6ZA-05

TPM の AIK 証明書と関連付く公開鍵証明書の発行について

松田　育也†　福田　洋治†　廣友　雅徳‡　毛利　公美*　掛井　将平††　白石　善明††
近畿大学†　佐賀大学‡　岐阜大学*　神戸大学††

1. はじめに

TPM (Trusted Platform Module) は IC チップに耐タンパ性をもたせたものであり,PC に内蔵されている.TPM に内蔵されている AIK の秘密鍵は外部に流出しないよう管理されており,これに公開鍵証明書を発行すると AIK の署名を用いて端末を認証トークンとして使うことができる[1].

AIK 公開鍵証明書を発行する際にはプライバシーCA で本人確認を受ける必要がある[2]が,公開鍵証明書を用いた認証を使う場合,証明書内に登録された名前や所属,メールアドレス等の個人情報(サブジェクト)がプライバシーCA に開示される課題がある.

著者らはこれまで証明書発行時に求められる利用者の認証を OpenID Prover に委託し,プライバシーCA に渡る個人情報を限定する TPM の AIK 証明書発行方式[3]を提案している.

本研究では, AIK 公開鍵証明書の発行過程で, 公開鍵証明書を用いた認証を想定し, 証明書内のサブジェクトを開示しなくても済むように,利用者が所有している公開鍵証明書を変更,これを提示,検証できる証明書発行・検証の一方式を提案し,その実現方法について述べる.

2. 縮退証明書とその発行と検証

公開鍵証明書内の個人情報を削除し, 証明書を縮退させたとき, このことを CA とは別の機関（縮退証明局と呼ぶことにする）が証明書（縮退証明書と呼ぶことにする）を発行し, 証明することを考える.

縮退証明書は X.509 形式に従い図 1 のような構成とする. 通常の公開鍵証明書と比べて Subject と SubjectPublicKeyInfo が無く, Extensions には, 変更された証明書 ModifiedPKC と検証用のハッシュ値の差分 Difference を含める.

ModifiedPKC には, AIK 公開鍵証明書の発行申請者の公開鍵証明書 PKC から Subject を除いた変更した証明書の情報を格納する. Difference には, 完全な証明書の Info のハッシュ値と, 変更した証明書の Info のハッシュ値の差分を格納する. Signature には, 縮退証明書の Info に対する, 縮退証明局の秘密鍵による署名が格納される.

