JP-LINK に参加する方法

2022 年 4 月版

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

2/16 Adapter Server でのサービスの作成と、セキュリティサーバへのサービスの登録を追記

2/17 ネットワーク要件に Adapter Server との通信用のポート設定の記述を追加

2/18 9.疎通確認についての記述を変更

3/10 ソフトトークン PIN に関する注意を追記、メッセージログの BODY 部をログに登録しない設定方法について追記

3/18 Adapter Server Installation guide/User guide のバージョン表記更新

3/27 RHEL 版のインストール手順を記載

3/31 RHEL 版のインストール手順に記載ミスがあったので訂正

4/1 [7.証明書をインポートします]セクションに手順番号の採番に不備があったためこれを訂正

4/5 メッセージログの推奨設定に関する記載を追記、アダプターサーバにおけるサブシステム登録時の注意事項を追記

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。セキュリティサーバ合、セキュリティサーバ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）

注：2022 年 2 月現在組織名にカンマ(,)が文字区切りと認識されてしまうため入れられません。修正時期は未定です。

3. ソフトウェア情報

セキュリティサーバは、現在 Ubuntu 18.04 LTSx86-64 及び Red Hat Enterprise Linux (RHEL)　7.3 以降または 8 以降で実行するように設計されています。

最小要件は、OS 毎に異なります。以下の通りです。

Ubuntu 18.04 LTSx86-64

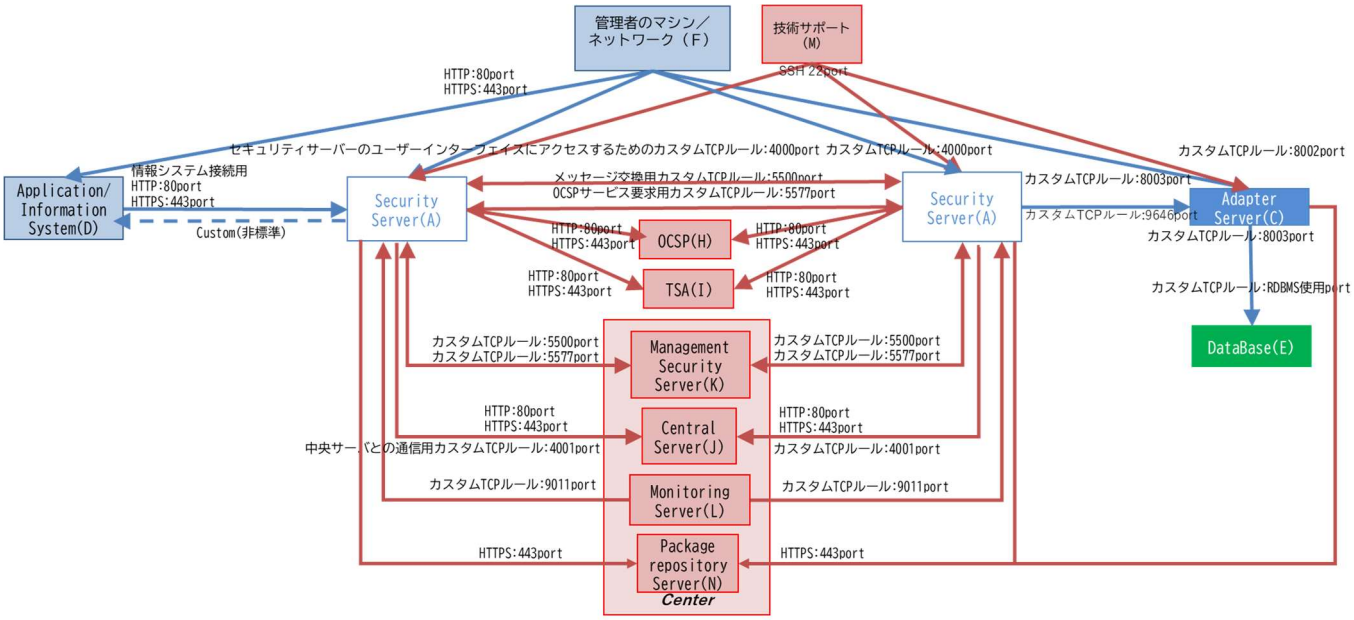
メモリ	3GB 以上
ストレージ	10GB 以上

Red Hat Enterprise Linux (RHEL)　7.3 and 8

メモリ	3GB 以上
ストレージ	OS パーティション 10GB 他パーティション(/var 配下) 20GB 以上

解放するポート:

- セキュリティサーバ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）
- (RHEL のみ)情報システム接続用の TCP8080/8443 インバウンド/アウトバウンド（ローカル）
- アダプターサーバとの通信用の TCP80/8085/8003 アウトバウンド



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のインストール

Ubuntu の場合

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。

```
sudo apt-add-repository -y "deb https://artifactory.niis.org/xroad-release-deb $(lsb_release -s
c)-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。

```
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。

```
sudo apt-get update

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。

Red Hat Enterprise Linux (RHEL) の場合

1. 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
```

2. yum と統合してそのネイティブ機能を拡張するユーティリティのコレクションをインストールします。

```
sudo yum install yum-utils
```

3. X-Road パッケージリポジトリと Extra Packages for Enterprise Linux (EPEL) リポジトリを追加します。

```
RHEL_MAJOR_VERSION=$(source /etc/os-release;echo ${VERSION_ID%.*})

sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-${RHEL_MAJOR_VERSION}.noarch.rpm

sudo yum-config-manager --add-repo https://artifactory.niis.org/xroad-release-rpm/rhel/${RHEL_MAJOR_VERSION}/current
```

4. X-Road リポジトリの署名鍵を信頼できる鍵のリストに追加します

```
sudo rpm --import https://artifactory.niis.org/api/gpg/key/public
```

5. セキュリティサーバのインストール

   ※Ubuntu と異なり、インストール中に各種情報の入力は求められません。インストール確認のための質問はありますので、内容を確認の上、インストールを進めてください。

```
sudo yum install xroad-securityserver
```

6. ユーザインタフェースのすべてのロールが付与されているシステムユーザを追加します。

   <ユーザー名>の箇所を任意の名称に置き換えてください。

```
sudo xroad-add-admin-user <ユーザー名>
```

7. セキュリティサーバを起動します。（インストール完了後、自動的に起動しないため）

```
sudo systemctl start xroad-proxy
```

インストール後のチェック(Ubuntu/RHEL 共通)

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。

```
$ 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
```

【推奨】メッセージロギング設定の変更(Ubuntu/RHEL 共通)

セキュリティサーバはメッセージ交換を行った際のログを保管する機能があります。
メッセージログは後述の XML 形式で HEADER(メッセージ交換の送信元と送信先の情報、メタデータ)と BODY (メッセージ交換における業務データ、メッセージ本文)の両方を保管しており、この保管設定は変更することができます。
保管の設定は以下の 3 通りです。

1. メタデータ（HEADER）・メッセージ本文(BODY)の両方の保管 (デフォルト設定)
2. メタデータ（HEADER）のみ保管
3. メッセージログを一切保管しない

OZ1 では、セキュリティ・コンプライアンスの観点から、業務データ(=メッセージ本文(BODY))をセキュリティサーバ上に保管することを推奨しておりません。
よって、上述設定の“2. メタデータ（HEADER）のみの保管”の設定とすることを推奨しています。
メッセージロギング設定の変更方法はこちらに記載しておりますので、ご確認ください。

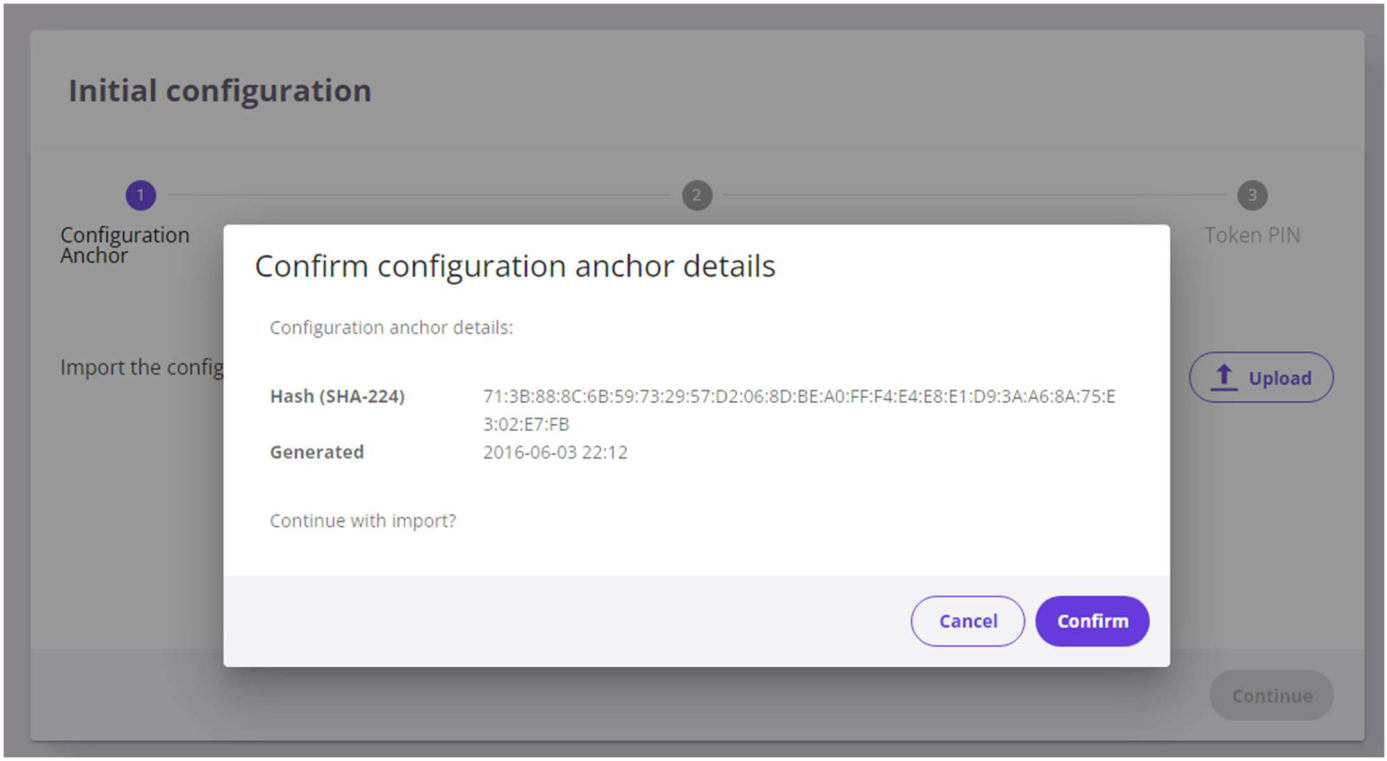
5.セキュリティサーバのセットアップ

セットアップ(Ubuntu/RHEL 共通)

セキュリティサーバ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。

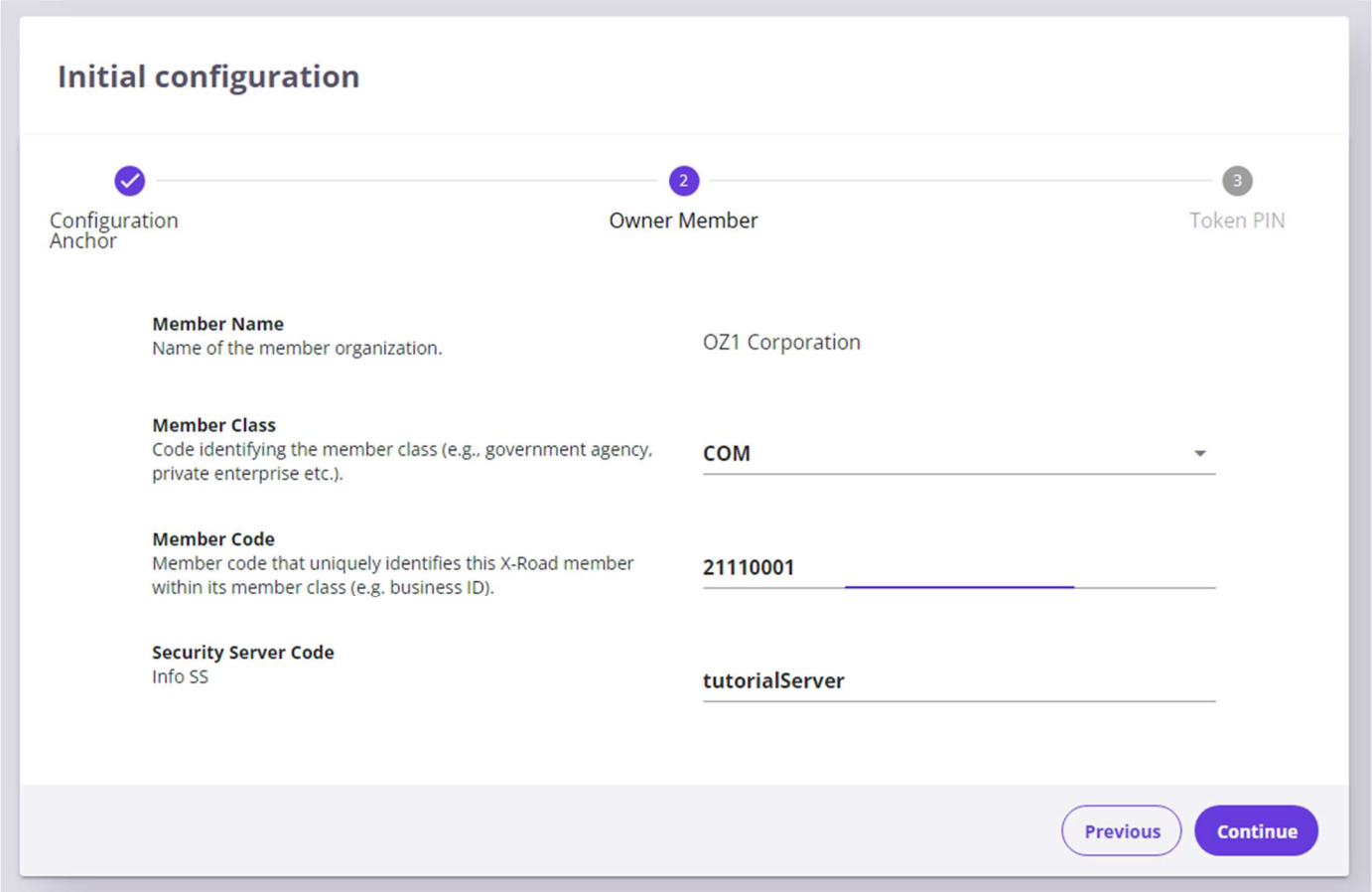
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<ns3:configurationAnchor xmlns:ns2="http://x-road.eu/xsd/identifiers" xmlns:ns3="http://x-road.eu/xsd/xroad.xsd">
<generatedAt>2016-06-03T13:12:15.255Z</generatedAt>
<instanceIdentifier>roksnet-dev</instanceIdentifier>
<source>
<downloadURL>http://198.211.127.118/internalconf</downloadURL>
<verificationCert>MIICqTCCAZGgAwIBAgIBATANBgkqhkiG9w0BAQ0FADAOMQwwCgYDVQQDDANOL0EwHhcNNzAwMTAxMDAwMDAwWhcNMzgwMTAxMDAwMDAwWjAOMQwwCgYDVQQDDANOL0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCYR91E0/waxqiK3sCjs7+DH1tpLCkQEdab9cFfQE717u8KMNjT/N0S3v6KiMWPBJbmB722Bk6/ykqSBN6yqog/Qp6ZKiLmghRIKwTB2I8OcHdOp5ExRhVC8qS0k0j6TzXKwKQDi3fVTLVJIq3RpdILu1tHqbAh31GWsBuoP4ahb4W5+cvjE9UdHxVq+5DY5EwG/FeiSfIlhn44BiUY5uJ4gPx8ACV2f4z8Dqfq0immTHIkDjEdNDuGO4eFxYt4FPfq2FuodYE48rEMW/NcmmoR6pniixbI8L6IGL5/nP92SEe/JfqwCvTgTFkIlnNXpsofeWqOCAihUY1T9L+qyCKLAgMBAAGjEjAQMA4GA1UdDwEB/wQEAwIGQDANBgkqhkiG9w0BAQ0FAAOCAQEAhWmXvp/hTG/lmFYV6PRNGYW2T/04PAL476D1mR6l550lchhcW68I+A0ydTiKAnnBEBqgqVKD5skvyyDkxZXnG6Z8vzXjAjYt4JPaYNuXCJxzAqoxB+rg9iqktSt3mp5tZ466qMXKt8r/MxoCnz+NbIGLZF1AnjKR2JbFDyuaOjGGJ+OtcZFqX0Cp0vcy2Z1fEICrwfySE3NoJRifDy3W/XUVejr4uRQ0CDT8PG8CkdqtezWLEeEP05rrBf3Z0AoZhqbH0gGDmH/cR1U7h3NxXPVVmrvgwIgqQIqAdN3iiMKTnba5ITKDh63sU0D/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。

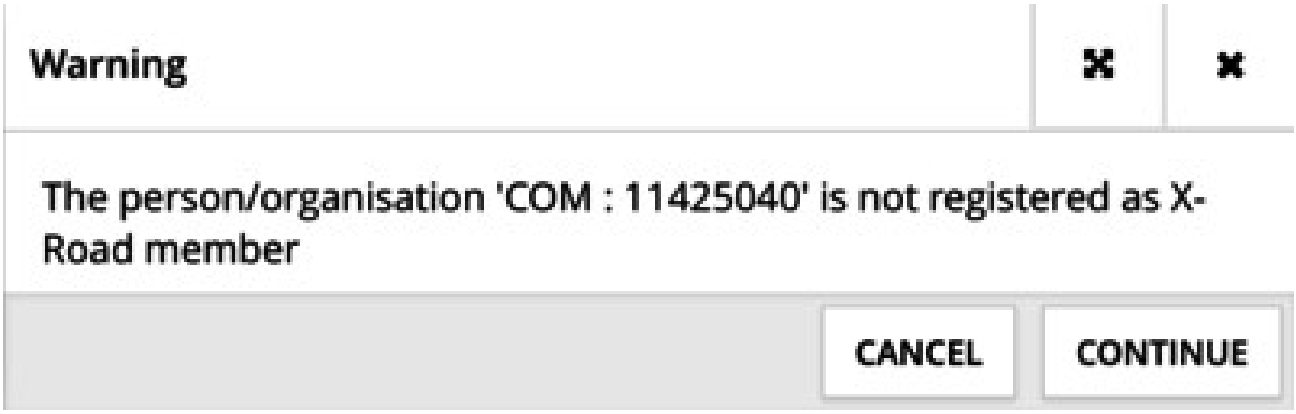
- メンバークラス–セキュリティサーバの所有者のメンバークラス（民間企業の場合は COM、政府機関の場合は GOV、非営利団体の場合は NGO）
- メンバーコード–OZ1 から送信されたセキュリティサーバ所有者のメンバーコード。
- セキュリティサーバーコード–自由形式
- PIN–サーバーが証明書にアクセスするために使用されるソフトウェアトークンの PIN

  !!注意!! ソフトウェアトークン PIN を失念した場合、**PIN を復旧する手段はありません。**PIN を失念してしまった場合、再インストールを行っていただく必要があります

