L-039　X.509 との後方互換性を持つ新しい公開鍵証明書フォーマット
An X.509-compatible new format of public key certificates

須賀 祐治 *
Yuji SUGA

あらまし　実生活のあらゆる場面で認証のために利用されるようになった X.509 公開鍵証明書は本来の「公開鍵とエンティティをバインドする」という機能を拡大する傾向が見られるようになってきた．v3 拡張部など証明書の独自解釈を行うことで，認可・承認，権限委譲，仮名，匿名など様々な用途に拡大解釈されている．本稿は，(1) 証明書フィールドの解釈の違いにより利用者の意図しない利用，(2) 解釈しないフィールドの存在，(3) 属性変更時の証明書再発行という X.509 証明書フォーマットの 3 つの問題点を指摘し，これらを解決するための新しい公開鍵証明書の形式を提案する．その際には X.509 証明書との後方互換性を保持できるように設計しており，次世代 PKI への移行がスムーズな方式である．

キーワード　PKI, X.509 公開鍵証明書, 部分抽出可能性，追記可能性

1　はじめに

公開鍵証明書は公開鍵とエンティティ(仮想世界における識別子/ID や現実世界に存在する個人もしくは組織体) を結びつける役割を持つ．現在最も一般的な公開鍵証明書フォーマットは ISO/IEC X.509 [1] で規定されている．X.509 公開鍵証明書は SSL/TLS, IPsec IKE, WS-Security, DNSSEC などのセキュリティプロトコル規定，さらに S/MIME, XML Signature/Encryption, PKCS#11 などのセキュアデータフォーマット規定で広く利用されている．証明書の利用時に証明書に内包されるデータ群に対する一般的な解釈は IETF PKIX WG [?] で定められている．しかし内容の解釈には前述したプロトコル規定やデータフォーマット規定等において独自の解釈や拡張が規定されている．そのほか，法規制に則るために拡張規定が存在する．つまり，証明書の用途・利用される環境に応じて個々のプロファイルが用意されており（公開鍵証明書の形式は同一だったとしても）プロファイルに応じた証明書解釈プログラムが必要であることを意味する．

証明書発行ルールと検証ルールが定められている，つまり，証明書フィールドの解釈に合意/共通認識が得られている証明書流通範囲を解釈レルムと呼ぶこととする．変換プログラムによる変換だけでは移行できない解釈レルムの一つに「利用可能な暗号アルゴリズム/鍵長」ポリシーによる解釈レルムがある．現在流通している RSA 以外の X.509 証明書として楕円曲線暗号ベースのものも存在するが，一般的に普及するまでに至っていないのが現状であり「楕円曲線暗号利用」レルムが存在しているものと捉えることができる．この場合，エンティティは同一であっても，公開鍵暗号アルゴリズムごとに異なる鍵ペアを保持する，つまり，異なるレルムごとに別々の証明書を保持する必要がある．

1.1　X.509 フォーマットの問題点

前節にて解釈レルムに応じて別々の証明書を保持する必要がある例を紹介した．これは X.509 フォーマットに関する以下の 3 つの問題に起因すると考えられる．

(P1) 解釈の違いによる意図しない利用

異なるレルム用の証明書を利用した場合，証明書フィールドの解釈の違いにより利用者の意図しない利用などの不具合が生じる可能性がある．現在の X.509 証明書の枠組みにおいてこの問題を解決するためには，証明書マネージャアプリケーションを利用するなどして，解釈レルムごとに証明書を登録し，他のレルムで利用できない仕組みを導入する方法が考えられる．

(P2) 解釈しないフィールドの存在

MD5 コリジョンを用いた中間 CA 証明書偽造攻撃では，X.509v3 拡張の一つである Netscape Comment Extension フィールドは一般的なブラウザの証明書検証時には無視する（パースはするが内容の解釈を行わない）ことを利用して，この拡張部分をダミーデータとして利用されている点が問題であった．今後もハッシュ関数の脆弱性を用いた同様の攻撃が発生する可能性が高い．この問題には，被署名データの定義域やデータ長に制約をつける方法と，証明書フィールドで解釈できない v3 拡張が存在した場合には証明書利用を中止する（証明書内のすべてのフィールドの解釈を MUST にする）方法の 2 つの解決が考えられる．しかしいずれの場合も解釈レルムの領域が狭まり，既に指摘したように管理すべき証明書が増大する問題が改めて発生することとなる．

* 株式会社インターネットイニシアティブ, 〒 101-0051 東京都千代田区神田神保町 1-105, Internet Initiative Japan Inc., Jinbocho Mitsui Bldg. 1-105 Kandajinbo-cho suga@iij.ad.jp

