JP-LINK セキュリティ・サーバ・ユーザーガイド

17.3 障害の詳細 UUID

1 はじめに

このドキュメントでは、X-Road バージョン 6 セキュリティ・サーバの管理とメンテナンスについて説明する。

1.1 X-Road セキュリティ・サーバ

セキュリティ・サーバの主な機能は、リクエストの証拠能力を担保した上で、リクエストを仲介することである。

セキュリティ・サーバは、一方の側からパブリックインターネットに接続され、他方の側から組織内ネットワークの情報システムに接続されている。ある意味で、セキュリティ・サーバは SOAP プロトコルをサポートする特殊なアプリケーション・ファイアウォールとして考えられる。したがって、他のプロトコルを仲介するファイアウォールなどと並行して設定する必要がある。

セキュリティ・サーバには、クライアントとサービス・プロバイダの間のメッセージ交換を保護する機能が備わっている。

- パブリックインターネットを通じて送信されるメッセージは、デジタル署名と暗号化によって保護されている。
- サービス・プロバイダのセキュリティ・サーバは受信するメッセージに対してアクセス制御を行う。したがって、データにアクセスできる者は、サービス・プロバイダと適切な契約を結んだユーザーだけに制限される。

システム全体の可用性を高めるために、サービス・ユーザーとサービス・プロバイダのセキュリティ・サーバは、次のように冗長化できる。

- サービス・ユーザーはリクエストをするために、複数台のセキュリティ・サーバを並行して動作させることができる。
- サービス・プロバイダがサービスを提供するために複数台のセキュリティ・サーバをネットワークに接続する場合、リクエストは複数のサーバにロードバランシング（負荷分散）される。
- サービス・プロバイダの一台のセキュリティ・サーバがオフラインになると、リクエストは自動的に利用可能な他のセキュリティ・サーバに振り分けられる。

セキュリティ・サーバは、グローバル・コンフィグレーションを提供するセントラル・サーバにも依存する。

1.2 X-Road のコンセプト

ローバル・コンフィギュレーション

セキュリティ・サーバによって X-Road セントラル・サーバから定期的にダウンロードされる XML ファイルからなる。

グローバル・コンフィギュレーションは、以下を含む。

- ✓ トラスト・アンカーのアドレスと公開鍵（認証サービスの CA およびタイムスタンプ・サービス）中間認証局の公開鍵
- ✓ OCSP サービスのアドレスと公開鍵（Authority Information Access 拡張により利用できない場合）X-Road メンバーとそのサブシステムに関する情報
- ✓ X-Road に登録されているメンバーのセキュリティ・サーバのアドレス
- ✓ X-Road に登録されているセキュリティ・サーバの認証用証明書に関する情報 X-Road に登録されているセキュリティ・サーバのクライアントに関する情報 グローバル・アクセス権グループに関する情報
- ✓ X-Road システム・パラメータ

- **メンバー・クラス** 共通のユニットの下で同様の特性を持つ X-Road メンバーをグループ化する。例えば、国の機関は”GOV”メンバー・クラスの下にグループ化され、民間組織は”COM”のメンバー・クラス下にグループ化される。
- **メンバー・コード**は、特定の X-Road メンバーと 1 対 1 で関連付く。特定のメンバー・クラス内のユニークな文字の組み合わせである。メンバー・コードは メンバーの存続期間中は変更されない。

例えば、エストニアの組織や国の機関のメンバー・コードは事業登録番号である。 - セキュリティ・サーバ・クライアントセキュリティ・サーバとの関係が X-Road 監督機関に登録されており、X-Road サービスを使用および/または提供するためにセキュリティ・サーバを使用する X-Road メンバーのサブシステムである

- **セキュリティ・サーバの所有者**特定のセキュリティ・サーバを法的に担当する X-Road メンバーである。セキュリティ・サーバの所有者は、太字のフォントでセキュリティ・サーバ・クライアント・リスト(”Configuration” -> ”Security Server Clients”) に表示される。
- サブシステムは、X-Road メンバーの情報システムの一部を表す。X-Road メンバーは、X-Road サービスを使用または提供するために、情報システムをサブシステムとして登録しなければならない。

サブシステムは、X-Road サービスの提供と使用の面において自立している。

- ✓ X-Road メンバーのサブシステムのアクセス権は独立している。一つのサブシステムに与えられたアクセス権は、メンバーの他のサブシステムのアクセス権には影響しない
- ✓ サブシステムによって提供されるサービスは、メンバーの他のサブシステムによって提供されるサービスから独立している

X-Roadサービスを使用または提供する際に、サブシステムから送信されたメッセージに署名するため、サブシステムを管理するメンバーの署名用証明書が使用される。X-Road メンバーは、複数のサブシステムを一台のセキュリティ・サーバに関連付けることができ、一つのサブシステムは複数台のセキュリティ・サーバに関連付けることができる。

- **X-Road 証明書** X-Road 監督機関で承認された認証サービス・プロバイダが発行する。X-Road 証明書は、次のいずれかである。
  - ✓ 署名用証明書 - X-Roadメンバーに発行され、セキュリティ・サーバが交換するデータにデジタル署名するために使用する
  - ✓ 認証用証明書 - セキュリティ・サーバに対して発行され、セキュリティ・サーバの間のセキュアな通信チャネルを確立するために使用される
  - **X-Road インスタンス** ID は異なる X-Road インスタンスを識別する。各インスタンスには識別コードが割り当てられている。例えば、エストニアの開発インスタンスのコードは ”ee-dev” であり、プロダクション・インスタンスのコードは ”EE” である。
  - **X-Road メンバー** X-Road に参加し、そのサービス・プロバイダおよび/またはユーザーの能力によって X-Road の機能を使用する法人あるいは人である。
  - **X-Road のメッセージ** X-Road メッセージ・プロトコルに基づいて記述されたサービス・リクエストとレスポンスである。サービスを利用または提供する 情報システムとセキュリティ・サーバ間で交換される。

1.3 用語の定義

ASiC
ETSI TS 102 918, Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)
CRON
[CRON] Quartz Scheduler CRON expression,
http://www.quartz-scheduler.org/generated/2.2.1/html/qs-all/#page/Quartz_Scheduler_Documentation_Set%2Fco-trg_crontriggers.html
INI file
http://en.wikipedia.org/wiki/INI_file
JDBC
[JDBC] Connecting to the Database, https://jdbc.postgresql.org/documentation/93/connect.html
JSON
[JSON] Introducing JSON, http://json.org/
JMX
[JMX] Monitoring and Management Using JMX Technology,
http://docs.oracle.com/javase/8/docs/technotes/guides/management/agent.html
Zabbix Gateway
[ZABBIX-GATEWAY] Zabbix Java Gateway,
https://www.zabbix.com/documentation/3.0/manual/concepts/java

Zabbix JMX

[ZABBIX-JMX] Zabbix JMX Monitoring,
https://www.zabbix.com/documentation/3.0/manual/config/items/itemtypes/jmx_monitoring

Zabbix API

[ZABBIX-API] Zabbix API,
https://www.zabbix.com/documentation/3.0/manual/api

2 ユーザー管理

2.1 ユーザーのロール(役割)

セキュリティ・サーバは、次のユーザーのロールをサポートする。

- X-Road セキュリティ担当者(xroad-security-officer)は鍵設定、鍵、および証明書の管理を含むセキュリティ・ポリシーとセキュリティ要件を担当する
- X-Road 登録担当者(xroad-registration-officer)は、セキュリティ・サーバ・クライアントの登録と削除を担当する
- X-Road サービス管理者(xroad-service-administrator)はサービスのデータとアクセス権を管理する
- X-Road システム管理者(xroad-system-administrator)は、セキュリティ・サーバのインストール、設定、およびメンテナンスを担当する
- X-Road セキュリティ・サーバ・オブザーバ(xroad-securityserver-observer) 設定の編集アクセス権なしでセキュリティ・サーバの状態を閲覧することができる。このロールを通じて、ユーザーにセキュリティ・サーバの管理ユーザー・インターフェイスへの読み取り専用アクセスを提供することができる

2.2 ユーザーの管理

ユーザー管理は、root ユーザー権限においてコマンド・ラインで実行される。新しいユーザーを追加するには、次のコマンドを入力する。

```
adduser username
```

作成したユーザーに権限を付与するには、該当するシステム・グループに追加する。たとえば、次のようにする。

```
adduser username xroad-security-officer adduser username xroad-registration-officer adduser username xroad-service-administrator adduser username xroad-system-administrator adduser username xroad-securityserver-observer
```

ユーザー権限を削除するためには、該当するシステム・グループからユーザーを削除する。たとえば、次のようにする。

```
deluser username xroad-security-officer
```

ユーザー権限は、xroad-jetty サービス(セクション 16.1 を参照)の再起動後にのみ適用される。 ユーザーを削除するには、次のように入力する。

```
deluser username
```

3 セキュリティ・サーバの登録

セキュリティ・サーバを介して、メッセージを仲介(交換)するためには、セキュリティ・サーバとその所有者が、X-Road 監督機関によって承認された認証サービス・プロバイダに証明される必要がある。また、セキュリティ・サーバは X-Road 監督機関に登録されなければならない。

3.1 セキュリティ・サーバ所有者用の署名用鍵と証明書の設定

X-Road メッセージを署名するのにセキュリティ・サーバが使用する署名用鍵は、X-Road インスタンスのセキュリティ・ポリシーに従って、ソフトウェアまたはハードウェア(ハードウェア・セキュリティ・モジュールまたはスマート・カード)のセキュリティ・トークンに保存できる。

証明書ポリシーに応じて、署名用鍵はセキュリティ・サーバまたは認証サービス・プロバイダが作成する。セクション 3.1.1 からセクション 3.1.3 までは、セキュリティ・サーバで鍵が作成された場合の署名用鍵と証明書を設定するのに必要なアクションについて説明する。セクション 3.1.4 は、認証サービス・プロバイダによって鍵が作成された場合の署名鍵および証明書のインポートについて説明する。

デバイス、鍵、証明書の背景色はセクション[5.1] (#51-availability-states-of-security-tokens-keys-and-certificates)で説明される。

3.1.1署名用鍵の作成

アクセス権:

すべてのアクティビティ:セキュリティ担当者

鍵デバイスへのログイン以外のすべてのアクティビティ:登録担当者

鍵デバイスへのログイン: システム管理者

署名用鍵を作成するのには、次の手順を実行する。

- Management メニューで、Keys and Certificates を選択する。
- ハードウェア・セキュリティ・トークンを使用する場合は、デバイスがセキュリティ・サーバに接続していることを確認する。デバイス情報は、Keys and Certificates テーブルに表示される必要がある。 3.トークンにログインするためには、テーブルのトークンの行にある Enter PIN をクリックし、PIN コードを入力する。正しい PIN を入力した後に、Enter PIN のボタンは Logout に変わる。 4.署名用鍵を作成するのには、該当する行をクリックして、テーブルからトークンを選択し、Generate key をクリックする。鍵のラベル値を入力し、 OK をクリックする。作成された鍵は、テーブルのトークンの行の下に表示される。ラベル値は、鍵の名前として表示される。