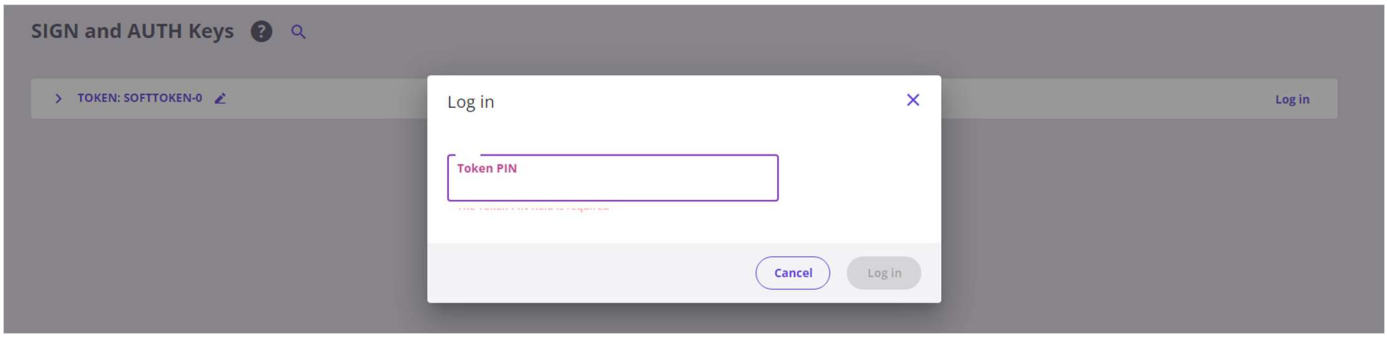
以下は入力例です：



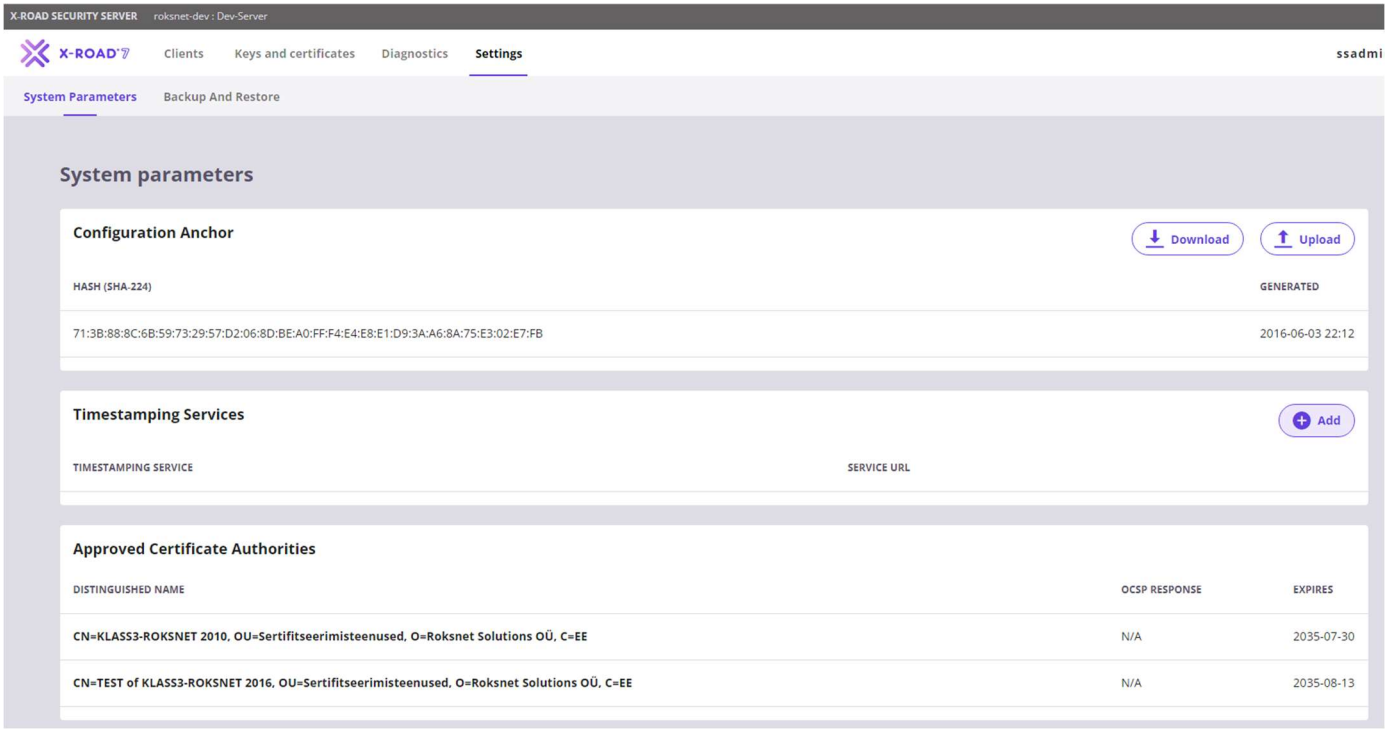
以下に示すように、サーバーが警告を表示する場合、これは問題なく、セットアップを続行できます。これは、メンバーがまだグローバル構成になっていないことを意味します。

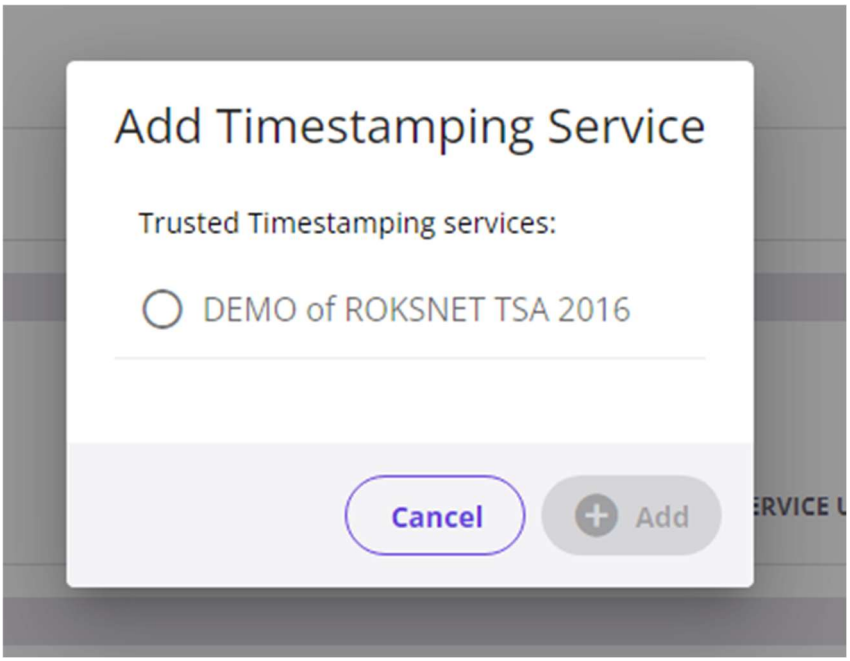


3.ページの上部にソフトトークンの PIN が入力されていないという警告メッセージが表示されます。赤いメッセージをクリックして PIN を入力します。または、[Keys and Certificate]メニューから、アクセスし、[Log in]テキストをクリックすることでも PIN の入力画面へ遷移できます。



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。



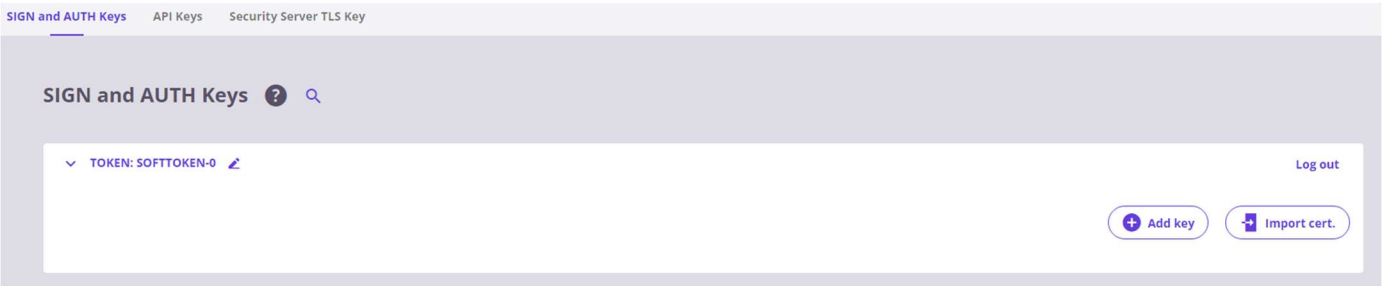


5. [Keys and Certificate]セクションでキーと証明書要求の生成を開始します

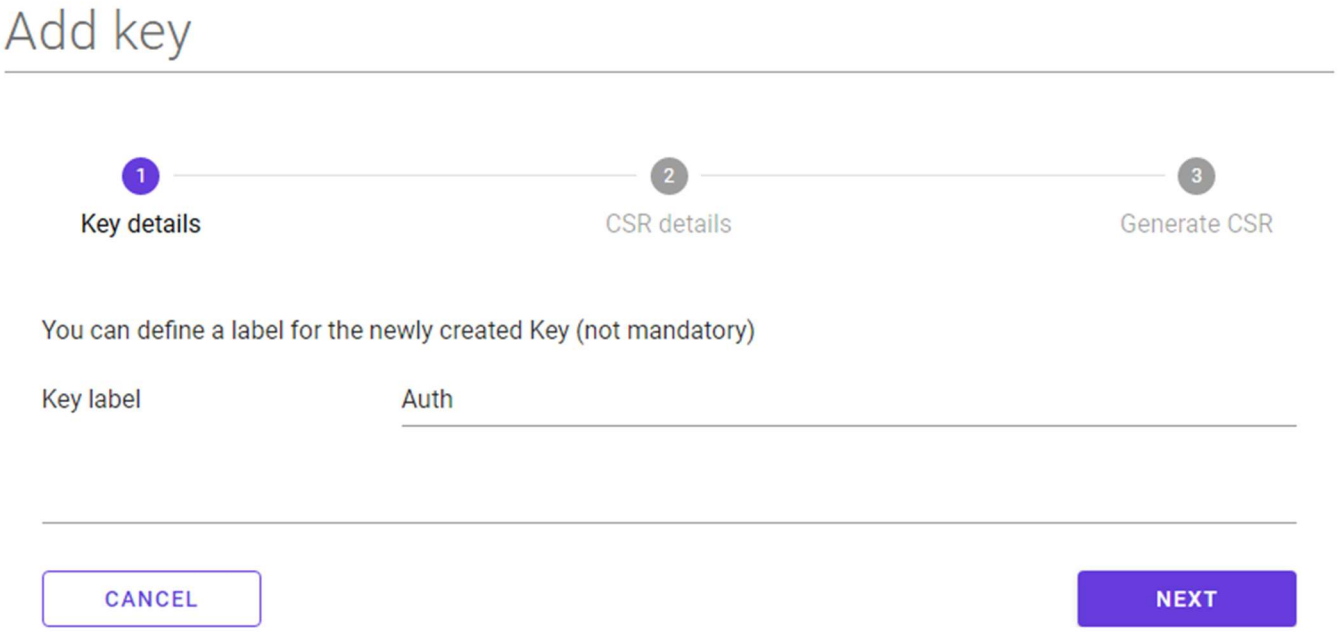
セキュリティサーバは 2 種類の証明書を使用します

- 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間の認証用の AUTH 証明書。AUTH 証明書は、セキュリティサーバごとに 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。

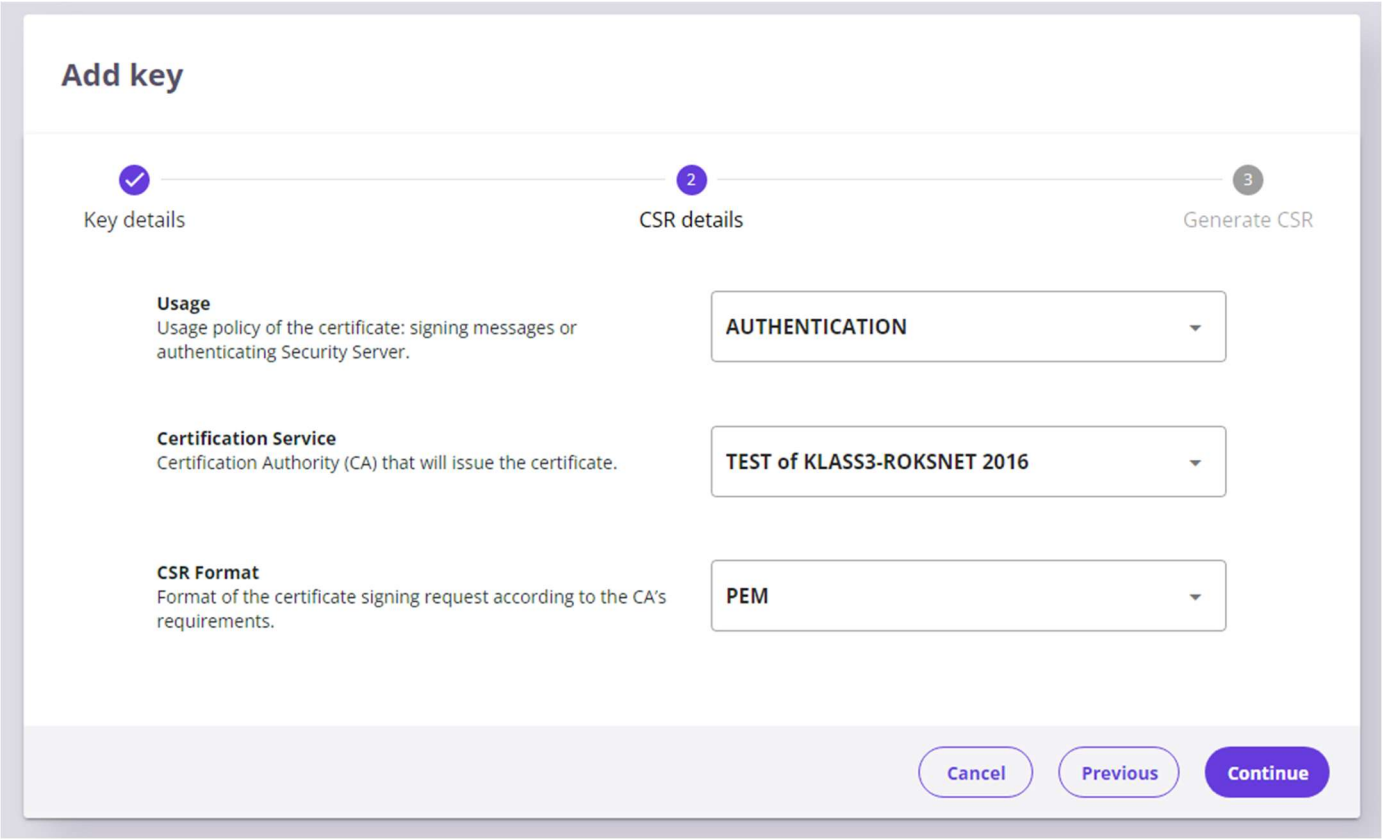
SoftToken-0 を選択して、[+Add Key]ボタンを押下し、AUTH キーと SIGN キーを生成します。



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。

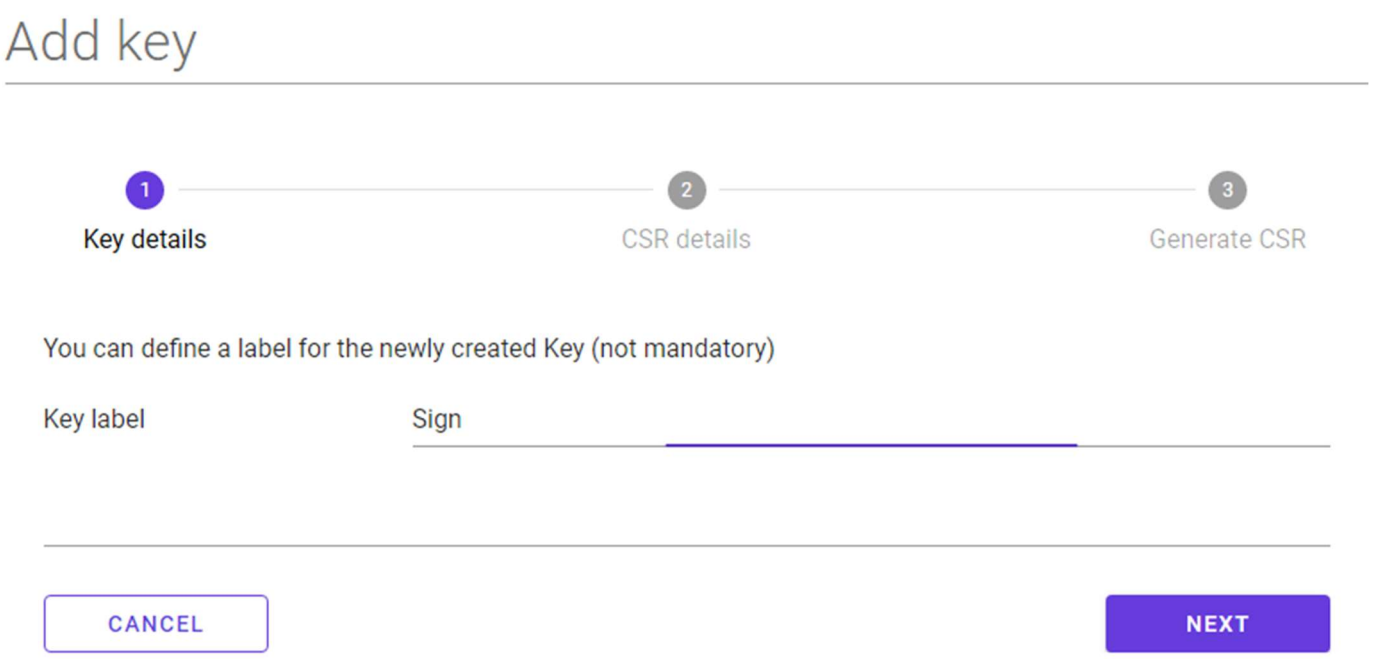


5-2.認証用 AUTH 証明書の入力内容は次の通りです。

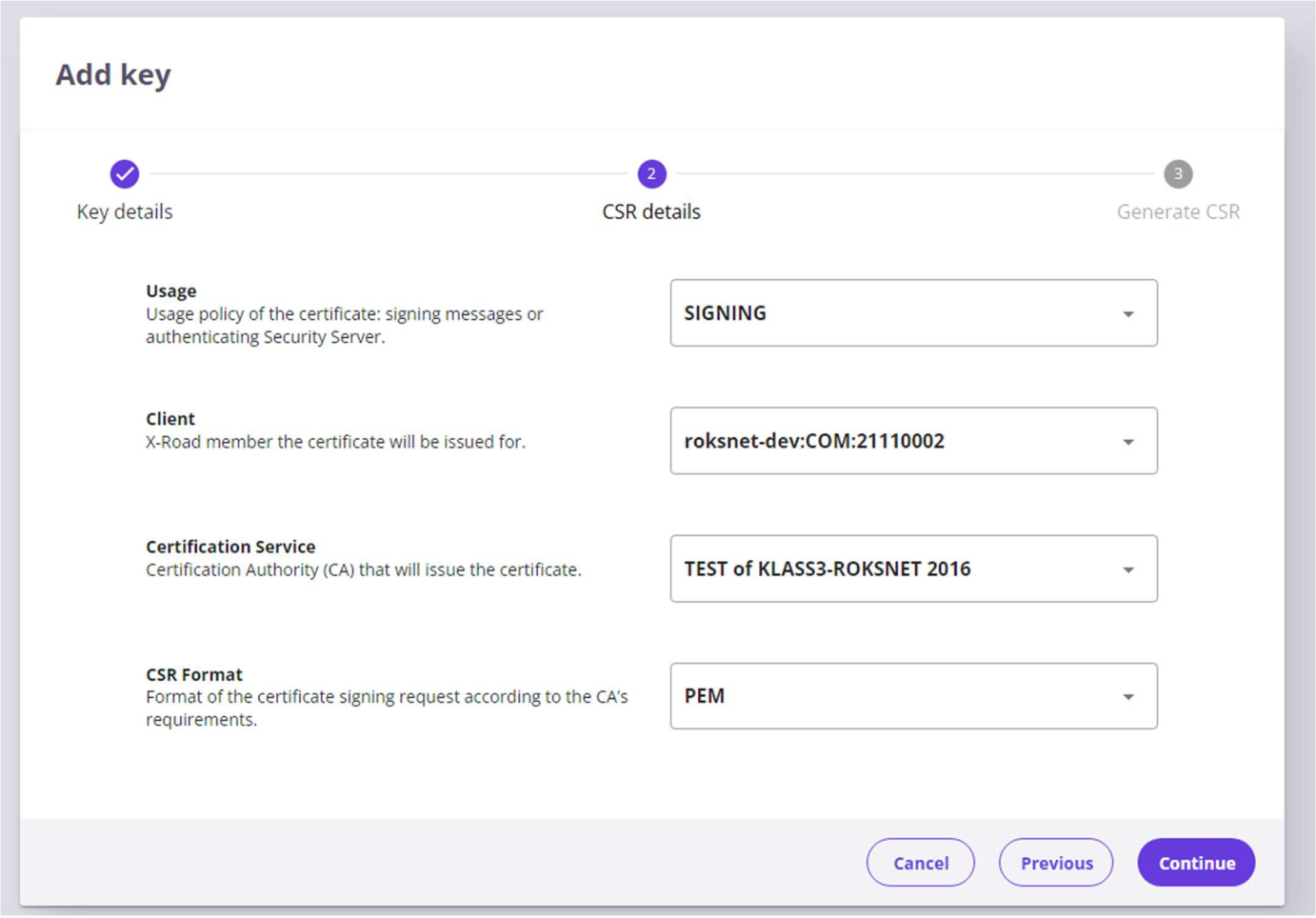


Continue ボタンを押下し、次の画面で CSR ファイルをダウンロード（生成)してください。

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。

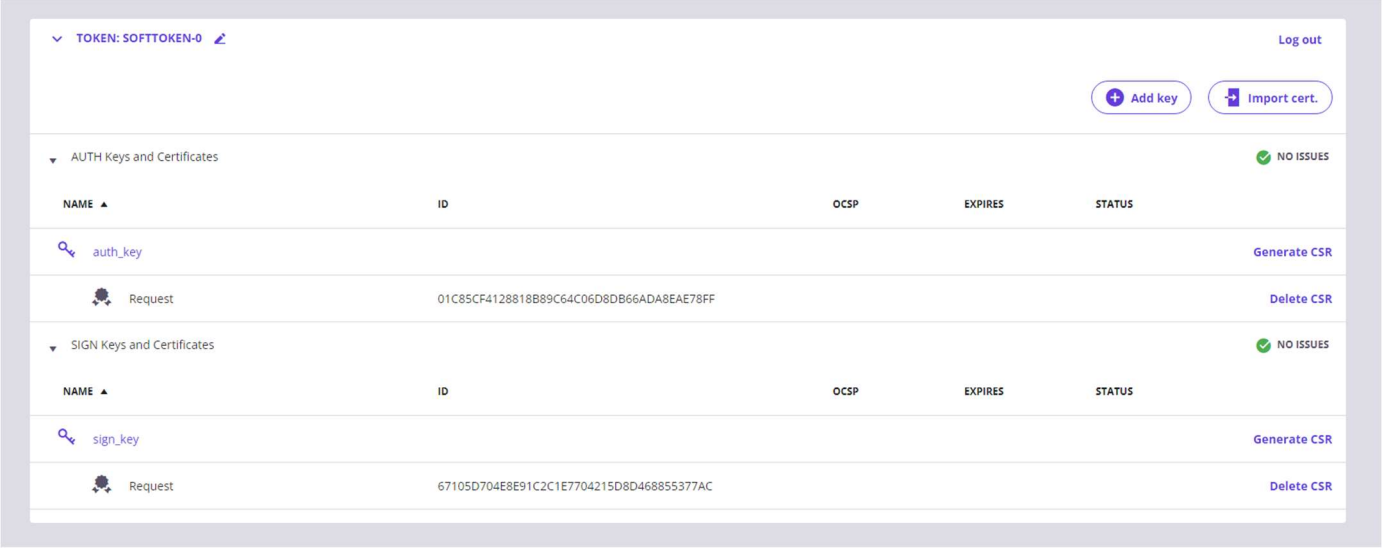


5-4.署名用の SIGN 証明書の入力内容は次の通りです。



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(生成)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。

