2022/2/9

JP-LINK に参加する方法

2022 年 2 月版

1. はじめに、と要件

2. JP-LINK のメンバーコードの取得(OZ1 へ依頼)

3. ソフトウェア情報

4. セキュリティサーバーのインストール

5. セキュリティサーバーのセットアップ

6. CSR を OZ1 へ送信する

注：CSR（Certificate Signing Request）とは、SSL/TLS サーバー証明書を発行するための証明書署名要求のこと

7. 証明書のインポート

以下は参加・インストール後のセットアップ作業の一つです。

8.疎通確認

Security Server と Adapter Server の技術サポート問い合わせ先：OZ1 (techoz1@oz1.life)

MISP2 はサポート対象外です。

改訂履歴

2022.2.1 2 月版

4.セキュリティサーバーのインストール　インストール画面中の CN の指定方法を CN:ではなく、/CN=に修正

5.セキュリティサーバーのセットアップ　開発アンカーの URL を update、URL にアクセス時にファイルダウンロードできず、表示された場合は XML にして保存を追加。キーラベルの任意の入力に関して追記。

2/3 8.疎通確認の項目を追記

2/8 疎通確認の前に、内部通信プロトコルの選択を追記

1. はじめに、と要件

JP-LINK の使用を開始するには、セキュリティサーバーを設定する必要があります。Security Server は、ネットワーク内の他のメンバーと通信するための安全な方法を提供します。

セキュリティサーバーの主な役割は、メンバー間ピアツーピアで送信されるメッセージの認証と検証を提供することです。サービスプロバイダーの場合、セキュリティサーバーは独自の情報システムへのアクセス制御も提供します。

2. メンバーコードの取得(OZ1 へ依頼)

JP-LINK に参加するには、メンバーとして承認されるためにメンバーコードの取得が最初に必要になります。

各メンバーが機能するために一意のメンバーコードを持っている必要があります。コードを生成するために、以下の情報を OZ1 (techoz1@oz1.life)へ送信してください。

管理者の e メールアドレス

組織名

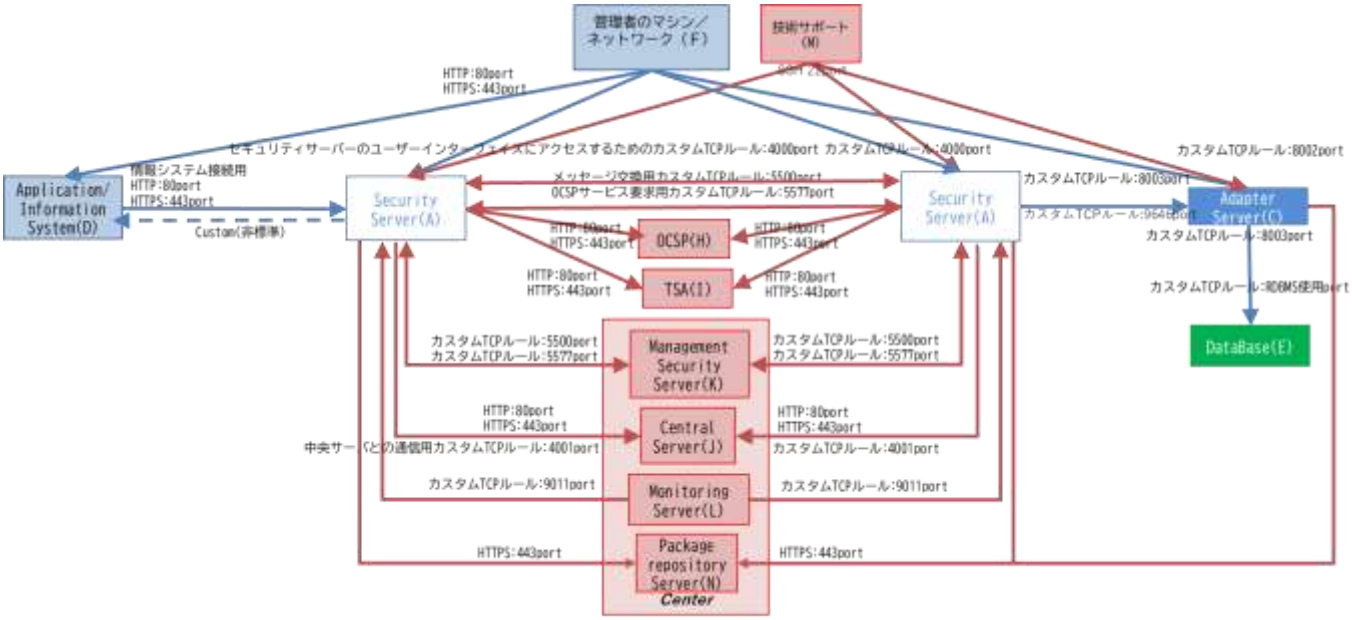
追加情報（任意）

3. ソフトウェア情報

セキュリティサーバーは、現在 Ubuntu 18.04 LTSx86-64 で実行するように設計されています。最小要件は、3GB のメモリと 10GB のドライブスペースです。

解放するポート:

- セキュリティサーバー間のメッセージ交換のための TCP5500 インバウンド/アウトバウンド
- セキュリティサーバー間の OCSP サービス要求の TCP5577 インバウンド/アウトバウンド
- 中央サーバーとの通信用の TCP4001 アウトバウンド
- グローバル設定をダウンロードするための TCP80 アウトバウンド
- タイムスタンプサービスおよび OCSP サービスとの通信用の TCP80 / 443 アウトバウンド
- セキュリティサーバーのユーザーインターフェイスにアクセスするための TCP4000 インバウンド（ローカル）
- 情報システム接続用の TCP80 / 443 インバウンド/アウトバウンド（ローカル）



通信フロー図

注：技術サポートからのリモートサポートサービスは将来構想の為、現在は想定不要です。

4.セキュリティサーバーのインストール

1.ユーザーインターフェイスのすべての役割が付与されているシステムユーザーを追加します。

```
Sudo adduser ユーザー名
```

2.オペレーティングシステムのロケールを設定します。次の行を**/etc/environment** に追加します。

```
LC_ALL=en_US.UTF-8
```

3.X-Road パッケージリポジトリと nginx リポジトリのアドレスを apt リポジトリに追加します。下記コマンドは途中で改行を挟まず、1行で入力してください。

```
1. sudo apt-add-repository -y "deb https://artifactory.niis.org/xroad-release-deb $(lsb_rele
   ase -sc)-current main"
```

4.X-Road リポジトリの署名キーを信頼できるキーのリストに追加します。下記コマンドは途中で改行を挟まず、1行で入力してください。

```
1. curl https://artifactory.niis.org/api/gpg/key/public | sudo apt-key add -
```

5.セキュリティサーバーソフトウェアをインストールします。インストール作業は次項の設定等の作業も含め、最大で数十分程度を要する可能性があります。

```
1. sudo apt-get update
2. sudo apt-get install xroad-securityserver
```

6.インストール中に、いくつかの設定を行う必要があります。基本はデフォルト値ですが、変更が必要な場合もあります。求められる設定の内容と、その設定例を以下に記載します。

1. ユーザーインターフェイスですべてのアクティビティを実行する権限が付与されるシステムユーザーを指定するように求められます。手順 1 で追加したユーザーを指定してください。
2. データベースの設定については、デフォルトの内容(127.0.0.1:5432)のままで OK です。
3. WEB UI の CN(Common Name)設定は、/CN=以降をいったんすべて消去し、/CN={DNS 名}または/CN={グローバル IP アドレス}を設定ください。注意点として値は 63 文字以内に収めてください。例：/CN=XX.XX.XX.XX
4. WEB UI の SANs(Subject Alternate Names)設定は IP:以降をいったんすべて消去し、IP:{グローバル IP アドレス}をご設定ください。例：IP:XX.XX.XX.XX

5. 組織内のクライアントから Security Server にアクセスする際の CN(Common Name)設定は、/CN=以降をいったんすべて消去し、/CN={DNS 名}または/CN={グローバル IP アドレス}を設定ください。注意点として値は 63 文字以内に収めてください。
6. 組織内のクライアントから Security Server にアクセスする際の SANs(Subject Alternate Names)設定は IP:{グローバル IP アドレス}をご設定ください。

インストール後のチェック

7.すべてのプロセスが開始されたかどうかを確認します。次のサービスが実行されている必要があります（プロセス番号は単なる例です）

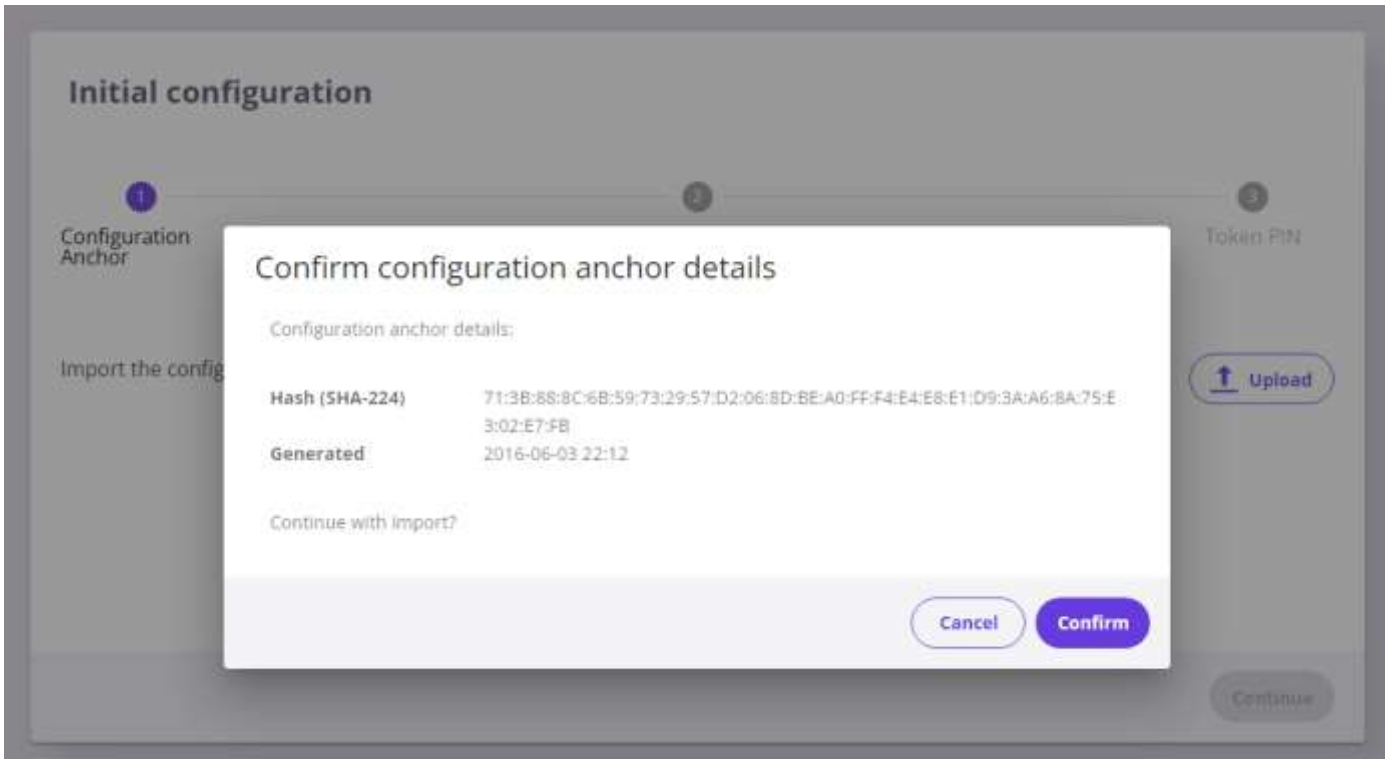
```
$ sudo systemctl list-units "xroad*"

UNIT                            LOAD   ACTIVE SUB     DESCRIPTION
xroad-addon-messagelog.service loaded active running X-Road Messagelog Archiver
xroad-base.service             loaded active exited  X-Road initialization
xroad-confclient.service       loaded active running X-Road confclient
xroad-monitor.service          loaded active running X-Road Monitor
xroad-proxy-ui-api.service     loaded active running X-Road Proxy UI REST API
xroad-proxy.service            loaded active running X-Road Proxy
xroad-signer.service           loaded active running X-Road signer
```