3.1.2 署名用 CSR の作成

アクセス権: セキュリティ担当者、登録担当者

署名用の CSR を作成するのには、次の手順を実行する。

- Management メニューで、Keys and Certificates を選択する。
- テーブルから鍵を選択し、Generate CSR をクリックする。開いたダイアログで 2.1 Usage ドロップ・ダウン・リストから証明書使用ポリシー(証明書を署名するための SIGN)を選択する。 2.2 Client のドロップ・ダウン・リストから証明書が発行される X-Road メンバーを選択する。 2.3 Certification Service ドロップ・ダウン・リストから証明書の発行者を選択する。 2.4 認証サービス・プロバイダの要件により、証明書の署名リクエスト(PEM または DER)のフォーマットを選択する。 2.5 OK をクリックする
- 開いたフォームで、CSR に含まれる証明書の所有者の情報を確認し、必要に応じて空欄に記入する。
- OK をクリックし、CSR の作成を完了し、ファイルをローカル・ファイル・システムに保存する。

CSR の作成後、テーブルの鍵の行の下に「リクエスト」レコードが追加され、この鍵に対して CSR が作成されたことが示される。リクエスト・ファイルがローカル・ファイル・システムに保存されなくても、レコードが追加される。

署名用鍵を認証するのには、承認された認証サービス・プロバイダに CSR を送信し、CSR によって作成された署名用証明書を承認する。

3.1.3 ローカル・ファイル・システムから証明書のインポート

アクセス権: セキュリティ担当者、登録担当者

- セキュリティ・トークンから証明書をインポートするのには、次の手順を実行する
- Management メニューで、Keys and Certificates を選択する。
- 署名用鍵と署名用証明書を含む鍵デバイスがセキュリティ・サーバに接続していることを確認する。デバイスに格納されているデバイスと鍵と証明書は、Keys and Certificates 画面に表示される必要がある。
- セキュリティ・トークンにログインするのには、テーブルのトークンの行に Enter PIN をクリックし、PIN を入力する。正しい PIN を入力した後に、Enter PIN のボタンは Logout に変わる。
- 証明書の行の Import ボタンをクリックする。デフォルトでは、証明書は「登録済」状態でインポートされる。

3.2 セキュリティ・サーバの認証用鍵と証明書の設定

デバイス、鍵、証明書の背景色はセクション 5.1 で説明する。

3.2.1 アクセス権

- すべてのアクティビティ：セキュリティ担当者
- 鍵デバイスへのログイン：システム管理者

セキュリティ・サーバの認証用鍵は、ソフトウェア・セキュリティ・トークンでのみ作成できる。

- Management メニューで、Keys and Certificates を選択する。
- ソフトウェア・トークンへログインするのには、テーブルのトークンの行で Enter PIN をクリックし、トークンの PIN コードを入力する。正しい PIN を入力した後に、Enter PIN のボタンは Logout に変わる。
- 認証用鍵を作成するのには、該当する行をクリックして、テーブルからソフトウェア・トークンを選択し、Generate key をクリックする。鍵のラベル値を入力し、OK をクリックする。作成された鍵は、テーブルのトークンの行の下に表示される。ラベル値は、鍵の名前として表示される。

3.2.2 認証用鍵のための CSR の作成

アクセス権： セキュリティ担当者

認証用鍵のための CSR を作成するためには、次の手順を実行する。

- Management メニューで、Keys and Certificates を選択する。
- テーブルから認証用鍵を選択し、 Generate CSR をクリックする。開いたダイアログで 2.1 Usage ドロップ・ダウン・リストから証明書使用ポリシー（認証用証明書の場合 AUTH）を選択する。 2.2 Certification Service ドロップ・ダウン・リストから証明書の発行者を選択する。 2.3 認証サービス・プロバイダの要件により、証明書の署名リクエスト（PEM または DER）のフォーマットを選択する 2.4 OK をクリックする。
- 開いたフォームで、CSR に含まれる情報を確認し、必要に応じて空欄に記入する。
- CSR の作成を完了するために、OK をクリックして、プロンプト・ファイルをローカル・ファイル・システムに保存する。

CSR の作成後、テーブルの鍵の行の下に「リクエスト」レコードが追加され、この鍵に対して証明書の署名リクエストが作成されたことが示される。リクエスト・ファイルがローカル・ファイル・システムに保存されなくても、レコードが追加される。

認証用鍵を認証するためには、承認された認証サービス・プロバイダに CSR を送信し、CSR によって作成された認証用証明書を承認する。

3.2.3 ローカル・ファイル・システムから認証用証明書のインポート

アクセス権： セキュリティ担当者

認証用証明書をセキュリティ・サーバにインポートするためには、次の手順を実行する。

- Management メニューで、Keys and Certificates を選択する。
- Import certificate をクリックする。
- ローカル・ファイル・システムから証明書ファイルを探し、OK をクリックする。証明書をインポートした後に、認証用鍵の行の下にある「リクエスト」レ コードは、インポートされた証明書の情報に置き換えられる。デフォルトでは、証明書は「保存済」（セクション 5.2.2（#522- registration-states-of- the-authentication-certificate））および「無効」状態（セクション 5.3（# 53- validity-states-of-certificates））を参照）にインポートされる。
-

3.3 X-Road 監督機関においてセキュリティ・サーバを登録する

セキュリティ・サーバを X-Road 監督機関において登録するためには、以下のアクションを完了する必要がある。

- 認証用証明書の登録リクエストをセキュリティ・サーバから送信する必要がある（[3.3.1] - registering-an-authentication-certificate））を参照）。
- セキュリティ・サーバの登録リクエストは、X-Road インスタンスのプロセスに従って、X-

Road 監督機関に送信する必要がある。
- 登録リクエストは、X-Road 監督機関によって承認される必要がある。

3.3.1 認証用証明書の登録

アクセス権: セキュリティ担当者

セキュリティ・サーバの登録リクエストは、サーバ所有者の署名用鍵とサーバの認証用鍵を使用して、セキュリティ・サーバで署名される。したがって、それら証明書がセキュリティ・サーバにインポートされ、使用可能な状態になっていることを確認しなければならない(鍵を保持するトークンはログイン状態にあり、証明書の OCSP ステータスは「有効」であること)。

認証用証明書の登録リクエストを送信するためには、次の手順を実行する。

- Management メニューで、Keys and Certificates を選択する。
- 登録したい認証用証明書を選択し(「Saved」の状態である必要がある)、Register をクリックする。
- 開いたダイアログで、セキュリティ・サーバの公開 DNS 名、もしくはその外部 IP アドレスを入力し、OK をクリックする。 リクエストを送信すると、「Request sent」というメッセージが表示され、認証用証明書の状態は「登録中」に設定される。X-Road 監督機関が登録を承認した後に、認証用証明書の登録状態は「登録済」に設定され、登録プロセスが完了する。
-

4 セキュリティ・サーバ・クライアント

重要:X-Road サービスを使用または提供するためには、セキュリティ・サーバ・クライアントが X-Road 監督機関によって承認された認証サービス・プロバイダに認証される必要がある。 また、クライアントとクライアントが使用するセキュリティ・サーバ間の関連付けを X-Road 監督機関に登録しなければならない。

このセクションでは、セキュリティ・サーバの所有者を管理することについては言及していない。所有者の情報は、既にセキュリティ・サーバのインストール時に追加されており、セキュリティ・サーバの登録時に登録されている。Configuration メニューで Security Server Clients を選択すると、所有者の登録ステータスを確認できる。セキュリティ・サーバの所有者は太字で表示される。セキュリティ・サーバの登録前に、所有者は「保存済」状態にあり、登録プロセスが完了した後には「登録済」状態になる。

セキュリティ・サーバの所有者の登録は、所有者のサブシステムには関係しない。サブシステムはそれぞれ個別のクライアントとして登録する必要がある。

4.1 セキュリティ・サーバのクライアントの状態

セキュリティ・サーバは、以下のクライアント状態を区別する。

保存済 - クライアントの情報が入力され、セキュリティ・サーバの設定に保存済である。(4.2 を参照)。ただし、クライアントとセキュリティ・サーバ間の関連付けは、X-Road 監督機関に登録されていない。(関連付けがデータ入力前にセントラル・サーバに登録されている場合、クライアントはデータ入力後に「登録済」状態になる)。この状態から、クライアントは次の状態に移行できる:

- 「登録中」クライアントの登録リクエストがセキュリティ・サーバから送信された場合(4.4.1 を参照)。
- 「削除済」クライアントの情報がセキュリティ・サーバの設定から削除された場合(4.5.2 を参照)。

登録中 - クライアントの登録リクエストはセキュリティ・サーバからセントラル・サーバに送信されたが、クライアントとセキュリティ・サーバの関連付けはまだ X-Road 監督機関によって承認されていない状態。この状態から、クライアントは次の状態に遷移できる:

- 「登録済」クライアントとセキュリティ・サーバ間の関連が X-Road 監督機関によって承認された場合(4.4.1 を参照)。

- 「削除中」クライアント削除リクエストがセキュリティ・サーバから提出された場合(4.5.1 を参照)。

登録済 - クライアントとセキュリティ・サーバ間の関連付けは、X-Road 監督機関で承認されている。この状態では、クライアントは X-Road サービスを提供し、使用することができる(他のすべての条件が満たされていることが前提)。この状態から、クライアントは次の状態に遷移できる:

- 「グローバル・エラー」クライアントとセキュリティ・サーバの間の関連が X-Road 監督機関によって取り消された場合。
- 「削除中」クライアント削除リクエストがセキュリティ・サーバから送信された場合(4.5.1 を参照)

グローバル・エラー - クライアントとセキュリティ・サーバ間の関連付けがセントラル・サーバで取り消された。この状態から、クライアントは次の状態に遷移できる:

- 「登録済」クライアントとセキュリティ・サーバ間の関連付けがセントラル・サーバに復元された場合(例えば、クライアントとセキュリティ・サーバ間の関連付けがエラーのために失われた場合)。
- 「削除済」クライアントの情報がセキュリティ・サーバの設定から削除された場合(4.5.2 を参照)。

削除中 - クライアントの削除リクエストがセキュリティ・サーバから送信された。この状態から、クライアントは次の状態に遷移できる:

- 「削除済」クライアントの情報がセキュリティ・サーバの設定から削除された場合(4.5.2 を参照)。

4.2 セキュリティ・サーバにクライアントの追加

アクセス権: 登録担当者次の手順を実行する。

- Configuration メニューで、Security Server Clients を選択する。
- Add Client をクリックする。開いたウィンドウで、クライアントの情報を手動で入力するか、または Select Client from Global List をクリックし、すべての X-Road メンバーとそのサブシステムの中からクライアントの情報を探す。
- クライアントの情報を入力したら、OK をクリックする。新しいクライアントは、「保存済」状態でセキュリティ・サーバ・クライアントのリストに追加される。

4.3 セキュリティ・サーバ・クライアントの署名用鍵と証明書の設定

セキュリティ・サーバ・クライアントが X-Road を介して交換されるメッセージに署名するためには、署名用鍵と証明書を設定する必要がある。証明書はサブシステムには発行されない。したがって、サブシステムの所有者(すなわち、X-Road メンバー)の証明書をサブシステムは使用する。同じセキュリティ・サーバに登録されている X-Road メンバーのサブシステムは、メッセージを署名するのに同じ署名用証明書を使用する。したがって、セキュリティ・サーバは既にメンバーの署名用証明書を含む場合、そのメンバーのサブシステムを追加するときに、新しい署名用鍵および/または証明書を設定する必要はない。

セキュリティ・サーバ・クライアントの署名用鍵と証明書の設定プロセスは、セキュリティ・サーバの所有者の場合と同じである。このプロセスはセクション 3.1 で説明する。

