2Z-9

OpenID を用いた TPM の公開鍵証明書発行と SSL クライアント認証

篠田 昭人† 福田 洋治‡ 廣友 雅徳†† 毛利 公美‡‡ 白石 善明†††

†名古屋工業大学 ‡愛知教育大学 ††佐賀大学 ‡‡岐阜大学 †††神戸大学

1. はじめに

パスワードの盗用は被害にあうまで気がつきにくく，紛失はサービスへのアクセスができなくなったときに初めて気がつくことになる．サービス利用時に使われる利用者の所有物である端末を認証の要素とすれば，盗難や紛失に気がつきやすくなり不正アクセスによる被害を未然に防ぎやすくなる．端末に搭載されるセキュリティチップ TPM（Trusted Platform Module）で生成され秘密鍵を TPM の外部に漏らさないように管理される RSA 署名鍵 AIK に公開鍵証明書を発行すれば，AIK の署名に基づいて端末を認証トークンとして使えるようになる．

我々は OpenID を導入した AIK の公開鍵証明書（以下，AIK 証明書とする）を発行する方式を提案している[1]．文献[1]で提案する方式により，証明書発行時に求められる認証局による利用者の実在性確認と認証を OpenID Provider に委託することで，利用者が管理する秘密情報を減らし，認証局が持つ機能を減らせるようになった．

公開鍵証明書を用いてクライアントを認証する方法に SSL クライアント認証がある．SSL クライアント認証では，まず，クライアントが証明書およびサーバから受け取ったメッセージに対する署名をサーバに送付する．そして，サーバはクライアントから受け取った証明書を使って署名を検証し，証明書がクライアントのものであることが確認する．

TPM の外部で生成した鍵の証明書を TPM にインポートし，クライアント認証に使う方法がある．しかし，利用者が TPM とそれ以外の鍵の保管場所から選んでクライアント認証に利用するので，認証をするサーバからはクライアントが TPM に格納した鍵を用いている端末であることを識別できない．

AIK は TPM 内部で生成されたデータにのみ署名するものと規定されている[2]．任意のデータには署名しないように制御されるので，サーバから受け取ったメッセージに署名をしなければならない SSL クライアント認証に AIK を使うことはできない．

特定の TPM にのみ復号できるようにデータを暗号化する用途に使う RSA 鍵として Binding Key（以下，BK とする）がある[3]．BK が TPM で生成されたことを検証できるようにするには，AIK で BK へ署名できる TPM のコマンド TPM_CertifyKey[2]が使える．TPM では，TPM で生成され秘密鍵を他の TPM に移行できないように保管される鍵にのみできるように AIK による署名は制御される．AIK を使った BK の公開鍵に対する署名を AIK 証明書で検証できれば，AIK が保管される TPM で BK の秘密鍵が保管されていることを確認できるようになる．

本稿では，まず認証局が AIK と BK の紐付けを確認した上で，SSL クライアント証明書を発行する方式を提案する．SSL クライアント認証をするサーバは，SSL クライアント証明書が認証局により AIK と BK の紐付けを確認した上で発行されていることを信頼するという条件の下，SSL クライアント認証で端末を識別できるようになる．次に，提案する方式で発行した SSL クライアント証明書を用いた端末認証システムの構築方法を示す．提案方式により発行される SSL クライアント証明書を用いれば，認証サーバが端末を識別できるようになり，サービス利用者の認証の要素に端末が使えるようになる．また，TPM に保管した証明書を用いて SSL クライアント認証できるようになることから，AIK を使って端末を認証する文献[1]の認証システムとは異なり，例えば Apache のような広く使われているソフトウェアで端末を認証するサーバを構築できるようになる．

以下，2 章では AIK で署名をすることで TPM で生成された鍵であると証明できることを説明し，3 章では TPM で生成した BK を利用した SSL クライアント認証に利用できる SSL クライアント証明書の発行方式を提案する．4 章で提案方式の実装方法を示す．5 章で，提案方式により発行される SSL クライアント証明書を使った端末認証システムの構築方法を示し，6 章で本稿をまとめる．

