

署名鍵漏洩対策における MAC を付与した電子署名の実装方式

松崎 孝大[†] 松浦 幹太[†]

[†] 東京大学生産技術研究所 〒153-8505 東京都目黒区駒場 4-6-1

E-mail: [†]{matu,kanta}@iis.u-tokyo.ac.jp

あらまし 安全な電子社会を実現するためには、電子署名の技術が必要であり、今後さらに普及していくと思われる。しかし、様々な要因によって署名鍵が第三者に漏洩する可能性は否定できず、署名偽造によって発生する紛争を解決する手段が必要である。MAC 付き電子署名は、署名鍵漏洩対策における電子署名方式であり、紛争を解決する証拠として署名対象データに対する MAC を利用する技術である。しかし、各要素技術の組み合わせである MAC 付き電子署名において、その署名トークンの構成方法までは十分に検討されていない。そこで、本稿では、実装に適した MAC 付き電子署名の署名トークンの分析を行い、規定した署名トークンを利用した場合に MAC 付き電子署名のシステムが満たすべき条件を明確にする。

キーワード PKI, 電子署名, 署名鍵漏洩, MAC

Implementation of Digital Signature Scheme with MAC against Signing-Key Compromise

Takahiro MATSUZAKI[†] and Kanta MATSUURA[†]

[†] Institute of Industrial Science, University of Tokyo.

4-6-1 Komaba, Meguro-ku, Tokyo 153-8505, Tokyo, Japan.

E-mail: [†]{matu,kanta}@iis.u-tokyo.ac.jp

Abstract It is expected that digital signatures will be popular increasingly in the future to achieve a safe electronic society. However, the possibility of signing-key exposure cannot be denied, then the technique to solve the dispute generated by the signature counterfeit is necessary. Digital signature scheme with MAC is the technique that use MAC on the data to be signed as evidence to solve a dispute. However, the signature token is not examined enough. In this paper, we analyze the signature token of digital signature scheme with MAC suitable for implementation, and clarify the conditions that the system should meet when the signature token is defined.

Key words PKI, Digital Signature, Signing-Key Exposure, MAC

1. はじめに

電子署名は、安全な電子商取引や電子政府等を実現するために必要不可欠な技術となっている。また、2001 年 4 月に電子署名法が施行され、電子署名が手書きの署名や押印と同等に適用する法的基盤が整備されたことによって、今後電子署名に対する関心は更に高まっていくと思われる。

電子署名を利用する際には、署名鍵の所有者による厳重な鍵管理が前提となる。署名鍵が不正な第三者に渡った場合、署名を偽造して正当な署名者になりすます攻撃が可能となり、既存の正当な署名も全て信頼できなくなる問題が発生する。そこで、署名鍵の管理には、IC カード等、ハードウェア内部の機密データを保護する機能を持つ記憶媒体を利用することが望まれる。

しかし、こうした場合においても、署名鍵の漏洩を完全に防

ぐことは困難であり、電子署名のアルゴリズムや実装方法の欠陥、ハードウェアの解析、または運用上の問題等の要因により、署名鍵が第三者に漏洩する可能性は否定できない。署名鍵が漏洩することによる影響は大きく、既存の PKI の枠組みでは十分な対応が困難なことから、署名鍵漏洩を前提とした対策技術が必要となってくる。

署名鍵漏洩を前提とした電子署名方式の既存研究として、フォワード・セキュア署名 [1]、Key-Insulated 署名 [2]、ヒステリシス署名 [3] [4]、実行ハードウェア確認タグ付き電子署名 [5] 等が挙げられる。これらの技術はいずれも研究段階であり、実システムに適用するためには、更なる検討が必要となっている。

同様に、MAC 付き電子署名 [6-9] は、署名鍵漏洩対策における電子署名方式の一つであり、署名生成と同時に署名対象データに対する MAC を生成し、署名鍵漏洩を要因とする署名偽造