4.4 X-Road 監督機関にセキュリティ・サーバ・クライアントを登録する

セキュリティ・サーバ・クライアントを X-Road 監督機関に登録するためには、次の手順を実行する。

- セキュリティ・サーバ・クライアント登録リクエストをセキュリティ・サーバから送信する(4.4.1 を参照)。
- クライアントの登録リクエストを X-Road インスタンスの組織手順に従って X-Road 監督機関に送信する。
- 登録リクエストは、X-Road 監督機関によって承認される必要がある。

4.4.1 セキュリティ・サーバ・クライアントの登録

アクセス権: 登録担当者
クライアント登録リクエストを送信するためには、次の手順を実行する。

- Configuration メニューで、Security Server Clients を選択する。
- セキュリティ・サーバ・クライアントのリストから「保存済」状態のクライアントを選択する。
- Details アイコンをクリックし、開いたウィンドウで Register をクリックする。
- Confirm をクリックしてリクエストを送信する。

リクエストを送信すると、「Request sent」というメッセージが表示され、クライアントの状態は「登録中」に設定される。 X-Road 監督機関が登録を承認した後に、クライアントの状態は「登録済」に設定され、登録プロセスは完了する。

4.5 セキュリティ・サーバからクライアントの削除

セキュリティ・サーバからクライアントを削除すると、クライアントに関連するすべての情報(つまり、WSDL、サービス、アクセス権、そして必要であれば証明書)もサーバから削除される。
1 クライアントが削除された場合でも、その署名用証明書がセキュリティ・サーバに登録された他のクライアント、たとえば削除されたクライアントが属する X- Road メンバーの他のサブシステムによって使用されている場合には、署名用証明書を削除することは推奨しない。
X-Road 監督機関に登録済みまたは登録中状態と表示されるクライアントは、削除する前に登録解除する必要がある。登録解除イベントは、セキュリティ・サーバからセキュリティ・サーバ・クライアント削除リクエストをセントラル・サーバに送信する。

4.5.1 クライアントの登録を解除する

アクセス権: 登録担当者
クライアントの登録を解除するには、次の手順を実行する。

- Configuration メニューで、Security Server Clients を選択する。
- サーバから削除したいクライアントを選択し、クライアントの行の Details アイコンをクリックする。
- 表示されたウィンドウで、Unregister をクリックし、Confirm をクリックする。セキュリティ・サーバは、自動的にクライアント削除リクエストをセントラル・サーバに送信し、セントラル・サーバはそれを受信するとセキュリティ・サーバとクライアント間の関連付けを削除する。
- 次に、削除リクエストのセントラル・サーバへの送信についての通知が表示され、クライアントの情報(証明書を除く)を削除するか確認する。
- クライアントの情報をすぐに削除したい場合は、Confirm をクリックする。次に、クライアントの証明書を削除するオプションが表示される。証明書を削除するには、もう一度 Confirm をクリックする。
- クライアントの情報を保持したい場合は、Cancel をクリックする。その場合、クライアントは、メッセージを仲介することができず、X-Road 監督機関に再度登録することができない「削除中」状態に移行される。
- 「削除中」状態のクライアントの情報を削除するためには、クライアントの行の Details アイコンをクリックし、クライアントを選択し、開いたウィンドウで Delete をクリックし、そして最後に Confirm をクリックする。

注意: セキュリティ・サーバを介し削除リクエストを送信することなく、登録されたクライアントをセントラル・サーバから登録削除することができる。この方法では、クライアントを担当するセキュリティ・サーバの管理者は、登録を解除するクライアントに関する情報を含むリクエストをセントラル・サーバの管理者に送信する必要がある。クライアントがセキュリティ・サーバからの削除リクエストなしでセントラル・サーバから削除された場合、クライアントはセキュリティ・サーバに「グローバル・エラー」状態で表示される。

4.5.2 クライアントを削除する

アクセス権: 登録担当者
セキュリティ・サーバ・クライアントは、状態が「保存済」、「グローバル・エラー」または「削除中」

であれば削除できる。「登録済」または「登録中」の状態にあるクライアントは、削除する前に登録解除する必要がある（セクション 4.5.1（451-unregistering-a-client）を参照）。
クライアントを削除するためには、次の手順を実行する。

- Configuration メニューで、Security Server Clients を選択する。
- セキュリティ・サーバから削除したいクライアントをテーブルから選択し、その行の Details アイコンをクリックする。
- 開いたウィンドウで、Delete をクリックする。Confirm をクリックして削除を確認する。

5 セキュリティ・トークン、鍵、および証明書

5.1 セキュリティ・トークン、鍵、および証明書の状態

オブジェクト（トークン、鍵または証明書）の可用性を表示するためには、「Keys and Certificates」画面で次の背景色が使用される。

- 黄色 背景 - オブジェクトはセキュリティ・サーバで利用可能であるが、オブジェクトの情報はセキュリティ・サーバの設定に保存されていない。たとえ ば、スマート・カードがサーバに接続されているが、スマート・カードの証明書がサーバにインポートされていないかもしれない。黄色の背景にある証明 書は、メッセージの仲介には使用できない。
- 白 背景 - オブジェクトはセキュリティ・サーバで利用可能であり、オブジェクトの情報はセキュリティ・サーバの設定に保存されている。白い背景の証明書は、メッセージの仲介に使用できる。
- グレー 背景 - オブジェクトはセキュリティ・サーバで利用不可能である。グレーの背景にある証明書は、メッセージの仲介には使用できない。

注意: 鍵デバイスおよび鍵の情報は次のいずれかの時点で自動的に設定に保存される。 - 鍵デバイスおよび鍵に関連する証明書がセキュリティ・サーバにインポートされた場合 - 鍵の CSR が作成される場合
同様に、鍵デバイスおよび鍵の情報は、最後の関連する証明書および/または CSR が削除された後に、セキュリティ・サーバ設定から自動的に削除される。

5.2 証明書の登録状態

登録状態は、証明書の X-Road システムにおける使用可否およびどのように使用できるかを示す。「Keys and Certificates」画面では、「状態」列に証明書の登録状態（「削除済み」を除く）が表示する。

5.2.1 署名用証明書の登録状態

セキュリティ・サーバの署名用証明書は、次の登録状態のいずれかになる。

- **登録済** - 証明書がセキュリティ・サーバにインポートされ、その設定に保存された。「登録済」状態の署名用証明書は、x-road メッセージに署名するために使用できる。
- **削除済** - サーバ設定から証明書が削除された。証明書が「削除済」状態であり、セキュリティ・サーバに接続されているハードウェア・キーデバイスに格納されている場合、証明書は黄色い背景に表示される。

5.2.2 認証用証明書の登録状態

セキュリティ・サーバの認証用証明書は、次の登録状態のいずれかになる。

保存済 - 証明書がセキュリティ・サーバにインポートされ、その設定に保存されたが、登録用に送信されていない。この状態から、証明書は次の状態に遷移する:

- 「登録中」セキュリティ・サーバからセントラル・サーバに認証用証明書の登録リクエストが送信された場合（3.3.1 を参照）。
- 「削除済」セキュリティ・サーバ設定から認証用証明書の情報が削除された場合（5.6 を参照）。

登録進行中 - 認証用証明書の登録リクエストが作成され、セントラル・サーバに送信されたが、証明書とセキュリティ・サーバ間の関連付けはまだ承認されていない。この状態から、証明書は次の状態に遷移する:

- 「登録済み」認証用証明書とセキュリティ・サーバとの間の関連付けが X-Road 監督機関によって承認された場合(3.3 を参照。
- 「削除中」証明書削除リクエストがセントラル・サーバに送信済みの場合(5.6.1 を参照)。ユーザーは、認証用証明書の削除リクエストの送信が失敗した場 合でも、この状態に強制的に遷移できる。

登録済み - 認証用証明書とセキュリティ・サーバの間の関連付けがセントラル・サーバで承認されている。この状態の認証用証明書を使用して、X-Road メッセージを交換するためのセキュアなデータ交換チャネルを確立することができる。この状態から、証明書は次の状態に遷移できる:

- 「グローバル・エラー」認証用証明書とセキュリティ・サーバの間の関連付けがセントラル・サーバで取り消された場合。
- 「削除中」証明書の削除リクエストがセントラル・サーバに送信されている場合(5.6.1 を参照)。ユーザーは、認証用証明書削除リクエストの送信が失敗しても、この状態に遷移することを強制することができる。

グローバル・エラー - 認証用証明書とセキュリティ・サーバの間の関連付けがセントラル・サーバで取り消された場合。この状態から、証明書は次の状態に遷移できる:

- 「登録済」認証用証明書とセキュリティ・サーバの間の関連付けがセントラル・サーバに復元された場合(例えば、クライアントとセキュリティ・サーバの間の関連付けがエラーのために失われた場合)。 -「削除済」セキュリティ・サーバ設定から認証用証明書の情報が削除された場合 (5.6 を参照)。

削除中 - 認証用証明書の登録リクエストが作成され、セントラル・サーバに送信された。この状態から、証明書は次の状態に遷移できる:

- 「削除済」セキュリティ・サーバ設定から認証用証明書の情報が削除された場合(5.6 を参照)。

削除済 - 証明書がセキュリティ・サーバ設定から削除された。

5.3 証明書の有効性状態

有効性状態は、証明書が X-Road システムから独立して使用できるか、またどのように使用できるかを示す。Keys and Certificates 画面では、証明書の有効性状態を OCSP レスポンス欄に表示する。有効性状態(「無効」を除く)は「登録済」状態にある証明書の場合に表示する。
セキュリティ・サーバの証明書は、次のいずれかの有効性状態になる。

- **不明 (有効情報がない)** 証明書に有効な OCSP レスポンスがない(OCSP レスポンス有効期間は X-Road 監督機関によって設定される)または最後の OCSP レスポンスが ”不明”(レスポンダがリクエストされた証明書について知らない)またはエラーだった場合。
- **中断** - 証明書に関する最後の OCSP レスポンスが「中断」された。
- **有効** - 証明書に関する最後の OCSP レスポンスが「有効」でした。「有効」状態の証明書のみを使用して、メッセージに署名し、セキュリティ・サーバの間の接続を確立することができる。
- **期限切れ** - 証明書の有効終了日が過ぎた。証明書はアクティブではなく、この証明書についての OCSP クエリは実行しない。
- **取消済** - 証明書に関する最後の OCSP レスポンスが ”Revoked” だった。証明書はアクティブではなく、この証明書についての OCSP クエリは実行しない。
- **無効** - ユーザーは証明書を無効とマークした。証明書はアクティブではなく、この証明書についての OCSP クエリは実行しない。

5.4 証明書の有効化と無効化

アクセス権
認証用証明書の場合:セキュリティ担当者
署名用証明書の場合:セキュリティ担当者、登録担当者
無効な証明書は、メッセージの署名やセキュリティ・サーバの間のセキュアなチャネルの確立(認

証)には使用できない。証明書が無効になっている場合、「鍵と証明書」テーブルの「OCSP レスポンス」欄のステータスは「無効」である。

証明書を有効または無効にするには、次の手順を実行する。

- Management メニューで、Keys and Certificates を選択する。
- 証明書を有効にするためには、テーブルから無効の証明書を選択し、Activate をクリックする。証明書を無効にするには、テーブルから有効な証明書を選択し、Disable をクリックする。

5.5 認証用鍵と証明書の設定と登録

セキュリティ・サーバは、複数の認証用鍵および証明書を有することができる(例えば、認証用鍵の変更中の場合)。 別の認証用鍵と証明書の設定プロセスは、3.2 で説明する。
認証用証明書の登録プロセスは、[3.3.1] (#331-registering-an-authentication-certificate)にて説明する。