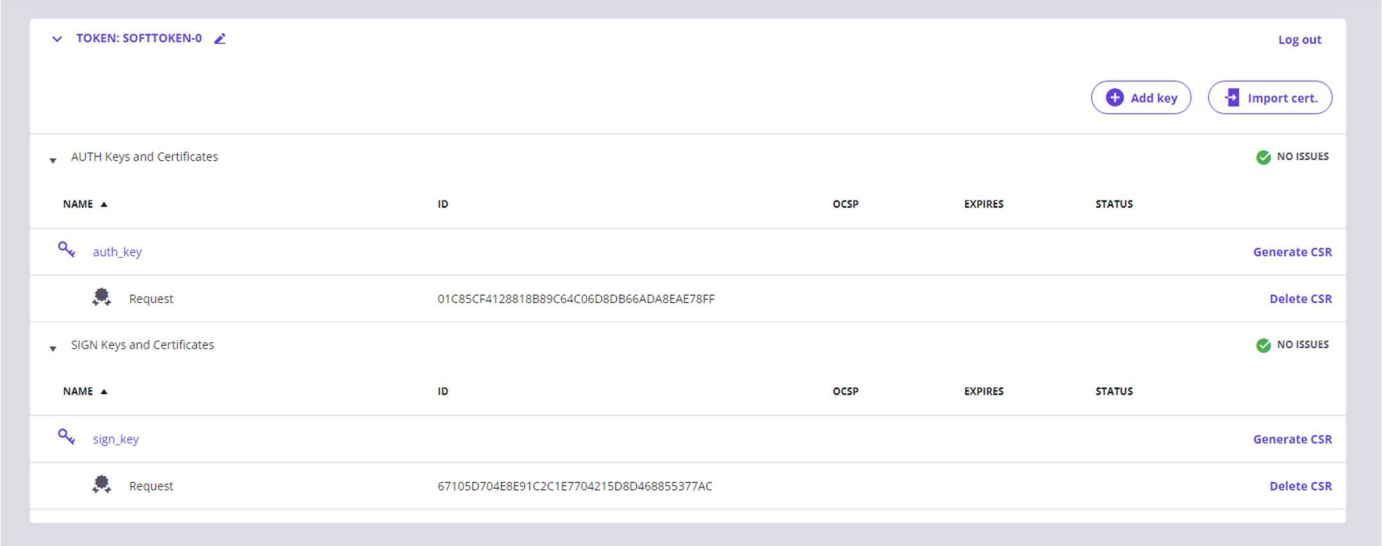
- [ ] OZ1 の利用規約、技術宣言、プライバシーポリシーを読み、同意します。
- [ ] OZ1 で公開されている価格表に従って、OZ1 からサービスを受けることを読み、同意します。

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。

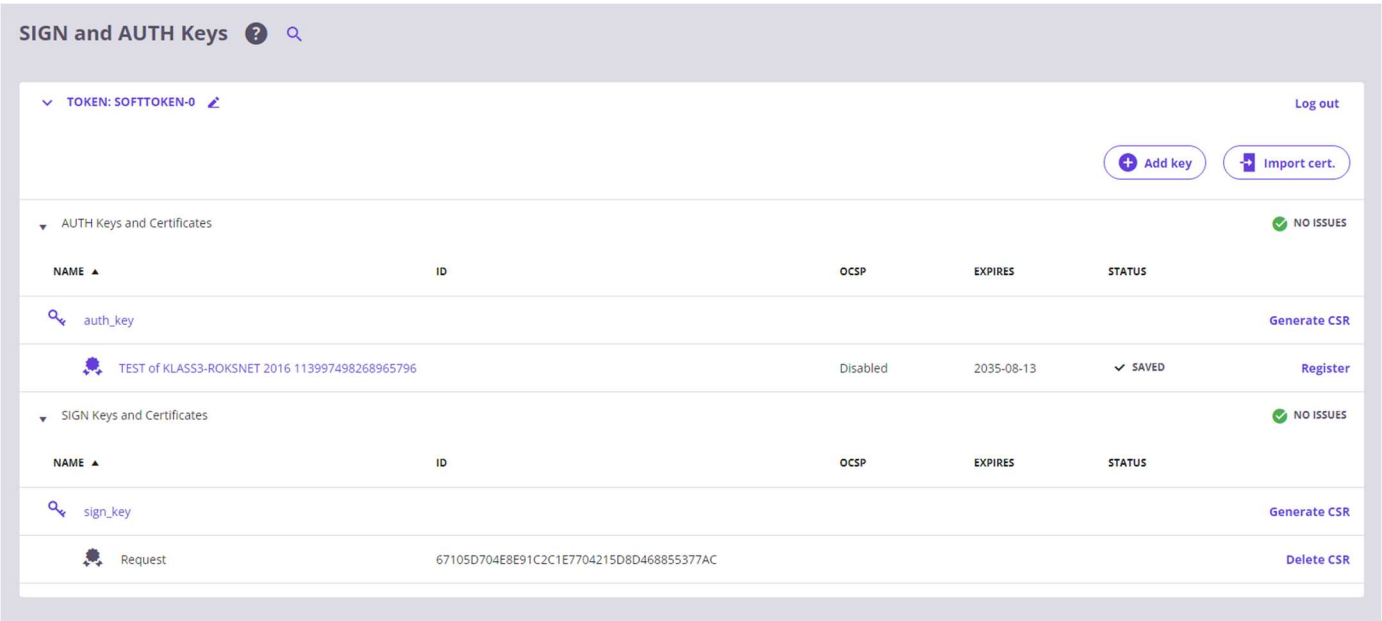
7.証明書をインポートします

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。

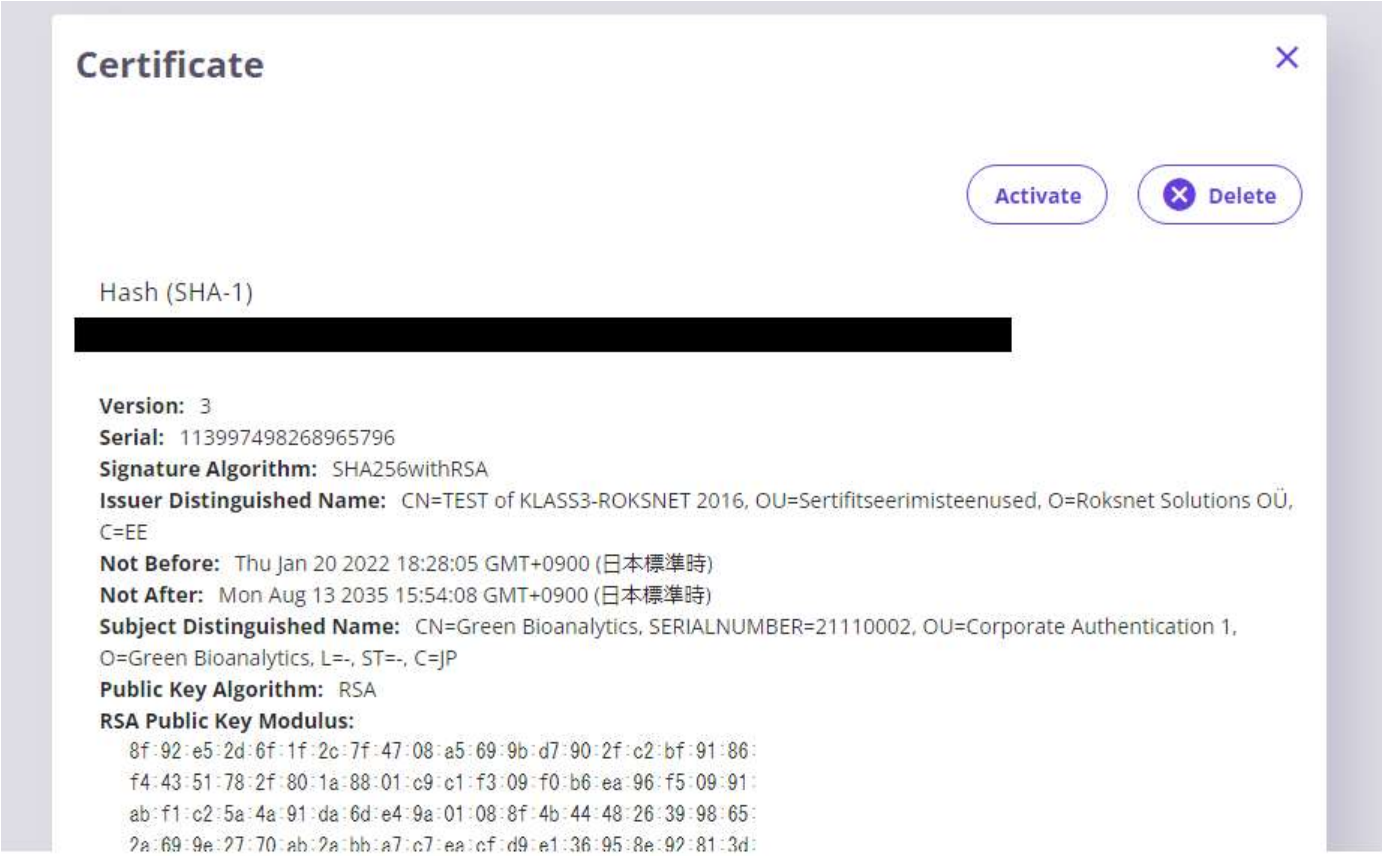
7-1.[Import cert.]ボタンを押下し、署名用(sign)CSR ファイルをインポートします。



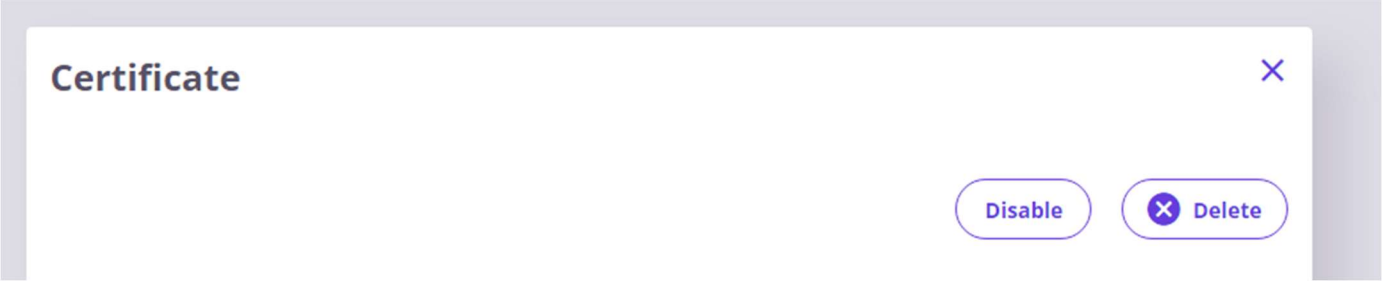
7-2.[Import cert.]ボタンを押下し、認証用(auth)CSR ファイルをインポートします。両方の CSR ファイルがインポートされると、下図のような状態となります。



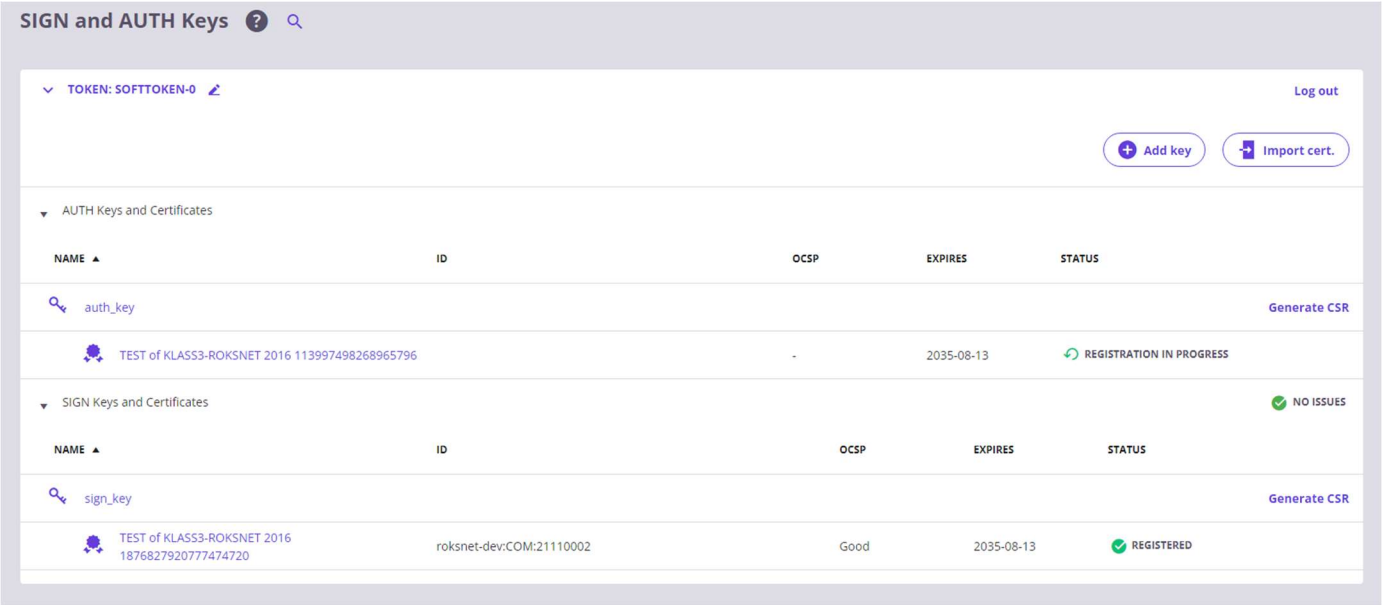
7-3.認証用(auth)CSR はインポートした直後は、無効(Disabled)の状態でインポートされます。 有効化するためには認証用 CSR のラベルを選択し、Certificate の画面を表示させます。その後、[Activate]ボタンを押下し、有効化してください。



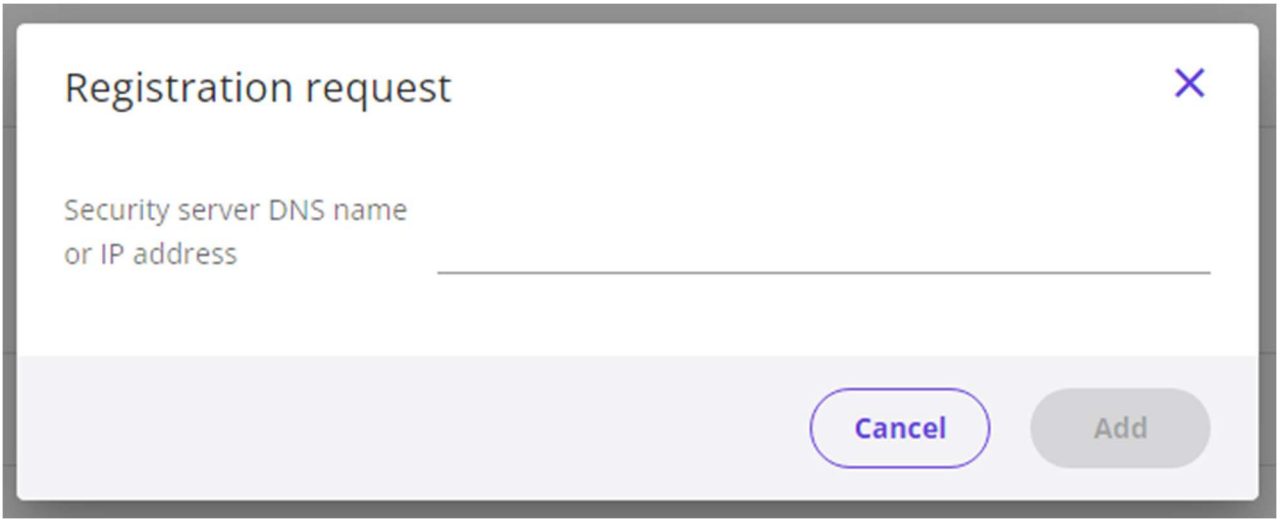
※認証用(auth)CSR を有効化した後、再度無効にしたい場合には、[Active]ボタンが[Disable]ボタンに更新されるので、[Disable]ボタンを押下してください。



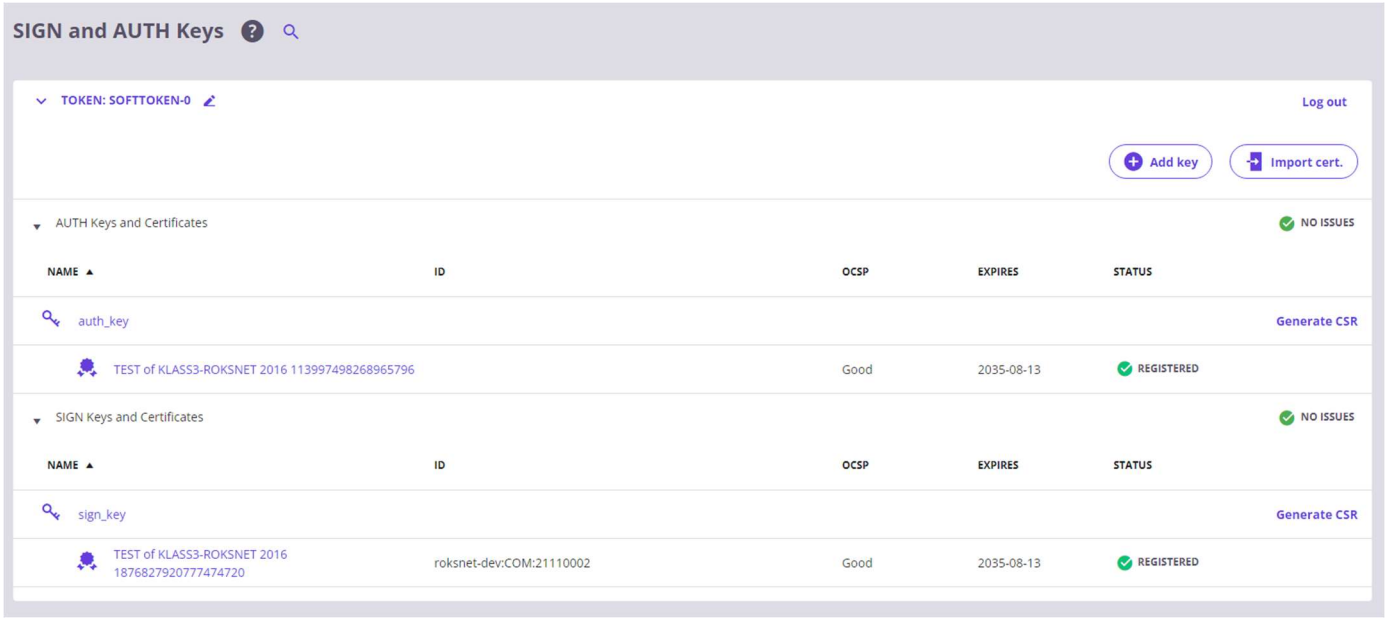
7-4.認証用(auth)CSR を有効化した後、[Register]ボタンを押下し、認証用 CSR の登録申請を行ってください。登録ボタン押下直後は、REGISTRATION IN PROGRESS(登録中)というステータスに更新されます。環境により申請が受理されるまでの待機時間は異なります。