5. セキュリティサーバーのセットアップ

セキュリティサーバーのユーザーインターフェイスには、https://{SECURITYSERVER}:4000/ からアクセスできます。ここで、{SECURITYSERVER}はセキュリティサーバーの IP 名または DNS 名です。

ログインするには、インストール時に選択したアカウント名を使用します。ユーザーインターフェイスの起動中に、Web ブラウザに「502 BadGateway」エラーが表示される場合があります。

1.サーバーが最初に要求するのは、グローバル構成アンカーファイルを提供することです。このファイルには、参加しているエコシステムに関する情報と、利用可能な CA および TSA サービスに関する重要な情報が含まれています。



開発アンカー

```
Hash （SHA-224）：71：3B：88：8C：6B：59：73：29：57：D2：06：8D：BE：A0：FF：F4：E4：E8：E1：D9：
3A：A6 ：8A：75：E3：02：E7：FB
```

ダウンロード https://www.roksnet.com/download/configuration_anchor_roksnet-dev_internal_UTC_2021-06-09_20_29_07.xml （この URL は将来変更になる可能性があります。それに伴いアンカーの Hash 内容の変更もあり得ます。）

プロダクションアンカー（これは将来本番運用時に利用されてください）

```
Hash （SHA-224）：3A：D4：74：FD：40：01：1B：1A：B5：7D：F3：C9：87：9C：EF：F0：C4：4D：F6：4A：
AD：02 ：C6：63：24：F0：A1：72
```

ダウンロード https://www.roksnet.com/download/configuration_anchor_roksnet_internal_UTC_2017-04-26_11_19_52.xml （この URL は将来変更になる可能性があります。）

ブラウザに以下のような xml の内容が表示された場合は、その内容を xml ファイルとして保存ください。

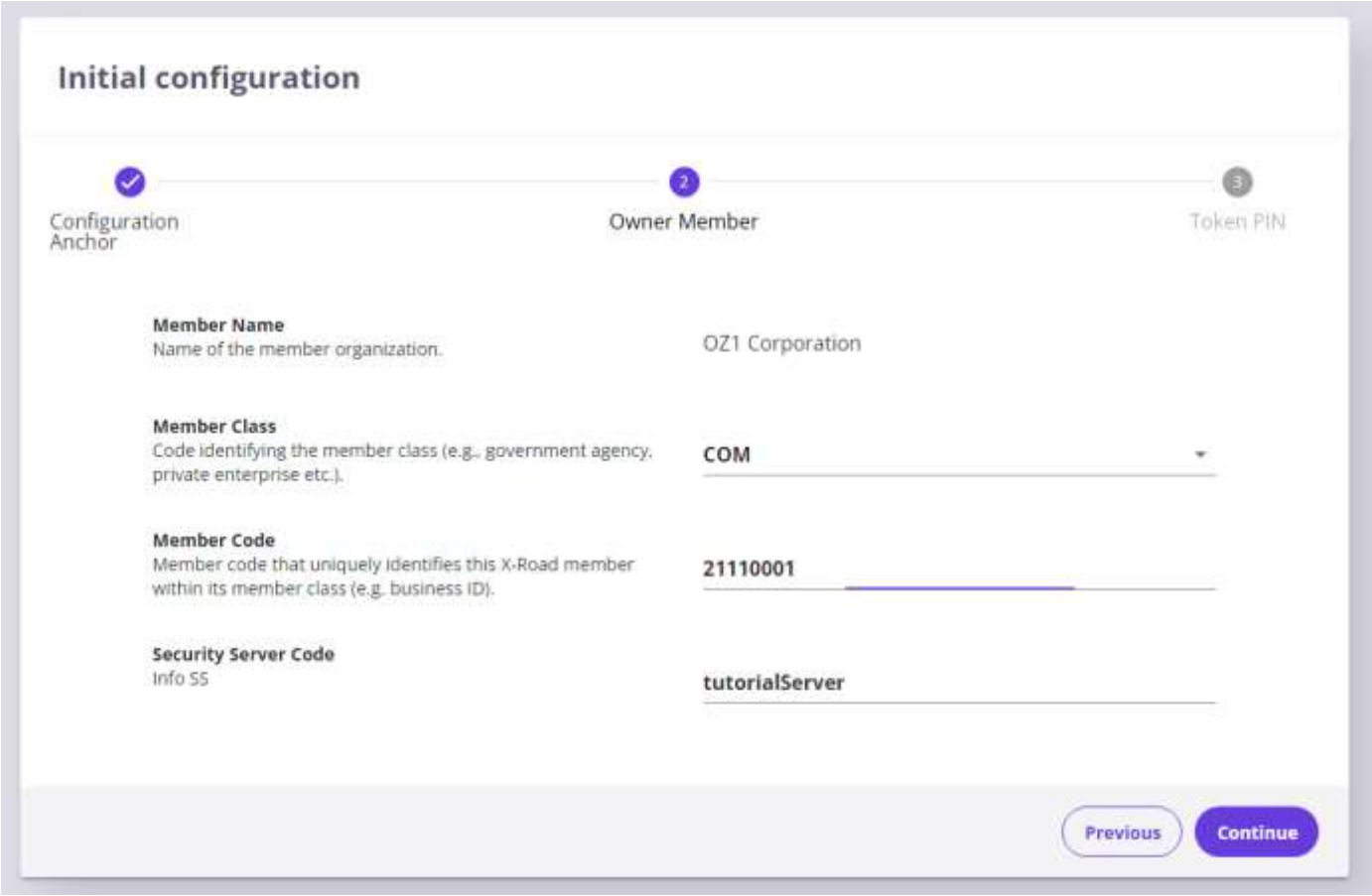
以下内容は URL のアップデートに伴い変更になるため、一致を確認する必要はございません。

This XML file does not appear to have any style information associated with it. The document tree is shown below.
<ns3:configurationAnchor xmlns:ns2="http://x-road.eu/xsd/identifiers" xmlns:ns3="http://x-road.eu/xsd/xroad.xsd">
<generatedAt>2016-06-03T13:12:15.255Z</generatedAt>
<instanceIdentifier>roksnet-dev</instanceIdentifier>
<source>
<downloadURL>http://198.211.127.118/internalconf</downloadURL>
<verificationCert>MIICqTCCAZGgAwIBAgIBATANBgkqhkiG9w0BAQ0FADAOMQwwCgYDVQQDDANOL0EwHhcNNzAwMTAxMDAwMDAwWhcNMzgwMTAxMDAwMDAwWjAOMQwwCgYDVQQDDANOL0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCYR91E0/waxqiK3sCjs7+DH1tpLCkQEdab9cFfQE717u8KMNjT/N0S3v6KiMWPBJbmB722Bk6/ykqSBN6yqog/Qp6ZKiLmghRIKwTB2I8OcHdOp5ExRhVC8qS0k0j6TzXKwKQDi3fVTLVJIq3RpdILu1tHqbAh31GWsBuoP4ahb4W5+cvjE9UdHxVq+5DY5EwG/FeiSfIhn44BiUY5uJ4gPx8ACV2f4z8Dqfq0immTHIkDjEdNDuGO4eFxYt4FPfq2FuodYE48rEMW/NcmmoR6pniixbI8L6IGL5/nP92SEe/JfqwCvTgTFkIlnNXpsofeWqOCAihUY1T9L+qyCKLAgMBAAGjEjAQMA4GA1UdDwEB/wQEAwIGQDANBgkqhkiG9w0BAQ0FAAOCAQEAhWmXvp/hTG/lmFYV6PRNGYW2T/04PAL476D1mR6l550lchhcW68I+A0ydTiKAnnBEBqgqVKD5skvyyDkxZXnG6Z8vzXjAjYt4JPaYNuXCJxzAqoxB+rg9iqktSt3mp5tZ466qMXKt8r/MxoCnz+NbIGLZF1AnjKR2JbFDyuaOjGGJ+OtcZFqX0Cp0vcy2Z1fEICrwfySE3NoJRifDy3W/XUVejr4uRQ0CDT8PG8CkdqtezWLEeEP05rrBf3Z0AoZhqbH0gGDmH/cR1U7h3NxXPVVmrvgwIgqQlqAdN3iiMKTnba5ITKDh63sU0D/fQ6tZxDj3IZuwS1hBLkz3ZatzQ==</verificationCert>
</source>
</ns3:configurationAnchor>

2.構成が正しくダウンロードされている場合（そうでない場合はポートを確認します）、サーバーは次の情報を要求します。

- メンバークラス–セキュリティサーバーの所有者のメンバークラス（民間企業の場合は COM、政府機関の場合は GOV、非営利団体の場合は NGO）
- メンバーコード–OZ1 から送信されたセキュリティサーバー所有者のメンバーコード。
- セキュリティサーバーコード–自由形式
- PIN–サーバーが証明書にアクセスするために使用されるソフトウェアトークンの PIN

