

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4972165号
(P4972165)

(45) 発行日 平成24年7月11日 (2012. 7. 11)

(24) 登録日 平成24年4月13日 (2012. 4. 13)

(51) Int. Cl.	F I		
G06F 21/24 (2006.01)	G06F 21/24	1 6 6 E	
G06F 12/00 (2006.01)	G06F 12/00	5 3 7 H	
G06F 21/20 (2006.01)	G06F 21/24	1 6 6 B	
G06K 19/073 (2006.01)	G06F 21/20	1 3 4	
H04L 9/32 (2006.01)	G06K 19/00	P	
請求項の数 17 (全 66 頁) 最終頁に続く			

(21) 出願番号	特願2009-518355 (P2009-518355)	(73) 特許権者	506197901
(86) (22) 出願日	平成19年6月28日 (2007. 6. 28)		サンディスク コーポレーション
(65) 公表番号	特表2009-543210 (P2009-543210A)		アメリカ合衆国、95035、カリフォルニア州、ミルピタス、マッカシー ブルバード 601
(43) 公表日	平成21年12月3日 (2009. 12. 3)	(74) 代理人	100075144
(86) 国際出願番号	PCT/US2007/015430		弁理士 井ノ口 壽
(87) 国際公開番号	W02008/008243	(72) 発明者	ホルツマン, マイケル
(87) 国際公開日	平成20年1月17日 (2008. 1. 17)		アメリカ合衆国、95014、カリフォルニア州、クペルティーノ、バーンハートプレイス 7602
審査請求日	平成22年6月23日 (2010. 6. 23)	(72) 発明者	バージライ, ロン
(31) 優先権主張番号	60/819, 507		イスラエル国、25147、クファールーブラディム、メロン ストリート 67
(32) 優先日	平成18年7月7日 (2006. 7. 7)		
(33) 優先権主張国	米国 (US)		
(31) 優先権主張番号	11/557, 039		
(32) 優先日	平成18年11月6日 (2006. 11. 6)		
(33) 優先権主張国	米国 (US)		
最終頁に続く			

(54) 【発明の名称】 アイデンティティオブジェクトを使用する制御システムおよび方法

(57) 【特許請求の範囲】

【請求項 1】

不揮発性記憶装置であって、
コントローラと、

秘密鍵と公開鍵とを備える鍵対と、前記鍵対を認証するための証明書とを記憶する不揮発性メモリと、

実体を認証するための前記コントローラによって使用可能な情報と、さらに前記実体が前記コントローラによって認証され次第、前記実体を許可できるかどうかを判断して前記鍵対と証明書とにアクセスするための前記コントローラによって使用可能な情報とを含むアクセス制御構造と、を備え、

前記コントローラは、

前記アクセス制御構造を用いて前記不揮発性記憶装置に対して実体を認証し、

前記実体が成功裏に認証された後、データとコマンドを受信して前記実体からのデータに署名し、

秘密鍵を使用してデータまたは前記データから検索される情報に署名し、

前記証明書と前記データまたは前記データから検索される情報とを前記実体へ送信するように操作される不揮発性記憶装置。

【請求項 2】

請求項 1 記載の不揮発性記憶装置において、

前記不揮発性メモリとコントローラとを囲い込む筐体をさらに備える不揮発性記憶装置

。

【請求項 3】

請求項 2 記載の不揮発性記憶装置において、
前記筐体は、カードの形状を有する不揮発性記憶装置。

【請求項 4】

請求項 1 記載の不揮発性記憶装置において、
前記証明書は、証明書チェーンである不揮発性メモリシステム。

【請求項 5】

請求項 1 記載の不揮発性記憶装置において、
前記不揮発性メモリは、フラッシュメモリである不揮発性記憶装置。

10

【請求項 6】

請求項 1 記載の不揮発性記憶装置において、
前記アクセス制御構造によって、認証済み実体のみがデータにアクセスできる不揮発性記憶装置。

【請求項 7】

請求項 1 記載の不揮発性記憶装置において、
前記コントローラは、前記アクセス制御構造を用いて実体を認証し、公開鍵を証明するために前記証明書を認証済み実体に供給する不揮発性記憶装置。

【請求項 8】

実体のアイデンティティの証拠を提供する方法であって、
(i) コントローラと、(i i) 秘密鍵と公開鍵とを備える鍵対と、前記鍵対を認証するための証明書とを記憶する不揮発性メモリと、(i i i) 実体を認証するための前記コントローラによって使用可能な情報と、さらに前記実体が前記コントローラによって認証され次第、前記実体を許可できるかどうかを判断して前記鍵対と証明書とにアクセスするための前記コントローラによって使用可能な情報とを含むアクセス制御構造とを備える不揮発性記憶装置内で次のステップを実行するステップであって、
前記アクセス制御構造を用いて前記不揮発性記憶装置に対して実体を認証するステップと、

20

前記実体が成功裏に認証された後、

データとコマンドを受信して前記実体からのデータに署名するステップと、
秘密鍵を使用してデータまたは前記データから検索される情報に署名するステップと

30

、
前記証明書と前記データまたは前記データから検索される情報とを前記実体へ送信するステップと、
を含む方法。

【請求項 9】

請求項 8 記載の方法において、
前記実体が成功裏に認証された後、公開鍵を証明するために前記証明書を実体に供給するステップと、

公開鍵によって暗号化されたデータを受信するステップと、
秘密鍵を用いてデータを復号化するステップと、
をさらに含む方法。

40

【請求項 10】

請求項 8 記載の方法において、
前記不揮発性記憶装置は、前記不揮発性メモリとコントローラとを囲い込む筐体を備える方法。

【請求項 11】

請求項 10 記載の方法において、
前記筐体は、カードの形状を有する方法。

【請求項 12】

50

請求項 8 記載の方法において、
前記証明書は、証明書チェーンである方法。

【請求項 13】

請求項 8 記載の方法において、
前記不揮発性メモリは、フラッシュメモリである方法。

【請求項 14】

請求項 8 記載の方法において、
前記アクセス制御構造によって、認証済み実体のみがデータにアクセスできる方法。

【請求項 15】

請求項 8 記載の方法において、
前記コントローラは、前記アクセス制御構造を用いて実体を認証し、公開鍵を証明するために前記証明書を認証済み実体に供給する方法。

10

【請求項 16】

請求項 1 記載の不揮発性記憶装置において、
前記実体は、取り外し可能な状態で記憶装置へ接続されるホスト装置を備える不揮発性記憶装置。

【請求項 17】

請求項 8 記載の方法において、
前記実体は、取り外し可能な状態で記憶装置へ接続されるホスト装置を備える方法。

【発明の詳細な説明】

20

【技術分野】

【0001】

本発明は、一般的にはメモリシステムに関し、具体的には汎用コンテンツ制御機能を備えるメモリシステムに関する。

【背景技術】

【0002】

関連出願の相互参照

本願は、2006年7月7日に出願された米国仮特許出願第60/819,507号（特許文献1）の利益を主張する。

【0003】

30

本願は、2005年12月20日に出願された米国特許出願第11/313,870号（特許文献2）に関し、この出願は2004年12月21日に出願された米国仮特許出願第60/638,804号（特許文献3）の利益を主張する。本願はさらに、2005年12月20日に出願された米国特許出願第11/314,411号（特許文献4）に関する。本願はさらに、2005年12月20日に出願された米国特許出願第11/314,410号（特許文献5）に関する。本願はさらに、2005年12月20日に出願された米国特許出願第11/313,536号（特許文献6）に関する。本願はさらに、2005年12月20日に出願された米国特許出願第11/313,538号（特許文献7）に関する。本願はさらに、2005年12月20日に出願された米国特許出願第11/314,055号（特許文献8）に関する。本願はさらに、2005年12月20日に出願された米国特許出願第11/314,052号（特許文献9）に関する。本願はさらに、2005年12月20日に出願された米国特許出願第11/314,053号（特許文献10）に関する。