Issuance of Public Key Certificate of TPM with OpenID and SSL Client Authentication

† Akihito SHINODA・Nagoya Institute of Technology
‡ Youji FUKUTA・Aichi University of Education
†† Masanori HIROTOMO・Saga University
‡‡ Masami MOHRI・Gifu University
††† Yoshiaki SHIRAISHI・Kobe University

2. TPM で生成される署名鍵 AIK と BK

TPM は鍵を生成し外部に出さないように保管できるセキュリティチップである．TPM は他の端末に移して利用できない[4]ことから，端末に搭載される TPM で外部に出さないように保管される鍵を使って認証ができれば，端末を認証の要素にできる．

公開鍵証明書を使ってクライアントを認証する方法に SSL クライアント認証がある．我々はこれまでに，端末固有の署名を生成できる鍵 AIK を認証に使うことで端末を識別できるとし，署名の検証に使う AIK 証明書を発行する方式を提案している[1]．しかし，AIK による署名（TPM_CertifyKey）は，TPM 内で生成されたデータのみを対象とするように用途が限定されており[2]，SSL クライアント認証の鍵として AIK は利用できない．

TPM に鍵と証明書をインポートして，認証に利用する方法がある．インポートした署名鍵は SSL クライアント認証に利用できるが，認証するサーバからは TPM で鍵を保管しているかどうかは確認できない．

TPM で扱う RSA 鍵の一つである Binding Key（以下，BK とする）は，移行不可能な鍵として TPM で生成すれば，TPM の外部において BK の公開鍵でデータを暗号化したときに，その TPM でのみ復号できるようにデータを受け渡す用途に使える[3]．また，BK の公開鍵に AIK により署名すれば，BK がその TPM で生成されたことを示せる．

次章では，発行要求した TPM を搭載する端末以外に漏らさないように TPM にインポートして SSL クライアント認証に使える証明書を発行する方式を示す．

3. TPM の SSL クライアント証明書発行方式

SSL クライアント証明書発行方式に関わるエンティティを示し，図 1 を用いて証明書の発行手順を説明する．なお，この手順の前には OpenID を用いた AIK 証明書発行方式[1]により利用者に AIK 証明書が発行されているものとする．

［エンティティ］

利用者：TPM を搭載する端末を操作する者，TPM を搭載する端末を認証の要素としてサーバの認証を受ける

認証局：SSL クライアント証明書を発行する

［SSL クライアント証明書発行の手順］

(1) 利用者は TPM で移行不可能な BK を生成する
(2) 利用者は AIK で BK 公開鍵に署名する
(3) 利用者は認証局に BK 公開鍵と署名 S, AIK 証明書を送付する
(4) 認証局は(3)で受け取った署名 S を AIK 証明書と BK 公開鍵を用いて検証する
(5) 認証局は検証結果を利用者に通知する
(6) 利用者は SSL クライアント証明書用の RSA 鍵ペアを生成する
(7) 利用者は SSL クライアント証明書用の CSR（Certificate Signing Request）を作成する
(8) 利用者は CSR と CSR の鍵と対の秘密鍵を認証局に送付する
(9) 認証局は CSR に対して SSL クライアント証明書を作成する
(10) 認証局は(8)で受け取った秘密鍵を用いて SSL クライアント証明書を TPM にインポートできる PKCS#12 形式に変換する
(11) 認証局は BK 公開鍵で SSL クライアント証明書を暗号化する
(12) 認証局は利用者に BK 公開鍵で暗号化された SSL クライアント証明書を返す
(13) 利用者は BK 秘密鍵で SSL クライアント証明書を復号する
(14) 利用者は TPM に SSL クライアント証明書をインポートする

手順(8)，(12)は利用者の生成した秘密鍵が認証局以外に漏えいするのを防ぐために SSL サーバ認証による暗号化通信をする．また，認証局は発行する SSL クライアント証明書と，(4)で署名の検