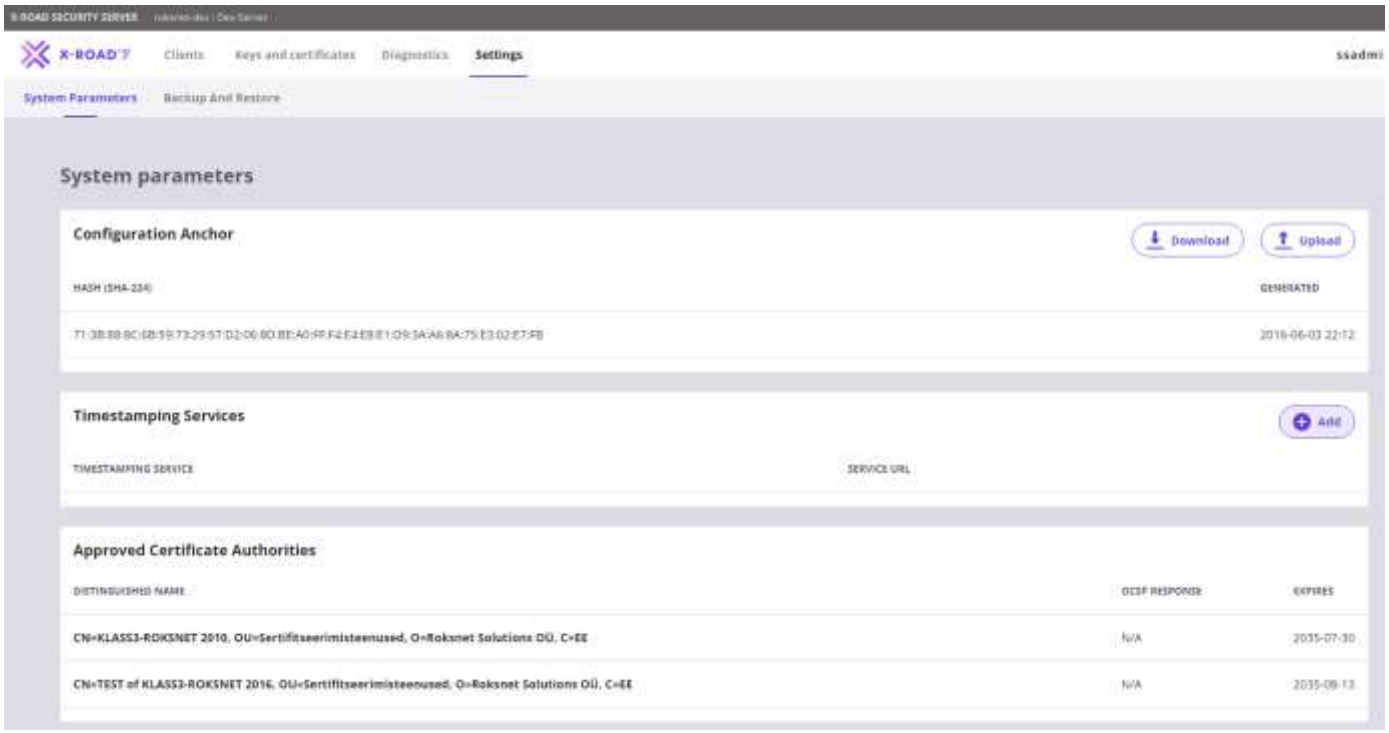
以下は入力例です：

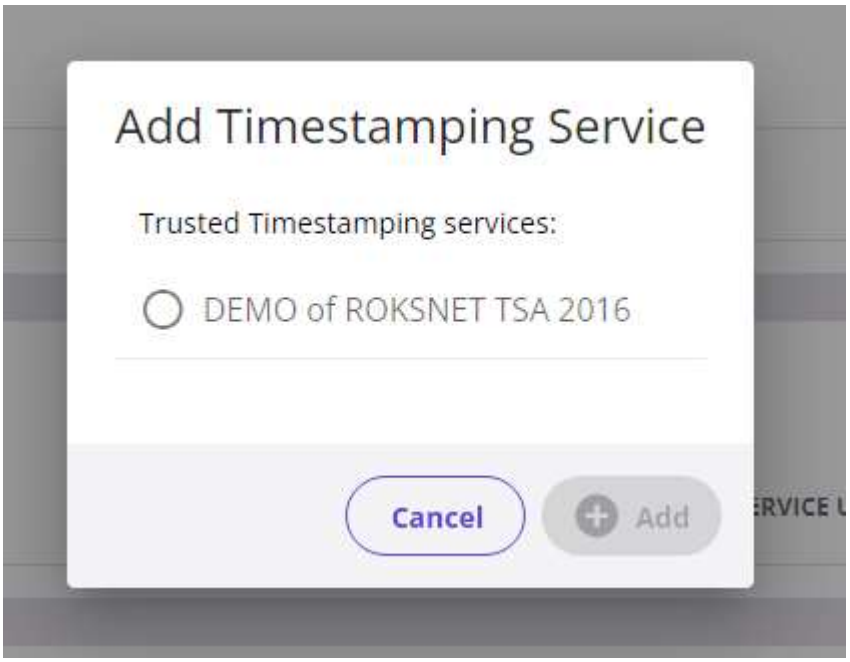


以下に示すように、サーバーが警告を表示する場合、これは問題なく、セットアップを続行できます。これは、メンバーがまだグローバル構成になっていないことを意味します。

3.ページの上部にソフトトークンの PIN が入力されていないという警告メッセージが表示されます。赤いメッセージをクリックして PIN を入力します。または、[Keys and Certificate]メニューから、アクセスし、[Log in]テキストをクリックすることでも PIN の入力画面へ遷移できます。

4. [Settings]＞[System Parameters]セクションに移動し、TSA サービスを追加します。利用可能なすべての TSA サービスが一覧表示されます。



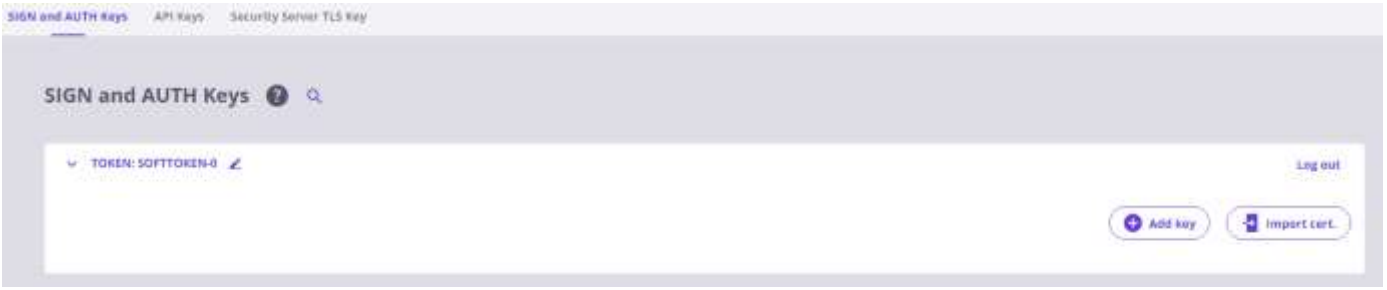


5. [Keys and Certificate]セクションでキーと証明書要求の生成を開始します

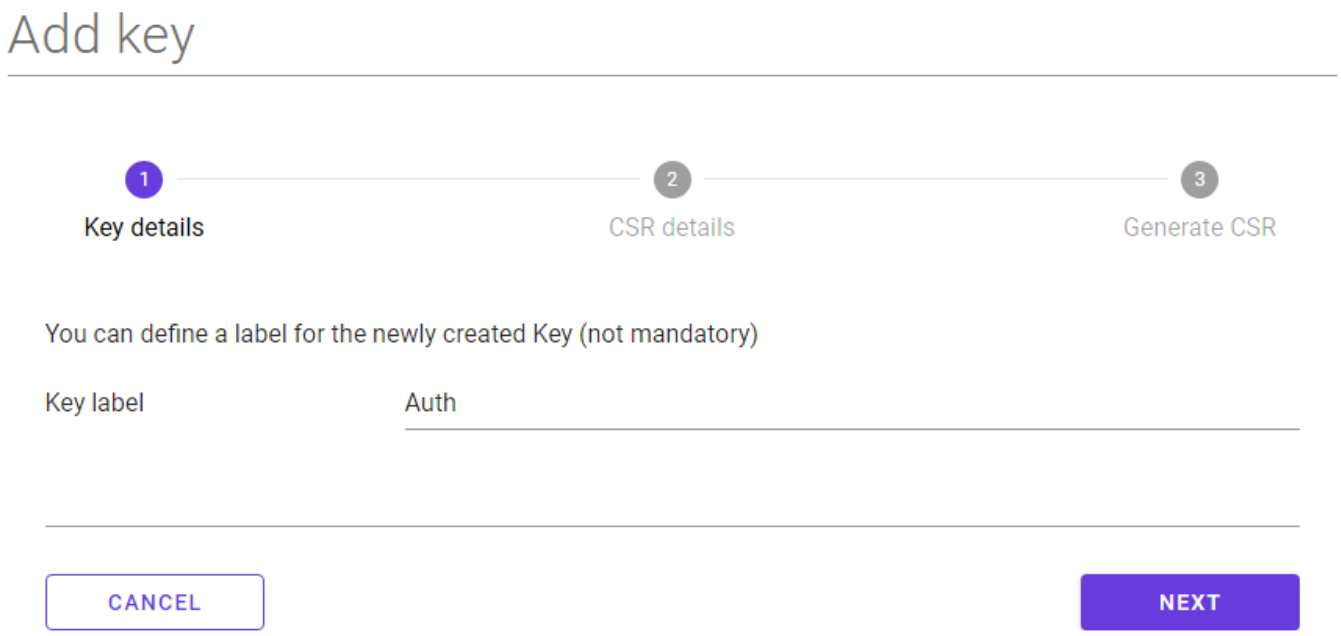
セキュリティサーバーは 2 種類の証明書を使用します

- 安全な TLS チャネルを開始するときのセキュリティサーバー間の認証用の AUTH 証明書。AUTH 証明書は、セキュリティサーバーごとに 1 つ使用されます。
- e スタンプの署名証明書。SIGN 証明書は、メンバー/ユーザー（つまり組織）ごとに 1 つ使用されます。

