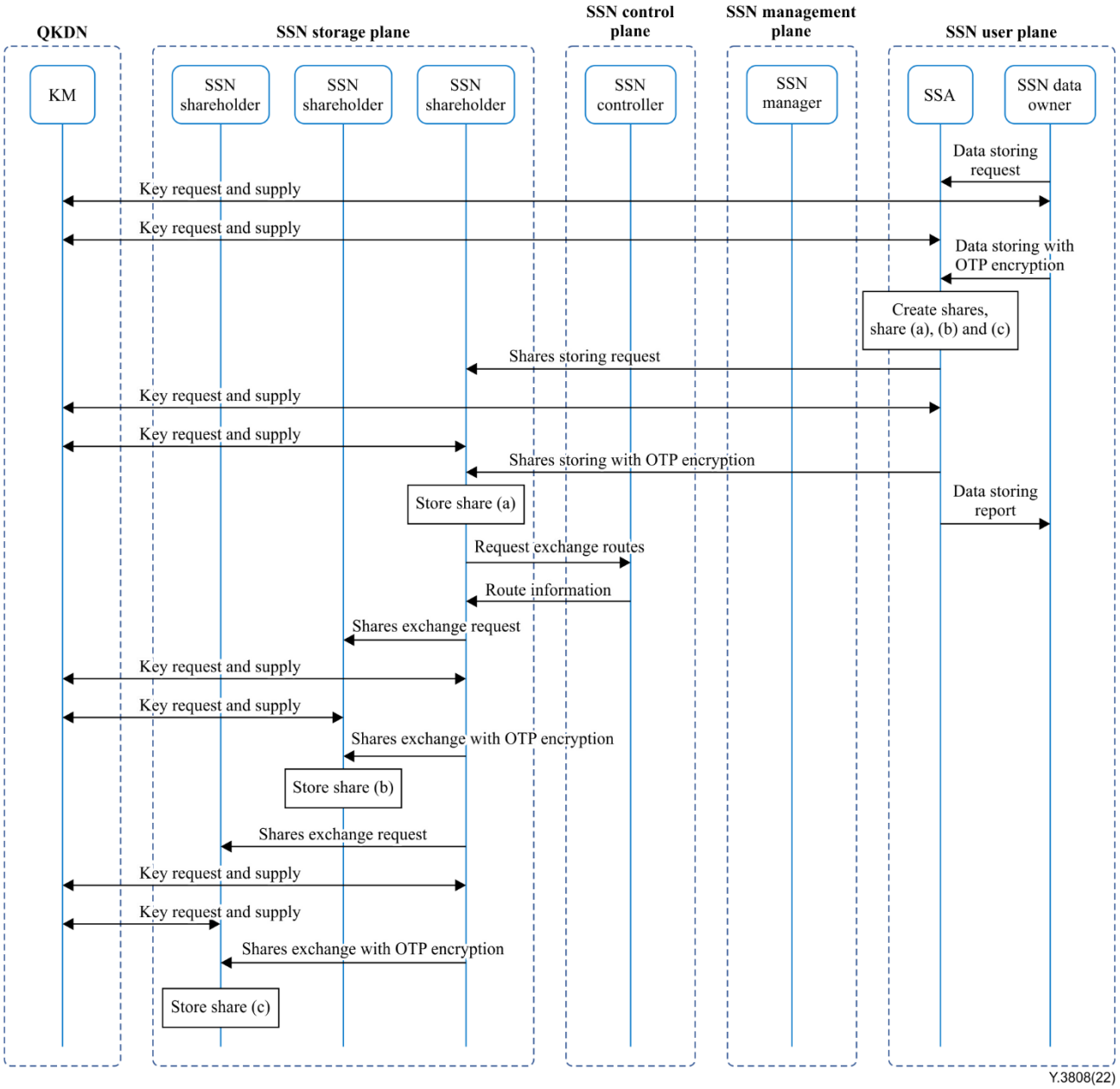

図3 - データ保存手順

12.2 データ取得手順

データ取得手順を図4に示し、その概要を以下に示す。

1) SSNデータオーナは、データ取得要求をSSAに送信する。

2) SSNシェアホルダーがSSAからデータ取得要求を受信すると、SSAはシェアの一部を取得し、残りのシェアを他のSSNシェアホルダーに取得するためのルート情報をSSNコントローラに要求する。