(P3) 属性変更時の証明書再発行

秘密鍵の漏洩・危殆化などの理由により公開鍵の差し替えを行う場合，証明書の再発行が伴う．同様に（公開鍵はそのままで）公開鍵情報以外の属性情報（例えばコンタクト先としてのメールアドレス）の一部を変更するだけでも再発行が必要となる．これは証書の裏書のように，公開鍵証明書に追記する機能がないために起こる問題である．現在の X.509 証明書の枠組みにおいては，被署名データが証明書に含まれる形式しか認められていないため，再発行を行うことでしか対処できない．再発行は CRL 発行など認証機関側の運用コスト増大の要因になりうる．

2 提案方式

X.509 証明書は前述したように様々な場面で登場しており，今後も利用され続けると考えられる．そのため後方互換性を考慮，つまり現 PKI で流通している X.509 証明書への変換可能な新しい公開鍵証明書を策定する時期が来ているという結論に至った．本章で提案する新しい公開鍵証明書は「証明書発行は 1 度で，ユーザは（解釈レルムに応じて）自由に開示する属性情報を選択可能とする」というシンプルな考えに基づく．具体的な提案方式を提示する前に，前章で指摘した X.509 に関する問題を解決するために，新しい公開鍵証明書が持つべき要件は部分抽出可能性（所有者が証明書の一部を抽出して解釈レルムのポリシーに応じて必要なフィールドのみ抽出できること），追記可能性（証明書発行時に包含されていない情報を証明書に追加できること），署名検証可能性（部分抽出または追記された証明書の署名検証が可能であること），後方互換性（X.509 証明書への変換が可能であること）であると考えた．

上記の要件を満たす具体的構成を以下に示す．本稿では RSA 署名のみ取り上げるが，同様に有限体上の加算を併用することで他の暗号方式にも適用可能である．本方式は大久保らによるリング署名 [2] をベースに構成している．本来リング署名が持つべき要件と異なるが，署名偽造可能性に関する安全性証明は原論文 [2] と同様に満たす．公開鍵 (n, e) と秘密鍵 d を持つ有上の RSA 暗号方式と一方向性ハッシュ関数 $H()$ において，以下の操作を行う．

1. $T_x \in Z_n$ をランダムに選択する
2. $C_y = H(M_y||T_x)$ を算出する
3. $T_y = C_y + T_x^e$ とする
4. $C_x = H(M_x||T_y)$ を算出する
5. $S = (T_x - C_x)^d$ と署名処理を行う

ここで M_x, M_y は解釈レルム $Realm_X$, $Realm_Y$ における被署名データとし，|| はデータ連結を意味するとする．T_x, T_y はノンスのように利用していると考えてよい．解釈レルム $Realm_X$ においては M_x が証明書として保証する内容であり，解釈レルム $Realm_Y$ に移動した際には M_y が証明書として保証する内容に変形する利用方法である．

署名データ S の検証は証明書 (M_y, T_x, S) もしくは (M_x, T_y, S) のいずれかに対して行われる．前者の場合，上記処理 (5) にて $S =? = (T_x - C_x)^d$ と S の正当性チェックを行うことで実現できる．また後者の場合，$C_x = H(M_x||T_y)$ と $T_x = C_x + S^e$ を算出し $C_y = H(M_y||T_x)$ から得られた C_y を用いて $T_y^e =? = T_y - C_y$ かどうかをチェックすることで署名の正当性が保証される．この具体的構成に加え，$T_x = H(M_z)^d$ ($M_z \in Realm_Z$ = X.509 の解釈レルム) を付け加えることで X.509 への後方互換性の要件を満たし，かつ各解釈レルムへの互換性を保持することができることがわかる．ただしナイーブな本方式には各解釈レルム上のメッセージ M_x, M_y, M_z 間のコンバータが必要である．しかし M_x とともに $H(M_y)$ を保持するなどコンバータが必要でないように構成することも可能である．

3 まとめ

本稿では X.509 証明書フォーマットの 3 つの問題点を指摘し，それを解決するための新しい公開鍵証明書の形式を提案した．今後プロトタイプを通して本手法の有効性とスケーラビリティについて検証を行う．また，解釈レルムを識別するための情報交換プロトコルを含め，実運用に向けての課題を取りまとめることを検討する．現時点では SSL/TLS のように，セキュア通信を行う前に暗号鍵やアルゴリズムを交換するサブプロトコルが存在するセキュリティプロトコルにおいて，軽微な拡張を行うことで解釈レルムを識別することが可能であると考えられる．

参考文献

[1] ITU-T Recommendation X.509 (08/05) — ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. 2005.

[2] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280, May 2008.

[3] K.Suzuki M.Abe, M.Ohkubo, 1-out-of-n signatures from a variety of keys. In *ASIACRYPT*, pp. 415–432, 2002.