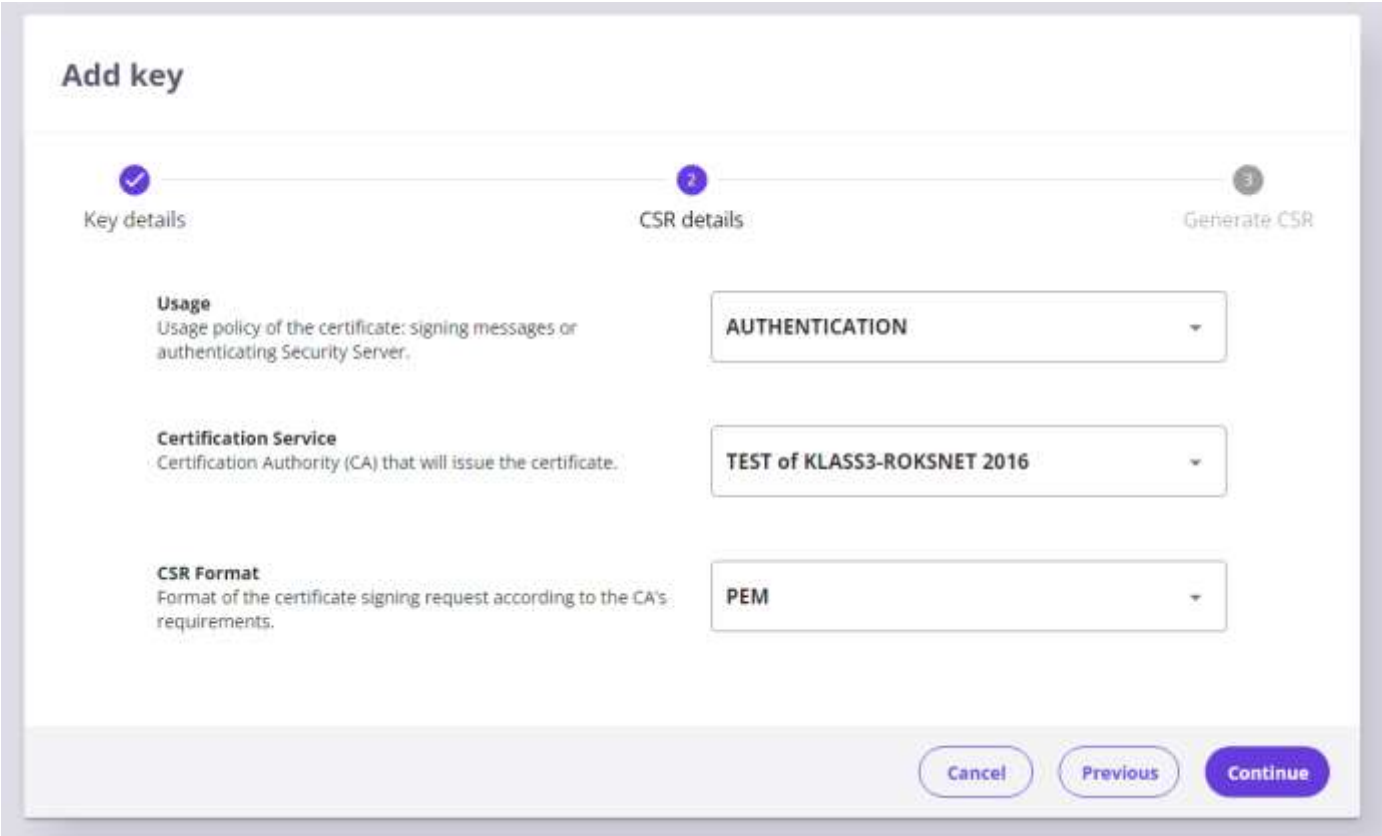
SoftToken-0 を選択して、[+Add Key]ボタンを押下し、AUTH キーと SIGN キーを生成します。