本稿の構成は次の通りである。まず、2章ではMAC付き電子署名について説明し、その課題点を述べる。3章では、MAC付き電子署名の署名トークンを規定する。4章では、MACの検証可能性について分析する。最後に5章で本稿のまとめとする。

2.4 課題点

MAC 付き電子署名は、想定する環境において、鍵漏洩による署名偽造に対して有効な技術であるといえる。しかし、署名や MAC 等の要素技術を複数含む MAC 付き電子署名において、署名トークン内の対象データや属性情報等の構成法については述べられていない。署名トークンがシステムの要件を満たし、かつ効果を発揮する条件を明らかにする分析の必要性は、既に長期署名フォーマット [11] に関して示されている [12] [13]。そこで、実装手法の検討として、MAC 付き電子署名に関して署名トークンの分析を行う必要がある。

3. 署名トークン

3.1 要素技術

MAC 付き電子署名のアルゴリズムを実現するために必要な要素技術は主に、電子署名、ハッシュ関数、暗号、MAC である。署名トークンでは、各要素技術を実行するために必要な属性情報や対象データがフォーマットに従って含まれていなければならない。各要素技術のフォーマットは既に標準化されており十分な検討がなされている。したがって、MAC 付き電子署名の署名トークンは、各要素技術のフォーマットを基準として用いるのが望ましい。そこで、各要素技術のフォーマットを定義している標準として、CMS を利用する。

3.2 CMS

CMS (Cryptographic Message Syntax) は、署名文書や暗号文書等のフォーマットと構文を定めた標準であり、PKI のアプリケーションの多くに実装されている。CMS の構文は、OID で記述するコンテンツタイプと、コンテンツタイプの指定するコンテンツからなる。CMS では、署名データ、暗号データ等、6 種類のコンテンツタイプを定義している。MAC 付き電子署名の署名トークンでは、署名と MAC に係る部分のフォーマットとして、CMS のコンテンツタイプである署名データ (Signed-data)、と認証データ (Authenticated-data) を利用する。Fig.2 と Fig.3 は、それぞれ署名データ・コンテンツタイプと認証データコンテンツ・タイプのフォーマットである。

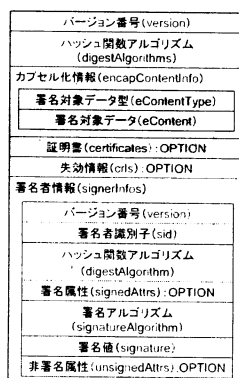


Fig. 2 Data Structure of Signed-Data in CMS

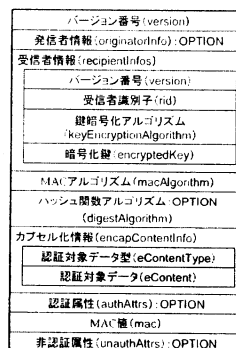


Fig. 3 Data Structure of Authenticated-Data in CMS

3.3 MAC 付き電子署名トークン

Fig.4 に、CMS に準拠した MAC 付き電子署名の署名トークンを示す。CMS の署名データ・コンテンツタイプの署名属性に、認証データ・コンテンツタイプを含む構造となっている。

受信者識別子として、署名検証者ではなく、IC カード情報管理者の証明書の発行者名およびシリアル番号、もしくは IC カード情報管理者の主体者鍵識別子を記述する。CMS の認証データ・コンテンツタイプでは、MAC の検証者と MAC 生成用秘密鍵を共有するために、受信者情報に暗号化した MAC 生成用秘密鍵を含める構造となっているが、MAC 付き電子署名では、IC カード情報管理者が MAC 生成用秘密鍵を特定するために必要とする署名生成回数である CNT を暗号化して含める。

MAC アルゴリズムの入力は署名対象データと同じ M であり、MAC 生成用秘密鍵によって MAC 値が計算される。一方、署名アルゴリズムの入力は、署名対象データ型と署名対象データ M のハッシュ値、そして、認証データ・コンテンツタイプ全体であり、署名生成用秘密鍵によって、署名値が計算される。