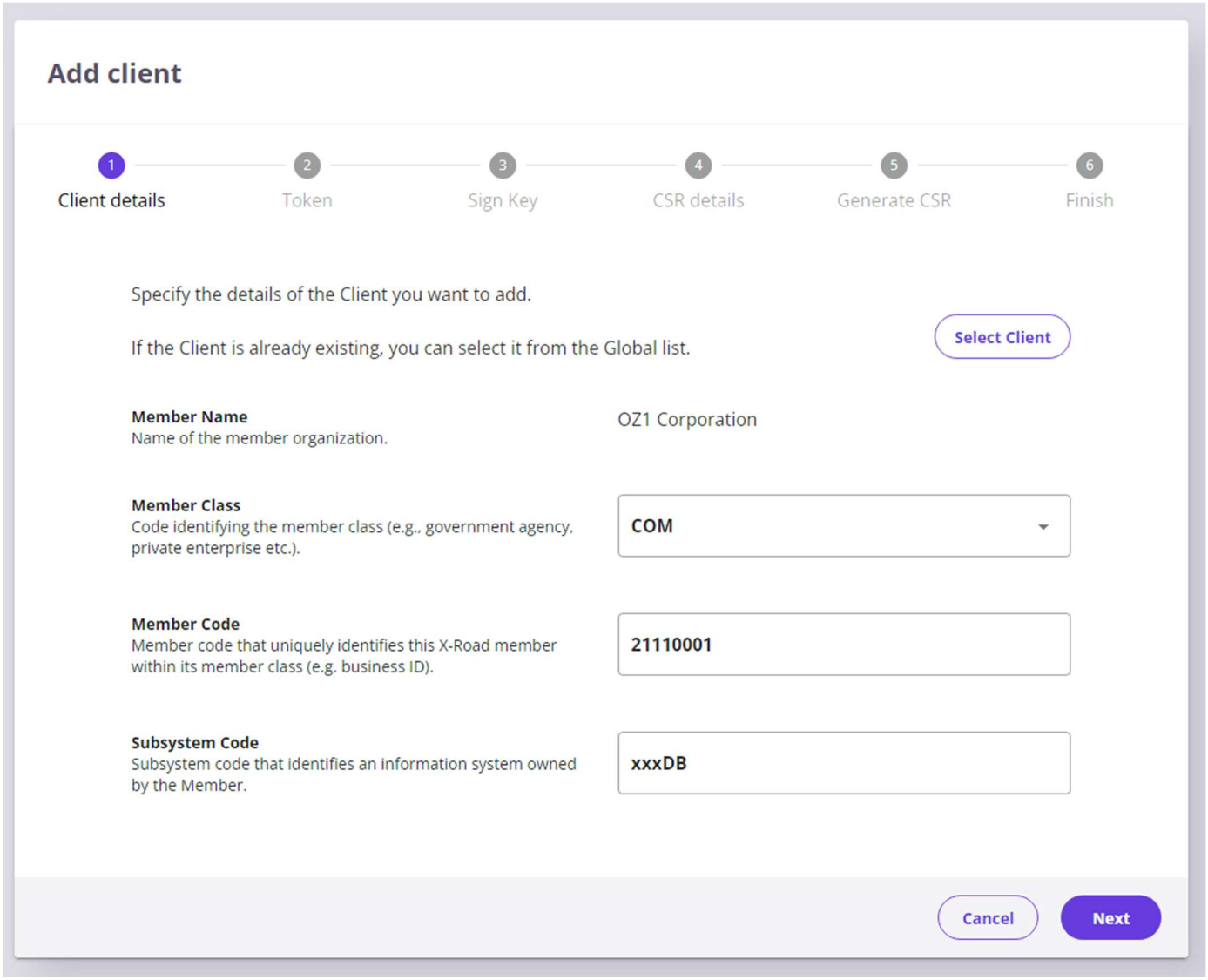
以下のウィンドウが表示され、IP アドレスまたは DNS の入力を求められます。
外部から当セキュリティサーバへアクセス可能である IP アドレス(グローバル IP アドレス)または DNS を 63 文字以内で入力してください。



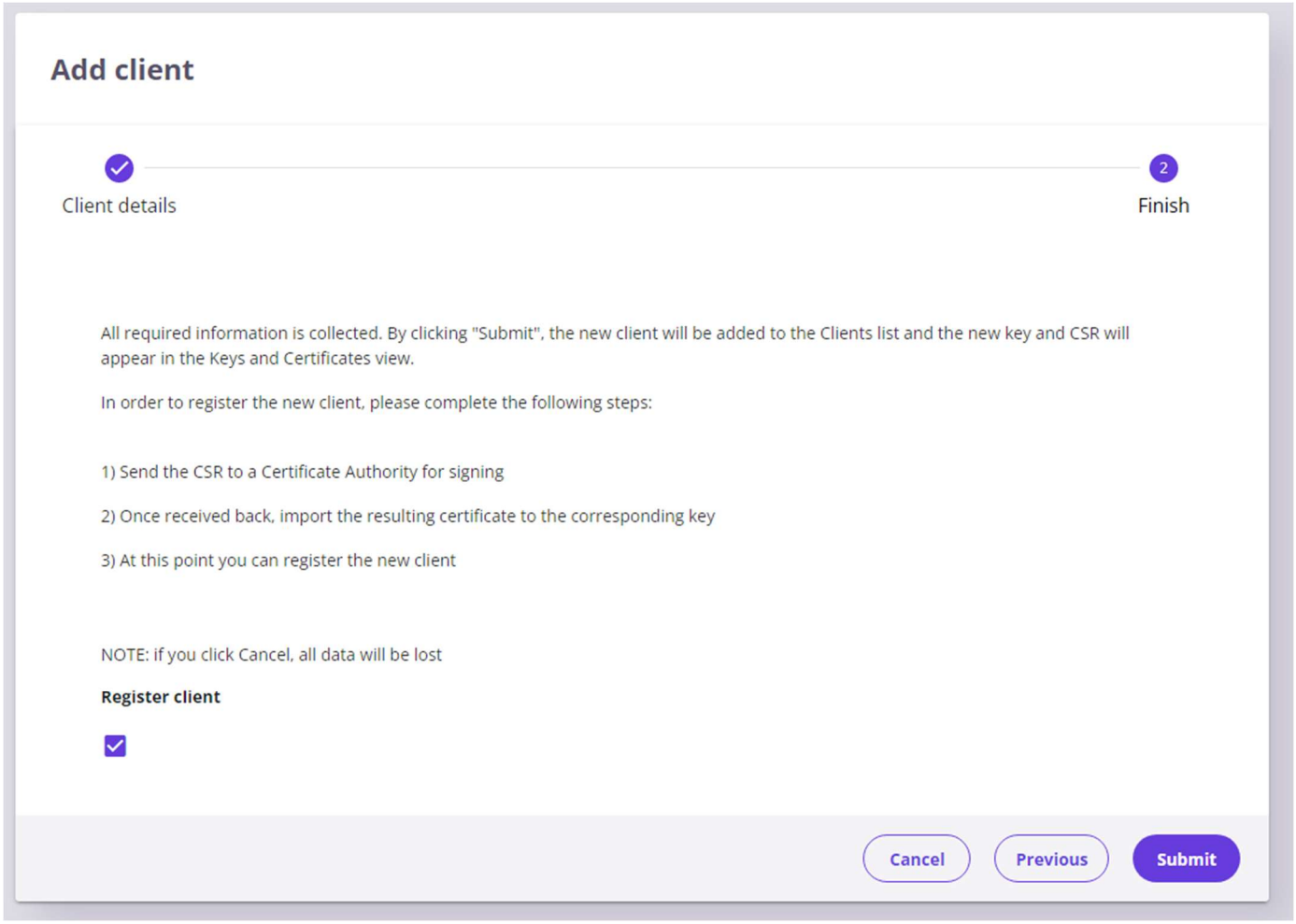
7-5.登録申請が受理されると、それぞれ OCSP が Good、ステータスが REGISTRED(登録済み)に更新されます。OCSP 及びステータスが更新されたことを確認してから次のステップへ進んでください。



7-6.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。



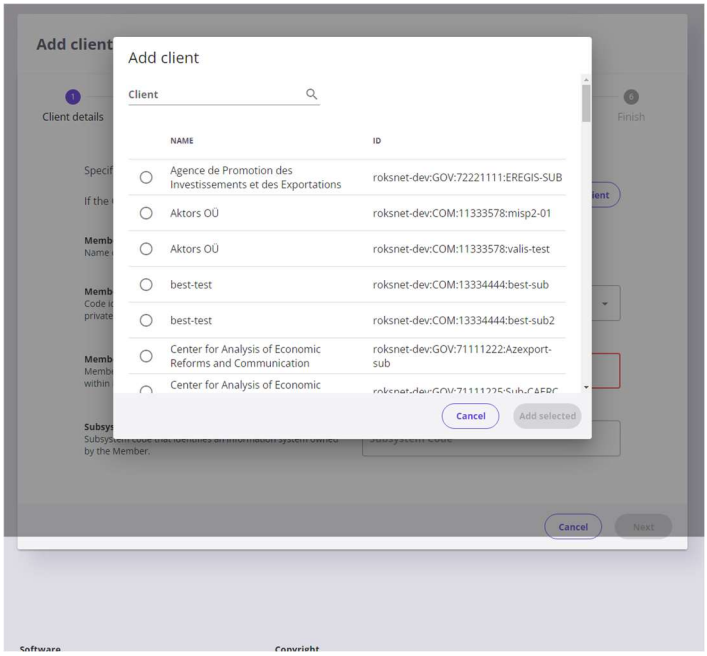
7-7.次のプロンプトで「確認」を選択します。



7-8.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

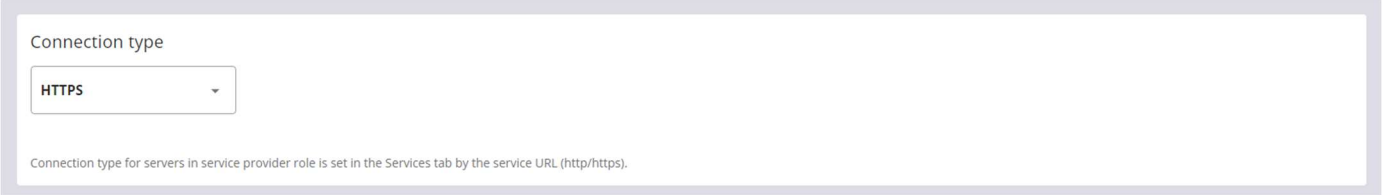
※クライアントは新たに追加する方法とは別に、すでに用意された他のセキュリティサーバのクライアントから選択して、登録する方法もあります。~~これは対向システムのサービスを利用する場合に必要な手順となります。（当ガイドでは当該登録方法についての説明は行いません）~~
この手順は組織内でセキュリティサーバを更改した場合等に、構築済みクライアントを新しいセキュリティサーバへ移行するなどの目的で利用されるものです。

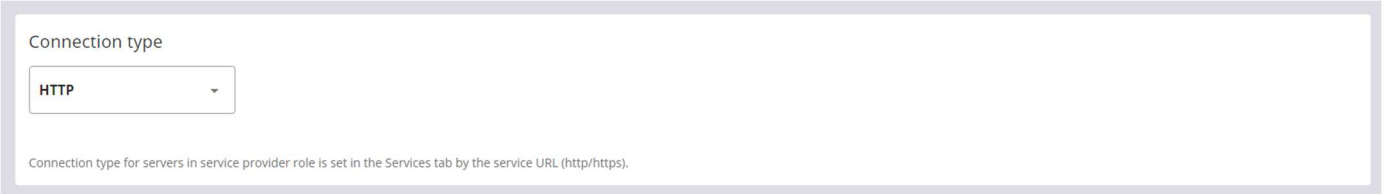


8.クライアントの内部接続方式の変更

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で設定したサブシステムコードを指定してください。

｛施設名称｝ ： 旅館の名称を記述ください。LIKE 句を利用した検索となりますので、ワイルドカード指定が可能です。（例：`大阪%` や `%大阪%` など）

※疎通確認用サービスは大阪市オープンデータポータルサイトに掲載されている「旅館業施設一覧」の施設名称に対して、LIKE 句を利用した検索を行います。

民泊等宿泊施設一覧 - データセット - Open Data Osaka

[ファイル名] ryokan_search_for_name.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:iden="http://x-road.eu/xsd/identifiers" xmlns:repr="http://x-
road.eu/xsd/representation.xsd" xmlns:tns="http://testSecurityServer.x-road.eu/producer"
xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">
    <SOAP-ENV:Header>
        <xrd:protocolVersion xmlns:xrd="http://x-
road.eu/xsd/xroad.xsd">4.0</xrd:protocolVersion>
        <xrd:id xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">ce6daaff-11d6-4e1a-8a67-
2d0447004a7f</xrd:id>
        <xrd:userId xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">admin</xrd:userId>
        <xrd:service xmlns:iden="http://x-road.eu/xsd/identifiers" iden:objectType="SERVICE"
xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">
            <iden:xRoadInstance>roksnet-dev</iden:xRoadInstance>
            <iden:memberClass>COM</iden:memberClass>
            <iden:memberCode>21110001</iden:memberCode>
            <iden:subsystemCode>testSecurityServer</iden:subsystemCode>
            <iden:serviceCode>ryokan_search_for_name</iden:serviceCode>
            <iden:serviceVersion>v1</iden:serviceVersion>
        </xrd:service>
        <xrd:client xmlns:iden="http://x-road.eu/xsd/identifiers" iden:objectType="SUBSYSTEM"
xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">
            <iden:xRoadInstance>roksnet-dev</iden:xRoadInstance>
            <iden:memberClass>COM</iden:memberClass>
            <iden:memberCode>{メンバーコード}</iden:memberCode>
            <iden:subsystemCode>{サブシステムコード}</iden:subsystemCode>
        </xrd:client>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body>
        <tns:ryokan_search_for_name xmlns:tns="http://testSecurityServer.x-road.eu/producer">
                <name>{施設名称}</name>
        </tns:ryokan_search_for_name>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

9-4. セキュリティサーバ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[大阪市立%]と入力してください。

※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。

```
Select
  no
  ,name
  ,location
  ,business_name
From
  ryokan
Where
  name like :name
;
```

