UPKI サーバ証明書管理用ツールの開発

宇田川　暢

新潟大学　学術情報基盤機構情報基盤センター

udagawa@cais.niigata-u.ac.jp

Development of Management Utility for UPKI Server Certificate

UDAGAWA Mitsuru

Center for Academic Information Service, Niigata Univ.

概要

国立情報学研究所の提供する UPKI 電子証明書発行サービスの運用において、サーバについて専門的な知識が必要な場合があり、利用者に対するサポートが負担となる場面がある。この問題を軽減するために専用のシステム開発を行った。

1　はじめに

学術機関を対象として国立情報学研究所により「UPKI 電子証明書発行サービス（以下、UPKI）」[1]が提供されており、規定の費用を支払うことで利用機関は任意の数のサーバ証明書やクライアント証明書等の証明書を利用する事が可能となっている。

この UPKI は国立情報学研究所が中間 CA となり、利用機関が登録業務の一部を行う LRA（Local Registration Authority）という形態を取っている。証明書発行のために必要な審査項目の確認を利用機関側で実施することで証明書発行手続きの迅速化や低コストでの運用を可能にしている。

2　UPKI 支援システムと問題

UPKI では利用機関に対してウェブインターフェイスを持つ「支援システム」が提供され、登録業務の一部を行うこととなっている。これは主に申請用の TSV（Tab Separated Values）ファイルのアップロードにより行われるが、この申請用 TSV 作成を支援するために「TSV 作成ツール」と呼ばれるシステム[2]が別途提供されている。

UPKI において証明書の利用を希望するサーバ管理者などのエンドユーザは「利用管理者」、利用機関でエンドユーザからの申請を受け付け、登録業務を行う担当者は「登録担当者」と呼ばれている。著者の所属する新潟大学においてはサーバ証明書が UPKI の主要な利用対象サービスとなっているが、以下のような申請手続き上の問題が発生している。

- 利用管理者となる学内の利用者、およびウェブサイト作成を請け負う業者はサーバに対する知識が十分でない場合もあり、CSR の作成が困難で情報基盤センターのサポートを必要とする場合が少なくない。
- CSR は規定の方法で作成する必要があり、問題がある場合は再作成を要求することになるため不備があると手戻りとなりやすい。また、利用管理者の側で CSR が UPKI で利用可能か事前に確認する手段が提供されていない。
- 更新申請用 TSV ファイルの場合は DN の一致、CSR が再利用されていないかどうかの確認が必要となっており、また、更新・失効申請時には利用中の証明書のシリアル番号を記述する必要がある。そのため、証明書の更新・失効申請用 TSV は利用管理者が単独で作成することが困難であり、登録担当者が代行して作成している。

3　サーバ証明書管理用ツールの開発

著者は登録担当者として UPKI のサービスデスク業務を担当しており、これらの問題に対応するため専用のウェブインターフェイスを持つシステムを作成することとした。この「サーバ証明書管理ツール」（以下、本システム）の主な機能は下記のとおりとなる。

3.1 利用管理者向け機能

本システムは利用管理者によるサーバ証明書の利用申請および導入手続きの支援を目的とし、利用管理者に以下の機能を提供している。

・DN および利用管理者の情報をフォームに入力することで、CSR と暗号鍵を生成して申請用 TSV と共に出力する。セキュリティ上の理由で暗号鍵はダウンロード後に削除される。

・予め生成された CSR を利用して利用管理者の情報を入力することで、申請用 TSV を出力する。本システムは申請用 TSV 出力時に DB を確認し、新規および更新に合わせた形式を自動的に選択する。

・申請用 TSV 出力時に予め生成された CSR が支援システムでの申請に問題が無いか確認する。

・証明書の内容および証明書と暗号鍵がペアであるか確認する。

・PEM 形式と PKCS #12 形式の相互変換や暗号鍵のパスフレーズ設定・解除を行う。

・ネットワーク越しにサーバに導入された証明書チェーンを HTTPS、SMTPS、FTPS などのサービス毎に検証する。

3.2 登録担当者向け機能

本システムは登録担当者の業務を支援するため、次の機能を持っている。

・支援システムからサーバ証明書情報一覧をダウンロードし、DB に保存する。

・DB に保存されたサーバ証明書情報を一覧表示する。

・一覧から選択した証明書の情報を詳細表示する。また、証明書をダウンロードする。

・ホスト名（利用管理者 FQDN）およびサブジェクト別名（dNSName）が共通する他のサーバ証明書を表示する。

・指定したサーバ証明書の更新・失効申請用 TSV を生成して支援システムへ送信する。

・DN および利用管理者の情報をフォームに入力させ、CSR と暗号鍵、申請用 TSV を生成して申請用 TSV を支援システムへ送信する。

・利用管理者の作成した申請用 TSV の内容を確認し、支援システムへ送信する。

・支援システムへ申請用 TSV を送信するための登録担当者用クライアント証明書を本システムのアカウントに登録する。

4 システム導入による成果

本システムは本稿執筆時点では利用管理者に対して公開されていない。しかしながら、今までCLIでの操作やウェブサービス等の複数の手法を組み合わせて行っていた作業を一元化して対応できるなどの登録担当者向けの機能は既に実際の利用申請に対して有効であることを確認しており、既存のサーバ証明書の発行状況や申請システムに送信される申請用 TSV の直前の確認といった登録業務の軽減に役立っている。

5 システムの改善

本システムでは CSR や TSV の生成といった UPKI 支援システムと関係する部分がほとんどで、システム化の際に他大学で実装していると思われるオンライン申請機能[3][4]を持っていない。これは新潟大学特有の運用上の都合によるものであるが、今後の利用状況によっては周辺環境の整備も含めて対応を検討したい。

参考文献

[1] 島岡政基ほか、学術機関のためのサーバ証明書発行フレームワーク、信学論 B、J95B (7)、871-882、2012

[2] 島岡政基ほか、UPKI サーバ証明書プロジェクトにおける証明書自動発行支援システムの開発、信学技報、109 (437)、229-234、2010

[3] 平野靖・内藤久資、UPKI イニシアティブ「サーバ証明書発行・導入における啓発・評価研究プロジェクト」と名古屋大学における事例、名古屋大学情報連携基盤センターニュース 6 (4)、379-391、2007

[4] 永井好和ほか、サーバ証明書申請・発行システムの構築―山口大学における UPKI 導入事例―、学術情報処理研究 12 (1)、59-67、2008