ここで規定した署名トークンに関して、MAC 検証可能性の観点から分析を行う。

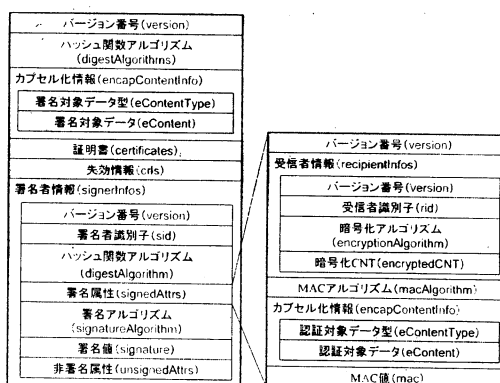


Fig. 4 Data Structure of Digital Signature with MAC

4. MAC 検証可能性

4.1 MAC 検証の要件

MAC 付き電子署名の検証を可能とするために必要な要件を以下に整理する。

- (1) 調停者は、事後的な MAC の検証に必要な全ての情報を、署名トークンを利用して正しく入手できる。
- (2) いかなる紛争時においても、調停者による MAC の検証は正しい結果が受理される。

以下では、3 章で規定した署名トークンの分析を行い、それぞれの MAC 検証要件を満足するための条件を明らかにする。

4.2 要件 (1)：調停者による MAC 検証情報の入手

調停者が MAC の検証を行うために最低限入手すべき情報としては以下のものが挙げられる。

- (a) 使用した MAC 生成用秘密鍵
- (b) 使用した MAC アルゴリズム
- (c) MAC 対象データ
- (d) MAC 値

MAC 付き電子署名のアルゴリズムでは、調停者は署名生成者から IC カードを受け取り ID を入手する。また、署名検証者からは保存されていた署名トークンを受け取る。紛争の当事者から入手した ID と署名トークンを利用して MAC の検証可能性を、入手すべき情報の観点から分析する。

(a) 使用した MAC 生成用秘密鍵

署名生成と同時に使用した MAC 生成用秘密鍵を入手するためには、まず、署名トークンの受信者識別子を利用して IC カード情報管理者を特定する。

次に、署名生成者から得る IC カードの ID をインデックスとして、当該 IC カードの MAC 生成用秘密鍵のシードを検索する。ここで、ID は IC カードに固有の識別子であり、MAC 付き電子署名では厳重な発行プロセスを経ていることを想定しているので、署名生成者に固有の識別子であるともいえる。よって、ID の本人性は保証されており、ID を要因として検証が不可能となる事態は生じないとする。

次に、MAC 生成用秘密鍵のシードからハッシュ関数による更新を繰り返して、署名生成時に利用した MAC 生成用秘密鍵を特定する。このとき、署名トークンに含まれている受信者情報から、IC カード情報管理者は暗号化 CNT を復号可能である。ここで、事後的な検証であることを考慮すると、暗号化に利用した IC カード情報管理者の公開鍵は何らかの理由により失効している可能性がある。そのため、IC カード情報管理者には、過去の公開鍵で暗号化されたデータを復号するために、鍵履歴の管理が要求される。また、MAC 生成用秘密鍵の更新に利用したハッシュ関数のアルゴリズムを、MAC の非認証属性等にも含める必要がある。