5.6 証明書の削除

X-Road 監督機関で「登録済み」または「登録中」状態にある認証用証明書は、削除する前に登録解除する必要がある。登録解除イベントは、セキュリティ・サーバからセントラル・サーバへの認証用証明書の削除リクエストを送信する。

5.6.1 認証用証明書の登録を解除する

アクセス権: セキュリティ担当者

認証用証明書の登録を解除するには、次の手順を実行する。

- Management メニューで、Keys and Certificates を選択する。
- 「登録済み」または「登録中」の状態の認証用証明書を選択し、Unregister をクリックする。

その後、認証用証明書の削除リクエストが X-Road セントラル・サーバに自動的に送信され、セントラル・サーバではそれを受け取ると、認証用証明書が削除する。リクエストが正常に送信された場合、「リクエスト送信済」というメッセージが表示され、認証用証明書が「削除中」状態に移行する。
登録された認証用証明書は、セキュリティ・サーバを介して削除リクエストを送信することなくても、セントラル・サーバから削除することができる。この場合、セキュリティ・サーバの管理者は、削除する認証用証明書に関する情報を含むリクエストをセントラル・サーバの管理者に送信する必要がある。セキュリティ・サーバからの削除リクエストなしでセントラル・サーバから認証用証明書が削除された場合、その証明書はセキュリティ・サーバで「グローバル・エラー」状態で表示される。

5.6.2 証明書または CSR 通知の削除

アクセス権

認証用証明書の場合: セキュリティ担当者
署名用証明書の場合: セキュリティ担当者、登録担当者

システム設定に保存している認証用証明書は、状態が「保存済み」、「グローバル・エラー」または「削除中」であれば削除できる。署名用証明書および CSR 通知は、常にシステム設定から削除できる。
証明書がハードウェア・セキュリティ・トークンに格納されている場合、削除は 2 つのレベルで動作する:

- 証明書がサーバ設定に保存されている場合、削除は証明書をサーバ設定から削除するが、セキュリティ・トークンからは削除しない。
- 証明書がサーバ設定に保存されていない場合(証明書の背景が黄色の場合)、削除は証明書をセキュリティ・トークンから削除する(トークンがこの動作をサポートしていることが前提)。

証明書または CSR 通知を削除するためには、次の手順を実行する。

- Management メニューで、Keys and Certificates を選択する。
- テーブルから証明書または CSR 通知を選択し、Delete をクリックする。Confirm をクリックして、削除を確認する。
-

5.7 鍵を削除する

警告: サーバ設定から鍵を削除すると、その鍵に関連付けているすべての証明書(および CSR 通知)も削除される。アクセス権

認証用鍵の場合: セキュリティ担当者
署名用鍵の場合: セキュリティ担当者、登録担当者
役割を持たない鍵の場合: セキュリティ担当者、登録担当者

鍵の削除は 2 つのレベルで動作する:

- 鍵がサーバ設定に保存されている場合、削除はサーバ設定から鍵を削除(および関連する証明書)するが、セキュリティ・トークンからは削除しない。
- 鍵がサーバ設定に保存していない場合(鍵の背景が黄色の場合)、削除はセキュリティ・トークンから鍵を削除する(トークンがこの動作をサポートしていることを前提)。

鍵を削除するためには、次の手順を実行する。

- Management メニューで、Keys and Certificates を選択する。
- 鍵を選択し、Delete をクリックする。Confirm をクリックし、鍵(および関連する証明書)の削除を確認する。
-

6 X-Road サービス

サービスは 2 つのレベルで管理される。

- サービスの追加、削除、および無効化は WSDL レベルで実行する。
- サービスアドレス、内部ネットワーク接続方法、およびサービスタイムアウト値は、サービスレベルで設定される。ただし、一つのサービスの設定を同じ WSDL 内の他のすべてのサービスに簡単に拡張できる。

6.1 WSDL を追加する

アクセス権: サービス管理者

新しい WSDL ファイルが追加されると、セキュリティ・サーバはそこからサービス情報を読み取り、その情報をサービス一覧に表示する。サービス・コード、タイトル、アドレスは WSDL から読み込まれる。

WSDL を追加するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、テーブルからクライアントを選択し、その行の Services アイコンをクリックする。
- Add WSDL をクリックし、開いたウィンドウに WSDL アドレスを入力して、OK をクリックする。WSDL とそれに含まれるサービスに関する情報が一覧に追加される。デフォルトでは、WSDL は無効状態で追加される(6.3)。

WSDL に含まれるサービスの一覧を表示するには

- WSDL 行の前にある+記号をクリックして、リストを展開する。

6.2 WSDL の更新

アクセス権: サービス管理者

更新後、セキュリティ・サーバは WSDL ファイルを WSDL アドレスからセキュリティ・サーバに再読み込みし、再読み込みされたファイルのサービス情報を既存のサービスと照合してチェックする。新しい WSDL のサービスの構成に現在のバージョンと比較して変更があれば、警告が表示され、更新を続けるかキャンセルするかを選択する。

WSDL を更新するには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からクライア

ントを選択し、その行の Services アイコンをクリックする。
- 更新したい WSDL を一覧から選択し、Refresh をクリックする。
- 新しい WSDL に、セキュリティ・サーバの現行の WSDL と比較して、変更がある場合、警告が表示される。更新を続行するためには、Continue をクリックする。

WSDL を更新される際、既存のサービスの設定は上書きされない。

6.3 WSDL の有効化と無効化

アクセス権: サービス管理者

無効な WSDL はサービス一覧に赤で表示され、「Disabled」の注記が表示される。
無効な WSDL で記述されたサービスはサービス・クライアントからアクセスできない。そのようなサービスにアクセスしようとすると、セキュリティ・サーバの管理者が WSDL を無効化した時に入力した情報を含むエラー・メッセージが返信される。
WSDL が有効化されると、そこに記述されているサービスにはユーザーがアクセスできるようになる。したがって、WSDL を有効にする前に、すべてのサービスのパラメータが正しく設定されているかを確認する必要がある(6.6 を参照)。
WSDL を有効化するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からクライアントを選択し、その行の Services アイコンをクリックする。
- 一覧から無効な WSDL を選択し、Enable をクリックする。

WSDL を無効化するためには、以下の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からクライアントを選択し、その行の Services アイコンをクリックする。
- WSDL を無効化するためには、一覧から有効な WSDL を選択し、Disable をクリックする。
- 開いたウィンドウで、エラー・メッセージを入力する。そのエラー・メッセージは、WSDL のサービスにアクセスしようとするクライアントに表示される。最後に OK をクリックする。

6.4 WSDL のアドレスの変更

アクセス権: サービス管理者

WSDL アドレスを変更するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からクライアントを選択し、その行の Services アイコンをクリックする。
- 一覧から、アドレスを変更したい WSDL を選択し、Edit をクリックする。
- 開いたウィンドウで、WSDL アドレスを編集して OK をクリックする。アドレスを変更すると、WSDL は更新される(6.2 を参照)。

6.5 WSDL の削除

アクセス権: サービス管理者

WSDL が削除されると、アクセス権を含めて WSDL に記述されているサービスに関連するすべての情報が削除される。WSDL を削除するには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からクライアントを選択し、その行の Services アイコンをクリックする。
- 削除したい WSDL を一覧から選択し、Delete をクリックする。
- 開いたウィンドウで Confirm をクリックして削除を確認する。

6.6 サービス・パラメータの変更

アクセス権: サービス管理者

サービス・パラメータは
「サービス URL」 - サービスを対象とするリクエストを送信する URL。
「タイムアウト」 - データベースへのリクエストの最長時間(秒単位)。

「TLS 証明書の確認」 - TLS 接続が確立された時に、証明書の検証の有無をトグルする。

サービス・パラメータを変更するには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からクライアントを選択し、その行の Services アイコンをクリックする。
- 一覧からサービスを選択し、Edit をクリックする。
- 開いたウィンドウで、サービス・パラメータを設定する。選択したパラメータを同じ WSDL に記述されているすべてのサービスに適用するためには、Apply to All in WSDL 欄で、このパラメータの横にあるチェックボックスを選択する。設定したパラメータを適用するには、OK をクリックする。

7 アクセス権

アクセス権は、以下のアクセス権の対象に付与することができる。

- X-Road メンバーのサブシステム
- グローバル・アクセス権グループ - グローバル・グループは、X-Road 監督機関で作成される。グループにアクセス権が付与されている場合は、そのすべてのグループ・メンバーにも適用される。
- ローカル・アクセス権グループ - アクセス管理を簡素化するために、セキュリティ・サーバの各クライアントはローカル・アクセス権グループを作成できる(セクション 8 を参照)。グループにアクセス権が付与されている場合は、そのすべてのグループ・メンバーにも適用される。

セキュリティ・サーバのアクセス権を管理するには、2 つのオプションがある。

- サービスベース・アクセス権管理 - 複数のサービス・クライアントに対して単一のサービスを公開/非公開する必要がある場合(7.1 を参照)。サービス・クライアント・ベース・アクセス権管理 - 単一のクライアントが複数のサービスを公開/非公開する必要がある場合(7.2 を参照)。
-

7.1 サービスのアクセス権の変更

アクセス権: サービス管理者

サービスのアクセス権を変更するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からクライアントを選択し、その行の Services アイコンをクリックする。
- 一覧からサービスを選択し、Access Rights をクリックする。
- 開いたウィンドウで、アクセス権一覧には、選択したサービスにアクセスできるすべての X-Road サブシステムおよびグループに関する情報が表示される。
- サブジェクト(X-Road サブシステムまたはグループ)にサービスのアクセス権を追加するためには、Add Subject をクリックする。サブジェクト検索ウィンドウが表示される。X-Road の監督機関に登録されているすべてのサブシステムとグローバル・グループ、およびセキュリティ・サーバ・クライアントのローカル・グループの中から検索できる。
- 一覧から 1 つまたは複数のサブジェクトを選択し、Add Selected to ACL**をクリックする。検索結果のすべてのサブジェクトにアクセス権を付与するには、Add All to ACL*をクリックする。
- アクセス権のサブジェクトを削除するには、アクセス権一覧の対応する行を選択して、Remove Selected をクリックする。アクセス権リストをクリアする(つまり、すべてのサブジェクトを削除する)ためには、Remove All をクリックする。
-

7.2 サービス・クライアントの追加

アクセス権: サービス管理者

サービスクライアント画面(Configuration -> Security Server Clients -> Service Clients)は、このセキュリティ・サーバ・クライアントによって媒介されるサービスのすべてのアクセス権サブジェクトを表示する。つまり、X-Road サブシステムまたはグループにこのクライアントのサービスへのアクセス権が付与されている場合、この画面にサブジェクトが表示される。

サービス・クライアントを追加するには、次の手順を実行する。

- Configuration メニューで、Security Server Clients を選択する。
- 一覧からクライアントを選択し、Service Clients アイコンをクリックし、次に、Add をクリ

ックする。

- 開いたウィンドウで、アクセス権を付与したいサブジェクト(サブシステム、ローカルまたはグローバル・グループ)を見つけて選択し、Next をクリックする。
- 選択したサブジェクトにアクセス権を付与したいサービスを探す。Add Selected to ACL をクリックして、選択したサービスへのアクセス権をこのサブジェクトに付与する。Add All to ACL をクリックして、フィルタ内のすべてのサービスに対するアクセス権をサブジェクトに付与する。