40

【0004】

本願は、2006年11月6日に出願されたHoltzmanらの「Content Control Method Using Certificate Chains」という米国特許出願第11/557,028号（特許文献11）と、2006年11月6日に出願されたHoltzmanらの「Content Control System Using Certificate Chains」という米国特許出願第11/557,010号（特許文献12）と、2006年11月6日に出願されたHoltzmanらの「Content Control Method Using Certificate Revocation Lists」という米国特許出願第11/557,006号（特許

50

文献13)と、2006年11月6日に出願されたHoltzmanらの「Content Control System Using Certificate Revocation Lists」という米国特許出願第11/557,026号(特許文献4)と、2006年11月6日に出願されたHoltzmanらの「Content Control Method Using Versatile Control Structure」という米国特許出願第11/557,049号(特許文献15)と、2006年11月6日に出願されたHoltzmanらの「Content Control System Using Versatile Control Structure」という米国特許出願第11/557,056号(特許文献16)と、2006年11月6日に出願されたHoltzmanらの「Method for Controlling Information Supplied From Memory Device」という米国特許出願第11/557,052号(特許文献17)と、2006年11月6日に出願されたHoltzmanらの「System for Controlling Information Supplied From Memory Device」という米国特許出願第11/557,051号(特許文献18)と、2006年11月6日に
10
出願されたHoltzmanらの「Control Method Using Identity Objects」という米国特許出願第11/557,041号(特許文献19)と、2006年11月6日に出願されたHoltzmanらの「Control System Using Identity Objects」という米国特許出願第11/557,039号(特許文献20)とに関する。

【0005】

これらの特許出願は、あたかも本願にもれなく記載されているかのごとく、それぞれの全体が本願明細書において参照により援用されている。

【0006】

フラッシュメモリカード等の記憶装置が、写真等のデジタルコンテンツを記憶する記憶媒体として好んで使われるようになってきている。フラッシュメモリカードはタイプの異なるメディアコンテンツの配布に使われる場合がある。コンピュータ、デジタルカメラ、携帯電話機、個人用携帯情報端末(PDA)、MP3プレーヤをはじめとするメディアプレーヤ等のホスト装置の多様化が進み、フラッシュメモリカードに記憶されたメディアコンテンツを再生できるようになっている。このため、フラッシュメモリカードやその他の可搬型記憶装置がデジタルコンテンツの配布手段として幅広く利用される可能性が大きい。

【0007】

用途によっては、メモリカード等のメモリ装置と関連付けられた実体に自身のアイデンティティの証拠を提示することが求められる。このアイデンティティの証拠を容易く入手できないと都合が生じることがある。この他にも用途によっては、メモリカード等のメモリ装置に記憶されるデータを安全な方法で保護することが必要な場合がある。

【先行技術文献】

【特許文献】

【0008】

【特許文献1】米国仮特許出願第60/819,507号

【特許文献2】米国特許出願第11/313,870号

【特許文献3】米国仮特許出願第60/638,804号

【特許文献4】米国特許出願第11/314,411号

【特許文献5】米国特許出願第11/314,410号

【特許文献6】米国特許出願第11/313,536号

【特許文献7】米国特許出願第11/313,538号

【特許文献8】米国特許出願第11/314,055号

【特許文献9】米国特許出願第11/314,052号

【特許文献10】米国特許出願第11/314,053号

【特許文献11】米国特許出願第11/557,028号

【特許文献12】米国特許出願第11/557,010号

【特許文献13】米国特許出願第11/557,006号

【特許文献14】米国特許出願第11/557,026号

【特許文献15】米国特許出願第11/557,049号

【特許文献16】米国特許出願第11/557,056号

10

20

30

40

50

【特許文献 17】米国特許出願第 11 / 557, 052 号

【特許文献 18】米国特許出願第 11 / 557, 051 号

【特許文献 19】米国特許出願第 11 / 557, 041 号

【特許文献 20】米国特許出願第 11 / 557, 039 号

【発明の概要】

【0009】

アイデンティティオブジェクトと呼ばれるオブジェクトは、公開鍵と秘密鍵からなる対と、対の公開鍵が真正であることを証明するために証明機関によって発行される少なくとも 1 つの証明書とを備える。一実施形態において、提供されるデータまたはデータから検索される信号に、秘密鍵を使って署名することにより、このオブジェクトを同定の証拠として使用してもよい。アイデンティティオブジェクトはアイデンティティの証拠として不揮発性メモリに記憶され、このメモリはコントローラによって制御されてもよい。好ましくは、メモリとコントローラとを筐体で取り囲む。

10

【0010】

別の実施形態において、アイデンティティオブジェクトがアイデンティティの証拠としてメモリシステムの不揮発性メモリに記憶される。このメモリシステムは脱着自在な状態でホスト装置へ接続される。ホスト装置の認証に成功した後は、ホスト装置からのデータまたは前記データから検索される信号をオブジェクトの秘密鍵を用いて暗号化し、少なくとも 1 つの証明書と暗号化されたデータまたは信号とをホスト装置へ送信する。

【0011】

20

さらに別の実施形態において、メモリシステムの制御データ構造によって実体が認証された後に、アイデンティティオブジェクトの公開鍵と、公開鍵を証明するための少なくとも 1 つの証明書とを、実体へ提供する。この実施形態の一実用的応用において、アイデンティティオブジェクトの公開鍵によって暗号化された暗号化データを実体から受信する場合、メモリシステムは、アイデンティティオブジェクトの中にある秘密鍵を使って暗号化データを復号化できる。アイデンティティオブジェクトと少なくとも 1 つの証明書とが不揮発性メモリに記憶され、このメモリはコントローラによって制御される。好ましくは、メモリとコントローラとを筐体で取り囲む。

【0012】

別の実施形態において、メモリシステムの不揮発性メモリにアイデンティティオブジェクトが記憶されてもよい。このメモリシステムは脱着自在な状態でホスト装置へ接続される。ホスト装置の認証に成功した後は、アイデンティティオブジェクトの公開鍵と、公開鍵を証明するための少なくとも 1 つの証明書とが、ホスト装置に提供される。アイデンティティオブジェクトの公開鍵によって暗号化された暗号化データをホスト装置から受信したメモリシステムは、アイデンティティオブジェクトの中にある秘密鍵を使って暗号化データを復号化する。

30

【0013】

ここで参照する特許、特許出願、記事、書籍、仕様書、規格書、その他の出版物、文書、物事はいずれも、あらゆる目的のためにその全体が本願明細書において参照により援用されている。援用する出版物、文書、または物事のいずれかと本願明細書の本文との間で用語の定義または使用に矛盾や食い違いがある場合、本願明細書における用語の定義または使用が優先するものとする。