5-1.認証用 Auth 証明書にキーラベルの入力を行います。認証用と署名用の 2 種類のキーを登録するため、分かりやすい名前を入力することを推奨します。

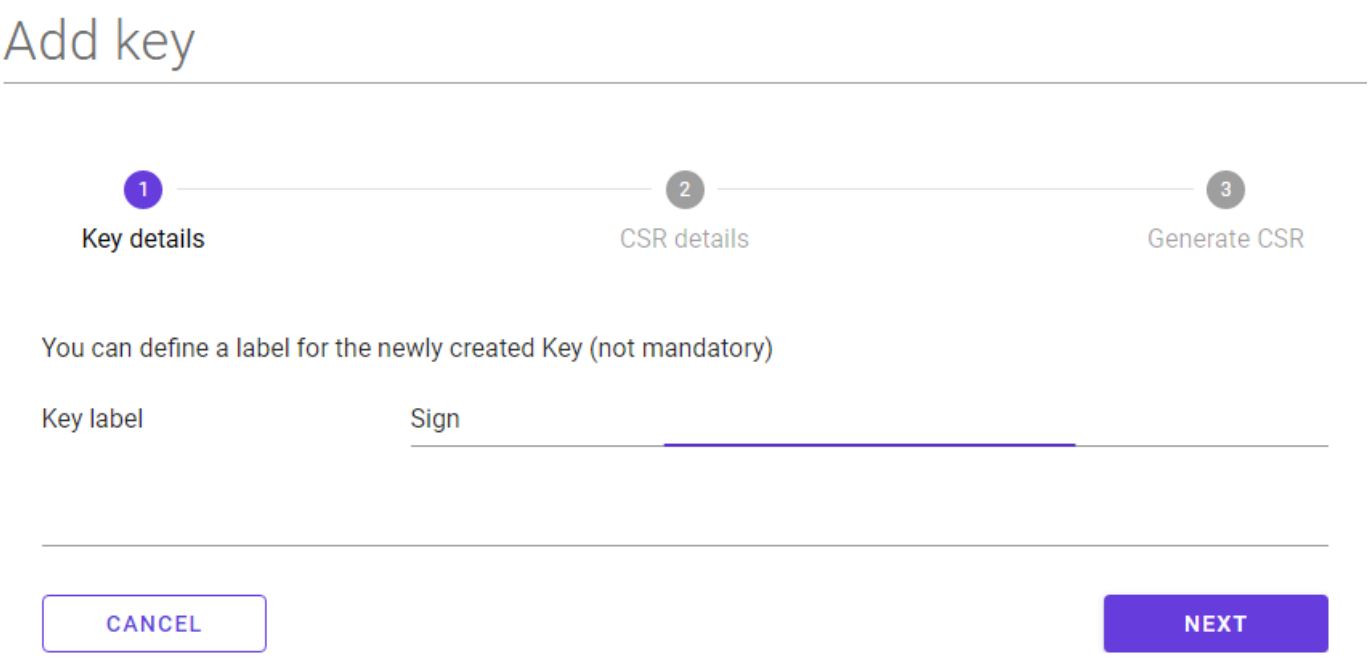


5-2.認証用 AUTH 証明書の入力内容は次の通りです。

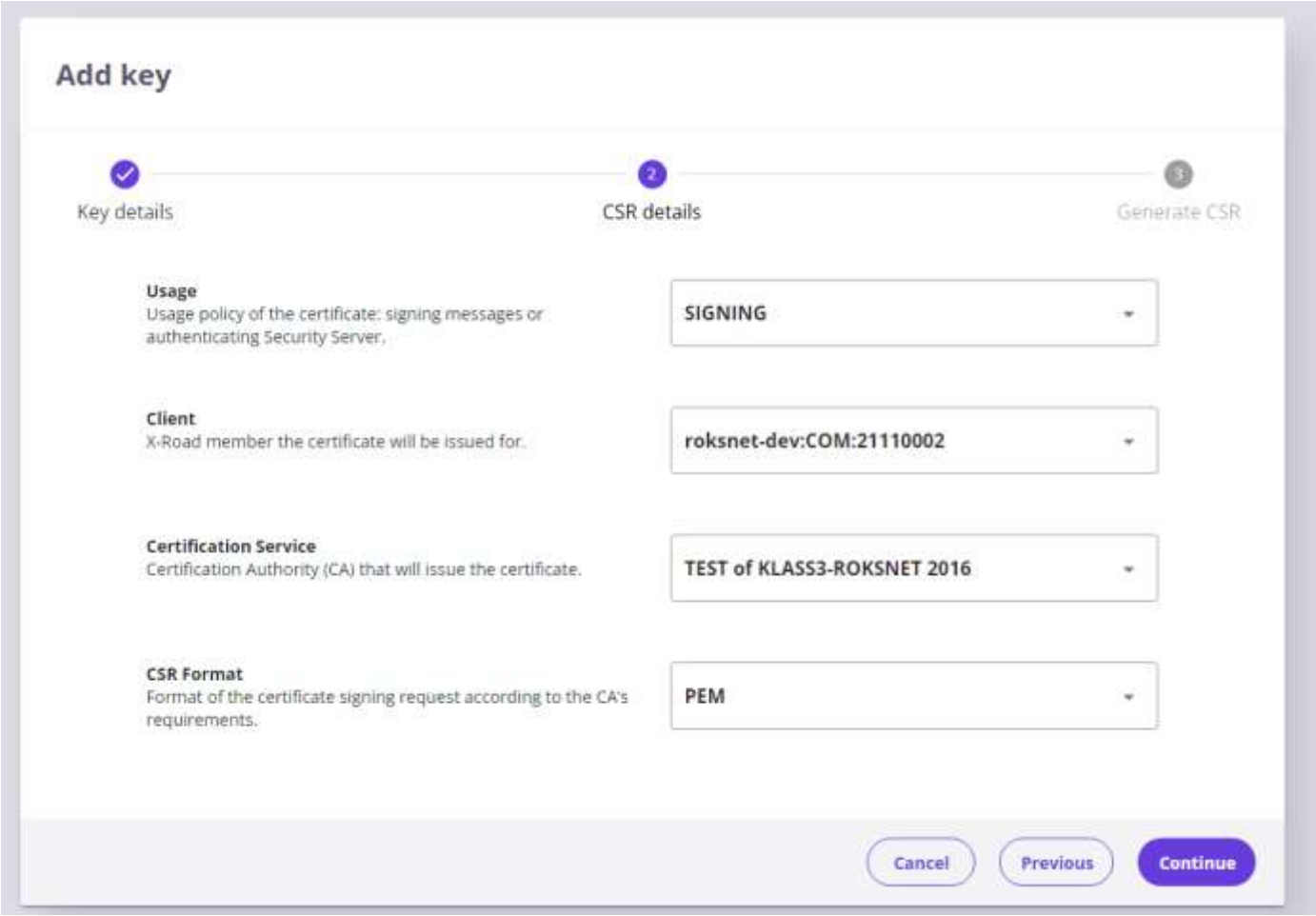


Continue ボタンを押下し、次の画面で CSR ファイルをダウンロードしてください。

5-3.続いて同様に Add key ボタンを押下し、署名用 SIGN 証明書のキーラベルの入力を行います。分かりやすい名前を入力することを推奨します。

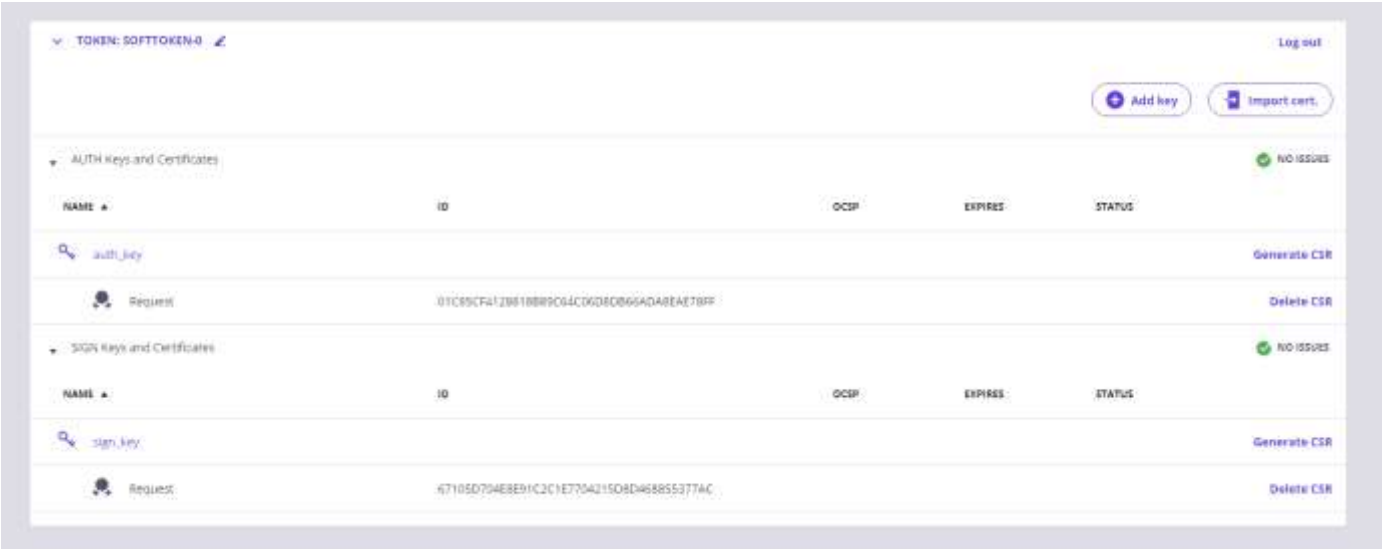


5-4.署名用の SIGN 証明書の入力内容は次の通りです。



Continue ボタンを押下し、次の画面で CSR ファイルをダウンロードしてください。

5-5.認証用・署名用の鍵の作成が完了すると次のような画面になります。



6. 認証用・署名用の両方の CSR をダウンロードした後、次のステップ（CSR の送信）に進みます。

6. CSR を OZ1 へ送信する

以下の内容を OZ1 (techoz1@oz1.life)にメールで送信してください。
メールアドレス
環境：開発環境もしくは本番環境
メンバーコード：
メンバー名：
所属国：日本
認証用の CSR ファイル名、及び認証用の CSR ファイルの添付
署名用の CSR ファイル名、及び署名用の CSR ファイルの添付

将来、以下のように利用規約などを準備してご確認いただく予定です。

- [ ] OZ1 の利用規約、技術宣言、プライバシーポリシーを読み、同意します。
- [ ] OZ1 で公開されている価格表に従って、OZ1 からサービスを受けることを読み、同意します。

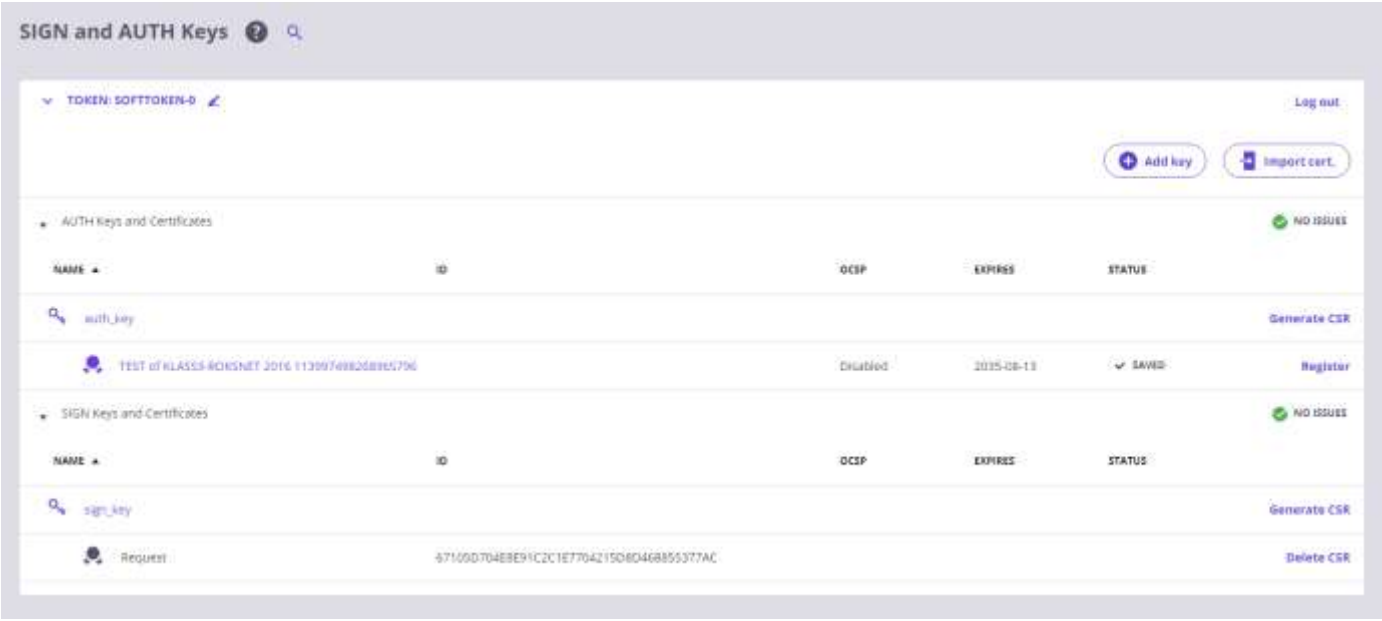
注：個人の同意に基づく個人情報データの移動を伴わない情報連携に関しては将来も費用が発生しない予定です。

7.証明書をインポートします

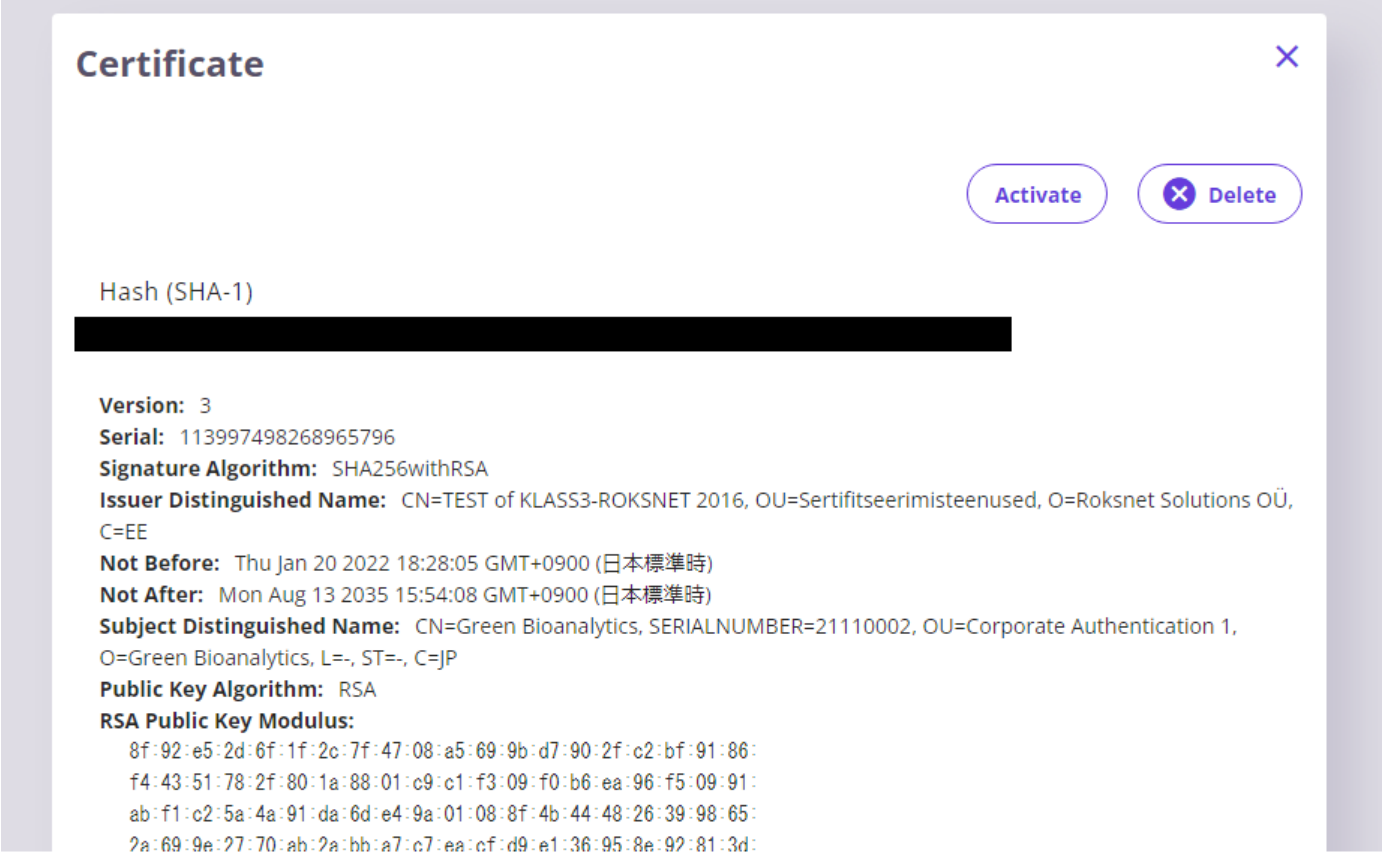
証明書を受け取ったら、「キーと証明書」ビューでそれらをインポートできるようになります。