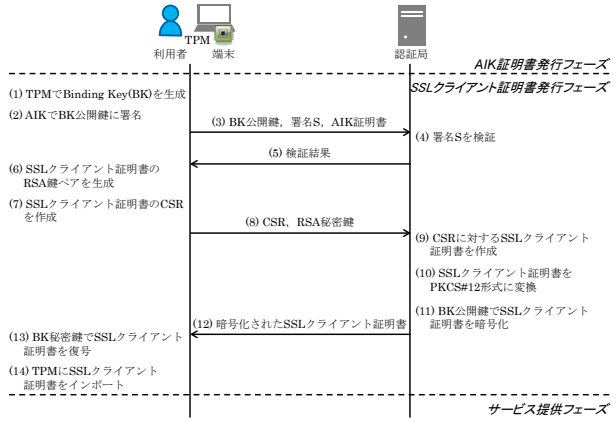

図 1　SSL クライアント証明書発行方式

証に用いた AIK 証明書の対応関係を管理しておき，SSL クライアント証明書を利用し認証するものの問い合わせを受けて，対応をする AIK 証明書を確認できるようにしておくものとする．

この方式では，認証局が AIK と BK の紐付けを確認した上で証明書を暗号化することで，証明書発行を要求した利用者の端末に搭載される TPM でしか復号できないように SSL クライアント証明書を発行している．認証するサーバは，認証局により SSL クライアント証明書が TPM を搭載する端末に発行され，インポートされるという信頼をすることで端末を認証できるようになる．

4.　提案方式の実装

図 2 に示す構成で実装した．利用したライブラリや言語は図中の各部に併記している．以下，図 1 の証明書発行手順に沿って説明する．

利用者は TPM アクセスプログラムの BK 生成要求部から TPM にアクセスし BK を生成(1)，AIK 署名生成要求部から TPM にアクセスし BK 公開鍵に署名をする(2)．(1), (2)でストレージに保存された BK 公開鍵，署名 S，AIK 証明書をブラウザを介して認証局に送信(3)すると，認証局は AIK 署名検証部で署名の検証(4)し，利用者に検証結果を通知する(5)．利用者は CSR 作成部でクライアント証明書用の RSA 鍵ペアを生成(6)し CSR を作成(7)し，ストレージに保存する．CSR と RSA 秘密鍵をブラウザを介して認証局に送信する(8)．認証局は利用者から受け取った CSR にクライアント証明書作成部で署名をし，クライアント証明書を作成(9)し，PKCS#12 形式に変換し(10)ストレージに保存する．クライアント証明書暗号化部ではストレージに保存されたクライアント証明書を BK 公開鍵で暗号化(11)し利用者にレスポンスとして暗号化されたクライアント証明書を返す(12)．利用者はブラウザを介して暗号化されたクライアント証明書をストレージに保存し，クライアント証明書復号要求部で TPM を使ってクライアント証明書を復号する(13)．最後に利用者は，復号したクライアント証明書を TPM アクセスツールを使って TPM にインポートする(14)．

5.　SSL クライアント証明書を用いた端末認証システム

3 章の提案方式により発行される SSL クライアント証明書を使って端末を認証するシステムの構築方法を示す．図 3 に構成を示し，各構成要素で動作を確認しているものを併記する．以下，図 3 を用いて手順を説明する．

あらかじめ，利用者が図 1 の手順(14)までを行い，提案方式で発行された SSL クライアント証明書が TPM にインポートされている状態とする．利用者はブラウザでサービス提供者にアクセスし，ユーザ情報の登録をする．サービス提供者はアカウント作成部でユーザ情報をユーザ管理データベースに登録する．続いて利用者は，ブラウザでサービス提供者にアクセスすると，クライアント認証モジュールにより，SSL クライアント認証が要求され，利用者は提示する証明書の選択をする．証明書が選択されると，TPM アクセスツールは SSL クライアント証明書に対応する鍵を