40

【図面の簡単な説明】

【0014】

【図 1】本発明を例示するのに有用である、ホスト装置と通信するメモリシステムのブロック図である。

【図 2】本発明の種々の実施形態を例示するのに有用である、特定のパーティションと暗号化ファイルへのアクセスをアクセス方針と認証手続きとによって制御するメモリの種々のパーティションと種々のパーティションに記憶される非暗号化および暗号化ファイルとの概略図である。

50

【図 3】メモリ内の種々のパーティションを示すメモリの概略図である。

【図 4】本発明の種々の実施形態を例示するのに有用である、パーティション内のいくつかのファイルが暗号化される図 3 に示すメモリの種々のパーティションのファイルロケーションテーブルの概略図である。

【図 5】本発明の種々の実施形態を例示するのに有用である、アクセス制御記録グループ内のアクセス制御記録と対応する鍵参照符との概略図である。

【図 6】本発明の種々の実施形態を例示するのに有用である、アクセス制御記録グループとアクセス制御記録とによって形成されるツリー構造の概略図である。

【図 7】ツリーの形成プロセスを例示するための、アクセス制御記録グループからなる 3 つの階層ツリーを示すツリーの概略図である。

10

【図 8 A】システムアクセス制御記録を作成し、かつ使用する場合にホスト装置とメモリカード等のメモリ装置とによって実行されるプロセスを示すフローチャートである。

【図 8 B】システムアクセス制御記録を作成し、かつ使用する場合にホスト装置とメモリカード等のメモリ装置とによって実行されるプロセスを示すフローチャートである。

【図 9】種々の実施形態を例示するのに有用である、システムアクセス制御記録を使ってアクセス制御記録グループを作成するプロセスを示すフローチャートである。

【図 10】アクセス制御記録を作成するプロセスを示すフローチャートである。

【図 11】階層ツリーの一応用を例示するのに有用である、2 つのアクセス制御記録グループの概略図である。

【図 12】特定の権利を委譲するプロセスを示すフローチャートである。

20

【図 13】図 12 の委譲プロセスを例示するための、アクセス制御記録グループとアクセス制御記録との概略図である。

【図 14】暗号化および／または復号化の目的で鍵を作成するプロセスを示すフローチャートである。

【図 15】アクセス制御記録に従いアクセス権および／またはデータアクセス権限を削除するプロセスを示すフローチャートである。

【図 16】アクセス権および／またはアクセス権限が削除されたか、あるいは期限切れになった場合にアクセスを要求するプロセスを示すフローチャートである。

【図 17 A】本発明の種々の実施形態の例示に有用である、認証ルール構造と暗号鍵アクセス許諾方針の構成を示す概略図である。

30

【図 17 B】本発明の種々の実施形態の例示に有用である、認証ルール構造と暗号鍵アクセス許諾方針の構成を示す概略図である。

【図 18】方針に従い被保護情報へのアクセスを制御する代替的な方法を示すデータベース構造のブロック図である。

【図 19】パスワードを用いた認証プロセスを示すフローチャートである。

【図 20】多数のホスト証明書チェーンを示す図である。

【図 21】多数のデバイス証明書チェーンを示す図である。

【図 22】一方向および相互認証方式のプロセスを示すプロトコル図である。

【図 23】一方向および相互認証方式のプロセスを示すプロトコル図である。

【図 24】本発明の一実施形態を例示するのに有用である、証明書チェーンの図である。

40

【図 25】本発明の別の実施形態を例示するための、メモリ装置へ最終証明書を送信する場合のホストによって送信される証明書バッファに先行する制御セクタ内の情報を示す表であって、この証明書が証明書チェーンにおける最終証明書であることを伝える標示を示す。

【図 26】メモリカードがホスト装置を認証する認証方式でカードとホストのプロセスをそれぞれ示すフローチャートである。

【図 27】メモリカードがホスト装置を認証する認証方式でカードとホストのプロセスをそれぞれ示すフローチャートである。

【図 28】ホスト装置がメモリカードを認証する認証方式でカードとホストのプロセスをそれぞれ示すフローチャートである。

50

【図 29】ホスト装置がメモリカードを認証する認証方式でカードとホストのプロセスをそれぞれ示すフローチャートである。

【図 30】本発明の別の実施形態を例示するための、メモリ装置に記憶された証明書失効リストがホスト装置によって検索される場合にホスト装置とメモリ装置とによってそれぞれ実行されるプロセスを示すフローチャートである。

【図 31】本発明の別の実施形態を例示するための、メモリ装置に記憶された証明書失効リストがホスト装置によって検索される場合にホスト装置とメモリ装置とによってそれぞれ実行されるプロセスを示すフローチャートである。

【図 32】本発明のさらに別の実施形態を示すための、証明書失効リスト内のフィールドを示す証明書失効リストの図である。

10

【図 33】証明書失効リストを使って証明書をベリファイするカードとホストのプロセスをそれぞれ示すフローチャートである。

【図 34】証明書失効リストを使って証明書をベリファイするカードとホストのプロセスをそれぞれ示すフローチャートである。

【図 35】カードがホストへ送信されるデータに署名し、かつホストからのデータを復号化するカードプロセスを示すフローチャートである。

【図 36】カードがホストへ送信されるデータに署名する場合のホストプロセスを示すフローチャートである。

【図 37】ホストが暗号化データをメモリカードへ送信する場合のホストプロセスを示すフローチャートである。

20

【図 38】一般情報および非公開情報クエリのプロセスをそれぞれ示すフローチャートである。

【図 39】一般情報および非公開情報クエリのプロセスをそれぞれ示すフローチャートである。

【図 40A】本発明の一実施形態を例示するための、ホスト装置へ接続されたメモリ装置（フラッシュメモリカード等）におけるシステムアーキテクチャの機能ブロック図である。

【図 40B】図 40A の S S M コアの内部ソフトウェアモジュールの機能ブロック図である。

【図 41】使い捨てパスワードを生成するシステムのブロック図である。

30

【図 42】使い捨てパスワード（O T P）シード提供と O T P 生成とを示す機能ブロック図である。

【図 43】シード提供段階を示すプロトコル図である。

【図 44】使い捨てパスワード生成段階を示すプロトコル図である。

【図 45】D R M システムを示す機能ブロック図である。

【図 46】ライセンスオブジェクトの中で鍵が提供される場合のライセンス提供とコンテンツダウンロードのプロセスを示すプロトコル図である。

【図 47】再生操作のプロセスを示すプロトコル図である。

【図 48】ライセンスオブジェクトの中で鍵が提供されない場合のライセンス提供とコンテンツダウンロードのプロセスを示すプロトコル図である。

40

【0015】

図面は、本発明の態様の様々な実施形態の特徴を示すものである。説明を簡潔にするため、本願では同じ構成要素を同じ数字で標示する。

【発明を実施するための形態】

【0016】

図 1 のブロック図は、本発明の様々な態様を実装できる代表的なメモリシステムを示す。図 1 に示すように、メモリシステム 10 は、中央演算処理装置（C P U）12 と、バッファ管理部（B M U）14 と、ホストインターフェイスモジュール（H I M）16 と、フラッシュインターフェイスモジュール（F I M）18 と、フラッシュメモリ 20 と、周辺アクセスモジュール（P A M）22 とを含む。メモリシステム 10 は、ホストインターフ