出力例:

```
$ curl -d @ryokan_search_for_name.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:iden="http://x-
road.eu/xsd/identifiers"                          xmlns:repr="http://x-road.eu/xsd/representation.xsd"
xmlns:tns="http://testSecurityServer.x-road.eu/producer" xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">
    <SOAP-ENV:Header>
        <xrd:protocolVersion xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">4.0</xrd:protocolVersion>
        <xrd:id xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">ce6daaff-11d6-4e1a-8a67-2d0447004a7f</xrd:id>
        <xrd:requestHash                                    xmlns:xrd="http://x-road.eu/xsd/xroad.xsd"
algorithmId="http://www.w3.org/2001/04/xmlenc#sha512">oWryCWadJmmd9RwCpjRhPhwrYnkukrklKpAzDuO+KIqPMu6Pud
2++NO0OdH8BY6tOO1/CScjWbhoGuK+W92Xng==</xrd:requestHash>
        <xrd:userId xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">admin</xrd:userId>
        <xrd:service       xmlns:iden="http://x-road.eu/xsd/identifiers"       iden:objectType="SERVICE"
xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">
            <iden:xRoadInstance>roksnet-dev</iden:xRoadInstance>
            <iden:memberClass>COM</iden:memberClass>
            <iden:memberCode>21110001</iden:memberCode>
            <iden:subsystemCode>testSecurityServer</iden:subsystemCode>
            <iden:serviceCode>ryokan_search_for_name</iden:serviceCode>
            <iden:serviceVersion>v1</iden:serviceVersion>
        </xrd:service>
        <xrd:client       xmlns:iden="http://x-road.eu/xsd/identifiers"       iden:objectType="SUBSYSTEM"
xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">
            <iden:xRoadInstance>roksnet-dev</iden:xRoadInstance>
            <iden:memberClass>COM</iden:memberClass>
            <iden:memberCode>21110001</iden:memberCode>
            <iden:subsystemCode>testSecurityServer</iden:subsystemCode>
        </xrd:client>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body>
        <tns:ryokan_search_for_nameResponse xmlns:tns="http://testSecurityServer.x-road.eu/producer">
            <row>
                <no>1378</no>
                <name>大阪市立青少年センター</name>
                <location>東淀川区東中島１丁目１３番１３号</location>
                <business_name>大阪市こども青少年局</business_name>
            </row>
            <row>
                <no>1538</no>
                <name>大阪市立長居ユースホステル</name>
                <location>東住吉区長居公園１番１号長居陸上競技場</location>
                <business_name>大阪市</business_name>
            </row>
        </tns:ryokan_search_for_nameResponse>
    </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。

参考:SOAP メッセージ文/WSDL の情報　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

10. Adapter Server のインストール

Adapter Server のインストールについては、下記インストレーションガイドを参照ください。

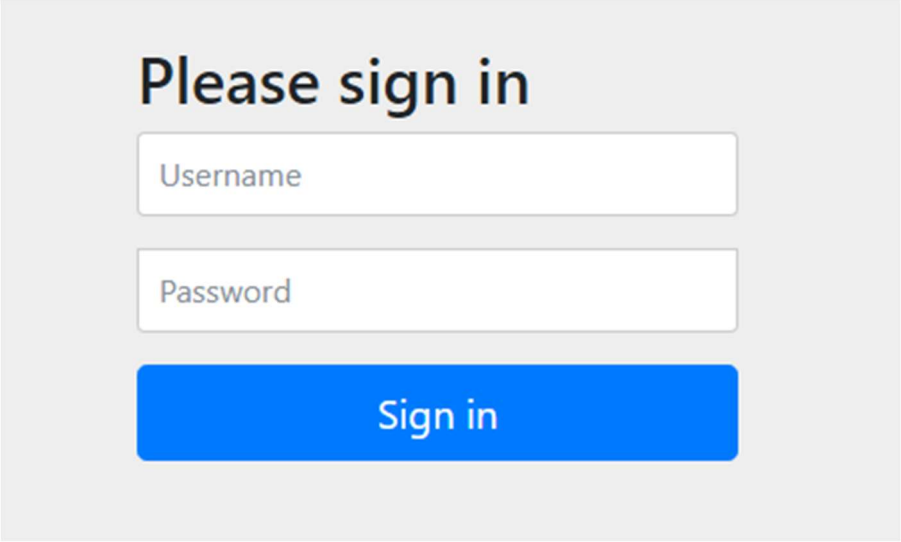
OZ1_JP-Link_AdaptorServer_installation_guide_v1.0(ja)20220318.pdf

11. Adapter Server でのサービスの作成

*前提：本書においてはデータベースの作成・設定に係る手順は記述しておりません。

11-1. ログイン

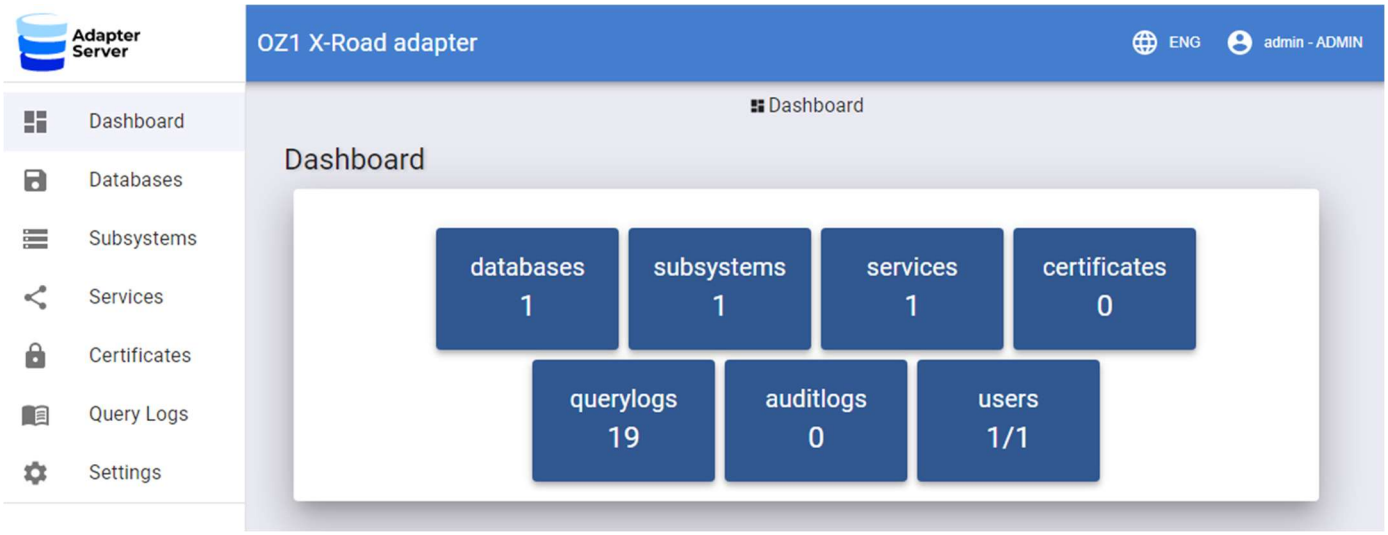