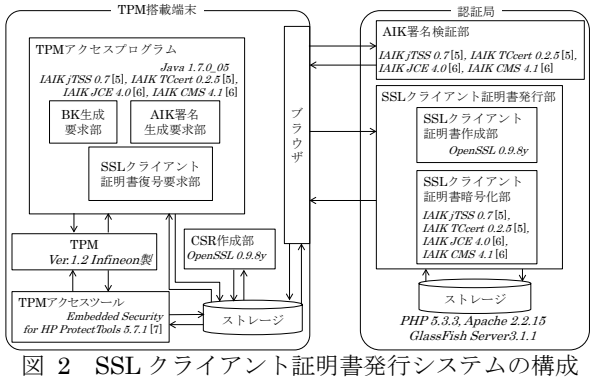

図 2　SSL クライアント証明書発行システムの構成

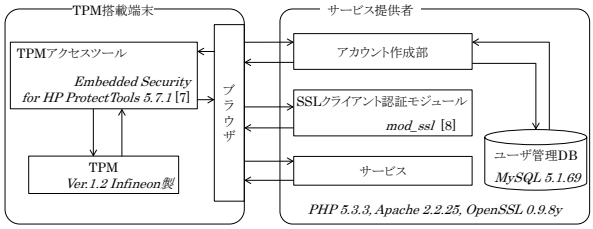

図 3　TPM 端末認証システムの構成

利用するためのパスワードの入力を利用者に求める．TPM の初期設定時に登録したパスワードを入力することで，ブラウザを介し TPM に保管されている SSL クライアント証明書でサービス提供者のクライアント認証モジュールと SSL クライアント認証が行われる．認証に成功したら，サービス提供者によりサービスの提供を開始する．以上の構成で，TPM に保管した証明書で SSL クライアント認証をする端末認証システムが構築できる．

6.　おわりに

本稿では，まず端末を利用者認証の要素とするために端末に搭載される TPM に保管した証明書で SSL クライアント認証に利用できる証明書を発行する方式を提案した．端末を認証するサーバは，認証局により AIK と BK の紐付けを確認した上でクライアント証明書が発行され，TPM に証明書がインポートされているという信頼の下で端末を認証できるようになった．次に提案方式の実装方法を示した．利用するライブラリや言語などの環境を図 2 に示し，その動作を説明した．最後に提案方式により発行されるクライアント証明書を用いて，端末を認証した上でサービスを提供できる端末認証システムの構築方法を示した．利用者が TPM とブラウザの連携に対応するツールで証明書をインポートし，サービス提供者が Apache に SSL 認証をするモジュール mod_ssl を追加し，クライアント認証を要求するように設定することで，TPM に保管した証明書で SSL クライアント認証できるようになった．

参考文献

[1] 篠田昭人，福田洋治，廣友雅徳，毛利公美，白石善明：OpenID により利用者認証を分離した TPM の公開鍵証明書発行方式，コンシューマ・デバイス＆システム(CDS)研究会，CDS9-10（2014）．
[2] 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 2014-01-14).
[3] Kerry Maletsky: Designing in A Trusted Platform Module (TPM) (online), available from<https://www.trustedcomputinggroup.org/files/resource_files/AC1C4247-1D09-3519-AD37DCA61C968B85/TCG_ESC_Atmel.pdf> (accessed 2014-01-14).
[4] 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）．
[5] Institute for Applied Information Processing and Communications (IAIK): Trusted Computing for the Java Platform (online), available from <http://trustedjava.sourceforge.net/> (accessed 2014-01-14).
[6] 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 2014-01-14).
[7] Hewlett-Packard Development Company：モバイル PC 向け TPM セキュリティソリューション（オンライン），入手先<http://h50146.www5.hp.com/solutions/infrastructure/security/products/tpm.html>（参照 2014-01-14）．
[8] Ralf S. Engelschall: mod_SSL The Apache Interface To OpenSSL, available from <http://www.modssl.org/> (accessed 2014-01-14).