50

ェイスバス26とポート26aとを通じてホスト装置24と通信する。フラッシュメモリ20はNANDタイプのものであってもよく、ホスト装置24のためのデータ記憶域を提供し、ホスト装置24はデジタルカメラ、パーソナルコンピュータ、個人用携帯情報端末(PDA)、MP3プレーヤ等のデジタルメディアプレーヤ、携帯電話機、セットトップボックス、その他のデジタル装置または家電品であってもよい。CPU12のソフトウェアコードもフラッシュメモリ20に記憶できる。FIM18は、フラッシュインターフェイスバス28とポート28aとを通じてフラッシュメモリ20へ接続する。HIM16はホスト装置への接続に適している。周辺装置アクセスモジュール22はCPU12との通信においてFIM、HIM、およびBMU等の適切なコントローラモジュールを選択する。一実施形態において、点線の枠内にあるシステム10の全構成要素をメモリカードまたはスティック10'等の単独装置で囲い込み、好ましくはこれに封入してもよい。メモリシステム10は脱着自在な状態でホスト装置24へ接続されるため、多数の異なるホスト装置からシステム10の内容にアクセスできる。

10

【0017】

以降の説明ではメモリシステム10をメモリ装置10と呼ぶ場合があり、あるいは単にメモリ装置または装置と呼ぶ場合がある。ここではフラッシュメモリを参照しながら本発明を例示するが、本発明は、磁気ディスク、光CD等のタイプの異なるメモリや他の書き換え可能な不揮発性メモリシステムにも応用できる。

【0018】

バッファ管理部14は、ホストダイレクトメモリアクセス(HDMA)32と、フラッシュダイレクトメモリアクセス(FDMA)34と、アービタ36と、バッファランダムアクセスメモリ(BRAM)38と、クリプトエンジン40とを含む。アービタ36は共有バスアービタであるため、常に1つのみのマスタまたはイニシエータ(HDMA32、FDMA34、またはCPU12)が稼動し、そのスレーブまたはターゲットはBRAM38である。アービタは、しかるべきイニシエータ要求をBRAM38へ振り向ける役割を果たす。HDMA32とFDMA34は、HIM16、FIM18、およびBRAM38、またはCPUランダムアクセスメモリ(CPU RAM)12a間でデータの転送を担当する。HDMA32の動作とFDMA34の動作は従来どおりであり、ここで詳述する必要はない。BRAM38は、ホスト装置24とフラッシュメモリ20との間で受け渡しされるデータを記憶するために使用する。HDMA32とFDMA34は、HIM16/FIM18およびBRAM38またはCPU RAM12a間でデータを転送し、さらにセクタの終了を指示する役割を果たす。

20

30

【0019】

メモリシステム10は、一実施形態において、暗号化および／または復号化に用いる鍵値を生成し、この値は、好ましくはホスト装置24等の外部装置にとって事実上アクセス不能である。代替的に、システム10の外部で、例えばライセンスサーバによって、鍵値を生成し、システム10へ送信することもできる。鍵値を生成する方法にかかわらず、いったんシステム10に記憶された鍵値にアクセスできるものは認証済み実体のみとなる。しかし、ホスト装置はメモリシステム10におけるデータの読み書きをファイルの形で行うため、暗号化と復号化は通常であればファイル単位で行われる。メモリ装置10は、タイプが異なる他の多数の記憶装置と同様に、ファイルを管理しない。メモリ20は、ファイルの論理アドレスを識別するファイルアロケーションテーブル(FAT)を記憶するが、このFATにアクセスし管理するのは通常であればホスト装置24であって、コントローラ12ではない。このため、ある特定のファイルのデータを暗号化する場合、コントローラ12はメモリ20におけるこのファイルのデータの論理アドレスをホスト装置に送信してもらう必要があり、このため、システム10はこのファイルのデータを見つけ、システム10のみが使用できる鍵値を使ってデータを暗号化および／または復号化できる。

40

【0020】

ファイルデータの暗号処理においてホスト装置24とメモリシステム10の双方が同じ鍵を参照するための名前を用意するため、ホスト装置は、システム10によって生成され

50

るか、あるいはシステム 10 へ送信される各鍵値につき参照符を提供し、この参照符とは要するに鍵 ID であってもよい。ホスト 24 は、システム 10 によって暗号処理される各ファイルに鍵 ID を割り振り、システム 10 は、データの暗号処理に用いる各鍵値にホストから提供される鍵 ID を割り振る。よって、ホストはデータの暗号処理を要求するときに、その要求を、鍵 ID と、メモリ 20 から取り出すか、またはメモリ 20 に記憶するデータの論理アドレスと併せて、システム 10 へ送信する。システム 10 は鍵値を生成または受信し、ホスト 24 から提供される鍵 ID をその値に割り振り、暗号処理を実行する。メモリシステム 10 の動作を変える必要はなく、メモリシステム 10 は、鍵値に対する独占的アクセス等、鍵を使った暗号処理を完全に制御できる。換言すると、いったん鍵値がシステム 10 に記憶されるか、あるいはシステム 10 によって生成されたら、システムは、FAT の独占的制御によるファイルの管理をホスト 24 に任せつつ、暗号処理に用いる鍵値の管理を一手に引き受ける。鍵値がメモリシステム 10 に記憶された後、ホスト装置 24 はデータの暗号処理に用いる鍵値の管理に関与しない。

10

【0021】

ホスト 24 から提供される鍵 ID とメモリシステムへ送信されるか、あるいはメモリシステムによって生成される鍵値は、一実施形態において、これ以降「コンテンツ暗号化鍵」もしくは CEK と呼ぶ数量の 2 つの属性を形成する。ホスト 24 は 1 つ以上のファイルに鍵 ID を割り振ってもよく、組織化されていないデータあるいは完全なファイルの形に組織化されたデータばかりでなく何らかのやり方で組織化されたデータに鍵 ID を割り振る場合がある。

20

【0022】

システム 10 で保護されたコンテンツや領域にユーザまたはアプリケーションがアクセスするには、システム 10 に予め登録された信用証明を使って認証を受ける必要がある。信用証明はアクセス権に関連付けられ、この信用証明によって特定のユーザまたはアプリケーションにアクセス権が付与される。このような事前登録ではユーザまたはアプリケーションのアイデンティティおよび信用証明の記録をシステム 10 に記憶し、ユーザまたはアプリケーションによって判定されたそのようなアイデンティティおよび信用証明に応じてアクセス権が割り振られ、ホスト 24 を通じて提供される。事前登録が完了した後、メモリ 20 へのデータ書き込みを要求するユーザまたはアプリケーションは、自身のアイデンティティおよび信用証明と、データを暗号化するための鍵 ID と、暗号化されたデータを記憶するところの論理アドレスとを、ホスト装置を通じて提供する必要がある。システム 10 は鍵値を生成または受信し、ホスト装置から提供される鍵 ID をこの値に割り振り、書き込みデータの暗号化に用いる鍵値の鍵 ID をこのユーザまたはアプリケーションの記録またはテーブルに記憶する。そして、システム 10 はデータを暗号化し、ホストによって指定されたアドレスに暗号化されたデータを記憶するほか、生成または受信した鍵値を記憶する。