縮退証明書の発行は図 2 のように行う. 証明書

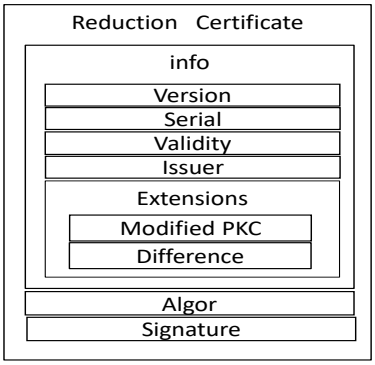

図1　縮退証明書の構成

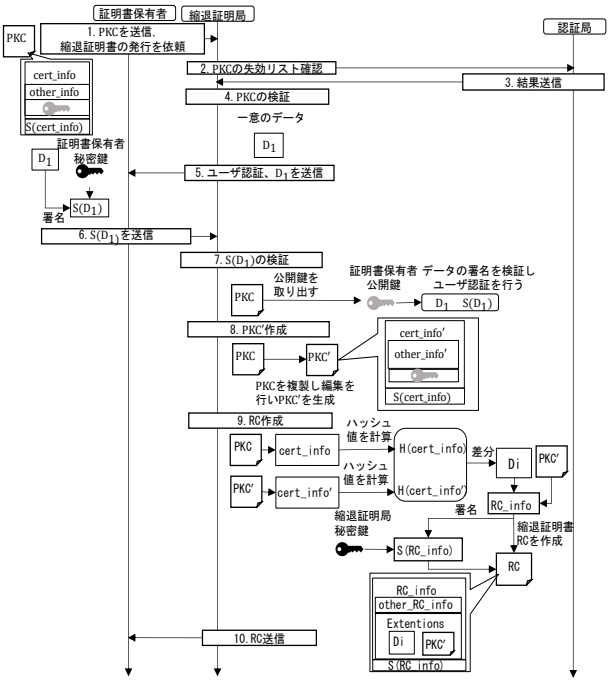

図 2　縮退証明書の発行の流れ

保有者は縮退証明局に自身の公開鍵証明書 PKC を送信し,縮退証明書の発行を依頼する.縮退証明局は PKC を確認し,一般的な公開鍵証明書を用いた発行依頼者の認証を行う. 認証をパスした後, 縮退証明局は公開鍵証明書を複製し,証明情報 cert_info（証明書内の Info の情報）に対して,サブジェクトなどの隠したい情報を削除する.サブジェクトを削除した証明情報を cert_info'とし,これを格納した証明書を PKC'とする.cert_info と cert_info'のハッシュ値をそれぞれ計算する. 計算に使うアルゴリズムは PKC の署名に使われたアルゴリズムと同じとする.これらハッシュ値をビット単位で排他的論理和し差分 Di を求める. Di と

On Issuance of Public Key Certificate Relating to AIK Certificate of TPM

† Ikuya MATSUDA, Youji FUKUTA, Kindai University
‡ Masanori HIROTOMO, Saga University
* Masami MOHRI, Gifu University
†† Shohei KAKEI, Yoshiaki SHIRAISHI, Kobe University

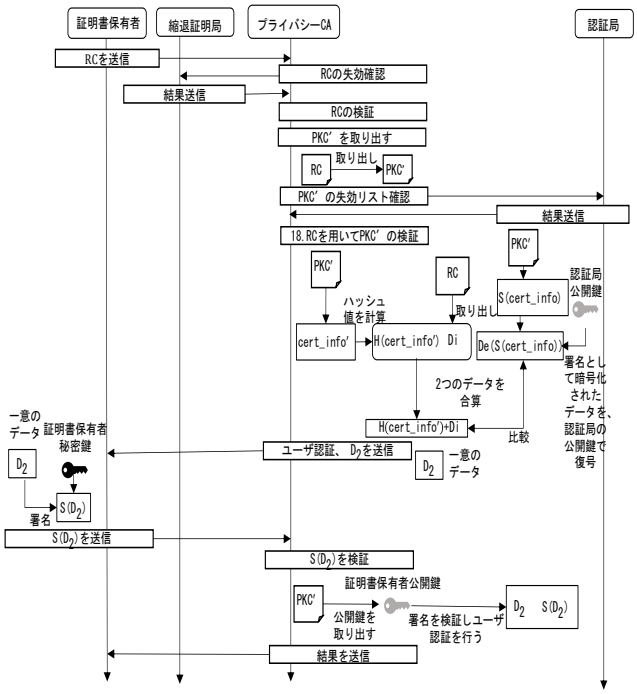

図 3　縮退証明書の検証の流れ

PKC’から証明情報を作り，縮退証明局の秘密鍵で署名を作り，縮退証明書 RC を構成し，証明書保有者に発行する．

縮退証明書の検証は，プライバシーCA に対する AIK 公開鍵証明書の発行過程において，図 3 のように行う．証明書保有者は縮退証明書 RC をプライバシーCA に提示し，AIK 公開鍵証明書の発行を依頼する．プライバシーCA は RC を確認した後，変更された証明書 PKC’と検証用のハッシュ値の差分 Di を取り出す．PKC’の証明情報 cert_info’のハッシュ値を計算し,Di とビット単位で排他的論理和を行う．この値は証明情報 cert_info のハッシュ値と一致するはずである．認証局の公開鍵で署名 S(Cert_info)を復号して,ハッシュ値を比較することで PKC’の検証を行う．検証をパスした場合，PKC’の公開鍵に対応する秘密鍵を証明書保有者が持っていることを確認するため，一般的な公開鍵証明書を用いた認証を行う．