https://{IP-ADDRESS}より Adapter Server のログイン画面を開き、インストールガイドにて作成したユーザーにて、ログインを行ってください。



11-2. ダッシュボード

ログインに成功すると、以下のようなダッシュボード画面が表示されます。

（下図、ダッシュボードは OZ1 開発環境にて準備した Adapter Server のため、すでに設定済みの状態です。そのため、databases や subsystems、services の欄が 1 となっておりますが、初期時点ではこれらは 0 になっております）



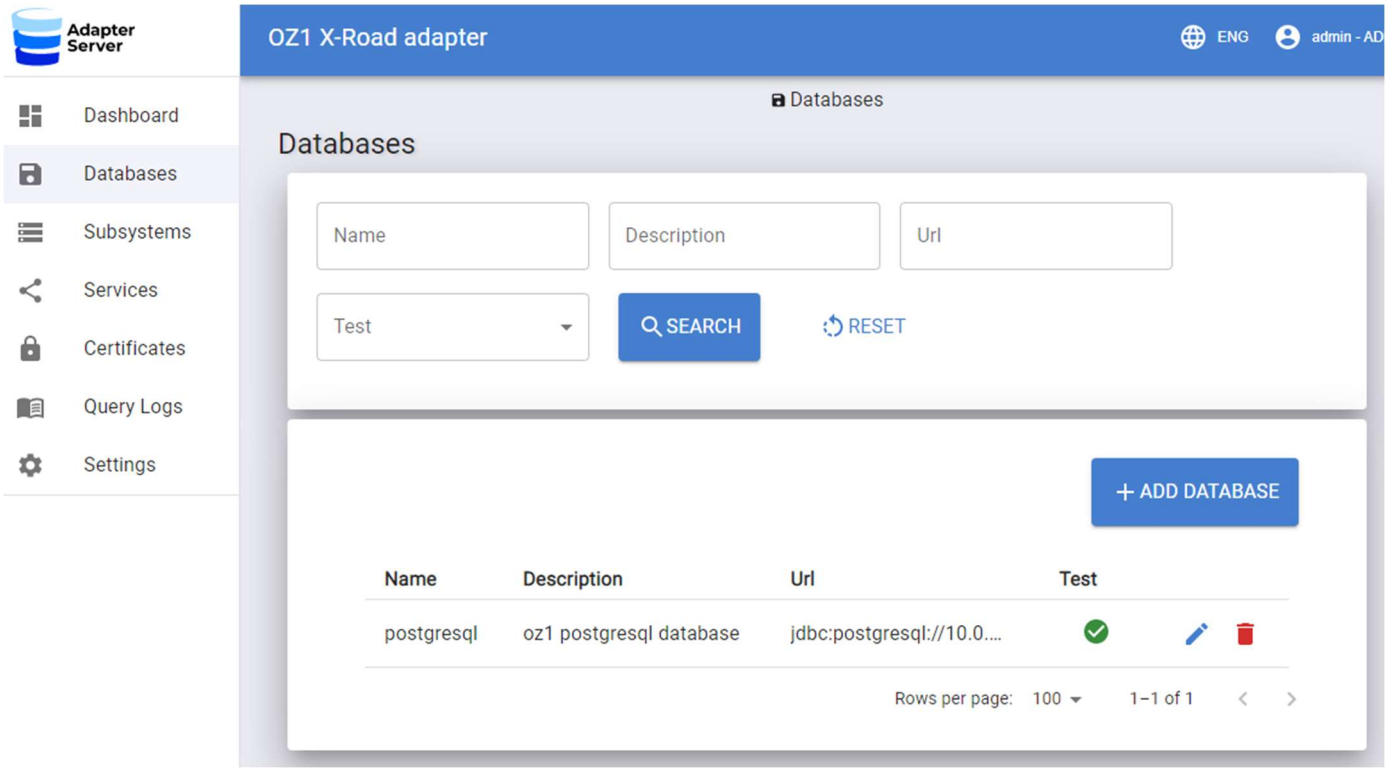
11-3. データソースの登録

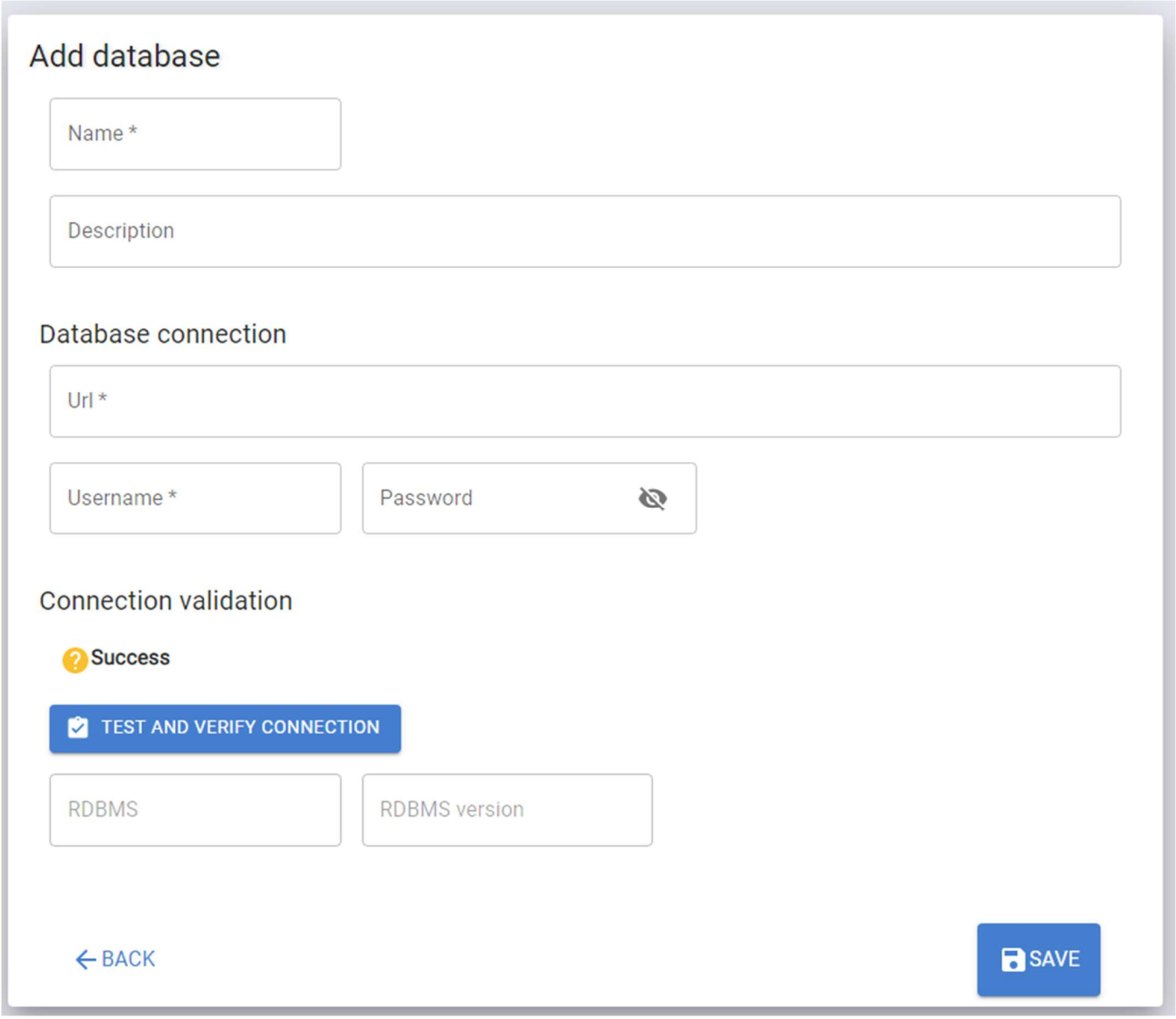
~~*前提：現在の Adapter Server は PostgreSQL のみ対応しており、PostgreSQL 12 以上のバージョンで動作することを確認しております。PostgreSQL 11 以下の動作については確認できておりませんが、動作すると思われます。~~

その他 RDBMS 製品にも対応致しました。

詳細はユーザーガイド(OZ1_JP-Link_AdapterServer_user_guide_v1.0(ja)20220318.pdf)を参照ください。

メニューより[Databases]を選択し、[+ADD DATABASE]ボタンを押下してください。





- Name : データソースの名称を入れてください。【必須】

- Description : 本データソースの説明の記入欄です。

- Url : jdbc url を各 RDBMS の記載ルールに従って、記述ください。【必須】

  (例) PostgreSQL の場合: [jdbc:postgresql://**{host}**:**{port}**/**{dbname}**]

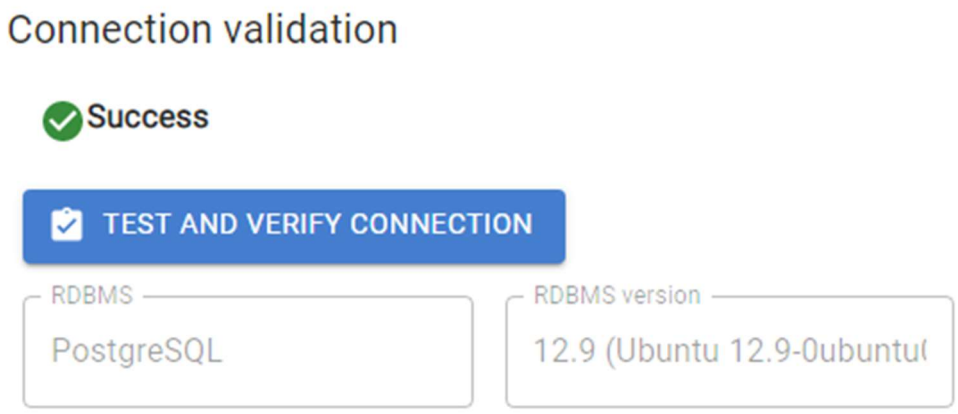
- Username : database へアクセスする際に用いるユーザー名を記載してください【必須】

- Password : database へアクセスする際に用いるユーザーのパスワードを記載してください【必須】

以上、必須項目を入力の上、[TEST AND VERIFY CONNECTION]ボタンを押下し、データベースに正常にアクセスされることを確認してください。

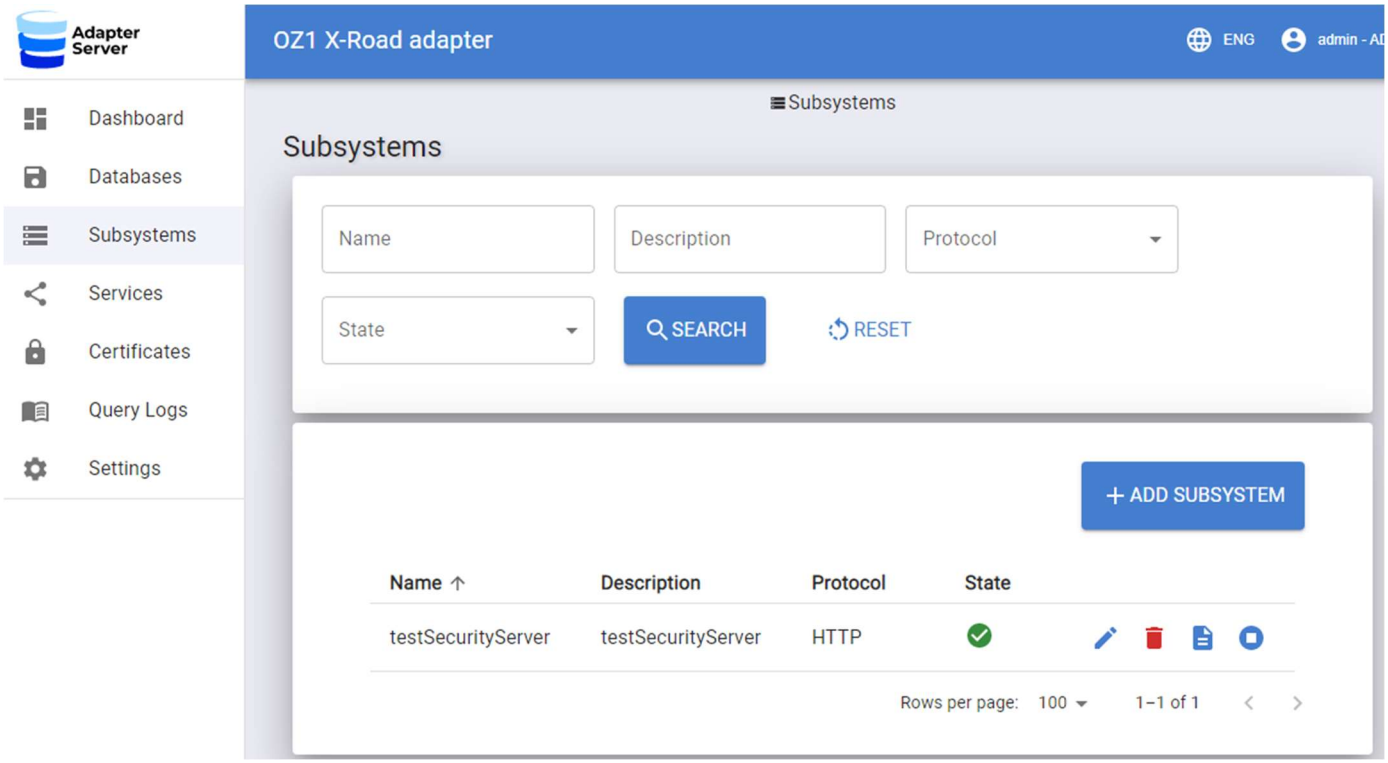
RDBMS 及び RDBMS Version については、[TEST AND VERIFY CONNECTION]ボタンを押下後、正常にアクセスできた場合に自動的に入力されます。

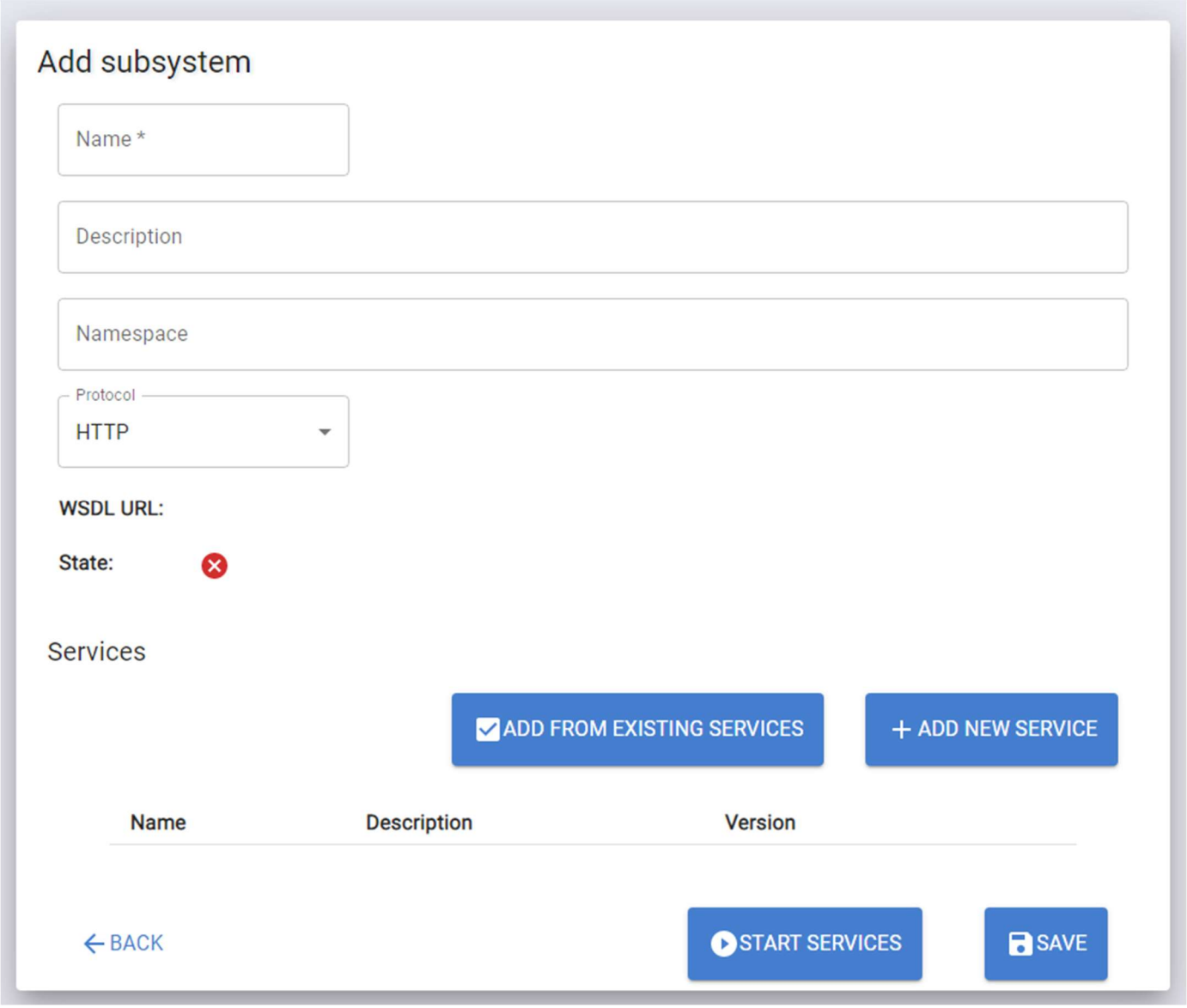
正常に成功した場合の表示例



11-4. Subsystems の登録

メニューより[Subsystems]を選択し、[+ADD SUBSYSTEM]ボタンを押下してください。





- Name: セキュリティサーバに登録した Subsystem Code を入力してください【必須】

- Description: Subsystem に関する説明を入力してください

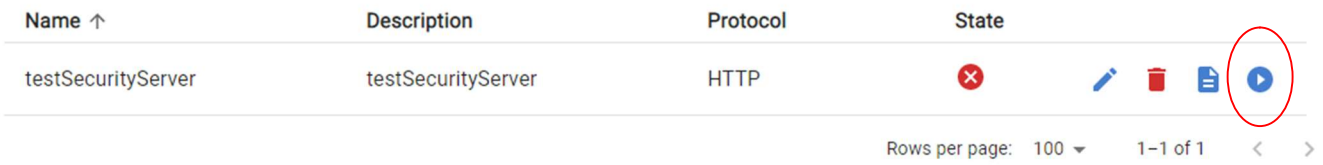
- Namespace: 名前空間を指定する場合に入力ください

必須項目を入力後、[SAVE]ボタンを押下し、保存してください。

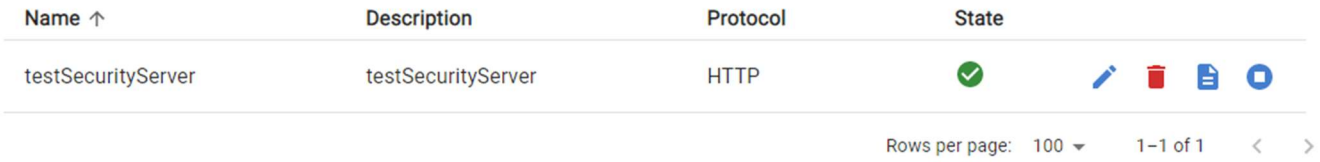
その後、[←BACK]ボタンを押下し、Subsystems 一覧画面へ遷移してください。

登録直後の subsystem は state が無効になっています。

Subsystem の有効化は下図赤丸で囲ったボタンを押下すると、state の状態が有効になります。

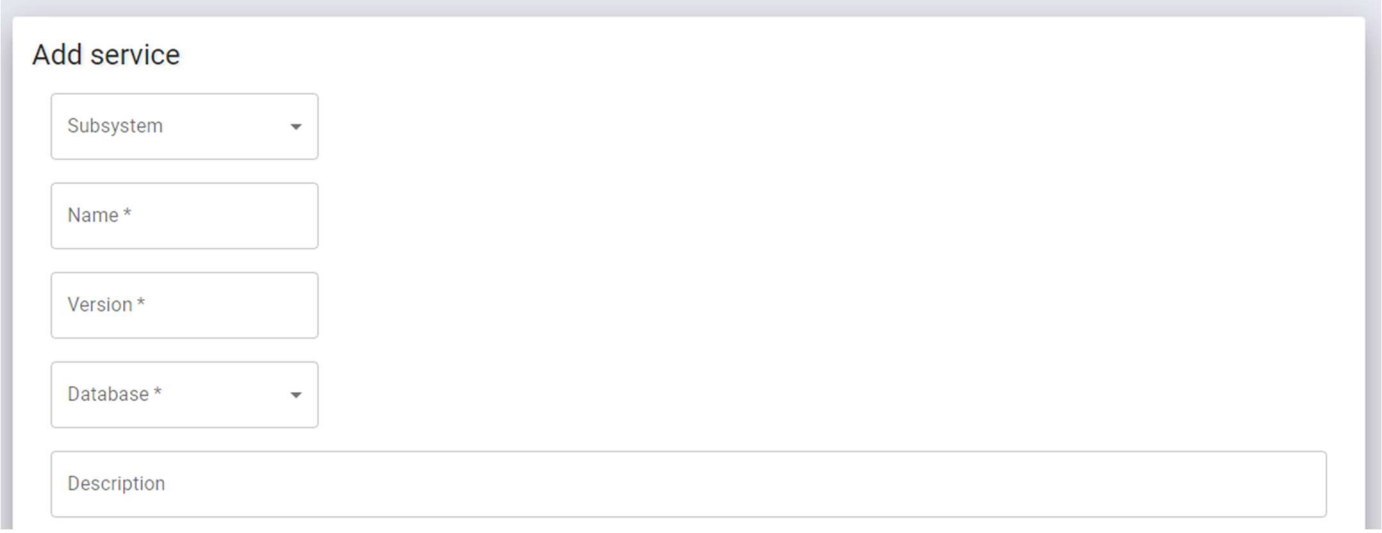


正常に subsystem が有効になると、state が更新されます。



※もう一度当該ボタンを押下すると、無効に切り替えることができます。

11-5. Service の作成



- Subsystem: 前項で作成した Subsystem を選択してください

- Name: Service の名称を入力してください【必須】

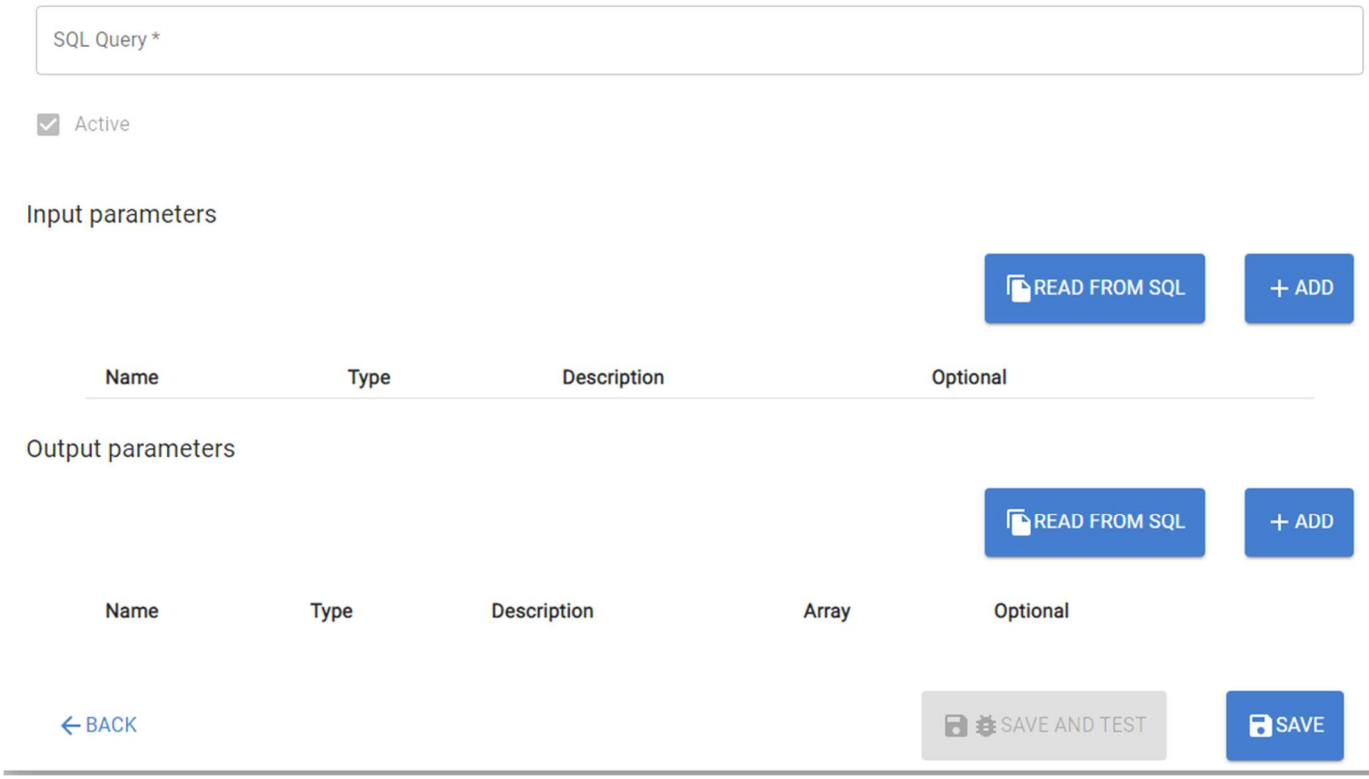
- Version: Service のバージョンを 1 以上の整数値で入力してください。【必須】

- Database: 前述の手順で登録したデータソースを選択してください【必須】

- Description: サービスに関する説明を入力してください

続いて、データソースとして登録したデータベースに対して、実行する SQL を記述します。

SQL の記述は、SQL そのものの記述と、インプットプレースホルダの設定、アウトプットフォーマットの設定の 3 つの設定を行う必要があり、これらの 3 つの設定は全て密接に関連しています。



* 2022/2/17 時点では、[READ FROM SQL]ボタンは実装されていません。押下しても想定通りの挙動にはならない為、実行しないでください。

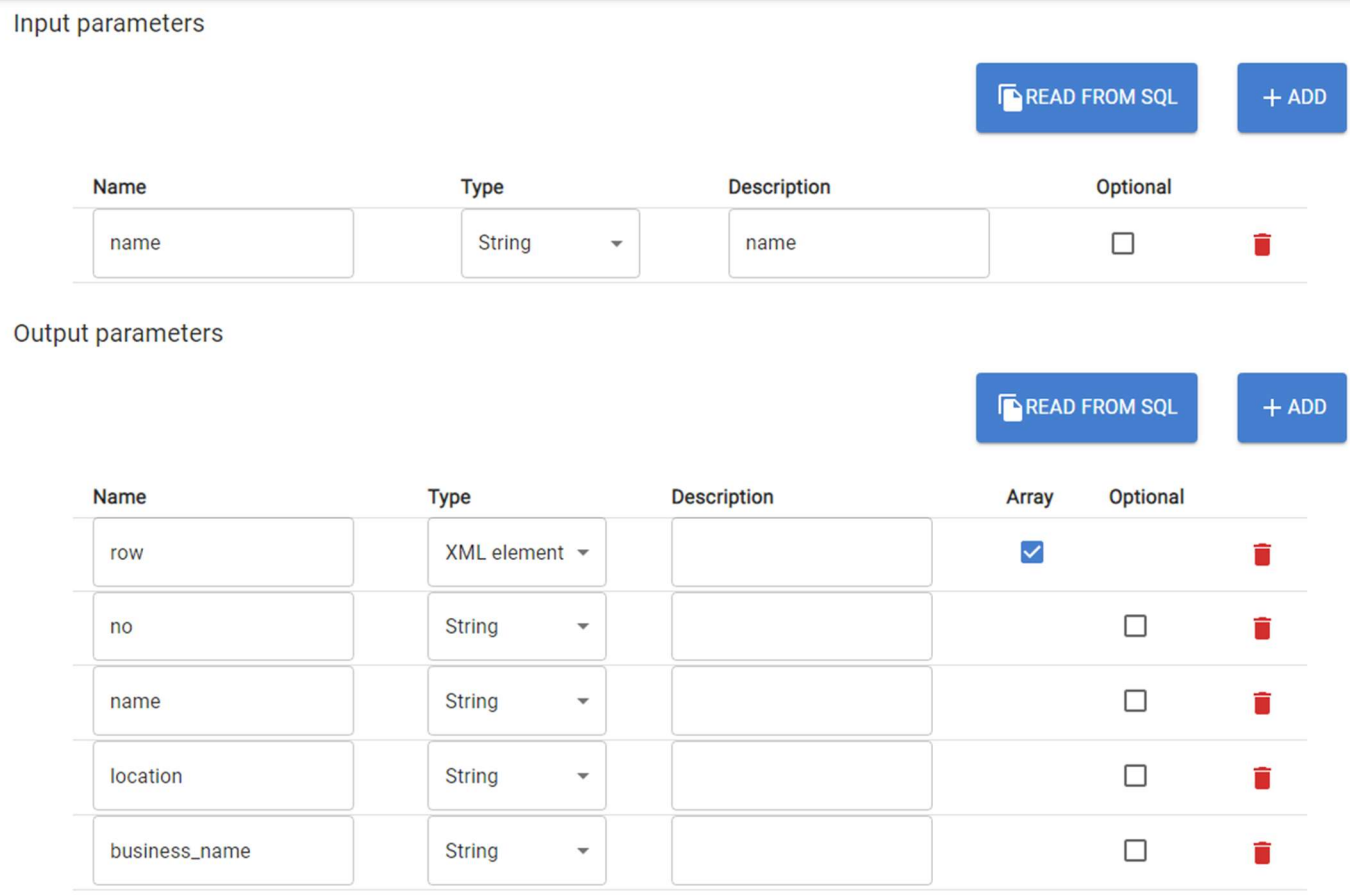
- SQL Query: SQL のクエリを SQL 言語フォーマットに従って入力してください。インプットプレースホルダは変数名の前に[:](コロン)をつけてください【必須】

- Input Parameters: インプットプレースホルダを利用する場合、必ず記述してください。利用しない場合には空欄でも問題ありません。[+ADD]ボタンを押下して行を追加できます。

- Output Parameters: サービスの実行結果の形式を定義します。SQL クエリと齟齬のないようご注意ください。[+ADD]ボタンを押下して行を追加できます。【必須】

次ページに、参考情報として設定方法の一例を記載しております。

SQL: `select no,name,location,business_name from ryokan where name like :name;`



* Output Parameters の row について

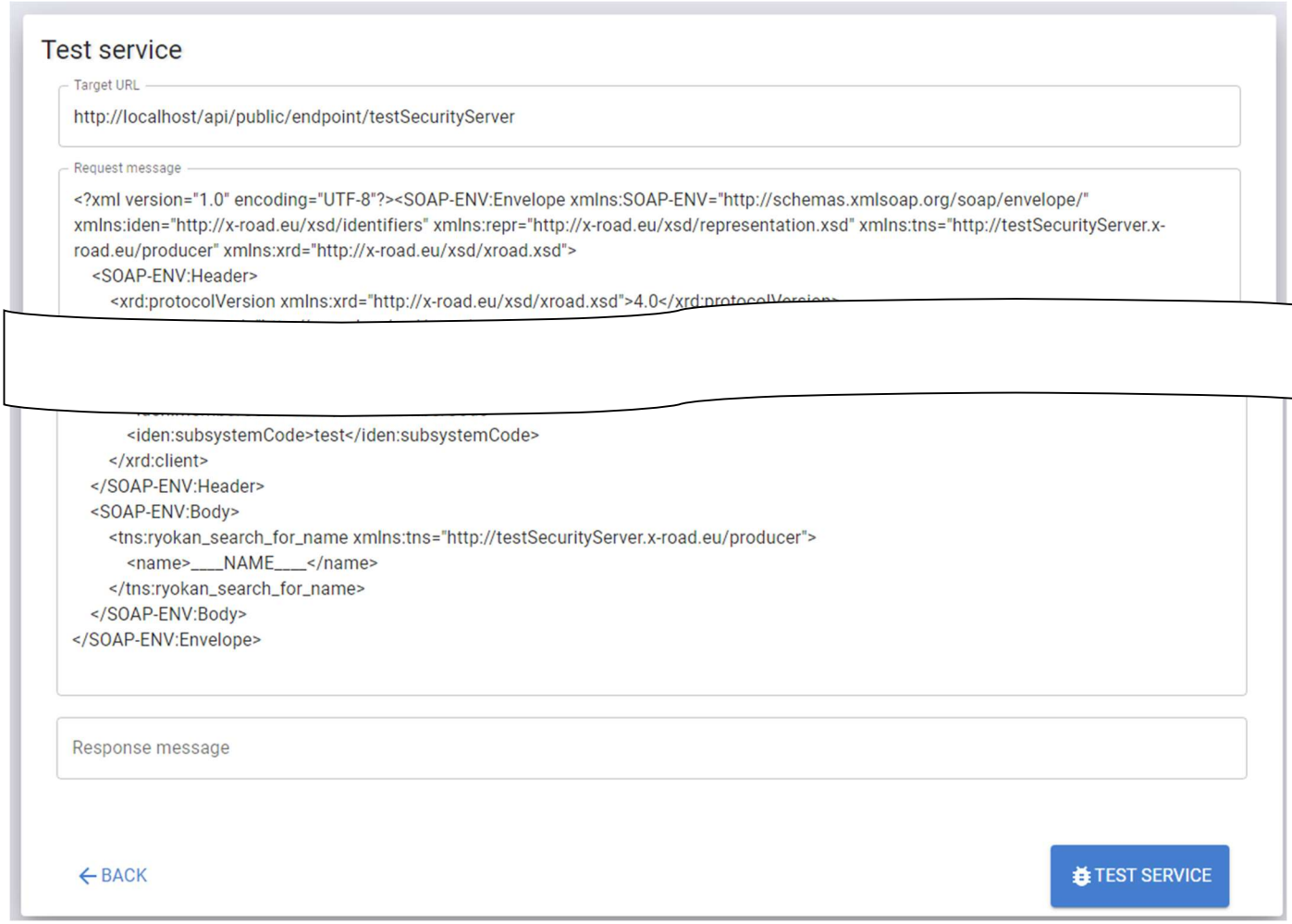
これは SQL 実行結果が複数行になる場合に、結果のレコードを配列として記述するために必要となります。SQL の実行結果が必ず 1 レコードしか取得されない場合には記述する必要はありません。

こうした定義のサービスの実行結果の BODY 部には例えば、次のように情報が設定されます。