30

【0023】

メモリ 20 から暗号化データを読み出すことを要求するユーザまたはアプリケーションは、自身のアイデンティティおよび信用証明と、要求するデータの暗号化に使われた鍵の鍵 ID と、暗号化データが記憶されているところの論理アドレスとを提供する必要がある。システム 10 は、ホストから提供されたユーザまたはアプリケーションのアイデンティティおよび信用証明を自身の記録に記憶されたものに突き合わせる。システム 10 は、それらが一致する場合、ユーザまたはアプリケーションから提供された鍵 ID と関連付けられた鍵値を自身のメモリから取り出し、ホスト装置が指定するアドレスに記憶されたデータを鍵値を用いて復号化し、復号化したデータをユーザまたはアプリケーションへ送信する。

40

【0024】

認証のための信用証明を暗号処理に用いる鍵の管理から分離することにより、異なる信用証明で共通のデータアクセス権を有することが可能となる。つまり、信用証明がそれぞれ異なる 1 グループのユーザまたはアプリケーションは同じ鍵にアクセスして同じデータ

50

にアクセスできても、このグループ以外のユーザはアクセスできない。1 グループ内のすべてのユーザまたはアプリケーションが同じデータにアクセスする場合でも、それらのユーザまたはアプリケーションの権利が依然として異なる場合がある。読み出し限定のアクセス権を有するものもあれば、書き込みアクセス権のみを有するものもあれば、両方を有するものもある。ユーザまたはアプリケーションのアイデンティティおよび信用証明と、アクセスできる鍵 ID と、各々の鍵 ID に関連するアクセス権との記録を維持するシステム 10 では、正式に認証されたホスト装置の管理下で鍵 ID を追加または削除したり、特定のユーザまたはアプリケーションの鍵 ID と関連付けられたアクセス権を変更したり、あるユーザまたはアプリケーションから別のユーザまたはアプリケーションにアクセス権を委譲できるほか、ユーザまたはアプリケーションの記録またはテーブルを削除または追加することもできる。記憶された記録では、特定の鍵へのアクセスにおいてセキュアチャネルを特定することができる。認証は、対称または非対称アルゴリズムとパスワードを使って果たすことができる。

10

【0025】

とりわけ重要なこととして、メモリシステム 10 の中で保護されたコンテンツは移動できる。鍵値へのアクセスがメモリシステムによって制御される実施形態において、メモリシステムまたはこのシステムを内蔵する記憶装置がある 1 つの外部システムから別の外部システムへ移される場合、そこに記憶されたコンテンツの安全は保たれる。鍵がメモリシステムによって生成されようが、メモリシステムの外から届くものであろうが、外部システムは、メモリシステムによって完全に統制されたやり方で認証されない限り、システム 10 のコンテンツにアクセスできない。そのとおりに認証された後でもアクセスはメモリシステムによって全面的に制御され、外部システムによるアクセスのあり方は、メモリシステムに予め設定された記録に従って制御される。このような記録に準拠しない要求は拒否される。

20

【0026】

コンテンツ保護の柔軟性を高めるため、これ以降パーティションと呼ぶメモリの特定領域が想定され、このパーティションには正式に認証されたユーザまたはアプリケーションのみがアクセスできる。これを前述した鍵方式のデータ暗号化機能と組み合わせることにより、システム 10 のデータ保護能力は向上する。図 2 に示すように、フラッシュメモリ 20 の記憶容量は、多数のパーティション、すなわちユーザ領域またはパーティションとカスタムパーティションに分割できる。ユーザ領域またはパーティション P0 には、すべてのユーザまたはアプリケーションが認証なしでアクセスできる。ユーザ領域に記憶されたデータのビット値のすべてがいずれのアプリケーションまたはユーザでも読み書きできるが、読み出しデータが暗号化されている場合、復号化の権限を有していないユーザまたはアプリケーションは、ユーザ領域に記憶されたビット値表現の情報にアクセスできない。例えば、ユーザ領域 P0 に記憶されたファイル 102 および 104 がこれにあたる。106 等のユーザ領域には暗号化されていないファイルも記憶され、すべてのアプリケーションおよびユーザがこれを読み出し、解釈できる。ファイル 102 および 104 等の暗号化されたファイルは錠前の記号に関連付けて表示されている。

30

【0027】

権限のないアプリケーションまたはユーザはユーザ領域 P0 で暗号化されたファイルを解釈できないが、そのようなアプリケーションまたはユーザであってもファイルを削除したり破壊したりすることは可能であり、用途によっては好ましくない場合がある。このため、メモリ 20 には、パーティション P1 および P2 等の事前の認証なくしてアクセスできない被保護カスタムパーティションもある。この用途の実施形態に使える認証プロセスをこれより説明する。

40

【0028】

同じく図 2 に示されているように、メモリ 20 のファイルには様々なユーザまたはアプリケーションがアクセスする。そこで図 2 には、ユーザ 1 および 2 とアプリケーション 1 ～ 4（装置上で実行）が示されている。これらの実体は、これより説明する認証プロセス

50

によって認証された後にメモリ20の被保護コンテンツへのアクセスが認められる。このプロセスでは、アクセスを要求する実体をロール方式のアクセス制御のためにホスト側で識別する必要がある。そこでアクセスを要求する実体はまず、「私はアプリケーション2であってファイル1を読み出したい」等の情報を供給することによって自身を識別する。コントローラ12はそのアイデンティティと、認証情報と、要求とを、メモリ20またはコントローラ12に記憶された記録に突き合わせる。すべての要件が満たされる場合、そのような実体にアクセスが認められる。図2に示すように、ユーザ1はパーティションP1のファイル101を読み書きでき、P0ではファイル106に対する無制限の読み出し・書き込み権利を有しているが、これ以外に読み出し可能なファイルはファイル102および104のみである。他方、ユーザ2は、ファイル101および104へのアクセスを許可されないが、ファイル102に対する読み出し・書き込みアクセス権は有している。図2に示すように、ユーザ1および2のログインアルゴリズム(AES)は同じであるが、アプリケーション1および3のログインアルゴリズムはそれぞれ異なり(例えば、RSAと001001)、ユーザ1および2のものとも異なる。

【0029】

セキュアストレージアプリケーション(SSA)は本発明の一実施形態を例示するメモリシステム10のセキュリティアプリケーションであり、前述した機能の多くはこれを用いて実行できる。SSAはソフトウェアまたはコンピュータコードとして実装でき、メモリ20またはCPU12の不揮発性メモリ(図示せず)に記憶されたデータベースがRAM12aに読み込まれ、CPU12によって実行される。次の表には、SSAに言及する場合に用いる頭字語が記されている。

定義、頭字語、および略語

ACR	アクセス制御記録
AGP	ACRグループ
CBC	連鎖ブロック暗号
CEK	コンテンツ暗号化鍵
ECB	電子コードブック
ACAM	ACR属性管理
PCR	権限制御記録
SSA	セキュアストレージアプリケーション
実体	単独の実体を有し(ホスト側)、 SSAにログインすることにより その機能を利用するもの