サブジェクトがサービス・クライアントのリストに追加した後に、アクセス権を変更できるクライアント・アクセス権ビューが表示される。

7.3 サービス・クライアントのアクセス権の変更

アクセス権: サービス管理者

サービス・クライアントのアクセス権を変更するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からクライアントを選択し、その行の Service Clients アイコンをクリックする。
- 開いたウィンドウで、アクセス権を変更したいサブジェクト(サブシステム、ローカルまたはグローバル・グループ)を見つけて選択し、Access Rights をクリックする。
- 開いたウィンドウに、選択したサブジェクトに対してセキュリティ・サーバでオープンであるサービスのリストが表示される。
- サービス・クライアントからアクセス権を削除するためには、一覧から 1 つまたは複数のサービスを選択し、Remove Selected をクリックし、次に、Confirm をクリックする。
- サービス・クライアントからすべてのアクセス権を削除するためには、Remove All をクリックし、次に Confirm をクリックする。
- サービス・クライアントにアクセス権を追加するには、まず Add Service をクリックする。開いたウィンドウで、サブジェクトに付与したいサービスを選択する(既に付与されているサービスはグレーで表示される)。Add Selected to ACL をクリックする。検索で見つかったサービスをすべて追加するには、Add All to ACL をクリックする。

注意: ページを更新すると、サービスへアクセス権を持たないすべてのサービス・クライアントがサービス・クライアントの画面から削除される。

8 ローカル・アクセス権グループ

同じサービスを使用する X-Road サブシステム・グループに対するサービス・アクセス権の管理を容易にするために、セキュリティ・サーバ・クライアント用ローカル・アクセス権グループを作成することができる。グループに付与されたアクセス権は、グループのすべてのメンバーに適用される。ローカル・グループはクライアント・ベースである。つまり、ローカル・グループは、一台のセキュリティ・サーバの一つのクライアントのサービス・アクセス権を管理するためにのみ使用できる。

8.1 ローカル・グループを追加する

アクセス権: サービス管理者

セキュリティ・サーバ・クライアントのローカル・グループを作成するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、クライアントを選択して、その行のローカル・グループアイコンをクリックする。開いたウィンドウに、クライアントのローカル・グループのリストが表示される。
- 新しいグループを作成するためには、Add Group をクリックする。開いたウィンドウで、新しいグループのコードと説明を入力し、OK をクリックする。
-

8.2 ローカル・グループのメンバーの表示と変更

アクセス権: サービス管理者

ローカル・グループのメンバーを表示するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、クライアントを選択し

て、その行の Local Groups アイコンをクリックする。

- 開いたウィンドウで、メンバーを表示または変更したいグループを選択し、Details をクリックして詳細画面を開く。

一つ以上のメンバーをローカル・グループに追加するためには、グループの詳細画面で次の手順を実行する。

- Add Members をクリックする。
- 開いたウィンドウで、グループに追加したいサブシステムを探して、選択し、Add Selected to Group をクリックする。検索機能で発見したすべてのサブシステムをグループに追加するためには、Add All to Group をクリックする。
- ローカル・グループからメンバーを削除するためには、グループの詳細画面で削除したいメンバーを選択し、Remove Selected Members をクリックする。グループからすべてのグループ・メンバーを削除するためには、Remove All Members をクリックする。

8.3 ローカル・グループの説明を変更する

アクセス権: サービス管理者

ローカル・グループの説明を変更するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からクライアントを選択して、その行の Local Groups アイコンをクリックする。
- ローカル・グループ・一覧からグループを選択し、Details をクリックする。
- グループ詳細画面で、Edit をクリックして、説明を変更する。
- グループの説明を入力し、OK をクリックする。

8.4 ローカル・グループの削除

アクセス権: サービス管理者

警告: ローカル・グループを削除すると、グループ・メンバーシップを通じて付与されたすべてのグループ・メンバー・アクセス権が取り消される。ローカル・グループを削除するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からクライアントを選択して、その行の Local Groups アイコンをクリックする。
- ローカル・グループ・一覧からグループを選択し、Details をクリックする。
- グループ詳細画面で、Delete Group をクリックし、開いたウィンドウで Confirm をクリックして、削除を確認する。
-

9 クライアント情報システムとの通信

アクセス権: 登録担当者、サービス管理者

セキュリティ・サーバは、HTTP、HTTPS、または HTTPS NOAUTH プロトコルのいずれかを通じて、サービスを提供および使用する情報システム・サーバと通信できる。

- 情報システム・サーバとセキュリティ・サーバが他のコンピューターが接続されていないプライベート・ネットワーク・セグメントを介して通信する場合 は、HTTP プロトコルを使用するべきである。さらに、情報システム・サーバは対話的ログインを許可してはならない。
- 情報システム・サーバとセキュリティ・サーバの間の通信に専用のネットワーク・セグメントを用意できない場合は、HTTPS プロトコルを使用するべきがある。その場合、盗聴および傍受の可能性から通信を保護するために暗号方式が使用される。HTTPS を使用する前には、情報システム・サーバに対して内部 TLS 証明書を作成し、セキュリティ・サーバにロードする必要がある。
- セキュリティ・サーバによって情報システムの TLS 証明書の検証をスキップしたい場合は、HTTPS NOAUTH プロトコルを使用する。

注: HTTP が選択されているが、情報システムが HTTPS 上でセキュリティ・サーバに接続する場合、接続は承認されるが、クライアントの内部 TLS 証明書は検証されない(HTTPS NOAUTH と同じ動作)。

デフォルトでは、セキュリティ・サーバ・クライアントが、セキュリティ・サーバ所有者として運用モニタリン

グ・データのリクエストを防止するために、セキュリティ・サーバの所有者の接続タイプは HTTPS に設定されている。

サービス・コンシューマーの内部ネットワーク・サーバの接続方法を設定するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からセキュリティ・サーバの所有者またはクライアントを選択し、その行の Internal Servers アイコンをクリックする。
- Connection Type のドロップ・ダウンで接続方法を選択し、Save をクリックする。

設定された接続方法により、情報システムのリクエスト URL は http://SECURITYSERVER/ または https://SECURITYSERVER/ である。リクエストをする際には、SECURITYSERVER というアドレスをセキュリティ・サーバの実際のアドレスに置き換える必要がある。

サービス・プロバイダの内部ネットワーク・サーバの接続方法は、URL によって決定される。接続方法を変更するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からクライアントを選択し、その行の Services アイコンをクリックする。
- 一覧からサービスを選択し、Edit をクリックする。
- サービス URL のプロトコルを HTTP または HTTPS に変更する。
- HTTPS プロトコルが選択されている場合、必要に応じて Verify TLS certificate のチェックボックスを選択する（6.6 を参照）。サービス・パラメータにより、内部ネットワーク・サーバとの接続は、次のプロトコルのいずれかを使用して作成される。
- HTTP - サービス/アダプタの URL は http://... で始まる。
- HTTPS - サービス/アダプタの URL は https://... で始まり、Verify TLS certificate チェックボックスが選択されている。
- HTTPS NOAUTH - サービス/アダプタの URL は https:// で始まり、Verify TLS certificate チェックボックスは選択されていない。

セキュリティ・サーバ所有者またはセキュリティ・サーバ・クライアントが HTTPS 接続できるように、内部 TLS 証明書を追加するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からセキュリティ・サーバの所有者またはクライアントを選択し、その行の Internal Servers アイコンをクリックする。
- 証明書を追加するには、Internal TLS Certificates セクションで、Add をクリックし、ローカル・ファイル・システムから証明書ファイルを選択して、OK をクリックする。証明書フィンガープリントが「内部 TLS 証明書」一覧に表示される。

内部 TLS 証明書の詳細情報を表示するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からセキュリティ・サーバの所有者またはクライアントを選択し、その行の Internal Servers アイコンをクリックする。
- 「Internal TLS Certificates」一覧から証明書を選択し、Details をクリックする。

内部 TLS 証明書を削除するためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からセキュリティ・サーバの所有者またはクライアントを選択し、その行の Internal Servers アイコンをクリックする。
- 「Internal TLS Certificates」 一覧から証明書を選択し、Delete をクリックする。
- 開いたウィンドウで Confirm をクリックし、削除を確認する。

セキュリティ・サーバの内部 TLS 証明書をエクスポートするためには、次の手順を実行する。

- Configuration メニューで Security Server Clients を選択し、一覧からセキュリティ・サーバの所有者またはクライアントを選択し、その行の Internal Servers アイコンをクリックする。
- Export をクリックし、ファイルをローカル・ファイル・システムに保存する。

10 システム・パラメータ

セキュリティ・サーバのシステム・パラメータは次のとおりである。

- コンフィギュレーション・アンカーの情報コンフィギュレーション・アンカーは、セントラル・サーバから署名された設定を定期的にダウンロードするため、およびダウンロードされた設定の署名を検証するためのデータを含む。
- タイムスタンプ・サービス情報 タイムスタンプは、X-Road を介して交換されるメッセージの証拠能力を担保するために使用される。
- 内部 TLS 鍵と証明書内部 TLS 証明書は、クライアントのサーバに対して HTTPS 接続が選択されている場合、セキュリティ・サーバ・クライアントの情報シ ステムとの TLS 接続を確立するために使用される。
-

10.1 コンフィギュレーション・アンカーの管理

アクセス権

コンフィギュレーション・アンカーのアップロード: セキュリティ担当者

コンフィギュレーション・アンカーのダウンロード: セキュリティ管理者、システム管理者

コンフィギュレーション・アンカーをアップロードするためには、次の手順を実行する。

- Configuration メニューで、System Parameters を選択する。システム・パラメータ画面が開く。
- Configuration Anchor セクションで、Upload をクリックする。
- ローカル・ファイル・システムからアンカー・ファイルを探し、Upload をクリックする。
- アップロードされたアンカー・ファイルのハッシュ値と、X-Road 監督機関によって発行された現在有効なアンカーのハッシュ値を比較することによって、アップロードしているアンカー・ファイルの有効性を確認する。ハッシュ値が一致する場合は、Confirm をクリックし、アップロードを確認する。

コンフィギュレーション・アンカーをダウンロードするためには、次の手順を実行する。

- Configuration メニューで、System Parameters を選択する。システム・パラメータ画面が開く。
- Configuration Anchor セクションで、Download をクリックし、ファイルを保存する。

10.2 タイムスタンプ・サービスの管理

アクセス権: セキュリティ担当者

タイムスタンプ・サービスを追加するためには、次の手順を実行する。

- Configuration メニューで、System Parameters を選択する。システム・パラメータ画面が開く。
- Timestamping Services セクションで、Add をクリックする。
- 開いたウィンドウで、サービスを選択し、OK をクリックする。

タイムスタンプ・サービスを削除するためには、次の手順を実行する。

- Configuration メニューで、System Parameters を選択する。システム・パラメータ画面が開く。
- Timestamping Services セクションで、削除するサービスを選択し、Delete をクリックする。

注: 複数のタイムスタンプ・サービスが設定されている場合、セキュリティ・サーバは、一覧の最上位のサービスからタイムスタンプを取得しようとする。それに失敗した場合は、次のサービスに移動する。

10.3 内部 TLS 鍵と証明書の変更

アクセス権: セキュリティ担当者、システム管理者

セキュリティ・サーバの内部 TLS 鍵と証明書を変更するためには、次の手順を実行する。

- Configuration メニューで、System Parameters を選択する。システム・パラメータ画面が開く。
- Internal TLS Certificate セクションで、Generate New TLS Key をクリック

し、開いたウィンドウで Confirm をクリックする。

セキュリティ・サーバは、クライアント情報システムとの通信に使用する鍵および自己署名証明書を作成する。セキュリティ・サーバの証明書フィンガープリントも変更する。セキュリティ・サーバのドメイン名は、証明書の Common Name フィールドに、内部 IP アドレスは subjectAltName 拡張フィールドに保存される。