```
    <SOAP-ENV:Body>
        <tns:ryokan_search_for_nameResponse xmlns:tns="http://testSecurityServer.x-road.eu/producer">
            <row>
                <no>1</no>
                <name>東横INN大阪天神橋筋六丁目</name>
                <location>北区浮田2丁目3番17号</location>
                <business_name>株式会社東横イン</business_name>
            </row>
            <row>
```

```
                <no>142</no>
                <name>東横INN梅田中津Ⅰ</name>
                <location>北区豊崎3丁目20番4号東横イン　梅田中津</location>
                <business_name>聖徳ビル企画株式会社</business_name>
            </row>
                                        ----- snip ------
            <row>
                <no>1372</no>
                <name>東横イン新大阪駅東口</name>
                <location>東淀川区西淡路2丁目8番5号</location>
                <business_name>株式会社東横イン</business_name>
            </row>
            <row>
                <no>1556</no>
                <name>東横INNあべの天王寺</name>
                <location>西成区山王1丁目1番7号</location>
                <business_name>株式会社ホテル聖徳</business_name>
            </row>
        </tns:ryokan_search_for_nameResponse>
    </SOAP-ENV:Body>
```

以上、ここまでの必須項目の入力が完了しましたら、[SAVE　AND　TEST]ボタンを押下し、サービスの稼働確認を実行します。



- Target URL: 自動的に入力されますが、宛先ホストが localhost 固定となりますので、Adapter Server をインストールしたサーバの IP アドレスに変更してください。【必須】

- Request message: プレースホルダを利用している場合には、インプットパラメータ定義部分に[___{プレースホルダ定義名}___]という固定値が入力されていますので、必要に応じて変更してください。

準備ができましたら、[TEST SERVICE]ボタンを押下してください。

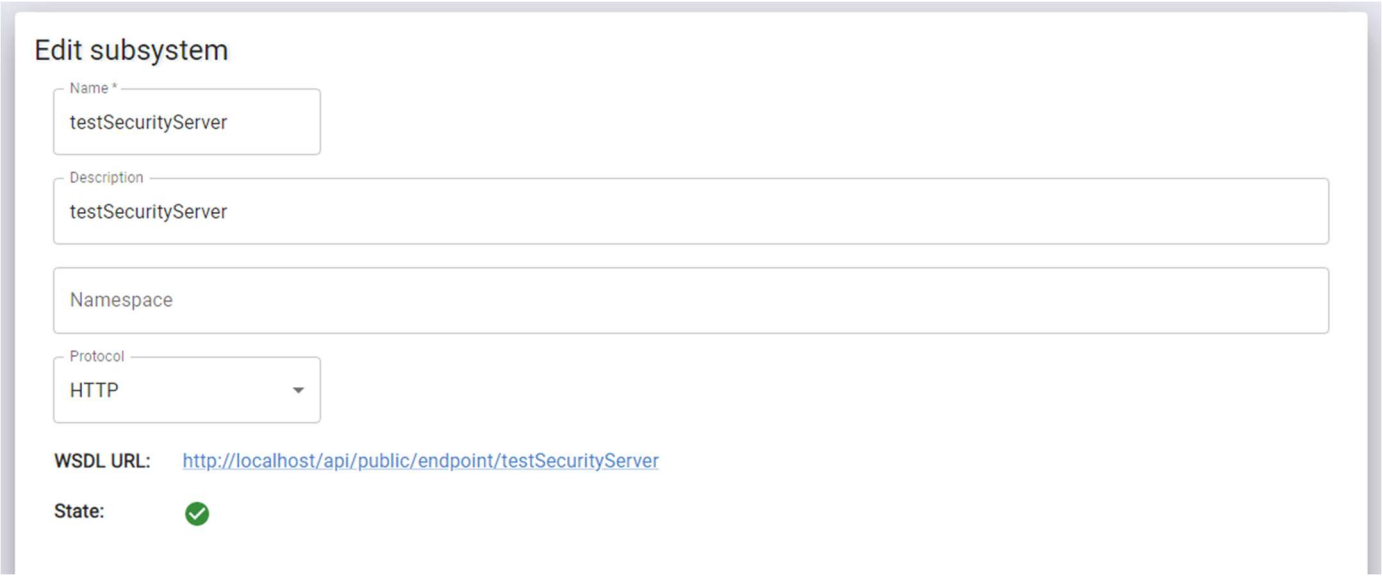
エラーが発生せず、Reponse message 欄に応答データが表示されれば、サービスのテストは完了です。

11-6. サービスのセキュリティサーバへの登録のための準備

セキュリティサーバへサービスを登録する為に、サービスの情報を記述した WSDL ファイルをセキュリティサーバへ連携する WSDL URL を控えておいてください。

WSDL URL は Subsystems から参照することができます。

*WSDL URL は宛先ホストが localhost 固定となっています。セキュリティサーバ登録時には Adapter Server をインストールしたサーバの IP アドレスに変更が必要です。



以上で Adapter Server での操作は終了ですので、ログアウトしてください。

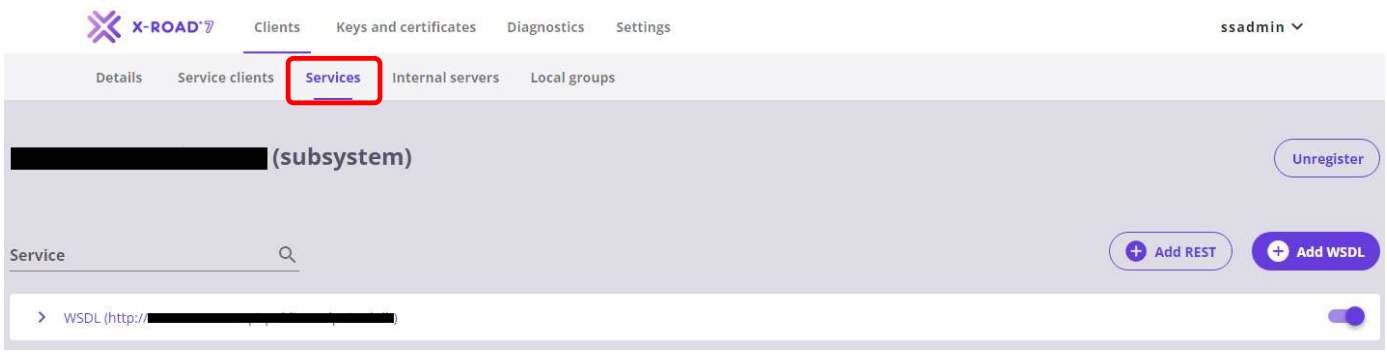
12.セキュリティサーバへのサービスの登録

12-1. セキュリティサーバへ WSDL の登録
続いて、web ブラウザに https://{security-server-ip-address}:4000/にアクセスし、セキュリティサーバの web ui 画面へアクセスしてください。

ログイン画面が表示されましたら、ユーザー名とパスワードを入力し、ログインしてください。

[Clients]セクションから、今回サービスを登録する[Clients]を Client の一覧の中から選んでください。

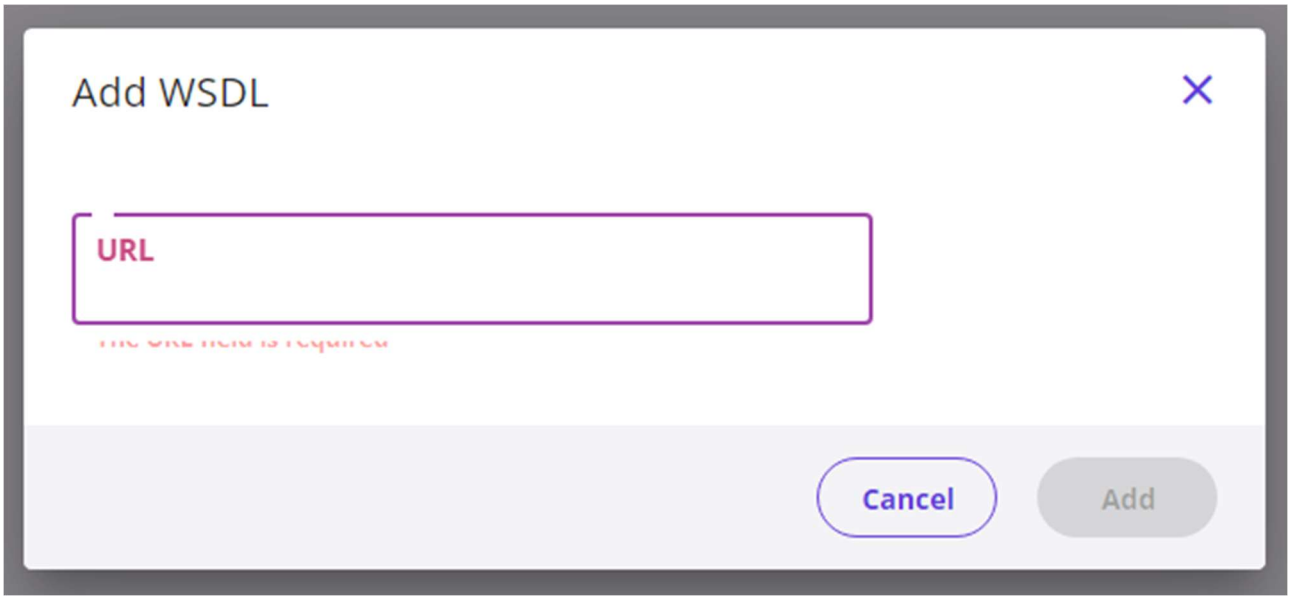
続いて、[Clients] ＞[Services]セクションを選択します。

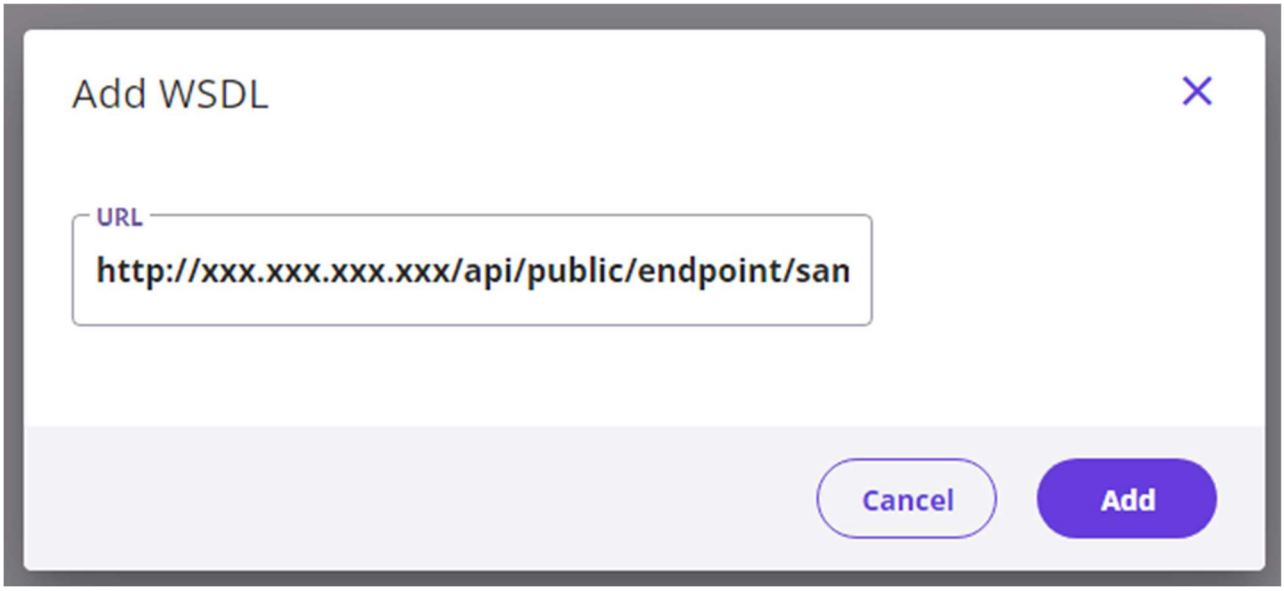


*例示の画面はすでにサービス 1 件の登録を試みた後である為、サービスが存在しています。

[+Add WSDL]ボタンを押下すると、URL の入力が求められる為、Adapter Server で控えた WSDL URL を URL 欄に貼り付けてください。

*繰り返しになりますが、WSDL URL は宛先ホストが localhost 固定となっています。セキュリティサーバ登録時には Adapter Server をインストールしたサーバの IP アドレスに変更が必要です。



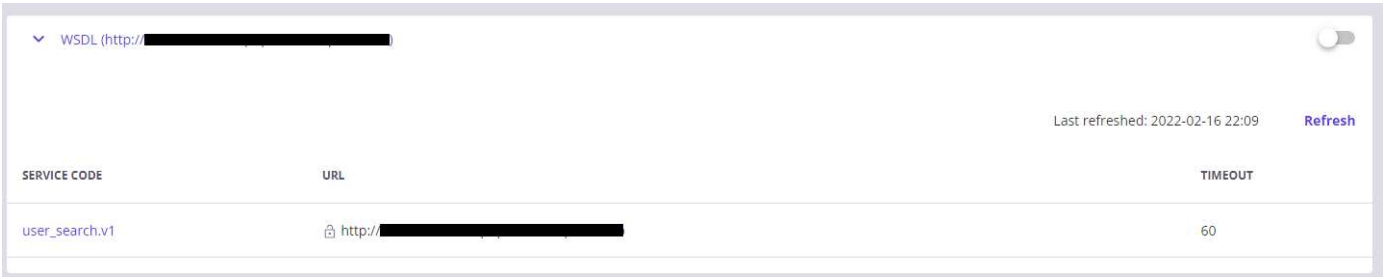


入力しましたら、[Add]ボタンを押下します。WSDL のダウンロードをセキュリティサーバが行いますので、5～10 秒前後、お待ちください。

無事ダウンロードが完了すると、下記のようになります。

WSDL(http://xxxx.xxx.xxx.xxx/api/public/endpoint/xxxxxx)の右にある[>]をクリックし展開します。

作成したサービス名が、SERVICE CODE 欄に表示されているか確認し、表示されていれば成功です。

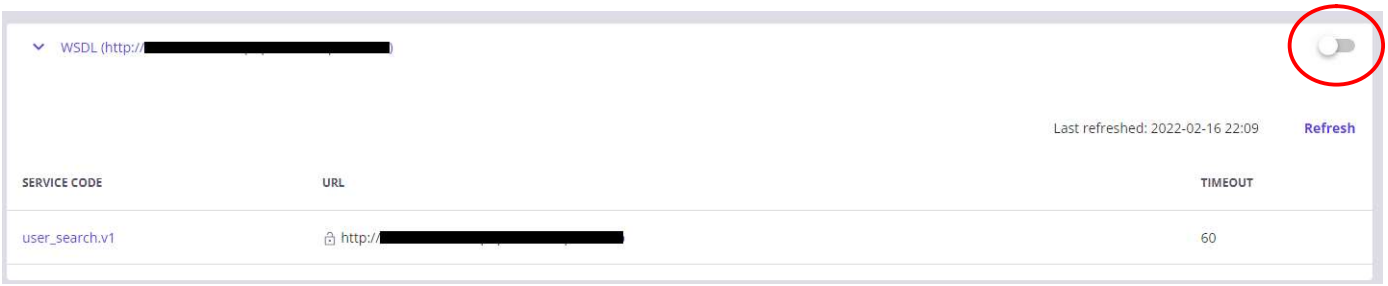


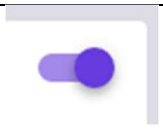
12-2. サービスの有効化

セキュリティサーバへサービスを登録するとき、サービスはデフォルトでは無効状態で登録されます。

よって、サービス登録後、手動でサービスを有効状態にする必要があります。

サービスの有効/無効は右上のスイッチで制御されます。クリックすることで有効/無効を切り替えます。

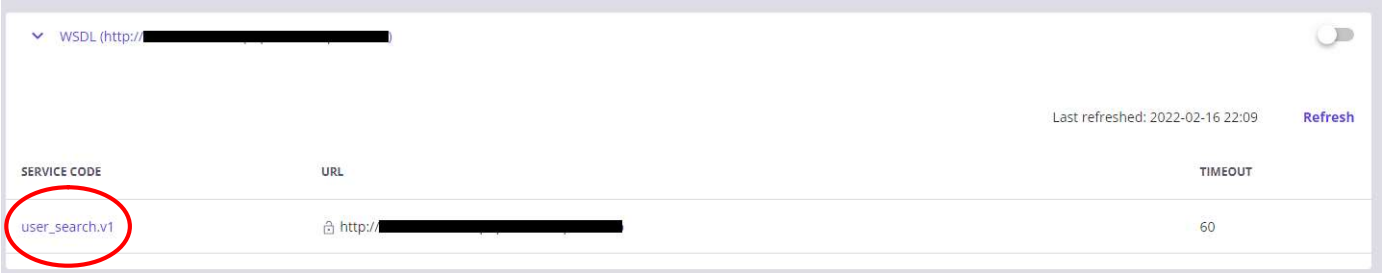


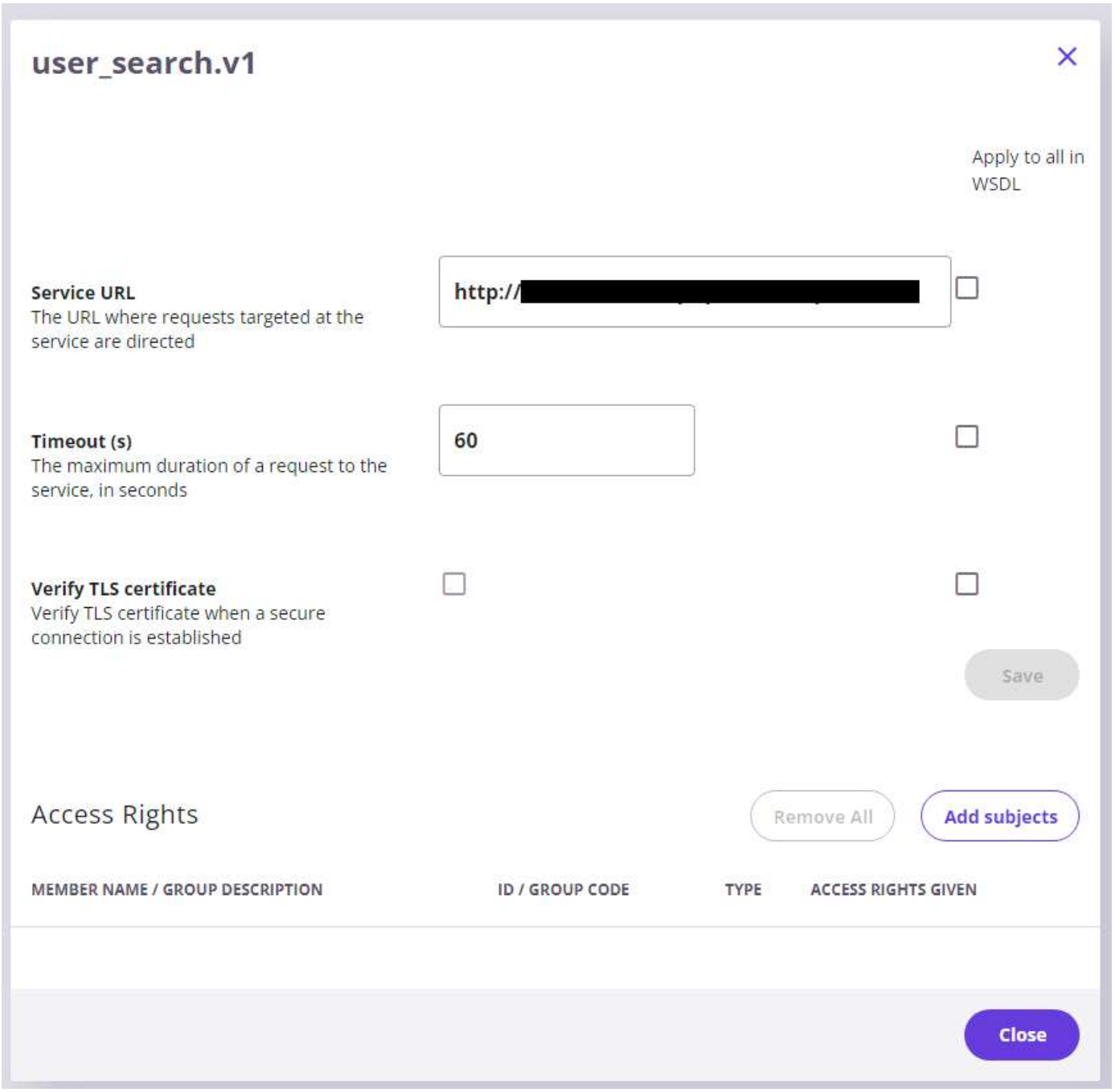
有効	
無効	

12-3. サービスの実行許可

サービスを JP LINK 参加者へ展開にするあたって、サービスの利用をしてもらうためには、サービス利用者にサービスの利用許可を与える必要があります。

サービス名のリンクをクリックし、サービスの詳細設定を開きます。



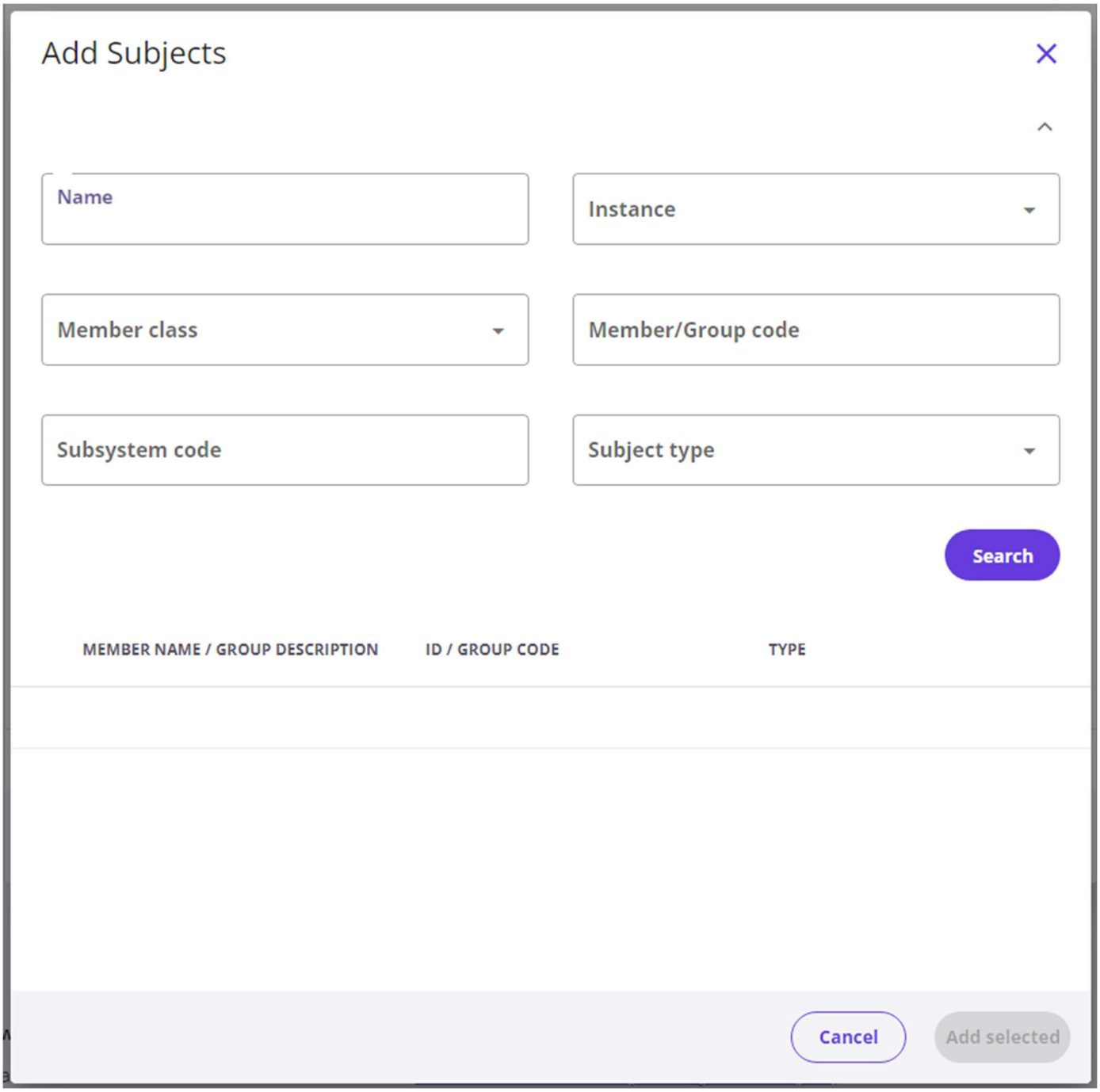


サービスの利用許可は、[Access Rights]で制御されます。

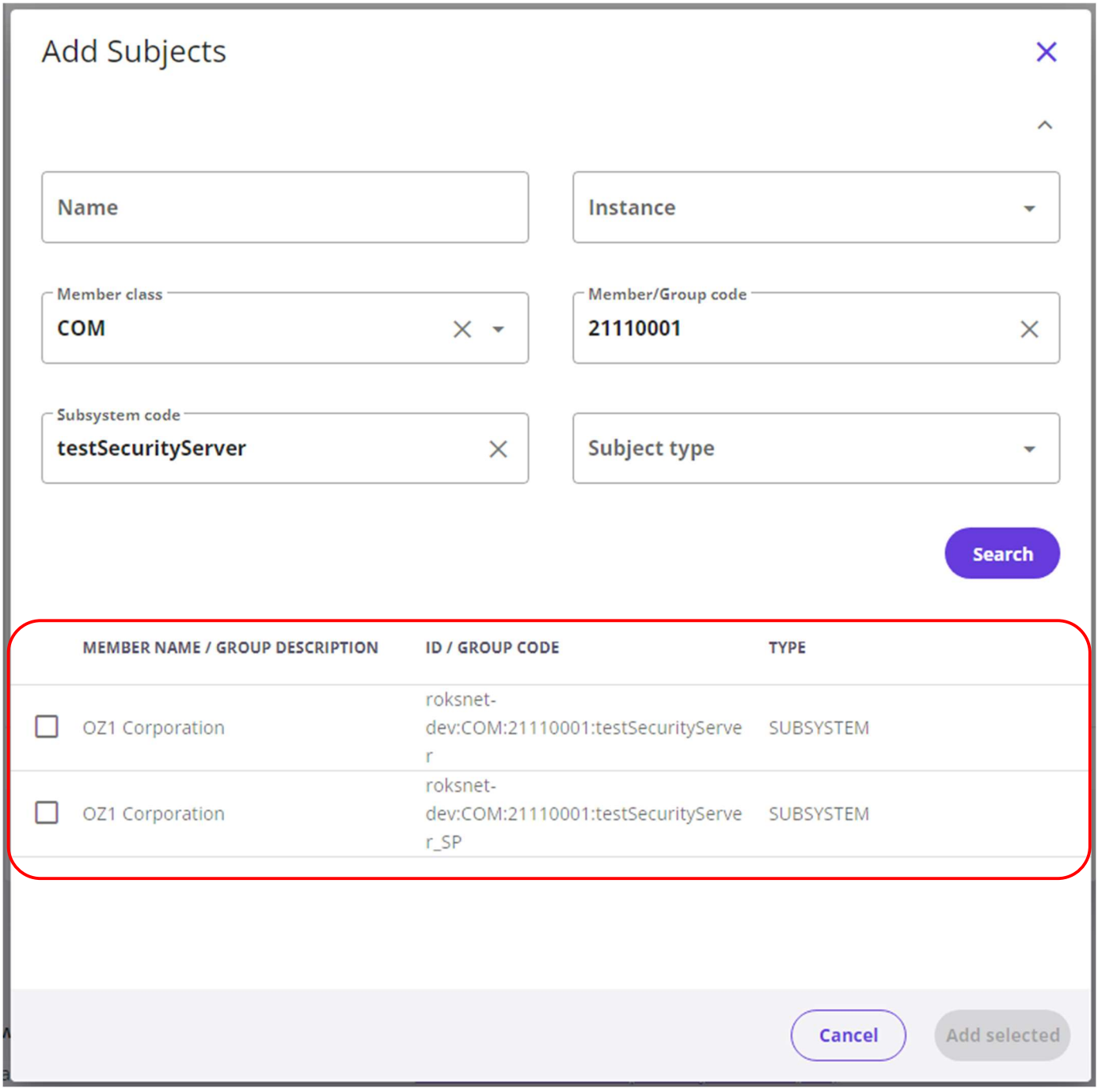
[Access Rights]はホワイトリスト方式です。[Access Rights]に追加されていない Client はサービスを利用することは出来ません。

サービスの利用許可を与えるためには、[Add subjects]ボタンを押下します。

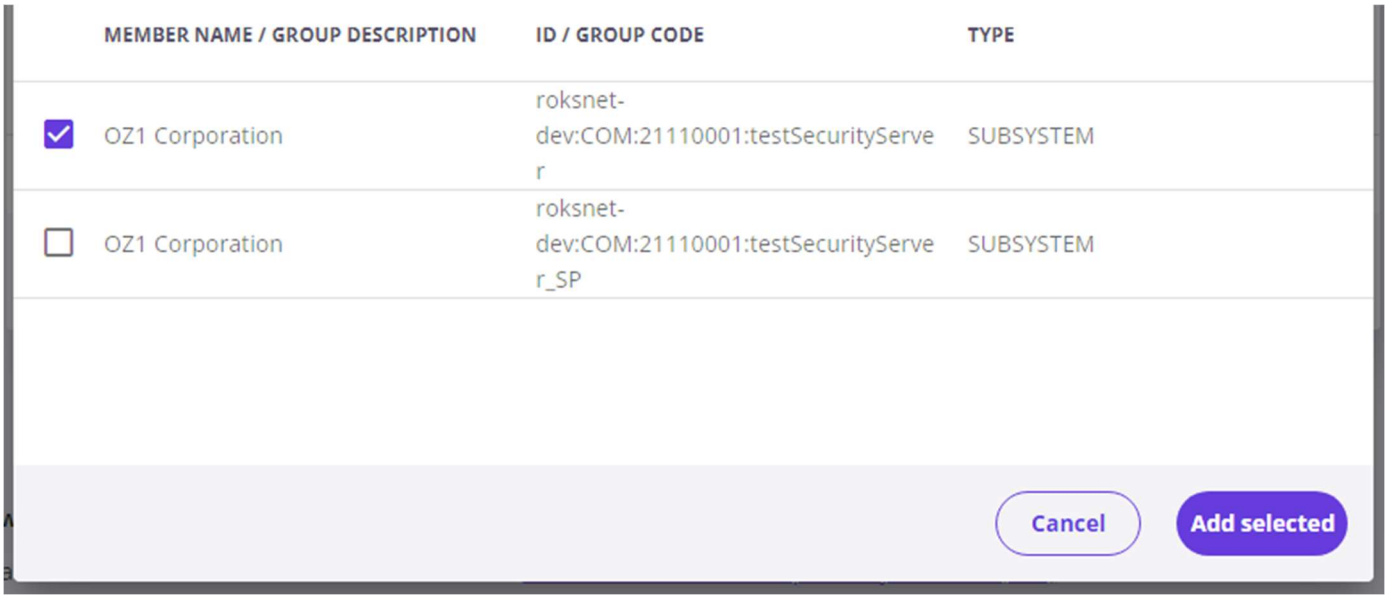
ここでサービスの利用許可を与える Client を各項目のフィルタをかけて探すことができます。



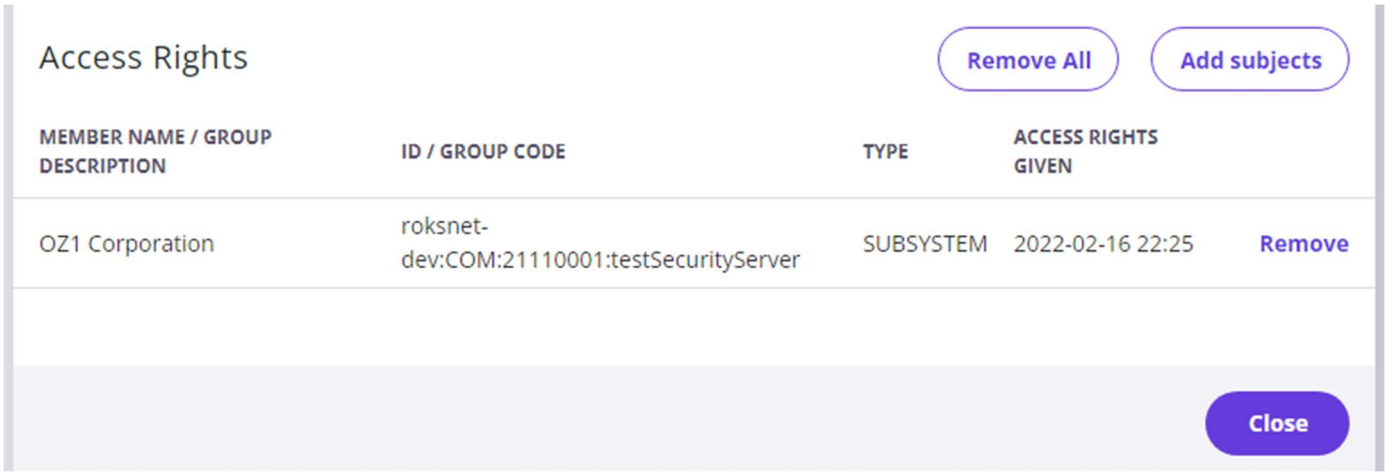
例えば、メンバークラス／メンバーコード／サブシステムコードで検索すると以下のように検索結果が表示されます。



この中から利用許可を与える Client を選び、[Add selected]ボタンを押下します。



Access Rights に OZ1 の Client である testSecurityServer が追加されましたので、testSecurityServer のクライアントはこのサービスに対して、データの要求を行う事ができるようになりました。



サービスの利用許可を取り消す場合には、[Remove]ボタンを押下してください。

以上でサービスの登録、有効化、利用許可という一連の作業が終了となります。

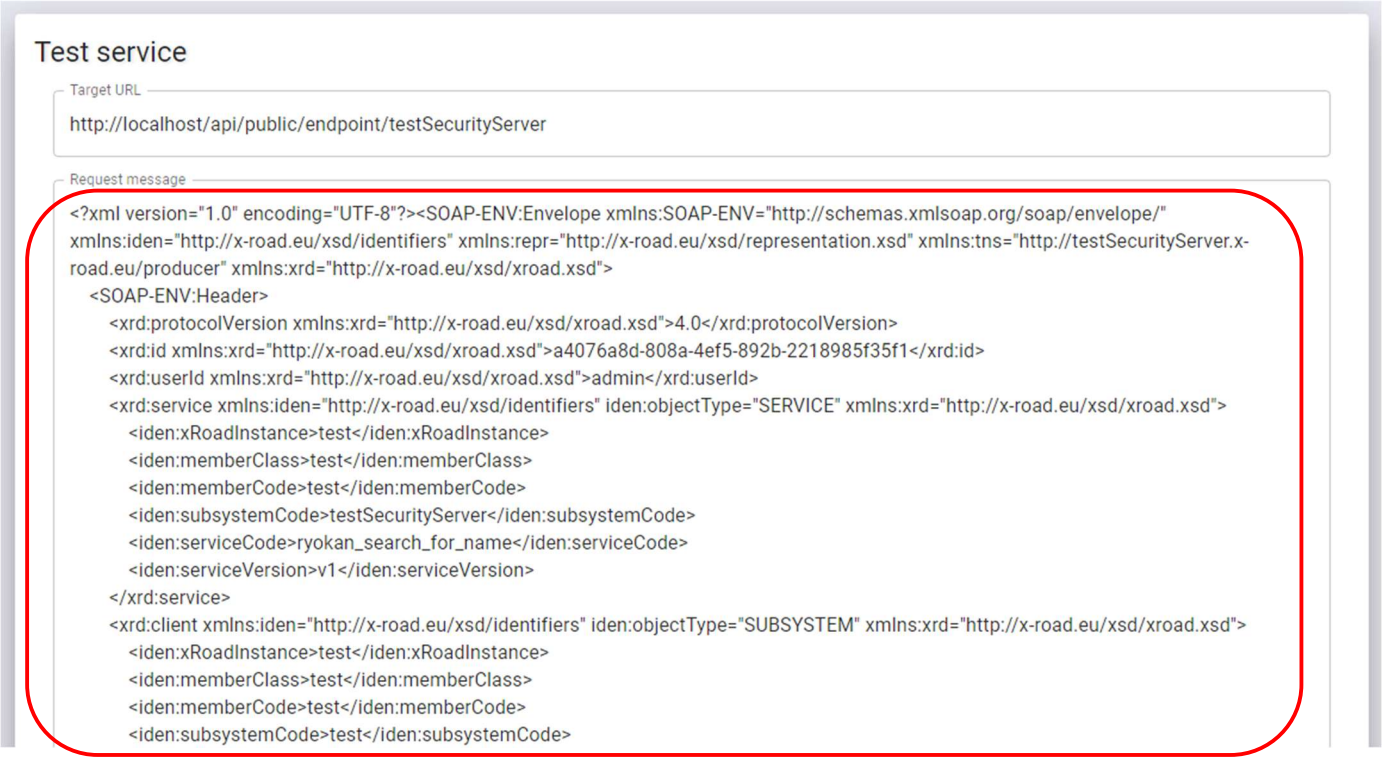
実際にサービスの利用許可を与える場合には、関係者間で事前に十分な打ち合わせの上、実施するようお願いいたします。

12-4. 疎通確認

疎通確認の実施方法は[9.疎通確認]で実施した方法と同じです。

リクエスト時の WSDL 定義情報ファイルを作成する場合は、Adapter Server のサービステスト時に利用した[Request message]欄に表示された内容を利用していただくと、スムーズです。

*下図、赤枠で囲った部分の情報です



*こちらの内容をコピーし、必要な情報を書き換えてください。

各要素へ入力すべき内容

要素	入力内容
SOAP-ENV:Header	
xrd:service	サービス提供側の情報を定義してください。(対向システム側の情報)
iden:xRoadInstance	roksnet-dev 固定。
iden:memberClass	相手先のメンバークラス(例:COM)
iden:memberCode	相手先のメンバーコード(例:21110001)
iden:subsystemCode	相手先のサブシステムコード(例:testSecurityServer)
iden:serviceCode	利用したいサービスコード(例:user_search)
iden:serviceVersion	利用したいサービスのバージョン(例:v1)
xrd:client	サービス利用側の情報を定義してください。(自分自身の情報)
iden:memberClass	自身のメンバークラス(例:GOV)
iden:memberCode	自身のメンバーコード(例:21119999)
iden:subsystemCode	自身のサブシステムコード(例:testSecurityServer_SP)
SOAP-ENV:BODY	
tns:<Service-Code>	tns:<Service Code>というルールで記載されます
{input-parameter}	インプットパラメータがあれば、インプットパラメータ名のタグに任意の情報を入力します

その後、下記 Curl コマンドを実行ください。