【0030】

SSAシステムの説明

SSAの主な役割はデータの保護と保全とアクセス制御である。データとは、いくつかの大容量記憶装置に一目瞭然な状態で記憶される場合があるファイルである。SSAシステムは記憶システムの上部に位置し、記憶されたホストファイルのためのセキュリティ層を加え、後述するセキュリティデータ構造を通じてセキュリティ機能を提供する。

【0031】

SSAの主な仕事は、メモリに記憶された(保護された)コンテンツに関わる様々な権利を管理することである。メモリアプリケーションは、複数の記憶コンテンツに対する複数のユーザおよびコンテンツ権利を管理する必要がある。ホストアプリケーションは提示されたドライブとパーティションをホスト側から看取するほか、記憶装置に記憶されたフ

ファイルの位置を管理し表現するファイルアロケーションテーブル（FAT）を看取する。

【0032】

この場合の記憶装置はパーティションに分割されたNANDフラッシュチップを使用するが、他の可搬型記憶装置も使用でき、本発明の範囲内にある。これらのパーティションは一連の論理アドレスであり、その境界は開始アドレスと終端アドレスで区切られる。したがって、所望により、非表示のパーティションへのアクセスに制限を設けることができ、それにはソフトウェア（メモリ20に記憶されたソフトウェア等）によってそのような境界内のアドレスにそのような制限を関連付ける。SSAは、自身が管理する論理アドレスの境界によってパーティションを完全に認識する。SSAシステムはパーティションを用いて権限を有していないホストアプリケーションからデータを物理的に保護する。ホストにとってのパーティションは、データファイルが記憶されるところの専有空間を規定するメカニズムである。これらのパーティションを公開する場合、記憶装置にアクセスできる者であれば誰でも装置におけるこれらのパーティションの存在を看取して認識し、パーティションを非公開にする場合もしくは非表示にする場合、選ばれたホストアプリケーションのみがこれらのパーティションにアクセスでき、記憶装置におけるこれらの存在をも認識できる。

10

【0033】

図3はメモリのパーティションP0、P1、P2、およびP3を示すメモリの概略図であり（言うまでもなく5つ以上のパーティションが使われることも、あるいは3つ以下のパーティションが使われることもある）、P0はいずれの実体でも認証なしでアクセスできる公開パーティションである。

20

【0034】

非公開パーティション（P1、P2、またはP3等）の中にあるファイルへのアクセスは非表示にされる。ホストによるパーティションへのアクセスを阻止することにより、フラッシュ装置（例えば、フラッシュカード）はパーティションの中でデータファイルの保護を達成する。しかし、この種の保護は、非表示パーティションの中で論理アドレスに記憶されたデータへのアクセスに制限を設けることによって、非表示パーティションの中にあるすべてのファイルを囲い込むものである。換言すると、一連の論理アドレスに制限を関連付けるものである。そのパーティションへアクセスできるユーザ／ホストはいずれも、内部にあるすべてのファイルに無制限にアクセスできる。ファイル（またはファイル群）を互いに分離するため、SSAシステムは鍵と鍵の参照符すなわち鍵IDとを用いて別の保護・保全レベルをファイル（またはファイル群）単位で提供する。様々なメモリアドレスでデータを暗号化するのに用いられる鍵値の鍵参照符すなわち鍵IDは、暗号化データを収容する容器または領域にたとえることができる。このため、図4では、鍵IDと関連付けられた鍵値を用いて暗号化されたファイルを取り囲む領域として鍵参照符すなわち鍵ID（例えば、「鍵1」および「鍵2」）が示されている。

30

【0035】

図4を参照し、例えばファイルAは鍵IDで囲まれていないため、いずれの実体でも認証なしでファイルAにアクセスできる。公開パーティションの中にあるファイルBはいずれの実体でも読み出しや上書きを行えるが、その中のデータはID「鍵1」を有する鍵で暗号化されているため、このような鍵にアクセスできるこのような実体でない限り、ファイルBの中にある情報にはアクセスできない。このような鍵値と鍵参照符すなわち鍵IDの使用は、前述したパーティションによる保護とは異なり、論理的な保護のみを提供する。つまり、パーティション（公開または非公開）にアクセスできるホストであればいずれでもそのパーティションの中で暗号化データを含むデータを読み書きできる。しかし、データは暗号化されているため、権限を有していないユーザはデータを壊すことしかできない。権限を有していないユーザは、好ましくは発覚することなくこのデータを変更できない。暗号化および／または復号化鍵へのアクセスを制限することにより、権限を有する実体のみにデータの使用を認めることができる。P0ではファイルBおよびCも鍵ID「鍵2」を有する鍵を使って暗号化されている。

40

50

【0036】

データの機密保護と保全は、コンテンツ暗号化鍵（CEK）をCEK当たり1つずつ使用する対称暗号化法で提供できる。SSAの実施形態では、CEKの鍵値がフラッシュ装置（例えば、フラッシュカード）によって生成または受信され、内部でのみ使用され、外部に対して秘密に保たれる。暗号化されるデータでハッシュ計算を行うか、あるいは暗号を連鎖ブロック化することによってデータ保全を徹底することもできる。

【0037】

パーティション内のすべてのデータが異なる鍵によって暗号化され、異なる鍵IDが割り振られるわけではない。公開またはユーザファイルの中またはオペレーティングシステム領域（すなわち、FAT）の中で、論理アドレスに鍵または鍵参照符が割り振られない場合があり、この場合、パーティション自体にアクセスできる実体であればいずれでもこれにアクセスできる。

10

【0038】

鍵やパーティションの作成や、パーティションにおけるデータの読み書きや、鍵の使用を望む実体は、アクセス制御記録（ACR）を通じてSSAシステムにログインする必要がある。SSAシステムにおけるACRの特権はアクションと呼ばれる。どのACRでも3種類のアクション、すなわちパーティションおよび鍵／鍵IDの作成と、パーティションおよび鍵へのアクセスと、他のACRの作成／更新とを実行する権限を有することができる。

【0039】

ACRは、ACRグループすなわちAGPと呼ばれるグループに整理する。ACRの認証に成功するとSSAシステムがセッションを開放し、このセッションの中でACRのアクションを実行できる。ACRとAGPは、方針に従ってパーティションや鍵へのアクセスを制御するためのセキュリティデータ構造である。

20

【0040】

ユーザパーティション

SSAシステムは、ユーザパーティションとも呼ばれる1つ以上の公開パーティションを管理する。このパーティションは記憶装置上に存在し、記憶装置の標準的な読み出し・書き込みコマンドを通じてアクセスできるパーティションである。このパーティションのサイズと装置上でのこのパーティションの存在に関する情報は、好ましくはホストに対して非表示にしない。

30

【0041】

SSAシステムでは、標準的な読み出し・書き込みコマンドまたはSSAコマンドを通じてこのパーティションにアクセスできる。このパーティションへのアクセスは、好ましくは特定のACRに制限しない。しかし、SSAシステムの場合、ホスト装置はユーザパーティションへのアクセスを制限できる。読み出し・書き込みアクセスは個別に有効／無効にできる。4通りの組み合わせすべて（例えば、書き込み限定、読み出し限定（書き込み保護）、読み出しおよび書き込み、アクセス不能）が可能である。