新しい証明書リクエストを作成するためには、次の手順を実行する。

- Configuration メニューで、System Parameters を選択する。システム・パラメータ画面が開く。
- Internal TLS Certificate セクションで、Generate Certificate Request をクリックし、識別名を入力し、証明書リクエスト・ファイルをローカル・ファイル・システムに保存する。

セキュリティ・サーバは、現在の鍵および提供された識別名を使用して証明書リクエストを作成する。

新しい TLS 証明書をインポートするためには、次の手順を実行する。

- Configuration メニューで、System Parameters を選択する。システム・パラメータ画面が開く。
- Internal TLS Certificate セクションで、Import Certificate をクリックし、インポートするファイルを指定する。

インポートする証明書は、PEM 形式でなければならない。新しい TLS 証明書をインポートすると、xroad-proxy は再起動し、セキュリティ・サーバからのサービスの提供に影響を与えることにご注意ください。

セキュリティ・サーバの内部 TLS 証明書をエクスポートするためには、次の手順を実行する。

- Configuration メニューで、System Parameters を選択する。システム・パラメータ画面が開く。
- Internal TLS Certificate セクションで、Export をクリックし、ファイルをローカル・ファイル・システムに保存する。

セキュリティ・サーバの内部 TLS 証明書の詳細情報を表示するには、次の手順を実行する。

- Configuration メニューで、System Parameters を選択する。システム・パラメータ画面が開く。
- Internal TLS Certificate セクションで、Certificate Details をクリックする。

11 メッセージ・ログ

メッセージ・ログの目的は、第三者へ通常のリクエストとレスポンス・メッセージの受信を証明する手段を提供することにある。セキュリティ・サーバの間で交換されるメッセージは署名され、暗号化される。全通常リクエストとレスポンス毎に、セキュリティ・サーバは署名とタイムスタンプ済の完全なドキュメント(Associated Signature Container [ASiC])を作成する。

メッセージ・ログ・データは、メッセージ交換中にセキュリティ・サーバのデータベースに格納される。設定(11.1 を参照)により、交換されたメッセージの署名のタイムスタンプ発行は、メッセージ交換プロセスと同期的に行われるか、あるいは X-Road 監督機関によって設定された期間内に非同期に行われる。

同期的にタイムスタンプを行う場合、タイムスタンプ発行はメッセージ交換プロセスの不可欠な部分である(リクエストに対して 1 つのタイムスタンプが発行され、レスポンスにも 1 つのタイムスタンプが発行される)。タイムスタンプの発行が失敗すると、メッセージ交換も失敗し、セキュリティ・サーバはエラー・メッセージでレスポンスする。

非同期にタイムスタンプを行う場合、前回の定期的なタイムスタンプ発行以降のすべての(最大値は設定で決定される 11.1 を参照)メッセージ・ログは単一のタイムスタンプ(バッチ)が発行される。デフォルトでは、セキュリティ・サーバはパフォーマンスと可用性を高めるために非同期タイムスタンプを使用する。

セキュリティ・サーバは、メッセージ・ログ・データから定期的に署名付き（およびタイムスタンプ付き）ドキュメントを作成し、それらをローカル・ファイル・システムにアーカイブする。アーカイブ・ファイルは、1 つ以上の署名付きドキュメントと、追加の完全性検証のための連携情報ファイルを含む ZIP コンテナである。

11.1 メッセージ・ログの設定の変更

コンフィギュレーシ・パラメータは、INI ファイル¥　[INI]に定義されている。各セクションは、特定のセキュリティ・サーバ・コンポーネントのパラメータを含む。デフォルトのメッセージ・ログ・設定は、ファイルにある。

/etc/xroad/conf.d/addons/message-log.ini

デフォルト値をオーバーライドするためには、以下のファイルを作成または編集する

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

ファイルに[message-log] セクションを作成する（存在しない場合）。セクションの開始点の下に、パラメータ値を 1 行に 1 つずつリストする。例えば、archive-path と archive-max-filesize を設定するためには、以下の行を設定・ファイルに追加する必要がある:

```
[message-log]
archive-path=/my/arhcive/path/
archive-max-filesize=67108864
```

11.1.1 共通パラメータ

- hash-algo-id　-　メッセージ・ログのハッシュに使用されるハッシュ・アルゴリズムである。SHA-256、SHA-384、SHA-512 を選択できる。デフォルトは SHA-512 である。
-

11.1.2 タイムスタンプ・パラメータ

- timestamp-immediately　-　true に設定する場合、タイムスタンプ発行はメッセージ交換と同期的に行われる。つまり、リクエストに対して 1 つのタイムスタンプが発行され、レスポンスに対してもう 1 つ発行される。これは、メッセージのロギング中にタイムスタンプを保証するためのセキュリティ・ポリシーであるが、タイムスタンプが失敗すれば、メッセージ交換も失敗し、セキュリティ・サーバへの負荷が増加するとともに、タイムスタンプ・サービスへの負荷も増加する。デフォルトでは、パフォーマンスと可用性を向上させるために、このパラメータ値は false になっている。パラメータ値が false になっている場合、タイムスタンプは定期的なバックグラウンド・プロセスとして行われる（期間は X-Road 監督機関によって決定され、グローバル・コンフィギュレーションを介してセキュリティ・サーバに伝播される）。決定された期間内に保存された署名に（parameter timestamp-records-limit を参照）は、1 つのバッチでタイムスタンプが発行される。
- timestamp-records-limit -　一つのバッチでタイムスタンプできる署名されたメッセージの最大数である。このパラメータのデフォルト値を変更するときは、メッセージ交換負荷（1 分あたりのメッセージ数）とセキュリティ・サーバのタイムスタンプ間隔を考慮する必要がある。正当な理由がなければ、このパラメータを変更しないでください。デフォルトは 10000 である。
- acceptable-timestamp-failure-period -　セキュリティ・サーバ間のメッセージ交換が停止する前に、非同期的タイムスタンプの失敗が許可される時間を秒単位で示す。このチェックを無効にするためには 0 に設定する。デフォルトは 14400 である。

11.1.3 パラメータ・アーカイブ

- keep-records-for - タイムスタンプとアーカイブされたレコードをデータベースに保存する日数である。デフォルトは 30 である。
- archive-max-filesize -　アーカイブ・ファイルの最大バイトサイズである。最大値に達すると、ファイルのローテーションがトリガーされる。デフォルトは 33554432（32

MB)である。

- archive-interval - タイムスタンプ付きレコードをアーカイブするための Cron 式[CRON]としての時間間隔である。デフォルトは 0 0 0/6 1/1 *? *
- (6 時間ごとにアーカイブする)。
- archive-path - タイムスタンプ付きログ・レコードがアーカイブされるディレクトリである。デフォルトは /var/lib/xroad/ である。
- clean-interval - データベースからアーカイブされたレコードをクリーニングするための Cron 式[CRON]としての時間間隔。デフォルトは 0 0 0/12 1/1 *? * (12 時間ごとにクリーニングする)である。
- archive-transfer-command - (定期的な)アーカイブ処理の後に実行されるコマンドである。この設定を使用して、セキュリティ・サーバからアーカイブ・ファイルを自動的に転送するための外部スクリプトを設定することができる。デフォルトでは動作なしである。

11.2 セキュリティ・サーバからのアーカイブ・ファイルの転送

ハードディスクの空き容量を節約するために、定期的にアーカイブ・ファイルをセキュリティ・サーバから(手動または自動で)外部のロケーションに転送することを推奨する。

アーカイブ・ファイル(ZIP コンテナー)は、設定・パラメーター archive-path で指定されたディレクトリにある。ファイル名は mlog-XYZ.zip の形式である。X は最初のメッセージ・ログ・レコードのタイムスタンプ(UTC time in the format YYYYMMDDHHmmss)、Y は最後のメッセージ・ログ・レコードのタイムスタンプ 、Z は 10 文字の長さの英数字のランダムである。次はアーカイブ・ファイル名の実例である。

mlog-20150504152559-20150504152559-a7JS05XAJC.zip

メッセージ・ログ・パッケージは、アーカイブ・ファイルを転送するためのヘルパース・クリプト /usr/share/xroad/scripts/archive-http-transporter.sh を提供する。このスクリプトはアーカイブ・ファイルをアーカイブ・サーバへ転送するために HTTP / HTTPS プロトコル(POST 方法、フォーム名はファイル)を使用する。

スクリプトの使用法:

```
Options:      | 説 明
-d, --dir DIR | アーカイブ・ディレクトリ。デフォルトは /var/lib/xroad
-r, --remove  | 正常にアーカイブ・ディレクトリから移動したファイルを削除する
-k, --key KEY| PEM 形式の秘密鍵ファイル名。TLS 用。デフォルトは /etc/xroad/ssl/internal.key
-c, --cert CERT | PEM 形式のクライアント証明書ファイル。TLS 用。デフォルトは /etc/xroad/ssl/internal.crt
-cacert FILE | ピアを確認するための CA 証明書ファイル。TLS 用。このファイルは複数の CA 証明書を含む場合がある 証明書は PEM 形式でなければならない。
-h, --help    | このヘルプテキスト。
```

アーカイブ・サーバが HTTP ステータスコード 200 を返すと、アーカイブ・ファイルは正常に転送されている。

転送スクリプトを設定するためには、設定・パラメータの archive-transfer-command をオーバーライドする(/etc/xroad/conf.d/local.ini ファイルを作成または編集する)。例えば:

```
[message-log]
archive-transfer-command=/usr/share/xroad/scripts/archive-http-transporter.sh -r http://my-archiving-server/cgi-bin/upload
```

メッセージ・ログ・パッケージには、テストおよび開発するためにデモ・アーカイブ・サーバー用 CGI スクリプト /usr/share/doc/xroad-addon-messagelog/archive-server/demo-upload.pl を含む。

11.3 リモート・データベースの使用

メッセージ・ログ・データベースは、セキュリティ・サーバの外部に置くことができる。次のガイドでは、メッセージ・ログのためにリモート・データベース・スキーマを設定および作成する方法について説明する。セキュリティ・サーバからデータベースへのアクセスが設定されていることが前提されている。データベース接続の設定の詳細については、[JDBC]を参照してください。

- リモート・データベース・ホストにデータベース・ユーザーを作成する。

postgres@db_host:~$ createuser -P messagelog_user Enter password for new role: <messagelog_password> Enter it again: <messagelog_password>

- リモート・データベース・ホストでメッセージ・ログ・ユーザーが所有するデータベースを作成する。
  postgres@db_host:~$ createdb messagelog_dbname -O messagelog_user -E UTF-8
- セキュリティ・サーバからリモート・データベースへの接続を確認する。
  user@security_server:~$ psql -h db_host -U messagelog_user messagelog_dbname Password for user messagelog_user: <messagelog_password>
  psql (9.3.9)
  SSL connection (cipher: DHE-RSA-AES256-GCM-SHA384, bits: 256) Type "help" for help.
  messagelog_dbname=>
- 設定のために xroad-proxy サービスを停止する:
  root@security_server:~ # service xroad-proxy stop
- /etc/xroad/db.properties で、暗号化された接続を実現するためにデータベース接続パラメータを設定する:

```
messagelog.hibernate.jdbc.use_streams_for_binary = true
messagelog.hibernate.dialect =
ee.ria.xroad.common.db.CustomPostgreSQLDialect
messagelog.hibernate.connection.driver_class =
org.postgresql.Driver
messagelog.hibernate.connection.url =
jdbc:postgresql://db_host:5432/messagelog_dbname?
ssl=true&sslfactory=org.postgresql.ssl.NonValidatingFactory
messagelog.hibernate.connection.username = messagelog_user
messagelog.hibernate.connection.password =
messagelog_password
```