- (b) 使用した MAC アルゴリズム
- (c) MAC 対象データ
- (d) MAC 値

それぞれ署名トークン内で指定されており、調停者による入手が可能となっている。ただし、署名検証者から受け取

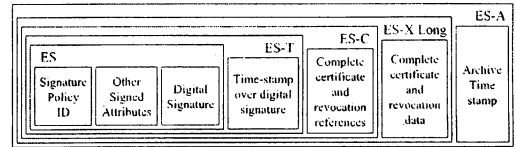


Fig. 5 ETSI TS 101 733

た署名トークンの長期に渡る非改ざん性を確認する必要がある。そこで、長期署名フォーマットである ETSI TS 101 733 (RFC3126) [11] を、MAC 付き電子署名とともに利用する。ETSI TS は、署名生成から一定期間後に改めて署名検証を行うための技術である。一定期間後において署名検証に必要なデータの損失や、CA 署名鍵の漏洩といった事態に対応可能であるとされており、その署名トークン (Fig.5) は標準的な技術仕様となっている。

ETSI TS の最も基本的な署名トークン (ES) は、CMS の署名データ・コンテンツタイプに準拠した構成となっているので、MAC 付き電子署名との整合性に優れている。また、ETSI TS は、署名生成者の署名鍵が漏洩した場合の対応が十分でない [14] ので、署名鍵漏洩を前提とした対策技術である MAC 付き電子署名とは互いに補完する関係にあるといえる。

以上より、MAC 付き電子署名の署名トークンを Fig.4 とした場合、調停者が MAC 検証に必要な情報を入手するために要求される条件を以下に示す。

- ・ 厳重な本人確認による IC カード発行
- ・ IC カード情報管理者による鍵履歴管理
- ・ 署名トークンの長期非改ざん性 (ETSI TS の利用)

4.3 要件 (2)：紛争時における MAC 検証可能性

4.3.1 紛争発生時の状況

まず、MAC 付き電子署名の利用において、調停者による MAC の検証を必要とする紛争が発生する状況を整理する。

紛争状況 1 (署名生成者による否認)

署名生成者は正当な手順により署名を生成する。署名を受け取った署名検証者による署名の検証結果は受理される。しかし、後日署名した事実を否認したいと考える署名生成者が調停者に依頼することによって紛争が発生する。

紛争状況 2 (攻撃者による署名偽造)

署名生成者の署名鍵を不当に入手した攻撃者を想定する。攻撃者は署名生成者になりすまして署名を作成する。偽造された署名を受け取った署名検証者による署名の検証結果は受理される。しかし、署名事実身に覚えのない署名生成者が調停者に依頼することによって紛争が発生する。

4.3.2 紛争状況 1 における MAC 検証可能性

署名生成者は正当な手順によって署名トークンを生成しているため、調停者が署名トークンから入手する情報の全ては、正当な MAC 検証結果、つまり当該署名トークンは確かに署名生成者の IC カードで生成されたものであるという判断を導く。署名生成者が MAC の検証に係るのは自らの IC カードの提出のみであるため、後日否認を考えた時点において、調停者によ

る MAC 検証を自らの望む結果とするための偽装工作は存在しない。よって、正当な MAC 検証を可能とするための条件は、要件 (1) を満たすための条件と同等である。

4.4 紛争状況 2 における MAC 検証可能性

攻撃者は署名生成者の署名生成用秘密鍵を入手すれば、偽造署名トークンを署名検証者に受理させることは可能である。さらに、調停者による MAC 検証によって、偽造署名トークンが攻撃対象である署名生成者の IC カードで生成されたものであるという不当な判断が導かれる可能性を考察する。

IC カード内の MAC 生成用秘密鍵は、処理を行う度にハッシュ関数によって更新される。したがって、複数回処理を実行して秘密鍵を推定する攻撃からは MAC 生成用秘密鍵が推定されることはない。攻撃者は偽造署名トークン内の MAC 値を生成するには任意の鍵を利用するしかない。この MAC 値と、調停者が MAC 検証時に再計算する MAC 値が等しければ、攻撃者による攻撃は完全に成功する。しかし、IC カード生成時点における IC カード情報管理者への *ID* と *MK* の登録が安全に行われていると想定している。攻撃された署名対象者が IC カードを調停者に提出することによって、調停者は MAC の検証に署名生成者の IC カードの *MK* を利用する。攻撃者が *MK* を入手することは困難であり、*MK* から導かれる MAC 検証用の鍵を自らが MAC 値を生成した任意の鍵と等しくすることも困難である。