認証後は，証明書保有者は AIK 公開鍵および EK 証明書をプライバシーCA に送信し,AIK 証明書の発行手続き[2]に移行する．

3.　動作確認

提案する証明書発行・検証の方式が実現可能であることを確認するため,C++言語と OpenSSL ライブラリを用いて確認用プログラムを作成，動作させて,OpenSSL のコマンドを用いて作成した公開鍵証明書に対して，縮退証明書の発行，検証が実際に行えることを確認した．確認用プログラムを動作させたときのターミナルの画面の様子を図 4 に示す．縮退証明書の発行，検証の処理を C++言語と

```
info-no-MacBook-Air-22:Debug info$ ./DegenerateVerification
-----証明書検証-----
-----拡張領域取り出し-----

-----取り出し完了-----
-----署名検証完了-----
-----差分-----
0:75:2b:0:1d:0:33:0:3f:0:14:8a:0:49:0:3:0:7:1d:1b:12:9:0:45:0:2f:6d:0:ba:80:48:4
a:c:0:16:0:88:0:49:0:b9:6:0:4:bd:0:1a:0:1:0:29:0:0:0:0:0:0:0:0:0:0:0:0:0:
-----復号後-----
30:31:30:d:6:9:60:86:48:1:65:3:4:2:1:5:0:4:20:42:fc:c0:97:2d:6:98:30:bd:23:20:24
:79:9c:87:b1:9f:35:a2:52:e7:d4:5f:67:31:7:21:ee:d2:14:4c:c9:0:0:0:0:0:0:0:0:0:
0:4:0:
---これを採用----
42:fc:c0:97:2d:6:98:30:bd:23:20:24:79:9c:87:b1:9f:35:a2:52:e7:d4:5f:67:31:7:21:e
e:d2:14:4c:c9:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
-----ハッシュ値生成-----
b7:d1:dd:ca:6c:1a:e:79:c0:2a:3:9:67:93:cc:e0:32:ef:22:a:9d:c0:75:ef:7a:c0:1b:f2:
15:2e:4d:f2:
-----合算後-----
42:fc:c0:97:2d:6:98:30:bd:23:20:24:79:9c:87:b1:9f:35:a2:52:e7:d4:5f:67:31:7:21:e
e:d2:14:4c:c9:
-----比較結果-----
11111111111111111111111111111111
```

図 4　確認用プログラムの動作の様子

OpenSSL ライブラリを用いて実現できることを確かに確認した．

4.　おわりに

端末に搭載されるセキュリティチップ TPM で生成される鍵を TPM の外部に流出させないように管理される署名鍵 AIK に公開鍵証明書を発行すると，AIK の署名を用いて端末を認証トークンとして使うことができる．

AIK の公開鍵証明書を発行する際には，プライバシーCA を運用し，そこで証明書発行依頼者を認証し，本人であることを確認した後，端末と証明書発行依頼者と AIK を紐づけた AKI 公開鍵証明書を発行，管理する．

プライバシーCA での利用者の認証の方法は，パスワードを用いた認証，利用者が既に所有する公開鍵証明書を用いた認証が考えられるが，前者はパスワード等の秘密情報の事前登録が必要であり，後者は証明書内の利用者の個人情報がプライバシーCA に開示される．

本稿では，証明書内の利用者の個人情報を開示しなくても済むように，利用者が所有している公開鍵証明書を変更，これを提示，検証できる，TPM の AIK 証明書発行における，証明書の提示・検証の一方式を提案し，その実現方法について述べた．

参考文献

1) 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,6Y-8(2011 年).

2) 大川雅士,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認証局の構築,情報処理学会　第 73 回全国大会講演論文集,6Y-7(2011 年).

3) 篠田昭人,福田洋治,廣友雅徳,毛利公美,白石善明: 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,情報処理学会第 76 回全国大会講演論文集,2Z-9(2014 年).

4) 電子署名のしくみと機能 本人証明と非改ざん証明｜電子契約,入手先<https://www.itis.nssol.nssmc.com/blog/contracthub/hint07.html>(参照 2018-12-17).