1.[Import cert.]ボタンを押下し、署名用(sign)CSR ファイルをインポートします。

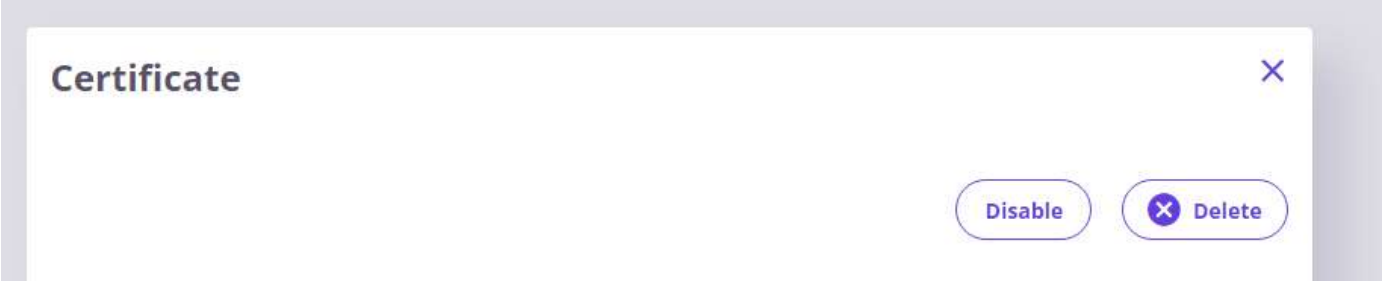
2.[Import cert.]ボタンを押下し、認証用(auth)CSR ファイルをインポートします。両方の CSR ファイルがインポートされると、下図のような状態となります。



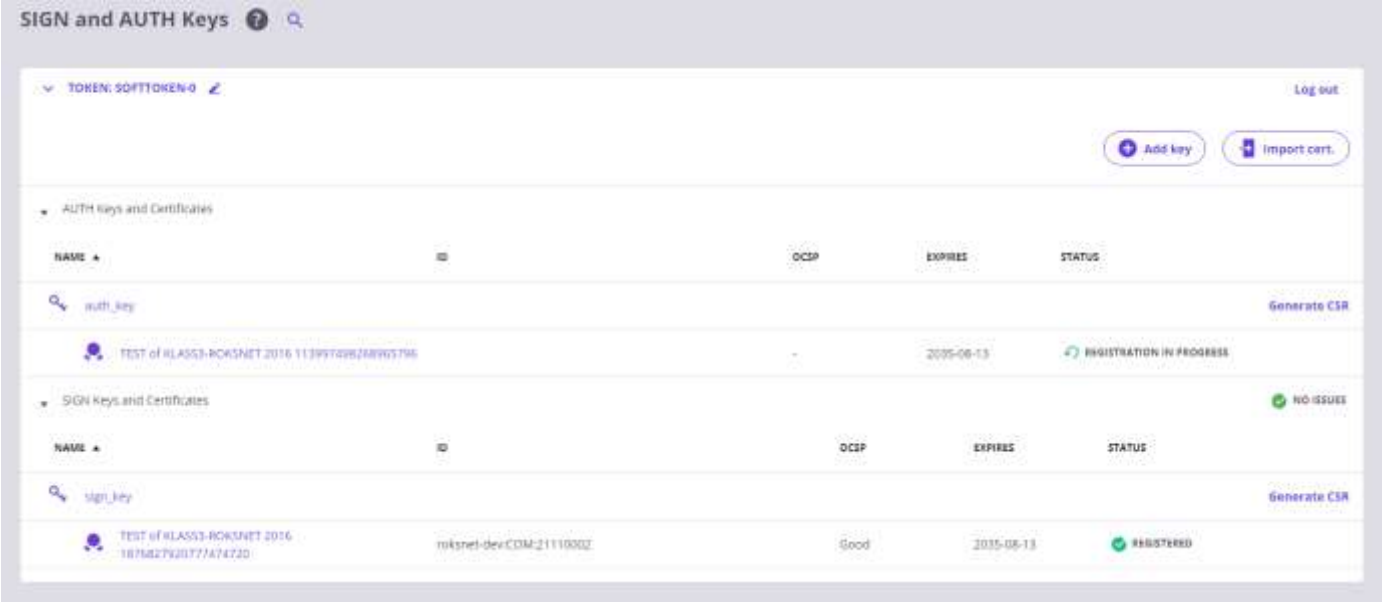
3.認証用(auth)CSR はインポートした直後は、無効(Disabled)の状態でインポートされます。 有効化するためには認証用 CSR のラベルを選択し、Certificate の画面を表示させます。その後、[Activate]ボタンを押下し、有効化してください。



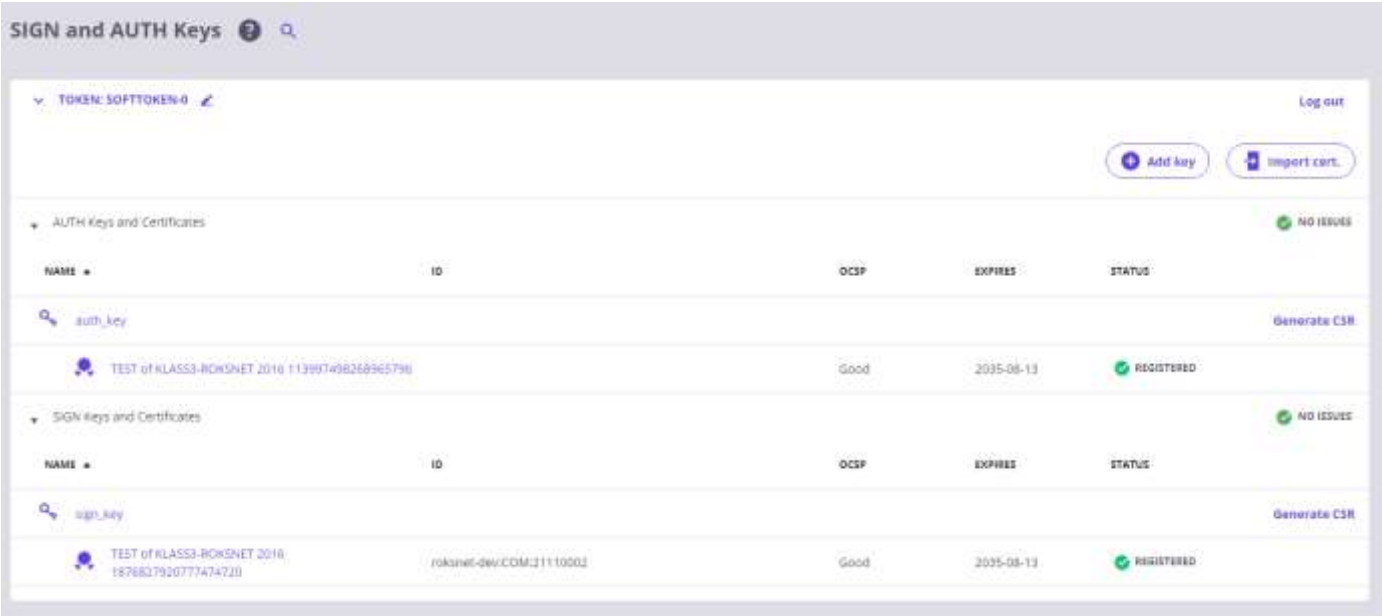
※認証用(auth)CSR を有効化した後、再度無効にしたい場合には、[Active]ボタンが[Disable]ボタンに更新されるので、[Disable]ボタンを押下してください。



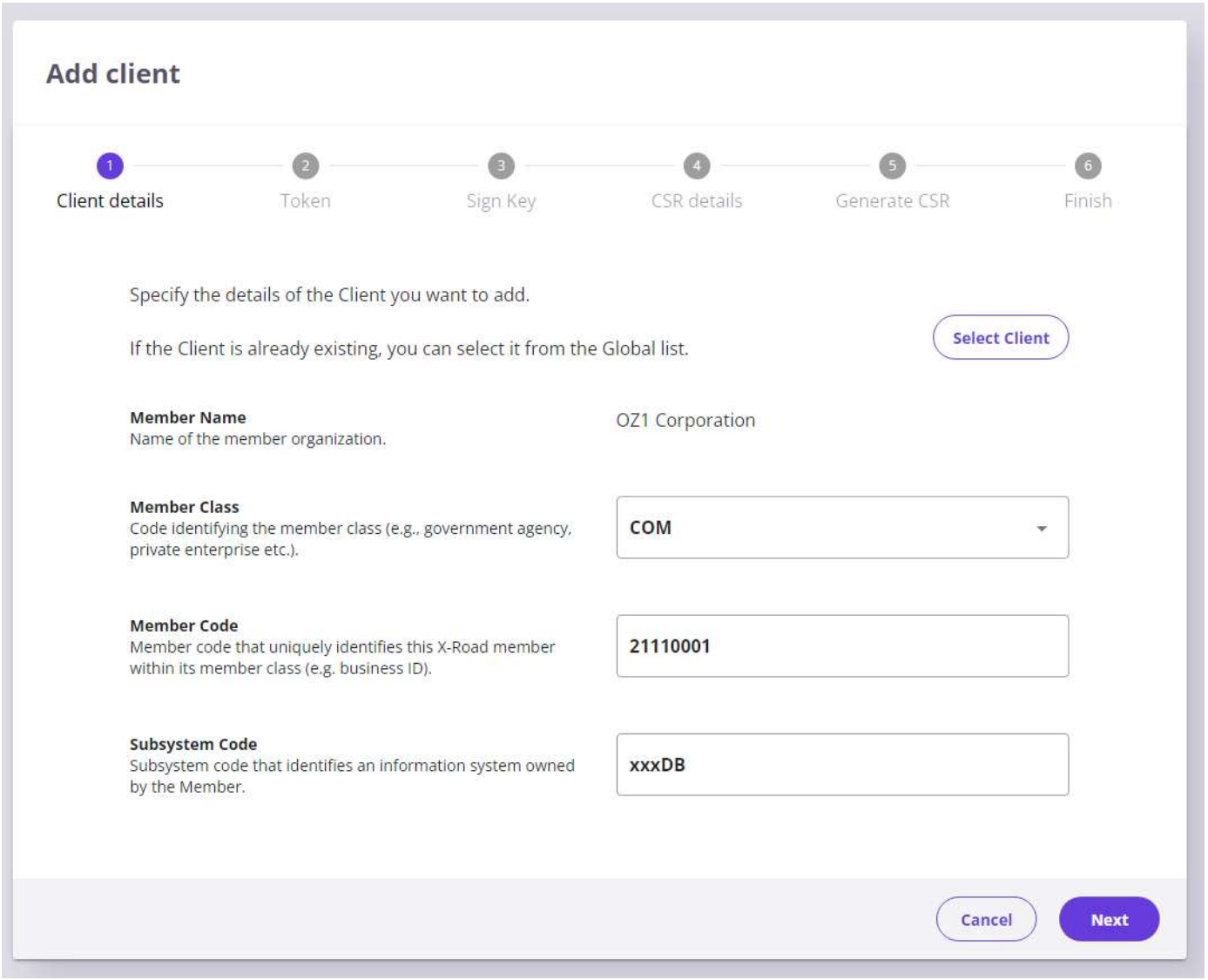
4.認証用(auth)CSR を有効化した後、[Register]ボタンを押下し、認証用 CSR の登録申請を行ってください。登録ボタン押下直後は、REGISTRATION IN PROGRESS(登録中)というステータスに更新されます。環境により申請が受理されるまでの待機時間は異なります。