- メッセージ・ログ・アドオン・パッケージの再インストールによってデータベース・スキーマを作成する(xroad-proxy サービスも開始する)。
  root@security_server:~ # apt-get install --reinstall xroad-addon-messagelog

12 監査ログ

セキュリティ・サーバは監査ログを保持する。監査ログ・イベントは、ユーザーがシステムの状態または設定を変更する時にユーザー・インターフェイスによって作成される。ユーザーのアクションは、結果が成功か失敗かに関係なく記録される。監査ログ・イベントの完全なリストは、[SPEC-AL]に記述されている。

ユーザー・インターフェイスを介して実行されていないシステム状態や設定を変更するアクションはログに記録されていない(たとえば、X-Road ソフトウェアのインストレーションとアップグレード、ユーザーの作成とアクセス権の付与、設定・ファイルの変更など)。

監査ログ・レコードは以下を含む。

- ユーザーアクションの説明
- イベントの日時
- アクションを実行しているユーザーのユーザー名
- イベントに関連するデータ

たとえば、新しいクライアントをセキュリティ・サーバに登録すると、次のログ・レコードが作成される。

2015-07-03T10:21:59+03:00 my-security-server-host INFO [X-Road Proxy UI] 2015-07-03 10:21:59+0300 - {"event":"Register client", "user":"admin1",

”data”:{”clientIdentifier”:{”xRoadInstance”:”EE”, ”memberClass”:”COM”, ”memberCode”:”member1”}, ”clientStatus”:”registration in progress”}}

イベントは、マシンの処理能力を確保するために、JSON [JSON]形式で表示される。イベントフィールドは、イベントの説明を表し、ユーザーフィールドは、実行者のユーザー名を表し、データフィールドは、イベントに関連するデータを表す。失敗したアクション・イベント・レコードは、追加としてエラー・メッセージの理由のフィールドを含む。例えば:

2015-07-03T11:55:39+03:00 my-security-server-host INFO [X-Road Proxy UI] 2015-07-03 11:55:39+0300 - {”event”:”Log in to token failed”, ”user”:”admin1”, ”reason”:”PIN incorrect”, ”data”:{”tokenId”:”0”, ”tokenSerialNumber”:null, ”tokenFriendlyName”:”softToken-0”}}

デフォルトでは、監査ログはファイルにある
/var/log/xroad/audit.log

12.1 監査ログの設定の変更

X-Road ソフトウェアは、UDP インターフェイス（デフォルト・ポートは 514）を使用して監査ログを syslog （rsyslog）に書き込む。該当する設定は以下のファイルにある。
/etc/rsyslog.d/90-udp.conf

監査ログ・レコードは、レベル INFO およびファシリティ LOCAL0 で書き込まれる。デフォルトでは、そのレベルとファシリティのログ・レコードは X-Road 監査ログ・ファイルに保存される
/var/log/xroad/audit.log

デフォルトの動作は、rsyslog 設定・ファイルを編集することで変更できる
/etc/rsyslog.d/40-xroad.conf

設定・ファイルの変更を追加するために rsyslog サービスを再起動してください
restart rsyslog

監査ログは、logrotate によって毎月ローテーションされる。監査ログのローテーションを設定するためには、logrotate 設定・ファイルを編集する
/etc/logrotate.d/xroad-proxy

12.2 監査ログのアーカイブ

ハードディスク・スペースを節約し、セキュリティ・サーバのクラッシュ中に、監査ログ・レコードが失われないようにするためには、監査ログ・ファイルを定期的に外部ストレージまたはログ・サーバーにアーカイブすることを推奨する。
X-Road ソフトウェアは、監査ログをアーカイブするために特別なツールを提供しない。
rsyslog は、監査ログを外部ロケーションにリダイレクトするように設定できる。

13 バックアップとリストア

13.1 ユーザー・インターフェイスでのバックアップとリストア

アクセス権: システム管理者

バックアップとリストアの表示は、Managment メニューから Back Up and Restore を選択してアクセスできる。
設定のバックアップをするためには、次の手順を実行する。

- Back Up Configuration をクリックする。
- 開いたウィンドウが、バックアップ・スクリプトのアウトプットを表示する。OK をクリックして閉じる。設定・バックアップ・ファイルが設定・バックアップ・ファイルのリストに表示される。
- 設定・バックアップ・ファイルをローカル・ファイル・システムに保存するためには、設定・ファイ

ルの行で Download をクリックし、ファイルを保存する。
設定をリストアするためには、次の手順を実行する。

- 設定・バックアップ・ファイルのリストの該当する行で Restore をクリックし、Confirm をクリックする。
- リストア・スクリプトのアウトプットを表示するウィンドウが開く。OK をクリックして閉じる。

設定・バックアップ・ファイルを削除するためには、設定・バックアップ・ファイルリストの該当する行で Delete をクリックし、Confirm をクリックする。
設定・ファイルをローカル・ファイル・システムからセキュリティ・サーバにアップロードするためには、Upload Backup File をクリックし、ファイルを選択して、OK をクリックする。アップロードされた設定・ファイルが設定・ファイルのリストに表示される。

13.2 コマンド・ラインからのリストア

コマンド・ラインから設定をリストアするには、次のデータが必要がある。

- セキュリティ・サーバの X-Road ID

レストア・コマンドは xroad ユーザーによって実行する。
設定をリストアするためには、次のコマンドを使用する必要がある。

```
/usr/share/xroad/scripts/restore_xroad_proxy_configuration.sh -s
<security server ID> -f <path + filename>
```

例えば（以下は一行で):

```
/usr/share/xroad/scripts/restore_xroad_proxy_configuration.sh ¥

-s AA/GOV/TS1OWNER/TS1 ¥
-f /var/lib/xroad/backup/conf_backup_20140703-110438.tar
```

別のセキュリティ・サーバによって作成されたバックアップからシステムをリストアすることが絶対に必要である場合は、F オプションによってリストア・コマンドの強制モードが使用できる。たとえば(すべて 1 行で):

```
/usr/share/xroad/scripts/restore_xroad_proxy_configuration.sh ¥
-F -f /var/lib/xroad/backup/conf_backup_20140703-110438.tar
```

14 診断

14.1 セキュリティ・サーバ・サービスの状態情報を調べる

アクセス権: システム管理者

Management メニューを開き、Diagnostics を選択する。
このページでは、次のサービスのステータスを調べることができる。

Service	Status	Message	Previous Update	Next Update
Global configuration	Green/yellow/red	Status message	The time of the global configuration client's last run	The estimated time of the global configuration client's next run
Timestamping	Green/yellow/red	Status message	The time of the last timestamping operation	Not used
OCSP-responders	Green/yellow/red	Status message	The time of the last contact with the OCSP-responder	The latest possible time for the next OCSP-refresh

サービス・ステータスを更新するためには、Management メニューの Diagnostics アイテムをクリックする。
ステータスの色は次のことを示す。

赤色の表示 - サービスに接続できないか、動作できない
黄色の表示 - サービスに接続できていますが、状態を確認するために使用されていない
緑色の表示 - サービスが正常に接続され、動作していることを確認するために使用されているステータス・メッセージには、現在のステータスに関する詳細情報が表示される。

診断画面のセクションが空になっている場合は、使用可能な設定済みのサービスは存在しない、あ

るいはサービスの状態を確認できなかったことを意味する。セクションが空の場合は、診断ビューを更新し、あるいはサービス・設定を確認してください。

15 運用モニタリング

運用モニタリング・データは、X-Road セキュリティ・サーバのリクエスト交換に関するデータ(クライアントおよびサービスの ID、メッセージ・ヘッダーが読み取ったメッセージの属性、リクエストとレスポンスのタイムスタンプ、SOAP サイズなど)を含む。
運用モニタリング・デーモンリクエスト交換の一部として X-Road セキュリティ・サーバの運用モニタリング・データを収集して共有する。このデータを共有し、正常性統計(タイムスタンプと成功/失敗のリクエスト数、持続時間の様々なメトリクス、およびリクエストの SOAP メッセージ・サイズなど)を計算し、共有する。格納され、共有されるデータフィールドは、[PR-OPMON]に記述されている。
セキュリティ・サーバは、運用モニタリング・データを運用モニタリング・バッファにキャッシュする。1 つの運用データレコードが、メッセージ交換中の各リクエストに対して作成される。セキュリティ・サーバは、運用モニタリング・バッファにキャッシュされた運用データを運用モニタリング・デーモンに転送する。正常に転送されたレコードは、運用モニタリング・バッファから削除される。
運用モニタリング・デーモンは、セキュリティ・サーバ所有者、通常のクライアント、およびセントラル・モニタリング・クライアントが、セキュリティ・サーバを介して運用データおよびヘルスデータを利用できるようにする。ローカルのヘルスデータは、[PR-OPMONJMX]で説明している JMXMP インターフェイスを介して外部モニタリング・システム(Zabbix など)で利用できる。
セキュリティ・サーバの所有者およびセントラル・モニタリング・クライアントは、すべてのクライアントの記録を照会することができる。通常のクライアントの場合、そのクライアントに関連付けられたレコードのみが使用可能である。セキュリティ・サーバの内部 IP は、セキュリティ・サーバの所有者とセントラル・モニタリング・クライアントに対するレスポンスのみに含まれる。
注: 以下のセクションのすべてのコマンドは、ルート権限を使用して実行する必要がある。

15.1 運用モニタリング・バッファ

一般に、運用モニタリング・バッファは、セキュリティ・サーバの内部コンポーネントであり、エンドユーザは直接使用しない。 運用モニタリング・バッファの設定に使用できる設定・パラメータは、[UG-OPMONSYSPAR]に記載されている。
パラメータのデフォルト値は、推奨最小ハードウェアを使用して予想される平均負荷の下で十分であるように設定されている。
デフォルトの設定値へのすべてのオーバーライドは [op-monitor-buffer] セクションの /etc/xroad/conf.d/local.ini ファイルで行う。

15.1.1 運用モニタリング・データの収集の停止

何らかの理由で運用データを収集して運用モニタリング・デーモンに転送することを避けたい場合は、パラメータサイズを 0 に設定できる。

```
[op-monitor-buffer]
size = 0
```

設定変更後、xroad-proxy サービスを再起動する必要がある。

```
service xroad-proxy restart
```

さらに、運用モニタリング・デーモンを停止する必要がある。

```
service xroad-opmonitor stop
```

再起動後にサービスを停止したままにするためには、次のコマンドを実行する必要がある。

```
echo manual > /etc/init/xroad-opmonitor.override
```

15.2 運用モニタリング・デーモン

運用モニタリング・デーモンの設定に使用できる設定・パラメータは、[UG-OPMONSYSPAR]に

記載されている。
運用モニタリング・バッファと同様に、パラメータのデフォルト値は、推奨最小ハードウェアを使用して予想される平均負荷の下で十分であるように設定されている。
デフォルトの設定値への上書きは、 /etc/xroad/conf.d/local.ini ファイルの[op-monitor] セクションで実行する。以下のセクションでは、変更する必要性が高いパラメータについて説明する。

