3E-6

TPM に基づく端末認証のための認証局の REST ベースの実装と公開鍵証明書発行支援

篠田　昭人[†]　脇田　知彦[†]　福田　洋治[‡]　毛利　公美[††]　白石　善明[†]　野口　亮司[†††]
名古屋工業大学[†]　愛知教育大学[‡]　岐阜大学[††]　（株）豊通シスコム[†††]

1. はじめに

企業などの組織において利用される情報システムでは，ユーザ認証によるアクセス制御が行われている．一方で，PC やスマートフォンなどの端末が安価に手に入るようになり，ユーザ認証だけのアクセス制御では正当な利用者による組織の把握しない端末からのアクセスを許すことになる．そのような端末から組織内の機密情報を漏洩させないためにはユーザ認証に加え，端末認証をする必要がある．

端末認証をするには耐タンパ性を備えたセキュリティチップが使える．TPM（Trusted Platform Module）は端末のマザーボードに実装されているセキュリティチップであり，公開鍵暗号の秘密鍵を安全に格納し利用できる．TPM で生成，格納される RSA 鍵ペア AIK（Attestation Identity Key）の秘密鍵と対の公開鍵に対して証明書を発行することで端末認証を実現できる[1].

これまでに，我々は組織での運用を想定した AIK 証明書を発行する手順を提案している[2]．本稿では，まず AIK 証明書発行システムの構成要素である認証局の要件を挙げ，REST ベースの認証局を実装する．次に，実装した認証局を用いた AIK 証明書発行システムの試作により要件を満たすことを説明する．また文献[2]の証明書発行手順に関わる主体を支援する TPM 利用インタフェースを作成する．

2. AIK 証明書発行に関わる主体

端末認証には TPM の AIK 証明書が使える[1]．AIK 証明書を利用するには，AIK 証明書を発行する認証局の構築が必要である．

文献[2]では AIK 証明書を発行する認証局構築のために，組織での利用を想定した AIK 証明書発行の手順を示した．TPM 搭載端末，登録担当者利用端末，登録局，認証局，端末利用者，セットアップ担当者，登録担当者が表 1に示した役割で，AIK 証明書の発行に関わる．それぞれの責任の所在を明らかにできる手順が書かれている．

3. AIK 証明書を発行する認証局の要件

開発する AIK 証明書発行支援システムは企業などの組織で利用されることを想定している．システムの構成要素である認証局は，必要な処理ができるだけでなく，システムごとの実装に依存しないインタフェースを有していれば企業の様々な利用形態に対応できる．疎結合なシステム構築をするためのモジュールとして使えるように AIK 証明書発行システムに利用する認証局の要件を次のように挙げる．

要件 1）TCG の規定に従った証明書発行処理をすること

AIK 証明書の発行については TPM の仕様を定める TCG（Trusted Computing Group）が処理内容やデータの型を規定している[3].

表 1 AIK 証明書発行に関わる主体とその役割

主体名	役割
TPM搭載端末	AIK証明書発行の対象となる端末，TPMを搭載
登録担当者利用端末	登録担当者が利用する端末，登録局と認証局にアクセスする
登録局	証明書発行に関する情報を管理するサーバ
認証局	AIK証明書の発行処理を行うサーバ．要求を受け付けて暗号化された証明書を返す
端末利用者	TPM搭載端末を通常業務で利用する者，AIK証明書発行中はTPM搭載端末にはふれない
セットアップ担当者	AIK証明書発行中に，TPM搭載端末を操作する者
登録担当者	登録局で情報を参照し，操作する者．認証局に証明書発行要求をする

認証局は TPM_IDENTITY_REQ（以降，証明書発行要求と書く）という構造体のデータを受け取って，それをもとに証明書を発行し，証明書発行要求を作成した TPM でしか復号できない暗号化をした TPM_ASYM_CA_CONTENTS，TPM_SYM_CA_ATTESTATION（以降，二つをまとめて暗号化された証明書と書く）を返す．

要件 2）クライアント開発が容易であること

AIK 証明書の発行処理をする認証局は，AIK 証明書発行システムを構築するために不可欠なものである．利用する組織によって，システムを新しく導入する場合と，すでにあるシステムに組み込む場合がある．どちらの場合の様々な状況に対応するため，認証局を利用するクライアントが異なっても，認証局の実装を書き換えることなく利用でき，容易に拡張できることが望ましい．

