6Y-8

TPMに基づく端末認証のための公開鍵証明書の発行支援

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

ノートPCやスマートフォンなどの端末が安価に入手できるようになり，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が把握していない端末からの情報システムへのアクセスが許されることになる．組織内の機密情報を守るためには，ユーザ認証に加えて，アクセス端末の特定をした後にサービス利用許可を出すような端末認証の導入が必要になってきている．

端末認証にはセキュリティチップと呼ばれる耐タンパー性を有するICチップが使える．特に，PCのマザーボードに実装されているTPM（Trusted Platform Module）はRSA暗号の演算・鍵生成・格納や，乱数生成・ハッシュ演算・ハッシュ値保管などの端末認証を安全に行うのに必要な機能が搭載されている[1]．

我々は，TPMによる端末認証を実現するために，文献[1]に示されているPKIに基づいた端末認証に必要な認証局（プライバシーCA）の構築について検討し，TPMのIdentity鍵に対する証明書発行をする認証局の設計をしている[2]．そこでは，モデルに基づく手順が示されている．

本稿では[2]の手順に従って，組織で利用することを想定したIdentity鍵に対する証明書発行に係る主体を支援するインターフェースを設計する．

2. 端末認証のための公開鍵証明書発行の手順

文献[2]では端末認証のためのIdentity鍵証明書発行の手順が示されている．図1に示すように端末，登録局，認証局で構成され，それぞれの処理について述べられている．

この手順は企業などの組織での利用を想定し，登録局（RA）を導入したプライバシーCAを設計している．実際の組織での利用においては管理者が適切に配置され，操作を行うものであることから，それぞれの手順で責任の所在を明らかにできるIdentity鍵証明書発行プロセスが必要となる．

3. 企業などの組織での利用を想定したIdentity鍵証明書発行プロセス

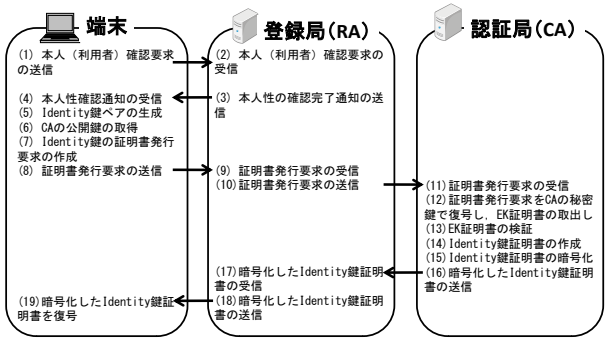

図1　Identity鍵証明書発行の手順

3.1 主体とその役割

Identity鍵証明書発行手続きに関わる主体と，その役割を説明する．

[端末]Identity鍵証明書を発行する端末．

[端末利用者]通常業務で端末を使う者．

[セットアップ担当者]Identity鍵証明書発行の際に端末を操作する者．証明書発行に必要な要求を作成，送信操作し，発行された証明書の復号を行う．

[登録局（RA）]端末からの要求受付等を行うサーバ．本人確認要求の受付，証明書発行要求の受付，暗号化したIdentity鍵証明書の配付を行う．

[登録担当者]登録局の管理を行う者．端末利用者の本人性確認，認証局に対する証明書の発行要求，端末へのIdentity鍵証明書配付のためのダウンロードURL通知を行う．

[認証局（CA）]証明書発行処理を行うサーバ．登録局からの証明書発行要求に対して証明書の発行をし，証明書を暗号化した状態で返す．

3.2 証明書発行手順

2章で述べたように，[2]のIdentity鍵証明書発行の手順(図 1)に対する，管理者を配したプロセスを示す．

3.1節で役割を説明した主体により，図2に示した次のような手順でIdentity鍵証明書を発行する．

1)【端末利用者】セットアップ担当者に端末を受け渡す
2)【セットアップ担当者】本人確認要求操作を行う
3)【登録担当者】対面による端末利用者の本人確認をした後に，本人確認完了通知操作をする
4)【セットアップ担当者】Identity鍵ペアと証明書発行要求作成の操作をする
5)【セットアップ担当者】証明書発行要求送信操作をする

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.