3) SSNシェアホルダーは、SSNコントローラから提供されたルート情報に従って、他のSSNシェアホルダーにシェア取得要求を送信する。

4) SSNシェアホルダーと他のSSNシェアホルダーは、QKDNに鍵を要求し、QKDNはそれらに鍵を提供する。

5) SSNシェアホルダーおよび他のSSNシェアホルダーは、OTP暗号化を使用し残りのシェアを取得する。

6) SSNシェアホルダーとSSAが同じトラステッドノードに収容されていない場合、SSAとSSNシェアホルダーはQKDNに鍵を要求し、QKDNはそれらに鍵を提供する。

7) SSNシェアホルダーは、OTP暗号化を使用してSSAにシェアを送信する。SSAとSSNシェアホルダーが同じトラステッドノードに収容されている場合、シェアを送信するためにOTP暗号化は必要としない。

8) SSAがSSNシェアホルダーから必要なシェアを取得し、SSAはシェアからオリジナルデータを再構築する。

9) SSAとSSNデータオーナは、QKDNに鍵を要求し、QKDNはそれらに鍵を提供する。

10) SSAは、OTP暗号化を使用しオリジナルデータをSSNデータオーナに送信する。

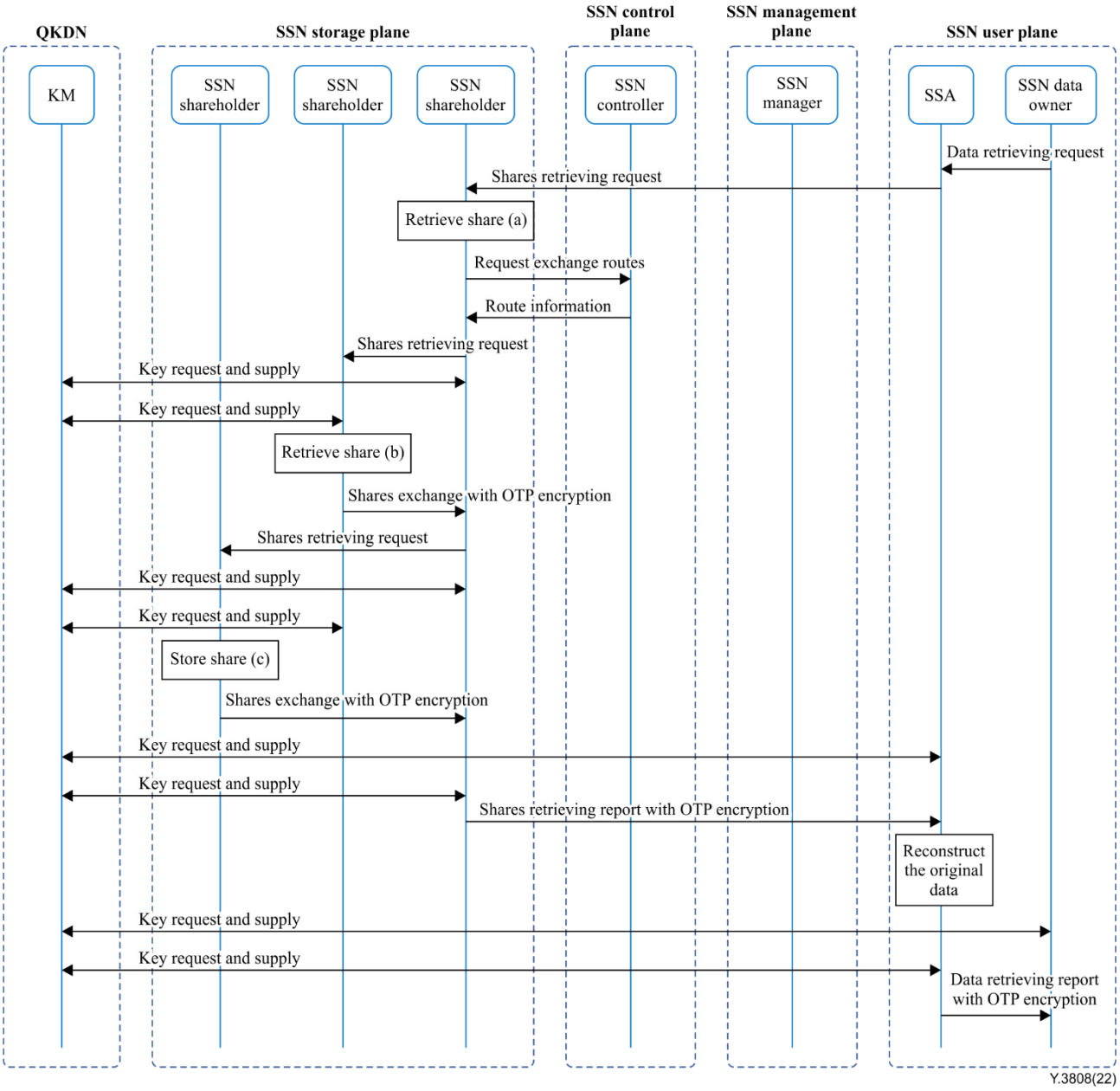

図4：データ取得手順

12.3　シェア更新手続

シェアの更新手続を図5に示し、その概要は以下に示す。

1) SSAは、SSNシェアホルダーにシェア更新要求を送付する。

2) SSNシェアホルダーがSSAからシェア更新要求を受けた場合、SSNシェアホルダーはシェアの一部を更新し、残りのシェアを他のSSNシェアホルダーに更新するためのルート情報をSSNコントローラーに要求する。