また，TPM の利用は API が規定されている[1]が，手動で TPM の処理を行うのは現実的ではない．容易に TPM を利用でき，証明書発行要求作成や暗号化された証明書の復号ができることが望ましい．

4. AIK 証明書発行システムの実装

認証局の実装と，AIK 証明書発行システムのためのクライアントの試作，TPM 利用インタフェースの作成をした．システムの構成は図 1のようになる．

開発環境は次のとおりである．PC は TPM 搭載の hp ProBook 6550b，OS は Windows 7 Professional（64bit）で，TPM は Infineon 製で ver.1.2 を用いた．サーバは GlassFish Server 3.1.1，Java 言語で実装した．ライブラリに Jersey 1.3, IAIK jTSS 0.7[4], IAIK TCcert 0.2.5[4], IAIK JCE 4.0[5], IAIK CMS 4.1[5]を用いている．

4.1 認証局サーバ

認証局機能を持つサーバを REST ベースで実装した．認証局の機能と動作を次に示す．以降，GET，POST という記述は，それぞれ HTTP メソッドの GET，POST を表す．

認証局公開鍵証明書配付：認証局の URI に GET をすると認証局の公開鍵証明書を返す．認証局の公開鍵証明書は認証局が署名に用いる秘密鍵と対になるもので，TPM 搭載端末で証明書発行要求を作成する際に利用する

証明書発行処理：認証局の URI に POST で証明書発行要求ファイルを送信すると，証明書発行要求の正当性を検証する．正当であると認められると証明書を発行し，証明書発行要求を作成した TPM で保護された秘密鍵でのみ復号できる暗号化をした証明書（暗号化された証明書）を返す

An Implementation of REST-based Privacy Certification Authority and Support to Issue Public Key Certificate for TPM-based Terminal Authentication

† Akihito SHINODA, Tomohiko WAKITA and Yoshiaki SHIRAISHI・Nagoya Institute of Technology
‡ Masami MOHRI・Gifu University
†† Youji FUKUTA・Aichi University of Education
††† Ryoji NOGUCHI・Toyotsu Syscom Corp.

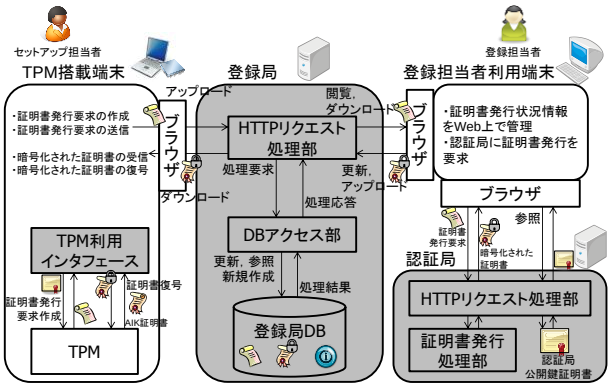

図 1 システム構成図（網かけ部分を実装）

4.2 AIK 証明書発行支援システムの試作

4.1節の認証局を利用して，文献[2]の手順に沿った AIK 証明書発行システムを試作した．

4.2.1 登録局サーバ

開発した機能は次のとおりである．

証明書発行状況参照：登録担当者が指定 URI に GET すると証明書発行状況の情報を返す

受付番号発行：登録担当者が端末利用者の氏名と所属，セットアップ担当者のユーザ名を POST で送ると受付番号を返す．証明書発行手続きにおけるそれぞれの操作は受付番号により識別する

証明書発行要求アップロード：セットアップ担当者の操作する TPM 搭載端末から証明書発行要求ファイルの送信を受け付ける．POST で証明書発行要求ファイルと，セットアップ担当者の認証情報，受付番号を受け取る．認証情報の検証に成功するとデータベースに証明書発行要求ファイルを登録し，証明書発行状況の発行要求受付の項を未から済に更新する

証明書発行要求ダウンロード：受付番号を POST すると対応する証明書発行要求ファイルを返す．登録担当者が証明書発行要求ファイルを認証局に送信するために利用する

暗号化された証明書アップロード：受付番号とともに暗号化された証明書ファイルを POST すると，登録局データベースの該当の受付番号のレコードにファイルが登録される．登録担当者が認証局から受け取った暗号化された証明書を登録局に保管し，セットアップ担当者がダウンロードできる状態にするために利用する