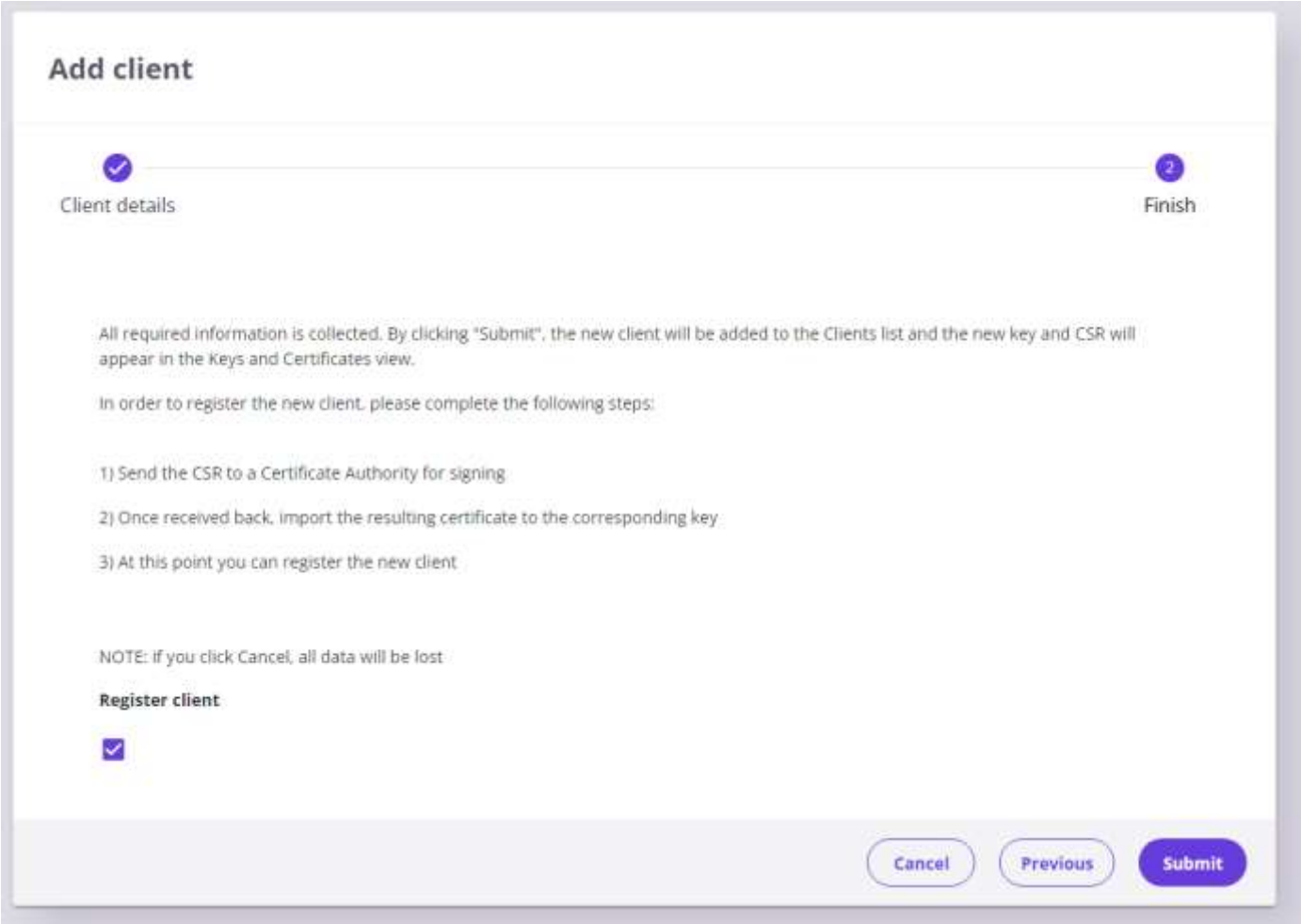
5.登録申請が受理されると、それぞれ OCSP が Good、ステータスが REGISTRED(登録済み)に更新されます。OCSP 及びステータスが更新されたことを確認してから次のステップへ進んでください。



5.次のステップは、サブシステムの登録です。[Client]ビューから[Add Client]を選択します。Member Code、Membar Class、Subsystem Code を入力します。



6.次のプロンプトで「確認」を選択します。



7.追加したクライアントのステータスが REGISTRATION IN PROGRESS(登録中)という状態で追加されます。ユーザーレジストリで登録リクエストを受け入れると、ステータスが REGISTERD（登録済）に更新されます。ステータスが登録済みになると、JP-LINK のエコシステムでユーザーコンテンツサービスを利用または提供する準備が整います。

※ステータスが登録済みになった状態

※クライアントは新たに追加する方法とは別に、すでに用意された他のセキュリティサーバーのクライアントから選択して、登録する方法もあります。~~これは対向システムのサービスを利用する場合に必要な手順となります。（当ガイドでは当該登録方法についての説明は行いません）~~
この手順は組織内でセキュリティサーバーを更改した場合等に、構築済みクライアントを新しいセキュリティサーバーへ移行するなどの目的で利用されるものです。

8.クライアントの内部接続方式の変更

Clients セクションから、登録したクライアントを選択し、Internal servers セクションを選択してください。

Connection type がデフォルトでは HTTPS が選択されておりますので、HTTP へ変更してください。

以上で JP-LINK への参加、セキュリティサーバーのインストール作業は終了です

9.疎通確認

以下の方法で構築済みのセキュリティサーバーから、OZ1　が用意した疎通確認用のサービスを実行して想定通り、JP-LINK に参加できているか確認することができます。

あくまで当サービスは疎通確認を目的としたサービスであるため、実際の業務において提供され運用されることを前提としたデータではなく、データ内容等については予告なく変更される可能性があります。

9-1. OZ1 へ疎通確認を実施したい旨の連絡とともに、次の情報を伝達ください。また、連絡する前に前手順 7.にて追加したサブシステムのステータスが登録済となっていることを確認してください。

・メンバーコード（Member Code）

・サブシステムコード（Subsystem Code）

9-2. OZ1 にて連絡頂いたメンバーコード及びサブシステムコードに対して、疎通確認用サービスの利用許可を設定致します。設定完了後、その旨を連絡しますので、設定完了の連絡を受けてから以下の手順を実施ください。

9-3. セキュリティサーバーがインストールされているサーバーにログインし、任意のフォルダ配下に次ページに表記した例を参考に WSDL ファイルを作成してください。

{}で囲っている箇所については、ご自身で任意の情報を入力ください。

｛メンバーコード｝ ： ご自身に割り振られたメンバーコードを指定してください。

｛サブシステムコード｝ ： セキュリティサーバーで設定したサブシステムコードを指定してください。

｛10 桁の特定健診機関番号｝ ： 10 桁の特定健診機関番号を入力してください。

※疎通確認用サービスは特定健診・特定保健指導機関検索の全国データをダウンロードし、そのデータを OZ1 側の検証環境用データベースに登録したものです。以下のデータに含まれる特定健診機関番号を 1 つ指定してください。（含まれない特定健診機関番号を指定した場合、空データが返却されます）

機関情報一括ダウンロード｜社会保険診療報酬支払基金（ssk.or.jp）

[ファイル名]tokuteikenshinkikan_search.xml

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP-ENV:Envelope
        xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:xroad="http://x-road.eu/xsd/xroad.xsd"
        xmlns:id="http://x-road.eu/xsd/identifiers">
    <SOAP-ENV:Header>
        <xroad:client id:objectType="MEMBER">
            <id:xRoadInstance>roksnet-dev</id:xRoadInstance>
            <id:memberClass>COM</id:memberClass>
            <id:memberCode>{メンバーコード}</id:memberCode>
            <id:subsystemCode>{サブシステムコード}</id:subsystemCode>
        </xroad:client>
        <xroad:service id:objectType="SERVICE">
            <id:xRoadInstance>roksnet-dev</id:xRoadInstance>
            <id:memberClass>COM</id:memberClass>
            <id:memberCode>21110001</id:memberCode>
            <id:subsystemCode>testSecurityServer</id:subsystemCode>
            <id:serviceCode>tokuteikenshinkikan_search</id:serviceCode>
            <id:serviceVersion>v1</id:serviceVersion>
        </xroad:service>
        <xroad:id>411d6755661409fed365ad8135f8210be07613da</xroad:id>
        <xroad:protocolVersion>4.0</xroad:protocolVersion>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body>
        <xroad:tokuteikenshinkikan_search xmlns:prod="http://test.x-
road.fi/producer">
                <prod:id>{10 桁の特定健診機関番号}</prod:id>
        </xroad:tokuteikenshinkikan_search>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

9-4. セキュリティサーバーがインストールされたサーバーにログインした状態で以下のコマンドを実行ください。

```
1. $ curl -d @tokuteikenshinkikan_search.xml --header "Content-Type: text/xml" -X POST
    http://localhost
```

9-5. 問題がなければ、WSDL 形式のレスポンスデータが返却されます。次ページに WSDL のレスポンスデータの例示を表示しますので、実際に返却されたデータを比較し、想定通りの結果になっている確認してください。

