相互認証を実現する証明証検証ソフトウェアの試作

5T－3

榊原 裕之 、辻　宏郷 、坂上 勉
三菱電機(株) 情報技術総合研究所

1 はじめに

PKI(Public Key Infrastructure)において、公開鍵証明証(以下、証明証)の利用は必須であり、その正当性の検証は、安全性の確保の面で非常に重要である[3]。しかし、認証局の運用形態によって、証明証の検証が複雑化する問題が生じ[1]、PKIアプリケーションの開発者にとっては、証明証検証機能の実装は容易ではなかった。我々は、この複雑な検証の問題を解決した、ライブラリ形式の証明証検証ソフトウェアを試作した。当ソフトウェアは、簡易なAPIと高い汎用性を持ち、相互認証環境においても利用可能なので、PKIアプリケーションの証明証検証機能の実装に、容易に利用可能である。

2 証明証の検証について

2.1 認証局の運用形態と証明証の発行

証明証の検証に影響する、認証局の運用形態について述べる。本稿では、証明証の発行・被発行の関係にある一連の認証局で構成されるドメインを、「認証局の系列(以下、系列)」と定義する。次に代表例を示す。

① 階層型の運用：認証局が階層構造を持つ形態である(図1-(1)の系列 A のみ)。証明証は上位認証局から下位認証局に発行される。系列内のエンティティは、頂点の認証局である CA0a の証明証 Cert_CA0a を信用する。

② 相互認証型の運用：異なる系列の認証局同士が、一方向、又は、双方向に証明証を発行する形態である(図1-(1)の系列 A と系列 B)。この例では、認証局 CA1a が CA1b に証明証を発行している。

2.2 証明証のパスの構築

証明証を検証するためには、証明証のパスを構築する必要がある。証明証のパスとは、検証対象の証明証を端点とし、上位の一連の証明証を含み、信頼する証明証で終わるパスである[1]。証明証のパスは、検証対象の証明証と検証者が属する系列によって、構築方法が異なる。図1に認証局の形態と証明証のパスを示す(CRL：Certificate Revocation Listも含める)。

2.2.1 階層型における証明証のパス

図1の(1)において、検証者 v は、EEa と同じ系列 A に属し、Cert_CA0a を信用する。v が、同じ系列である A 内の EEa の証明証 Cert_EEa を検証する場合、証明証のパスは図1の(2)-1となる。

2.2.2 相互認証型における証明証のパス

検証対象 Cert_EEbが、系列 B に属する場合、証明証のパスは、"v が信用する Cert_CA0a に辿り着くように"構築する。この場合、パスは、相互認証用証明証 CertCross_CA1b を利用し、図1の(2)-2となる。

2.3 証明証の検証

証明証のパスが構築された後は、パス上の証明証の正当性を、有効期限、エクステンション、署名等について検証を行う。パス上の全ての証明証の正当性が確認できた時点で、検証対象の証明証が有効となる[2]。

このように、証明証の検証処理は煩雑であり、さらに、証明証の発行形態によっては、証明証のパスが複数存在する場合もある[1]。従って、PKI アプリケーションに対しては、様々な証明証のパスに対応した汎用的な検証機能が要求される。

3 証明証検証ソフトウェアの試作

我々は、PKI アプリケーションの証明証検証機能の実装用に、汎用的で、相互認証環境においても利用可能な証明証検証ソフトウェアを、ライブラリ形式で試作した。ソフトウェアは、証明証のパスを構築し、パス上の証明証、及び CRL を検証する。以下に概要を示す。

[入力]

(a) 検証対象の証明証
(b) 現在時刻
(c) 信頼する証明証(複数可)
(d) 上位証明証(複数候補)
(e) 信頼する CRL(複数候補)
(f) CRL(複数候補)

Public Key Certificate Verification Software for Cross Certification Environment
Hiroyuki SAKAKIBARA, Hirosato TSUJI, Tsutomu SAKAGAMI
Information Technology R&D Center, Mitsubishi Electric Corporation