暗号化された証明書ダウンロード：セットアップ担当者の操作する TPM 搭載端末から，暗号化された証明書ファイルのダウンロード要求を受け付ける．POST でセットアップ担当者の認証情報と受付番号を受け取り，認証情報の検証に成功すると受付番号に対応する暗号化された証明書ファイルを返す

4.2.2 担当者が利用する Web インタフェース

セットアップ担当者と登録担当者が，認証局と登録局を利用するためのクライアントとして開発した Web インタフェースを表 2に示す．ブラウザで各機能に必要な入力をする．

4.2.3 TPM 利用インタフェース

TPM で行う処理を操作するインタフェースである．セットアップ担当者が利用する TPM 搭載端末で動作する．証明書発行要求の作成と，暗号化された証明書の復号をする．

証明書発行要求作成インタフェース：TPM を操作し AIK の生成，証明書発行要求の作成をする．認証局の公開鍵証明書ファイルの選択とボタンの押下で，証明書発行要求を作成しファイルに出力する．また，生成された AIK を TPM にロードするための識別子もファイル出力する

証明書復号インタフェース：TPM を操作し AIK 証明書の復号をする．証明書発行要求を作成した TPM でのみ復号できる．TPM 内の AIK を指定しロードするための識別子ファイルと暗号化された証明書ファイルを選択し，ボタンを押下すると AIK 証明書を復号しファイルに出力する

表 2 開発した Web インタフェースと利用できる機能

利用する担当者	インタフェース名	利用できる機能
登録担当者	受付登録インタフェース	登録局の受付番号発行機能
	登録局管理インタフェース	登録局の証明書発行状況参照機能，証明書発行要求ダウンロード機能，暗号化された証明書アップロード機能
	認証局インタフェース	認証局の認証局公開鍵証明書配付機能，証明書発行処理機能
セットアップ担当者	証明書発行要求アップロードインタフェース	登録局の証明書発行要求アップロード機能
	暗号化された証明書ダウンロードインタフェース	登録局の証明書発行要求ダウンロード機能

5. 評価

作成した認証局が3章で挙げた要件を満たしていることを説明する．

要件 1）TCG の規定に従った証明書発行処理をすること

認証局に入力として与える証明書発行要求と，証明書発行処理を経て出力される暗号化された証明書のデータの型が，TCG の TPM 仕様書[3]の記述と一致していることを確認した．また，暗号化された証明書を TPM で復号できることから AIK 証明書の発行処理ができる認証局が実装できたといえる．

要件 2）クライアント開発が容易であること

認証局操作のための Web インタフェースとして，html でファイル送信フォームを作成した．html の body 部分への 4 行の記述で，認証局の証明書発行機能を利用できることを確認した．このことからクライアント開発は容易であるといえる．

また，TPM 利用インタフェースはファイルの選択とボタン押下のみで操作できることから，TPM で行う処理を容易に利用できるといえる．

6. おわりに

本稿では AIK 証明書発行システム構築に利用する認証局の要件を挙げ，実装した．AIK 証明書発行システムの試作により，実装した認証局は TCG の規定に従った証明書発行が可能で，クライアントの開発が容易であることを示した．

これにより，モジュールの入れ替えが容易で，疎結合な AIK 証明書発行システムの実現が期待できる．

TPM 利用インタフェースを作成したことで，手動で TPM を利用したデータ作成に比べ容易に TPM での処理を実行できる．

参考文献

[1] 中村智久，東川淳紀：PC 搭載セキュリティチップ(TPM)の概要と最新動向，情報処理，Vol.47，No.5，pp.473-478（2006）．

[2] 篠田昭人，脇田知彦，福田洋治，毛利公美，白石善明，野口亮司：TPM に基づく端末認証のための公開鍵証明書の発行支援，情報処理学会 第 73 回全国大会講演論文集（分冊 3），pp.571-572（2011）．

[3] Trusted Computing Group: TPM Main Specification Level 2 Version 1.2, Revision 116 (online), available from http://www.trustedcomputinggroup.org/resources/tpm_main_specification (accessed 2012-01-13)

[4] Institute for Applied Information Processing and Communications (IAIK): Trusted Computing for the Java™ Platform (online), available from http://trustedjava.sourceforge.net/ (accessed 2012-01-13).

[5] Institute for Applied Information Processing and Communications (IAIK): Secure Information and Communication Technologies / Home - Stiftung SIC, available from http://jce.iaik.tugraz.at/sic (accessed 2012-01-13).