よって、正当な MAC 検証を可能とするための条件は、要件 (1) を満たすための条件と同等である。さらに、紛争状況 2 においては、IC カード情報管理者による *MK* の厳重な管理が特に要求される。

5. ま と め

本稿では、署名鍵漏洩を前提とした対策技術の一つである MAC 付き電子署名について、その署名トークンに関する分析を行った。調停者による MAC の検証を可能とするための要件を整理し、規定した署名トークンを利用した場合に要件を満足するための条件を明らかにした。今後は、新しい署名トークンを検討するとともに、本稿では想定しなかった紛争の状況についても同様の分析を行う。また、実装を踏まえたシステムを構築するためには、調停者や IC カード情報管理者等、各エンティティの運用ポリシー等も検討していく必要がある。

文 献

- [1] M. Bellare and S. K. Miner: "A forward-secure digital signature scheme", *Proceedings of CRYPT'99*, LNCS 1666, Springer-Verlag, pp. 431-448 (1999).
- [2] Y. Dodis, J. Katz, S. Xu and M. Yung: "Strong key-insulated signature schemes", *Proceedings of PKC 2003*, LNCS 2567, Springer-Verlag, pp. 130-144 (2003).
- [3] 松本, 岩村, 佐々木, 松本: "暗号ブレイク対応電子署名アリバイ実現機構 (その 1) - コンセプトと概要 -", 情報処理学会研究報告 2000-CSEC-8 (2000).
- [4] 洲崎, 宮崎, 宝木, 松本: "暗号ブレイク対応電子署名アリバイ実現機構 (その 2) - 詳細方式 -", 情報処理学会研究報告 2000-CSEC-8 (2000).
- [5] 宇根, 松本: "実行ハードウェア確認タグ付きデジタル署名方式", 情報処理学会研究報告 2002-CSEC-18 (2002).
- [6] 小森, 花岡, 松浦, 須藤: "署名鍵漏洩問題における電子証拠物生

成技術について", 2003 年暗号と情報セキュリティシンポジウム予稿集, pp. 983-988.

- [7] 小森, 松浦, 須藤: "電子商取引における紛争解決のための電子証拠物に関する分析", 2002 年暗号と情報セキュリティシンポジウム予稿集, pp. 627-632.
- [8] 小森, 松浦, 須藤: "契約時に添える付加的な MAC に関する総合的分析", 情報処理学会研究報告 2001-CSEC-15 (2001).
- [9] 小森, 松浦, 須藤: "PKI に基づく C/S 型アプリケーションの安全性分析と証拠性評価", コンピュータセキュリティシンポジウム 2001 論文集, pp. 319-324.
- [10] 宇根: "デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策", 『金融研究』第 22 巻別冊第 1 号, 日本銀行研究所 (2003).
- [11] D. Pinkas, J. Ross and N. Pope: "Request for comments 3126: Electronic signature formats for long term electronic signatures" (2001).
- [12] 宇根, 田村, 岩下, 松本, 松浦, 佐々木: "CA 鍵漏洩時における ETSI TS 101 733 に基づく署名の検証可能性", コンピュータセキュリティシンポジウム 2004 論文集, pp. 445-450.
- [13] 宇根, 田村, 岩下, 松本, 松浦, 佐々木: "公開鍵証明書・失効情報欠損時における ETSI TS 101 733 に基づく署名の検証可能性", コンピュータセキュリティシンポジウム 2004 論文集, pp. 439-444 (2004).
- [14] 宇根, 田村, 岩下, 松本, 松浦, 佐々木: "デジタル署名の長期利用に関する考察-ETSI TS 101 733 の効果-", IMES DISCUSSION PAPER SERIES 2004-J-27, 日本銀行研究所 (2004).