```
curl -d @{sample-service-xml-file-name} --header "Content-Type: text/xml" -X POST http://localhost
```

* sample-service.xml-file-name には、前段で作成した WSDL 定義情報ファイルのファイルパスを指定してください

13. Adapter Server のその他の操作方法

Adapter Server の各画面の操作方法や管理運用に関しては、下記ユーザーガイドを参照ください。

OZ1_JP-Link_AdapterServer_user_guide_v1.0(ja)20220318.pdf

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

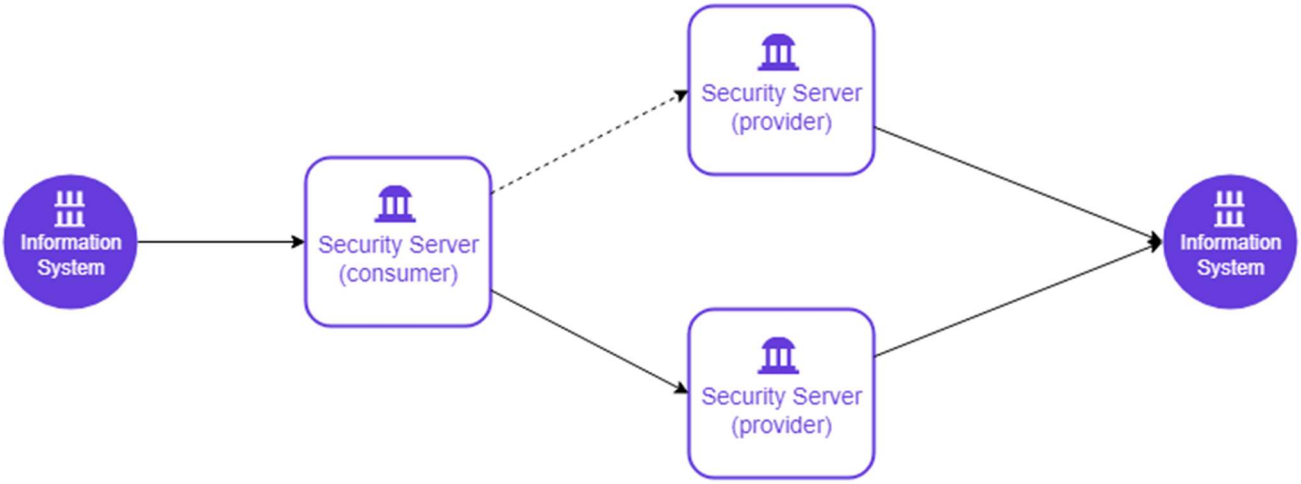
セキュリティサーバでリモートデータベースを使用することが可能です。このオプションは、データベースの状態を外部化する必要がある場合の開発およびテストで使用されることがあります。

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

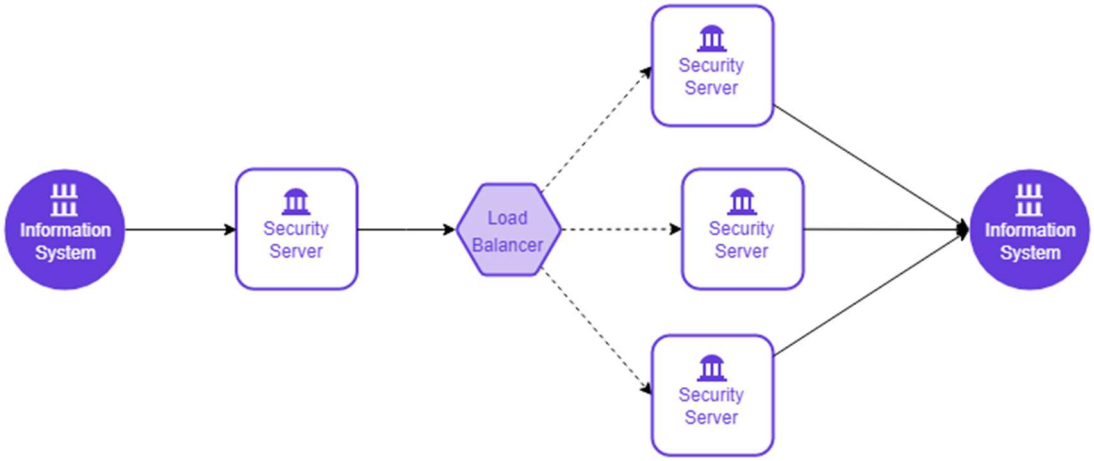
C.4 高可用性のセットアップ

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

C.7 メッセージログの設定

セキュリティサーバはデータ交換を行った際の通常のリクエスト及びレスポンスのメッセージを第三者へ証明するための手段として、メッセージの保管を行っています。

メッセージログには 3 種類のオプションが用意されています。

- 完全なログ記録　*デフォルト設定
  - メッセージ本文（BODY）とメタデータ（HEADER）の両方が保存されます。
- メタデータのみのログ記録
  - メタデータ（HEADER）のみが保存されます。
- ログを記録しない
  - メッセージログの保管を行いません。（非推奨）

完全なログ記録を行う場合、ログレコードは完全に検証可能な状態として保管され、第三者への証明として利用することができます。一方で大きなデータサイズのデータ交換を繰り返す場合、メッセージログの保管は大きなストレージを必要とする可能性があります。また、セキュリティサーバにメッセージ交換を行った業務データが、メッセージログの形式で保管されることに留意してください。

以下に、メッセージログの保管設定を変更する方法を記述します。

なお、メッセージログを一切記録しない設定もありますが、この設定は推奨致しません。

1. デフォルトの値を上書きするため、ローカル設定ファイルを作成または更新します。

```
vi /etc/xroad/conf.d/local.ini
```

2. ファイルに[message-log]セクション (存在しない場合) を作成します。セクションの下に、パラメータの値を 1 行に 1 つ記載してください。メッセージログをメタデータのみ保管する設定にする場合には以下のような記述となります。

```
[message-log]

message-body-logging=false
```

3. ファイルを保存し、xroad-proxy サービスを再起動します。

```
sudo systemctl restart xroad-proxy
```

メッセージログには他にも設定項目が存在します。

その他の設定内容については、以下のガイドを参照ください。

OZ1_JP-Link_SecurityServer_User_Guide.pdf