※例は OZ1 の検証環境上で実行しています。そのため、メンバーコード／サブシステムコードの送信元・送信先が同一になっております。

※正常に実行された場合、返却されるデータは指定した特定健診機関番号により、まったく異なる場合があります。例示のデータそのままの状態を確認したい場合には、特定健診機関番号には 0110111457 を指定ください。

※参考情報

当疎通確認サービスは以下のようなクエリを発行しています。指定できる ID は 1 つのみです。

```
select * from tokuteikenshinkikan_master where medical_institution_number = :id
```

```
$ curl -d @tokuteikenshinkikan_search.xml --header "Content-Type: text/xml" -X
POST http://localhost

<?xml version="1.0" encoding="UTF-8"?>

<SOAP-ENV:Envelope  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:px="http://xsd.planetcross.net/planetcross.xsd"     xmlns:xro="http://x-
road.eu/xsd/xroad.xsd"           xmlns:iden="http://x-road.eu/xsd/identifiers"
xmlns:xs="http://www.w3.org/2001/XMLSchema"            xmlns:xroad="http://x-
road.eu/xsd/xroad.xsd"><SOAP-
ENV:Header><xro:id>411d6755661409fed365ad8135f8210be07613da</xro:id><xro:reque
stHash
algorithmId="http://www.w3.org/2001/04/xmlenc#sha512">1+t/61Grff5ITmsguBO4ge1U
cBDTuKlYFb+M+oFJ4paTn3eP/0nh1IH6NJWBm/6m6pz+QTRWYC/yKf6ind+Fxw==</xro:requestH
ash><xro:protocolVersion>4.0</xro:protocolVersion><xro:service
iden:objectType="SERVICE"><iden:xRoadInstance>roksnet-
dev</iden:xRoadInstance><iden:memberClass>COM</iden:memberClass><iden:memberCo
de>21110001</iden:memberCode><iden:subsystemCode>testSecurityServer</iden:subs
ystemCode><iden:serviceCode>tokuteikenshinkikan_search</iden:serviceCode><iden
:serviceVersion>v1</iden:serviceVersion></xro:service><xro:client
iden:objectType="MEMBER"><iden:xRoadInstance>roksnet-
dev</iden:xRoadInstance><iden:memberClass>COM</iden:memberClass><iden:memberCo
de>21110001</iden:memberCode><iden:subsystemCode>testSecurityServer</iden:subs
ystemCode></xro:client></SOAP-ENV:Header><SOAP-
ENV:Body><xroad:tokuteikenshinkikan_searchResponse><row><medical_institution_n
umber
type="xs:string">0110111457</medical_institution_number><medical_institution_t
ype           type="xs:string">          特          定          健          診
</medical_institution_type><medical_institution_name type="xs:string">北海道銀
行  医  務  室  </medical_institution_name><zip_code   type="xs:string">060-
0042</zip_code><phone_number                          type="xs:string">011-261-
7111</phone_number><medical_institution_address type="xs:string">札幌市中央区大
通  西  4  丁  目  1  番  地  </medical_institution_address><url
type="xs:string">http://</url><management_entity type="xs:string">診療所 その他
の                                  法                                  人
</management_entity></row></xroad:tokuteikenshinkikan_searchResponse></SOAP-
ENV:Body></SOAP-ENV:Envelope>
```

上記は標準出力上に表示された状態そのままを表現しています。

Adapter Server を利用した DB へのアクセスと、その SQL を WSDL 化した内容の Security Server への登録、その検索の他組織 Security Server へのアクセス権限の設定や、通信のログについては別の資料で説明します。

SOAP メッセージ文/WSDL の参考情報：Security Server との通信のマニュアル　X-Road message protocol

https://github.com/nordic-institute/X-Road/blob/master/doc/Protocols/pr-mess_x-road_message_protocol.md

参考　付録 C Security Server 展開オプション

C.1 一般

セキュリティサーバーには、複数の展開オプションがあります。最も簡単な選択は、ローカルデータベースを備えた単一のセキュリティサーバーを使用することです。これは通常、ほとんどの場合は問題ありませんが、展開を調整する理由は複数あります。

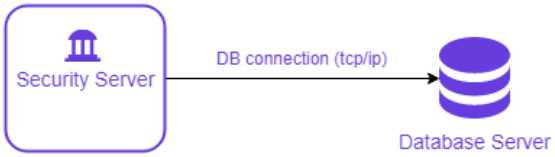
C.2 ローカルデータベース

最も簡単な展開オプションは、ローカルデータベースで単一のセキュリティサーバーを使用することです。開発とテストの目的で他のものが必要になることはめったにありませんが、本番環境では要件がより厳しくなる可能性があります。　注:ここでの DB は Adapter 経由でアクセスする DB ではなく、SS 内部 DB です。

C.3 リモートデータベース

セキュリティサーバーでリモートデータベースを使用することが可能です。このオプションは、データベースの状態を外部化する必要がある場合の開発およびテストで使用されることがあります。

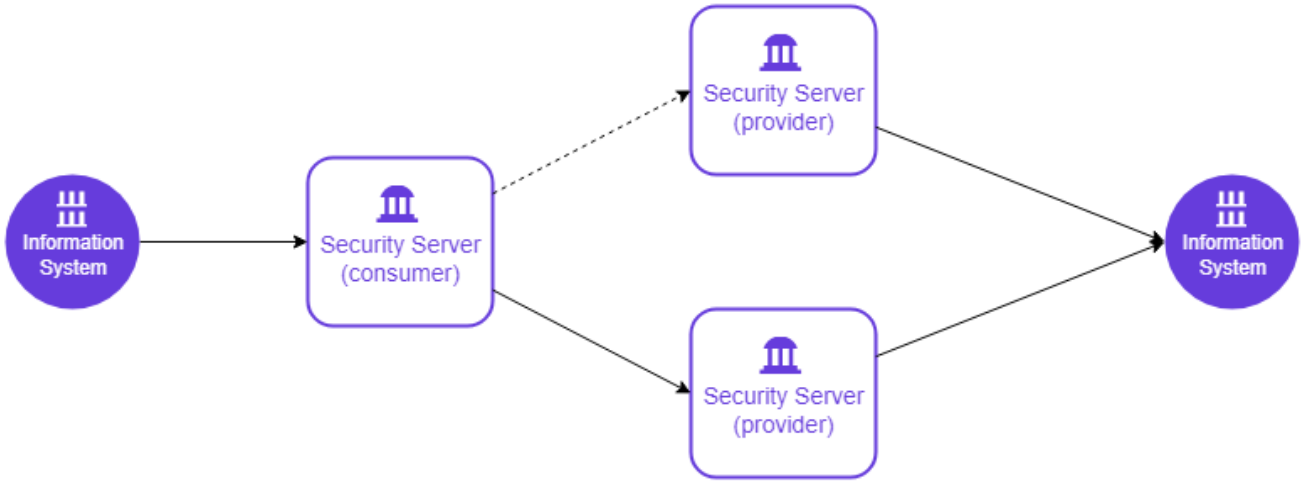
セキュリティサーバーは、AWSRDS や AzureDatabase forPostgreSQL などのさまざまなクラウドデータベースをサポートしています。この展開オプションは、クラウドネイティブデータベースの使用が最初の選択肢であるクラウド環境で開発を行う場合に役立ちます。



注:ここでの DB は Adapter 経由で接続される DB ではなく Security Server 内部で管理する DB です

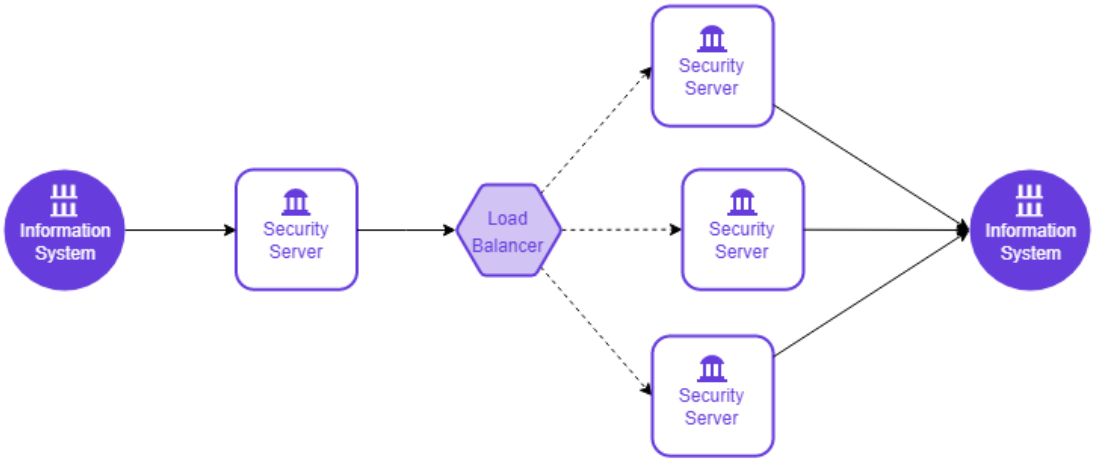
C.4 高可用性のセットアップ

実動システムでは、単一障害点が発生することはめったに受け入れられません。セキュリティサーバーは、いわゆる内部負荷分散メカニズムを介してプロバイダー側の高可用性セットアップをサポートします。セットアップは、同じメンバー/メンバークラス/メンバーコード/サブシステム/サービスコードが複数のセキュリティサーバーで構成され、最も高速に応答するサーバーに要求をルーティングするように機能します。この展開オプションは、パフォーマンス上の利点を提供するのではなく、冗長性を提供するだけであることに注意してください。



C.5 ロードバランシングの設定

ビジーな本番システムでは、高可用性に加えてスケーラブルなパフォーマンスが必要になる場合があります。これらの問題の両方に同時に対処するための外部負荷分散メカニズムをサポートしています。選択したアルゴリズムに基づいてリクエストをルーティングするために、セキュリティサーバークラスターの前にロードバランサーが追加されます。この展開オプションは、[IG-XLB]で詳細に文書化されています。



C.6 まとめ

次の表に、セキュリティサーバーの展開オプションの概要と、それらが開発用か実稼働用かを示します。

展開	開発者	製品
ローカルデータベース	○	
リモートデータベース	○	
高可用性のセットアップ		○
負荷分散の設定		○

参考：https://github.com/nordic-institute/X-Road/blob/master/doc/Manuals/ig-ss_x-road_v6_security_server_installation_guide.md#23-requirements-for-the-security-server