【0042】

SSAシステムでは、ACRを使ってユーザパーティションの中にあるファイルに鍵IDを割り振り、そのような鍵IDと関連付けられた鍵を使って個々のファイルを暗号化できる。ユーザパーティションの中にある暗号化ファイルへのアクセスとパーティションへのアクセス権設定は、SSAコマンドセットを使って行う。前述した機能はファイルの形に組織されていないデータにも当てはまる。

40

【0043】

SSAパーティション

これは、SSAコマンドでないとアクセスできない非表示（認証されていない者に対して非表示にされた）パーティションである。SSAシステムは好ましくは、ACRへのログインによって確立するセッション（後述）の中でアクセスが行われる場合を除き、ホスト装置によるSSAパーティションへのアクセスを許可しない。同様に、SSAは好まし

50

くは、SSAパーティションの存在と、サイズと、アクセス権限とに関する情報を、その要求が確立されたセッションの中で発生する場合を除き、提供しない。

【0044】

パーティションに対するアクセス権はACR権限から検索される。SSAシステムにログインしたACRは他のACRとパーティションを共用できる（後述）。パーティションが作成されると、ホストはそのパーティションに参照名またはID（例えば、図3および4におけるP0～P3）を与える。この参照名は、このパーティションに対する以降の読み出し・書き込みコマンドで使われる。

【0045】

記憶装置の分割

好ましくは、装置の使用可能な記憶容量のすべてをユーザパーティションとその時点で構成済みのSSAパーティションとに割り当てる。このため、再分割において既存のパーティションの再構成をとまなうことがある。装置容量（全パーティションの合計サイズ）の正味の変化はゼロである。装置メモリ空間におけるパーティションのIDはホストシステムによって設定される。

【0046】

ホストシステムは、既存パーティションのいずれか1つを2つのより小さいパーティションに再分割したり、2つの既存パーティション（隣接する場合とそうでない場合とがある）を1つに併合したりすることができる。分割されたパーティションや併合されたパーティションの中のデータは、ホストの判断で消去するか、あるいは現状のまま残すことができる。

【0047】

記憶装置の再分割によってデータが（記憶装置の論理アドレス空間の中での消去や移動により）失われるおそれがあるため、SSAシステムは再分割において厳重な制限を課す。つまり、ルートAGP（後述）の中にあるACRにのみ再分割コマンドの発行が許され、これが参照できるパーティションは自身が所有するパーティションのみである。パーティションの中でデータがどのように構成されているかはSSAシステムには分からないから（FATまたはその他のファイルシステム構造）、装置の再分割において構成を組み直す責任はホストにある。

【0048】

ユーザパーティションの再分割によって、ホストOSから見たこのパーティションのサイズやその他の属性は変化する。

【0049】

再分割の後、ホストシステムにはSSAシステムで存在しないパーティションをACRが参照していないことを確認する責任がある。これらのACRが適切に削除または更新されないと、不在パーティションに対してこれらのACRに代わって行われるアクセスの試みはシステムによって検出され、拒否される。削除される鍵や鍵IDについても同様の配慮がなされる。

【0050】

鍵、鍵ID、論理的保護

ある特定の非表示パーティションに書き込まれたファイルは公から非表示にされる。しかし、いったん実体（敵対的な実体、またはそうでない実体）が情報を得てこのパーティションにアクセスすると、そのファイルは使用可能となり一目瞭然となる。そのファイルのさらなる安全確保のため、SSAは非表示パーティションでファイルを暗号化でき、このファイルの復号化に用いる鍵にアクセスするための信用証明は、好ましくはパーティションにアクセスするためのものとは異なるものにする。ファイルはホストによって全面的に制御され、管理されるため、ファイルにCEKを割り振ることには問題がある。これを解決するには、SSAが了解する何か、すなわち鍵IDにファイルに関連付ける。つまりSSAによって鍵が作成されたら、ホストはその鍵を使って暗号化されるデータに鍵IDを割り振る。鍵が鍵IDと併せてSSAに送られる場合、鍵と鍵IDを互いに関連付ける

10

20

30

40

50

ことは容易い。

【0051】

鍵値と鍵IDは論理的セキュリティを提供する。特定の鍵IDが割り振られたデータはいずれも、その場所にかかわらず、コンテンツ暗号化鍵（CEK）の同じ鍵値で暗号化され、ホストアプリケーションからは一意な参照名すなわち鍵IDが提供される。（ACR認証により）非表示パーティションにアクセスし、そのパーティション内にある暗号化ファイルの読み出しまたは書き込みを望む実体は、そのファイルに割り振られた鍵IDにアクセスする必要がある。この鍵IDの鍵に対するアクセスを許諾する場合、SSAはこの鍵IDと関連付けられたCEKに鍵値をロードし、データを復号化してからホストへ送信するか、あるいはデータを暗号化してからフラッシュメモリ20に書き込む。一実施形態において、鍵IDと関連付けられたCEKの鍵値がSSAシステムによって無作為に作成され、SSAシステムによって維持される。SSAシステムの外でCEKの鍵値を知るか、あるいはアクセスする者はいない。外部から提供され外部で使用するのは参照符すなわち鍵IDのみであり、CEKの鍵値ではない。鍵値はSSAによって全面的に制御され、好ましくはSSAのみがこれにアクセスできる。代替的に、SSAシステムに鍵を提供することもできる。

10

【0052】

SSAシステムは、次の暗号モードのいずれか1つ（ユーザにより設定）を用いて鍵IDと関連付けられたデータを保護する（実際に使われる暗号アルゴリズムとCEKにおける鍵値はシステムの管理下であって、外部には明かされない）。

20

・ブロックモード：データをブロックに分割し、それぞれのブロックを個別に暗号化する。このモードは一般的に安全性が低いとされ、辞書攻撃を被りやすいが、ユーザはデータブロックのいずれか1つにランダムにアクセスできる。

・連鎖モード：データをブロックに分割し、暗号化の過程で鎖状に繋ぎ合わせる。ブロックはいずれも、次のブロックの暗号化プロセスへの入力として使われる。安全性は高いとされているが、データの読み書きが最初から最後まで順次に行われるため、ユーザにとって容認しがたいオーバーヘッドが発生することがある。

・ハッシュモード：連鎖モードに、データ保全性ベリファイに用いるデータダイジェストの作成を加えたもの。

【0053】

30

ACRとアクセス制御

SSAは多数のアプリケーションを取り扱うように設計され、システムデータベースの中では、ノードからなるツリーとしてそれぞれのアプリケーションを表現する。ツリーのブランチ間のクロストークをなくすことによりアプリケーション間の相互排除を達成する。

【0054】

SSAシステムにアクセスする場合、実体はシステムのいずれか1つのACRを通じて接続を確立する必要がある。SSAシステムは、接続する場合、ユーザが選ぶACRの規定に従ってログイン手続きを運営する。