15.2.1 ヘルス統計期間の設定

デフォルトでは、600 秒(10 分)の間、ヘルス統計が提供される。これは、10 分の間にリクエスト交換が行われなかった場合、すべての統計のメトリクスがリセットされることを意味する。利用可能なヘルス・メトリクスの詳細な概要については、[PR-OPMON]を参照してください。
ヘルス統計期間を変更するためには、health-statistics-period-seconds というパラメータの値を/etc/xroad/conf.d/local.ini ファイルの[op-monitor] セクションで設定あるいは編集する必要がある。

15.2.2 データベース・クリーンアップに関連するパラメータの設定

システムの負荷とリソースにより、古いデータベース・レコードの削除間隔を変更する必要がある。
次のパラメータは、[op-monitor] セクションの /etc/xroad/conf.d/local.ini ファイルに設定しなければならない。
keep-records-for-days というパラメータは、たとえば、クリーンアップが発生する前にディスクがいっぱいになる場合、または 7 日間のデフォルト期間が短すぎる場合などに編集する必要がある。clean-interval （Cron 式[CRON]）というパラメータは、システムがクリーンアップを実行する必要性を確認する頻度を定義する。デフォルトの期間である 12 時間が長すぎたり短すぎたりする場合は、必要に応じて編集する必要がある。

15.2.3 運用モニタリング・デーモンの HTTP エンドポイントに関連するパラメータの設定

運用モニタリング・デーモンのエンドポイントを設定するためには、設定の［op-monitor］セクションで以下のパラメータを実行できる。

- host - デーモンのリスニング・ホスト(デフォルトでは localhost に設定されている)。
- port - リスニング・ポート(デフォルトでは 2080 に設定されている)。
- scheme - 接続タイプ(デフォルトでは、HTTP に設定されている)。

これらの値のいずれかが変更された場合は、プロキシと運用モニタリング・デーモン・サービスの両方を再起動する必要がある。
service xroad-proxy restart service
xroad-opmonitor restart

15.2.4 外部運用モニタリング・デーモンのインストール

技術的には、運用モニタリング・デーモンをセキュリティ・サーバとは別のホストにインストールすることができる。外部運用モニタリング・デーモンを使用するように複数台のセキュリティ・サーバを設定することは可能だが、この設定はセキュリティ・サーバがロードバランサの背後にインストールされている同一のクローンである場合のみ正しい。
注意: クラスタ化されたセキュリティ・サーバのセット・アップは正式にサポートされておらず、将来の互換性のために実装されている。注意: セキュリティ・サーバと関連する外部運用モニタリング・デーモンの間のリクエストには HTTPS を使用することを強く推奨する。
分離されている運用モニタリング・デーモンを実行するには、xroad-opmonitor パッケージをインストールする必要がある。X-Road パッケージを入手する一般的な手順については、[IG-SS]を参照してください。

インストールの結果、次のサービスが実行される。
xroad-confclient

xroad-signer
xroad-opmonitor

15.2.5 外部運用モニタリング・デーモンと対応するセキュリティ・サーバの設定

セキュリティ・サーバを外部の運用モニタリング・デーモンと通信させるためには、デーモンとセキュリティ・サーバの両方を設定しなければならない。

デフォルトでは、運用モニタリング・デーモンはローカル・ホストをリッスンする。デーモンを他のホストのセキュリティ・サーバの上で使用できるようにするためには、前のセクションで説明したように、リスン・アドレスを特定のネットワーク内の適切な IP アドレスとして設定しなければならない。

忠告したように、scheme パラメータは ”https”に設定する必要がある。HTTPS を介した通信の場合、セキュリティ・サーバがモニタリング・デーモンを認証することができるために、セキュリティ・サーバと運用モニタリング・デーモンは、互いの TLS 証明書を知っていなければならない。

注意: 外部運用モニタリング・デーモンを使用する場合は、両方のホスト、スキーム(および任意にポート)のパラメータを変更する必要がある。

セキュリティ・サーバの内部 TLS 証明書は、運用モニタリング・デーモンに対するセキュリティ・サーバの認証に使用される。この証明書は、セキュリティ・サーバのインストール処理中に作成され、/etc/xroad/ssl/internal.crt ファイルで PEM 形式で使用できる。内部 TLS 証明書を UI からエクスポートする手順については、10.3 を参照してください。このファイルは、運用モニタリング・デーモンを実行しているホストにコピーしなければならない。システム・ユーザ xroad には、このファイルを読み取るための権限が必要である。
外部デーモンの設定においては、該当するパスは /etc/xroad/conf.d/local.ini で設定する必要がある:

```
[op-monitor]
client-tls-certificate = <path/to/security/server/internal/cert>
```

次に、以下のコマンドを使用して、TLS 鍵と該当する証明書を外部モニタリング・デーモンのホストにも作成する必要がある。

```
generate-opmonitor-certificate
```

スクリプトは、TLS 証明書への標準フィールドの入力を求め、またその出力(鍵ファイルと証明書)は /etc/xroad/ssl ディレクトリに作成される。

opmonitor.crt ファイルで作成された証明書は、該当するセキュリティ・サーバにコピーしなければならない。システム・ユーザ xroad は、このファイルを読むための権限を持つ必要がある。opmonitor.crt ファイルのパスはセキュリティ・サーバの設定に書き込まなければならない(セクションの名前に注意してください。設定を読み込むのはプロキシ・サービスです)。

```
[op-monitor]
tls-certificate = <path/to/external/daemon/tls/cert>
```

外部運用デーモンを使用するためには、セキュリティ・サーバのプロキシ・サービスを再起動する必要がある。

```
service xroad-proxy restart
```

さらに、該当するセキュリティ・サーバを実行しているホストの上では、運用モニタリング・デ

ーモンを停止する必要がある。
service xroad-opmonitor stop

再起動後にサービスを停止したままにするためには、次のコマンドを実行する必要がある。
echo manual > /etc/init/xroad-opmonitor.override

コンフィギュレーション・クライアントがグローバル・コンフィギュレーションをダウンロードできるようにするためには(デフォルト設定・ダウンロード間隔は 60 秒)、コンフィギュレーション・アンカー(configuration-anchor.xml に改名)ファイルを手動で外部モニタリング・デーモンの /etc/xroad ディレクトリにコピーする必要がある。システム・ユーザ xroad には、このファイルを読み取るための権限が必要である。

15.2.6 JMXMP を介してヘルス・データのモニタリング

運用モニタリング・デーモンは、JMXMP プロトコルを介してヘルス・データを利用可能にする。Zabbix モニタリング・ソフトウェアは、組み込みの JMX インターフェイス・タイプを使用して定期的にそのデータを収集するように設定できる。

デフォルトでは、運用モニタリング・デーモンは、認証が設定なし、TLS が無効になっている状態で、ローカル・ホストの JMXMP の 9011 ポートを介してヘルスデータを公開します(/etc/xroad/services/opmonitor.conf を参照)。この設定は、Zabbix などの外部ツールがデータにアクセスできるように、カスタマイズする必要がある。運用モニタリング・デーモンの JMX インターフェイスへのアクセス設定方法には、[JMX]のマニュアルを参照してください。

Zabbix が JMX を介してでデータを収集できるようにするには、Zabbix Java ゲートウェイをインストールする必要がある。手順については[ZABBIX-GATEWAY]を参照してください。

ヘルス・データを取得する必要がある Zabbix の各ホスト項目に JMX インターフェイスを設定する必要があります。手順については、[ZABBIX-JMX]を参照してください。

運用モニタリング・デーモンによって公開される JMX オブジェクトの名前と属性の詳細については、[PR-OPMONJMX]を参照してください。

xroad-opmonitor パッケージは、Zabbix にインポートできる JMX インターフェイス、サンプル・サービスに関連するアプリケーション、およびこれらのサービスのヘルス・データ項目が入っているサンプル・ホスト・データを含む。また、Zabbix API を使用して、ヘルスデータ関連のアプリケーションやアイテムを数人のホストにインポートするためのスクリプトも用意されている。サンプルファイルを /usr/share/doc/xroad-opmonitor/examples/zabbix/ のディレクトリから見てください。Zabbix API の詳細については、[ZABBIX-API]を参照してください。

16 環境モニタリング

環境モニタリングは、オペレーティング・システム、メモリ、ディスク容量、CPU 負荷、実行中のプロセスおよびインストールされたパッケージなどのセキュリティ・サーバの詳細を提供する。

16.1 SOAP API による使用

環境モニタリングは、X-Road メッセージ・プロトコル拡張を介して SOAP API を提供する。SOAP メッセージは、[PR-ENVMONMES]に記述されている。

モニタリング拡張のスキーマは、[MONITORING_XSD]で定義されている。

16.2 JMX API による使用

環境モニタリングには、JMX クライアント(例えば、Java の jconsole アプリケーションなど)がアクセスできる標準の JMX エンドポイントも提供する。詳細は、[ARC-ENVMON]を参照してください。

JMX はデフォルトでは無効になっている。JMX は、例えば、[ZABBIX-JMX]にあるように、標準の JMX 関連のオプションを実行可能な Java プロセスに追加することで有効になる。モニタリング・プロセスオプションはセキュリティ・サーバのパス /etc/xroad/services/monitor.conf に定義されている。

16.3 環境モニタリング・リモート・データセットを制限する

monitor-env limit-remote-data-set パラメータを変更することによって、許可された非所有者が環境モニタリング・データ・リクエストを介して、リクエストできるものを制限することができる。フラグを true に変更することにより、環境モニタリング・データの照会が許可された非所有者は、証明書、オペレーティング・システム、および xroad バージョン情報のみを取得できるようになる。このパラメータは、デフォルトでは false に設定されている。セキュリティ・サーバの所有者は、常にリクエスト通りの完全なデータ・セットを取得する。

17 ログとシステム・サービス

ログを読むためには、ユーザーは root ユーザーの権限をもつこと、あるいは xroad および/または adm システム・グループに属しなければならない。

17.1 システム・サービス

セキュリティ・サーバの最も重要なシステム・サービスは次のとおりである。

サービス	目的	ロ グ
xroad-confclient	グローバル・コンフィギュレーションのクライアント	/var/log/xroad/configuration_client.log
xroad-jetty	ユーザーインターフェースを実行するアプリケーションサーバ	/var/log/xroad/jetty/
xroad-proxy	メッセージ交換	/var/log/xroad/proxy.log
xroad-signer	鍵管理プロセス	/var/log/xroad/signer.log
nginx	ユーザーインターフェースを実行するアプリケーションサーバとメッセージ交換用のプロキシ	/var/log/nginx/

システム・サービスは upstart によって管理される。

サービスを開始するためには、root ユーザとして以下のコマンドを実行する:

```
service <service> start
```

サービスを停止するためには、以下のコマンドを実行する。

```
service <service> stop
```

17.2 ロギング設定

ロギングの場合、Logback システムが使用される。Logback 設定・ファイルは /etc/xroad/conf.d/ ディレクトリに保存される。

ロギングのデフォルト設定は次のとおりである。

logging level: INFO;

rolling policy: ファイルサイズが 100 MB に達する都度

17.3 障害の詳細 UUID

セキュリティ・サーバがメッセージ交換中にエラー状態に遭遇した場合、セキュリティ・サーバは、UUID(ユニバーサル・ユニーク ID、例えば 1328e974- 4fe5-412c-a4c4-f1ac36f20b14)をサービス・クライアントの情報システムにフォールト・ディテールとして追加する。UUID を使用して、xroad-proxy ログから発生したエラーの詳細を発見することができる。

以上 https://x-tee.ee/docs/live/xroad/ug-ss_x-road_6_security_server_user_guide.html より。Federation,REST 他以下略