電子化された証明書類の取得と提出に関する提案*

7K－2

榊原 裕之　江田敏郎　関 一則　岡田 謙一　松下 温†

慶應義塾大学 理工学部‡

1 はじめに

コンピューターネットワークの普及により、遠隔地において様々なサービスが享受できるようになった。電子メールなどは、従来の手紙を端末を目の前にして相手に送れるという、ネットワークならではのサービスの一つである。今後は益々デジタル情報の交換が活発になることが予想される。交換するデジタル情報の内容の機密性や出処を保証するためにセキュリティ技術を応用する必要性と方法が提案されてきている。我々は、日常生活で頻繁に利用する行政サービス (以下、簡単のため役所と称する) の発行する証明書類をデジタル情報として取り扱う場合の、取得方法とセキュリティ技術の応用方法について提案をする [3]。

2 セキュリティ技術と記法

証明書類のデジタル化において、その内容の正当性と安全な転送を実現するには、暗号技術が必要となる。暗号系としてはここでは、RSA 公開鍵暗号系を利用する [3]。

記法

KP_X	エンティティX の RSA の公開鍵
KS_X	エンティティX の RSA の秘密鍵
$E_k\{M\}$	M を鍵 k により暗号化する
$D_k\{C\}$	C を鍵 k により復号化する
$Sign_{U_i}\{M\}$	M を U_iがデジタル署名する

また、A || B は A と B を連結することを示す。

3 情報のデジタル化について

1. 発行された証明書の内容は役所が保証する
2. 発行される証明書は発行依頼人にのみ転送される
3. 複製がとれないこと
4. 現行の行政制度に準拠する手法であること

1については、現行の証明書は、多くの場合がその役所独自の用紙に内容を印字し、役所の印鑑が押されることにより保証される。これをデジタル情報に対して行なうにはデジタル署名技術の応用が有効である。

2については、公開鍵暗号系を用いて依頼者の公開鍵で必要な証明書等を暗号化することにより、依頼者のみが有効な内容を知ることができる。

3においては、現行の証明書の複製は不可能 (特殊な紙の使用による) なので、申請により必要枚数分の証明書を取得する形をとる。しかし、本提案で扱う証明書はデジタル情報なので管理方法によっては複製が可能となる。従って、証明書にタイムスタンプや通し番号などを付加して、役所側で管理し、証明書の最終的な受取人は役所に問い合わせて、その通し番号の証明書が使用済みかどうか調べる。

4については、以上の項目の他、発行対象者の限定や証明書の有効期限などが該当する。

4 実現方法

通信による証明書の取得と提出について実現方法を提案する。図1に、通信による証明書類発行の手続きと提出までの概念図を示す。暗号か技術の利用により安全に、証明書の発行、提出を実現する。ユーザーが証明書を複製した場合については、対策として役所においた証明書用データベースにおいて発行時に証明書の通し番号などを登録しておく。Uk(最終的な証明書の提出先) は提出された証明書の登録の有無を WO に問い合わせる。登録されていれば有効として使用する旨を WO に

*A proposal of acquirement and presentation of digital certificates

†Hiroyuki Sakakibara, Eda Toshiro, Kazunori Seki, Kenichi Okada, Yutaka Matsushita