3) SSNシェアホルダーは、SSNコントローラから提供されたルート情報に従って、他のSSNシェアホルダーにシェア更新要求を送信する。

4) 他のSSNシェアホルダーがSSNシェアホルダーからシェア更新要求を受けた場合、他のSSNシェアホルダーは残りのシェアを更新する。

5)　SSNシェアホルダーは、SSAにシェア更新報告を送付する。

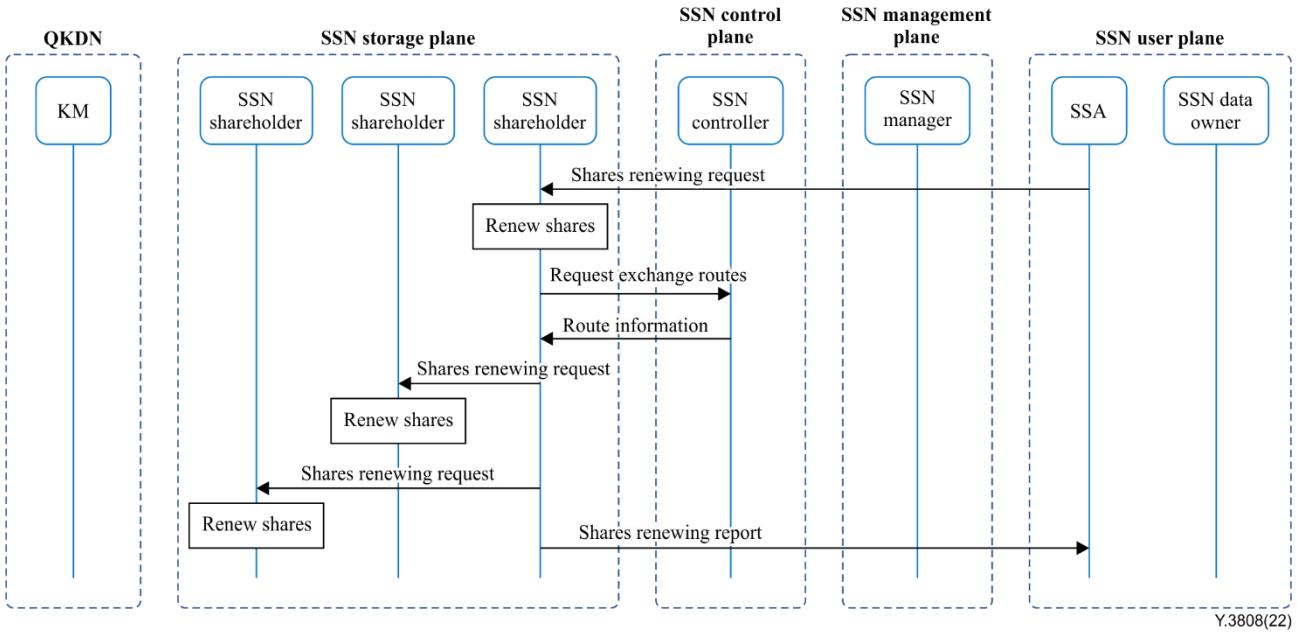

図5：シェア更新手順

参考文献

[b-ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), Overview on networks supporting quantum key distribution.

[b-ISO/IEC 27040] ISO/IEC 27040:2015, Information technology – Security techniques – Storage security.

[b-ETSI GR QKD 007] Group Report ETSI GR QKD 007 (2018), Quantum Key Distribution (QKD); Vocabulary.

[b-Shamir] Adi Shamir, How to share a secret, Communications of the ACM, vol. 22, No. 11, pp. 612-613, 1979.