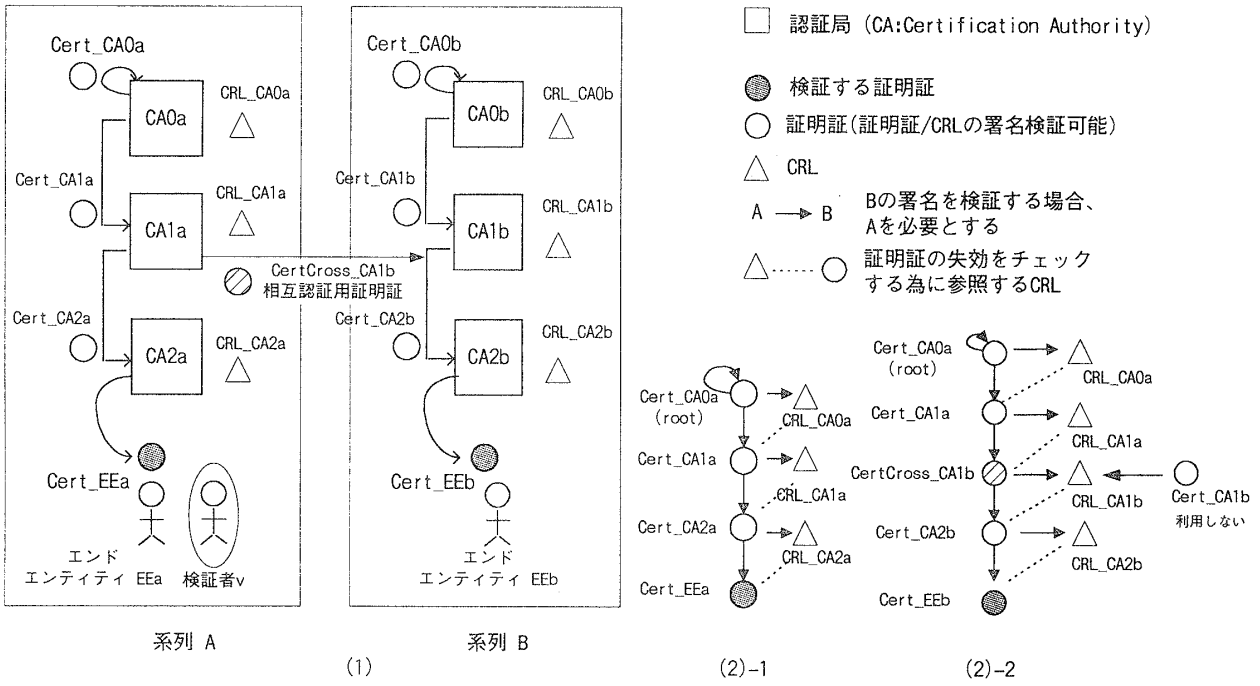

図 1 認証局の形態と証明証のパス

（ｇ） X.509[2]記載の、証明証の検証方式における状態変数値(パス上で受諾する certPolicy の ID 他)

（ｈ）その他　検証条件設定変数

（ｄ）の上位証明証に関しては、相互認証用証明証が含まれても良い。また、（ｄ），（ｆ）に関しては、パス構築に全く関係のないものが存在しても良い。

[動作]

（Ⅰ） 証明証のパスの構築

（Ⅱ） パスに関連付けられた CRL の検証

（Ⅲ） パス上の各証明証の検証

証明証のパスに関しては、2.2.1,2.2.2 で示した階層／相互認証の型にかかわらず、エクステンションの制限を満たし、かつ信頼する証明証に辿り着くパスを自動的に構築する。パスの候補が複数存在する場合も対応している。各動作は、X.509[2]記載の方式に準拠している。

[出力]

・検証成功時

(ア) 検証に成功した証明証

(イ) 検証に成功した CRL

(ウ) パス上で受諾された certPolicy のID

・検証失敗時

(エ) エラー理由

(オ) 検証に失敗した証明証

(カ) 検証に失敗した CRL

[特徴]　以下の特徴を持つ。

① 様々な証明証のパスに対応した検証が可能。

② 文献[1]に示される、「CRL の署名検証用の証明証のパスが、本体パスと別」の場合も検証可能である。

③ 入力項目（ｈ）において、CRL を利用しない(失効をチェックしない)検証を指定可能であり、この場合、出力項目の(ア)を、OCSP[4]など失効をチェックするサービスに与え、状態を確認することも可能である。

4 おわりに

相互認証環境でも、煩雑な証明証の検証処理が可能な、汎用性の高いライブラリ形式のソフトウェアを試作した。従来、容易ではなかったPKIアプリケーションの証明証検証機能の開発に、利用可能である。

[参考文献]

[1] 榊原、吉武：公開鍵証明証の検証方式の考察，情報処理学会 第一回コンピュータセキュリティ研究会発表予稿集 1-10, 1998

[2] ITU-T Recommendation X.509(1997E): Information Technology - Open Systems Interconnection – The Directory : Authentication Framework, 1997

[3] RFC 2459 : Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, January 1999

[4] RFC 2560 : X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP, June 1999