6)【登録担当者】証明書発行要求送信操作をする
7)【認証局】証明書発行処理をする
8)【登録担当者】暗号化した Identity 鍵証明書をダウンロード可能状態にし，ダウンロード URL をセットアップ担当者に通知する
9)【セットアップ担当者】暗号化した Identity 鍵証明書をダウンロードする
10)【セットアップ担当者】暗号化した Identity 鍵証明書を復号操作（アクティベート）する
11)【セットアップ担当者】端末利用者に端末を受け渡す

3.3 Web インターフェース

3.2 節の手続きを支援する Web インターフェースの実装について述べる．Web インターフェースは証明書発行手続きを処理ごとに分けた次の 4 つがある．通信は 4 つすべてにおいて SSL 相互認証をし，暗号化通信を行う．図 2 の番号に対応してそれぞれの説明をする．

[本人確認インターフェース] 手続き 2)～3)の処理で端末と登録局間で利用する．端末から登録局にセットアップ担当者が本人確認要求を送信し，それに対して登録担当者が本人性確認完了通知を送信する．登録局に本人性確認をした記録を残す．

[証明書発行要求インターフェース] 手続き 5)の処理で端末と登録局間で利用する．端末から登録局にセットアップ担当者が証明書発行要求を送信する．

[証明書発行インターフェース] 手続き 6)～7)の処理で登録局と認証局間で利用する．登録担当者により登録局から認証局に対し証明書発行要求を送信し，認証局で発行された証明書を暗号化した状態で出力する．

[証明書配付インターフェース] 手続き 9)の処理で端末と登録局間で利用する．端末からセットアップ担当者が登録局にアクセスし，暗号化した証明書をダウンロードする．

4. 評価

1) 端末利用者がセットアップ担当者に端末を渡し，証明書発行操作に関わらないことで端末利用者による不正な証明書発行を防げる．
2)～3) SSL 相互認証と暗号化通信により，本人確認要求や本人確認完了通知の改ざん・偽造を防げる．登録担当者は，対面による本人確認で端末利用者の本人性を保証し，本人確認について責任を持つ．
4) セットアップ担当者は証明書発行要求内容について責任を持つ．
5) SSL 相互認証と暗号化通信により，端末から登録局に送られる証明書発行要求の盗聴・改ざん・偽造を防げる．
6)～7) SSL 相互認証と暗号化通信により，登録局から認証局に送られる証明書発行要求，認証局から登録局に送られる暗号化した Identity 鍵証明書の盗聴・改ざん・偽造を防げる．また，証明書発行要求は認証局の秘密鍵でしか復号できない暗号化をされている[2]ため，登録局での改ざんによる不正な証明書発行も困難である．

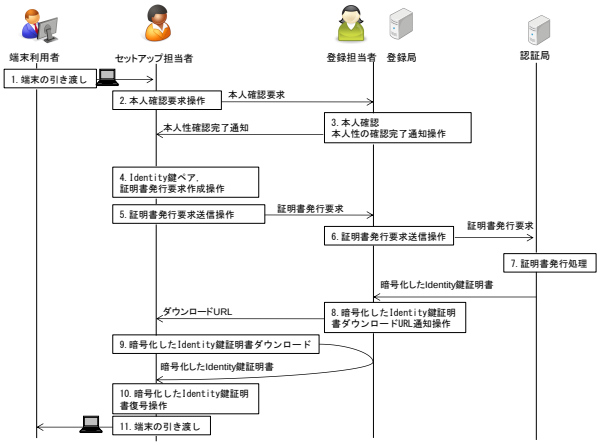

図 2　Identity 鍵証明書発行手続きの内容

8) 登録担当者からセットアップ担当者への暗号化した Identity 鍵証明書のダウンロード URL は署名付きメールで通知する．
9) SSL 相互認証と暗号化通信により，正規の登録局にセットアップ担当者はアクセスし，暗号化した証明書のダウンロード要求の改ざん・偽造を防げる．
10) 認証局は暗号化した Identity 鍵証明書に Identity 鍵のダイジェストを暗号化したものを添えている．その暗号化されたダイジェストで，証明書発行要求を出した Identity 鍵と対応した証明書かどうかを端末上で検証できる．
11) 端末利用者は証明書が発行されて引き渡されるまで端末を利用できないので，セットアップ担当者の責任のもとに不正な証明書発行を防げる．

その他，この手順では，登録担当者が証明書発行に必要な本人確認を担当することで，認証局と地理的に離れている登録局において証明書発行が可能である．

5. おわりに

本稿では，TPM による端末認証を行うための Identity 鍵証明書発行を企業で利用する際の流れと，その発行を支援するインターフェースを示した．これにより，登録局の登録担当者が端末利用者の本人性の保証に責任を持つことで，認証局と地理的に異なる環境でも，証明書発行が可能になった．

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”，IPSJ Magazine Vol.47 No.5, 2006 年 5 月
[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