‡Faculty of Science and Technology, Keio University

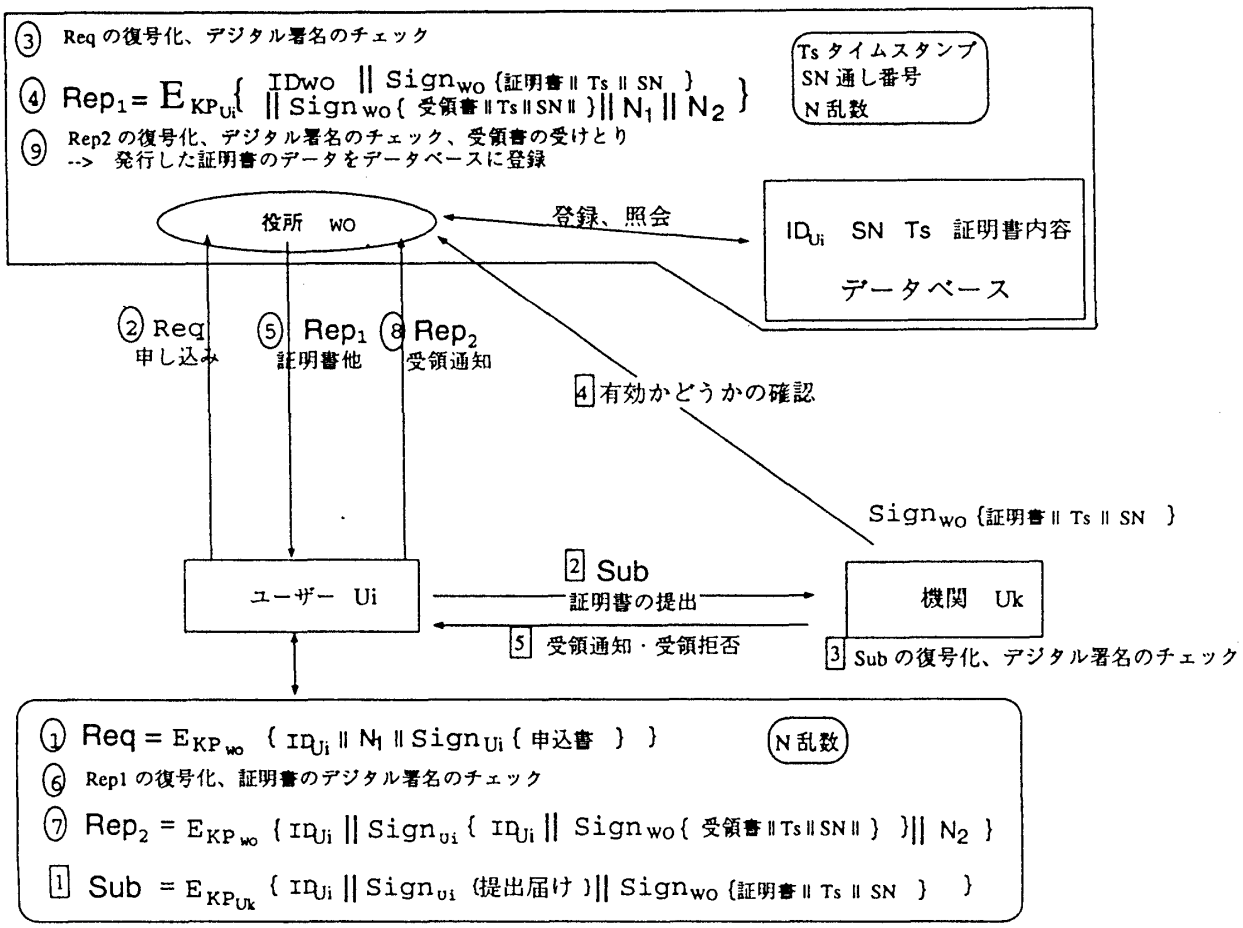

図 1: 概念図

通知し、同時に WO はデータを削除する。登録が無ければ複製の再利用　とみなし受領拒否を Ui に通知する。

5　検討

証明書類のデジタル情報化は現在のセキュリティ技術を用いれば実現可能と思われるが、証明書を画像データとして扱った場合に RSA 暗号は速度の点で問題が生じるものと思われる。最終的には通信で取得するのが簡便であろうが、実現段階における情報媒体を IC カードにすることが有効であると思われる。銀行のキャッシュディスペンサーの様な自動化窓口を役書に設置し、IC カードに証明書取得に必要な個人情報を収めておき、カード内に証明書を収める方法も考えられる [1]。或いは、カードからの情報により、自動化窓口で紙にプリントすることも可能であろう。IC カードに対する制御により、証明書の複製を防ぐことができ、有効である。

参考文献

[1] “平成 4 年度 電子メディアに関する調査研究 “IC カード等多目的利用に関する調査研究 報告書” ” 1993 年 3 月 財団法人 ニューメディア開発協会

[2] Davies,D.W.and Price, W.L. 著 上園忠弘 (代表) 訳、“ネットワーク・セキュリティ”, 日経マグロウヒル社, 1985

[3] 辻井重男・笠原正雄 編著, “暗号と情報セキュリティ”, 昭光堂, 1990.