相互認証に関する一考察

6F－1

吉武 淳
三菱電機（株）情報技術総合研究所

1．はじめに

電子商取引などのために認証局の設立が相次いできた。そして今後は異なる認証局間どうしの相互認証が重要になると考えられる。しかし、まだその技術面の方式だけでも、確立されたとは言い難い。

本稿では、電子商取引プロジェクト JapanNet における CommerceNet との相互認証実験（以下単に「実験」とする）を通して明らかになった問題点と解決策について述べる。

なお、実験は、階層型のエンティティ構成の 2 つの認証ドメインで、ルート CA どうしが X.509[2]で定める相互証明証対を使用して相互認証を行うというものであった。

2．相互認証の問題

相互認証での技術的課題については参考文献 [1]などに詳細に述べられている。実験でも同文献に述べられているような、暗号アルゴリズムの一致の問題などに直面し、プログラムの手直しなどを行った。

しかし、そのような既知の問題だけでなく、実験では次のような問題にも直面した。

・検証方式－特に相互証明証対中の証明証への辿り方の問題と、処理が"双方向"となる問題
・鍵の有効期間の問題
・失効の問題

また、実験を通し、ポリシーの体系化とオブジェクト識別子（以下 OID とする）の割当てに関するアイデアも生まれた。以下、順に説明する。

3．検証方式

3.1 相互証明証対中の証明証への辿り方

通常、証明証の検証において下位のエンティティの証明証から上位のエンティティの証明証を辿るには、issuer や authorityKeyIdentifier 等のフィールドが使われる。しかし、これらのフィールドでは、相互認証相手の CA の証明証（以下 P とする）から、自分の CA がその相手の CA に対して発行した証明証（相互証明証対中の証明証－以下 Q とする）を辿ることはできない（図 1 参照）。

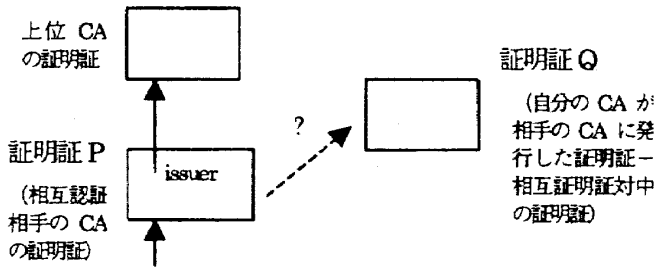

図1　証明証を辿る問題

この辿る方式として、実験では次の 3 つの方式が考えられた。

(1) P と Q での subject の一致の検証
(2) P と Q での subjectPublicKeyInfo の一致の検証
(3) 署名の検証

(1)だけでは、違う鍵でも subject を同じにすれば辿れてしまうため、この方式だけでは不十分である。(2)または(3)ならば単独でも十分であるが、実験では結局全部を組み合わせた方式を実装した。

3.2 処理が" 双方向" となる問題

一般に証明証の検証は下位のエンティティの証明証の検証から上位のエンティティの証明証の検証へ、というように bottom up に行われる。しかし、X.509[2]の policyConstraints の検証は（nameConstraints の検証も同様であるが）、階層型のエンティティ構成の場合、どれだけ下位のエンティティから、対象

A View on Cross Certification
Jun Yoshitake
Mitsubishi Electric Corp.

とするポリシーの OID がその証明証に設定されていることの検証を始めるかを指示する、top down のものである。このことは、原理的には、上位まで検証を行った後、そこから今度は下位に向かうという、"双方向"に検証を行う必要があることを意味している。これは、本質的には相互認証固有の問題ではないが、ポリシーの検証を特に意識する相互認証の実験を行ってみて初めてわかったことであった。

実験では 2 つのドメインが同じ OID のポリシーを持つものとして、その検証を bottom up の検証の中に含めた。また当然、上位の CA の証明証の検証を 1 度行った場合、その情報を持っておくことにより、毎回"双方向"の検証を行うことは避けられると考えられる。

4. 鍵の有効期間の問題

図 1 で証明証 Q の有効期間を、証明証 P の有効期間より短くするか長くするかという問題である。多くの場合、短くするか同じにすると考えられるが、最終的には各ドメインのポリシーと、そのすり合わせの問題であると考えられる。実験では同じとした。

5. 失効の問題

図 1 で証明証 P または Q が失効した時に、もう一方の証明証を失効させるかどうかという問題である。現在次のような案を考えているが、さらに検討が必要と考えている。

(1) 一方が鍵の危殆化の事由で失効した場合はもう一方も失効する。

(2) 一方が鍵の危殆化以外の事由で失効した場合は、もう一方を失効させるか否かはその具体的内容により判断する。

なお、いままで述べてきた証明証の辿り方の問題、有効期限の問題、失効の問題は、1 つの鍵に対して複数枚の証明証が発行される（図 1 で言えば、相互認証相手の CA の鍵に対して、P、Q という 2 つの証明証が発行される）という、相互認証ならではの特徴に起因する問題と考えられる。

6. ポリシーの体系化と OID の割当ての問題

2 つの認証局がすべての認証ポリシーについて一致するというのは非現実的である。やはり、ポリシーのある部分とある部分とが一致するから相互認証を行おうということになると考えられる。

認証ポリシーの検証はプログラムでは先に述べたように証明証中の OID の検証となる。上述したポリシーのある部分とある部分が一致することの検証のためには、ある認証局が持つすべてのポリシーに対してただ 1 つの OID が割り当てられているのではなく、その中がある単位でいくつかに分けられ、その単位ごとに OID が割り当てられているのが望ましいと考えられる。さらに、X.509[2]で述べられているような、世界共通とも言えるポリシーの採用という観点から考えると、世界共通にポリシーが体系立てて整理され、その中のある単位ごとに OID が割り当てられているのが望ましいと考えられる。

7. おわりに

JapanNet の実験を通しての相互認証の問題と解決策、新しいアイデアを示した。今後もこのような積重ねを継続し、よりよい相互認証の実現を目指す。

謝辞

本稿の作成にあたり、CommerceNet の方、NIST の方、東海大学の菊池先生、そして JapanNet の方々とのディスカッションがとても有効でした。ここに感謝の意を表します。

参考文献

1) FEDERAL PUBLIC KEY INFRASTRUCTURE (PKI) TECHNICAL SPECIFICATION: PART D - INTEROPERABILITY PROFILES, DRAFT, Federal PKI Technical Working Group (1995).

2) INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – THE DIRECTORY : AUTHENTICATION FRAMEWORK : ISO/IEC 9594-8 : 1995 (E), ITU-T Rec. X.509 (1993 E).