【0055】

40

ACRはSSAシステムに至る個々のログイン地点である。ACRはログイン信用証明と認証方法を保持する。読み出し特権や書き込み特権を含むSSAシステムの中でのログイン権限もこの記録の中にある。これを示す図5には、同じAGPの中にn個のACRがある。これは、n個のACRのうちの少なくとも種々のACRが同じ鍵へのアクセス権を共有することを意味する。つまり、ACR#1とACR#nは鍵ID「鍵3」を有する鍵へのアクセス権を共有し、ここでACR#1とACR#nはACRIDであって、「鍵3」は鍵の鍵IDであって、この鍵を用いて「鍵3」に関連するデータが暗号化される。複数ファイルまたは複数データ群の暗号化および／または復号化に同じ鍵を使うこともできる。

【0056】

50

SSAシステムは数通りのシステムログインをサポートし、認証アルゴリズムとユーザ信用証明は様々であってもよく、ログインに成功したユーザのシステムにおける特権も様々であってもよい。図5には様々なパスワードログインアルゴリズムと信用証明とが例示されている。ACR#1ではパスワードログインアルゴリズムとパスワードとが、信用証明として指定され、ACR#2ではPKI（公開鍵基盤）ログインアルゴリズムと公開鍵が信用証明として指定されている。したがって、実体はログインにおいて有効なACRIDを提示するほか、適切なログインアルゴリズムと信用証明とを提示する必要がある。

【0057】

SSAシステムのACRにログインした実体の権限、すなわちSSAコマンドを使用する権利は、ACRと関連付けられた権限制御記録（PCR）の中で設定する。図5のPCRに示すように、ACR#1は「鍵3」と関連付けられたデータに対して読み出し限定権限を許諾し、ACR#2は「鍵5」と関連付けられたデータの読み出し権限と書き込み権限とを許諾する。

【0058】

読み出しや書き込みに使う鍵等の異なるACRがシステムで共通の利権・特権を有することがある。このため、共通する部分があるACRはAGP、すなわちACRグループにグループ分けする。ACR#1とACR#nはいずれも、鍵ID「鍵3」を有する鍵へのアクセス権がある。

【0059】

AGPとその中にあるACRは階層状のツリーの中で編制されるため、ACRは重要データの安全性を保つ安全鍵を作成できるほか、好ましくは自身の鍵ID／パーティションに対応する他のACR項目を作成できる。これらの子ACRは、その父、すなわち作成元と同じ権限を有するかそれよりも少ない権限を有することになり、父ACR自身が作成した鍵の権限が付与される場合がある。言うまでもなく、子ACRは自身が作成する任意の鍵に対するアクセス権限を取得する。これは図6に例示されている。AGP120の中にあるACRはいずれもACR122によって作成されたものであり、これらのACRのうちの2つは、「鍵3」と関連付けられたデータへのアクセス権限をACR122から継承している。

【0060】

AGP

SSAシステムへのログインにおいて、AGPとそのAGPの中にあるACRを指定する。

AGPはいずれも一意なID（参照名）を有し、SSAデータベースにおける該当する項目への索引として使われる。AGP名はAGPの作成時にSSAシステムに支給される。SSAは、支給されるAGP名がシステムに既に存在する場合に作成動作を拒否する。

【0061】

以降のセクションで説明するように、アクセス権限や管理権限の委譲に関わる制限事項はAGPを使って管理運営する。完全に独立した実体、例えば2つの異なるアプリケーションまたは2つの異なるコンピュータユーザによるアクセスの制御運営は、図6の2つのツリーが果たす役割の1つである。ここで大切なり得ることは、2つのアクセスプロセスが、たとえ同時に発生する場合でも、事実上互いに独立する（すなわち、事実上クロストークをなくす）ことである。これは、それぞれのツリーにおけるACRとAGPの認証、権限、追加作成等が他のツリーにおけるものと無関係であり、かつ他のツリーにおけるものに左右されないことを意味する。このため、SSAシステムを使用するメモリシステム10では、複数のアプリケーションを同時に処理できる。また、2つのアプリケーションが互いに自立的に2つの別々のデータ群（例えば、1組の写真と1組の歌）にアクセスすることも可能になる。これは図6に例示されている。図6の上部で、ツリーの中にあるノード（ACR）を通じてアクセスするアプリケーションまたはユーザにとって、「鍵3」、「鍵X」、および「鍵Z」と関連付けられたデータは写真であってもよい。図6の下部で、ツリーのノード（ACR）を通じてアクセスするアプリケーションまたはユーザにと

10

20

30

40

50

って、「鍵5」および「鍵Y」と関連付けられたデータは歌であってもよい。AGPを作成したACRは、このAGPにACR項目がなく空になっている場合に限りこのAGPを削除できる。

【0062】

実体にとってのSSAの入口：アクセス制御記録（ACR）

SSAシステムのACRは、実体によるシステムログインのあり方を記述するものである。SSAシステムにログインする実体は、これから始まる認証プロセスに該当するACRを指定する必要がある。図5に示すように、ACRの中にある権限制御記録（PCR）は、ACRの認証を終えたユーザが実行できる許諾アクションを明らかにするものである。ホスト側実体はすべてのACRデータフィールドを提供する。

10

【0063】

ACRへのログインに成功した実体は、そのACRのパーティション・鍵アクセス権限やACAM権限（後述）を照会できる。

ACR ID

SSAシステムの実体はログインプロセスを開始するときに、そのログイン方法に該当するACR IDを指定する必要がある（ACRが作成される場合にホストより支給される）ので、SSAは正しいアルゴリズムを準備し、すべてのログイン条件が満たされたら正しいPCRを選択する。ACR IDはACRの作成時にSSAシステムに提供される。

【0064】

ログイン／認証アルゴリズム

実体によって使われるログイン手続きと、ユーザのアイデンティティを証明する場合に必要な信用証明は、認証アルゴリズムによって決まる。手続きなし（信用証明なし）からパスワードに基づく手続き、対称暗号法か非対称暗号法に基づく双方向認証プロトコルまで、SSAシステムは数通りの標準的なログインアルゴリズムをサポートする。

20

【0065】

信用証明

実体の信用証明はログインアルゴリズムに対応し、SSAがユーザをベリファイし認証するのに使われる。パスワード認証のためのパスワード／PIN番号やAES認証のためのAES鍵等は信用証明の一例であり得る。信用証明のタイプ／書式（PIN、対称鍵等）は予め決まり、認証モードから検索され、ACRの作成時にSSAシステムに提供される。SSAシステムはこれら信用証明の設定、配布、管理に関与しないが、例外としてPKI方式の認証では装置（例えば、フラッシュカード）を使ってRSA等の鍵対を生成でき、証明書生成のための公開鍵をエクスポートできる。

30

【0066】

権限制御記録（PCR）

PCRは、SSAシステムにログインしACRの認証プロセスに合格した後の実体に対する許諾事項を明らかにするものである。権限には、パーティションおよび鍵の作成権限と、パーティションおよび鍵へのアクセス権限と、実体－ACR属性の管理権限の3種類がある。

40

【0067】

パーティションへのアクセス

PCRのこの部分には、ACR段階を首尾よく完了した実体からアクセスできるパーティションのリストが入る（SSAシステムへ提供されるパーティションのIDを使用）。パーティションごとに書き込み限定または読み出し限定にアクセスのタイプが制限される場合があったり、あるいは完全書き込み／読み出しアクセス権が指定される場合もある。図5のACR#1はパーティション#2にアクセスできてもパーティション#1にはアクセスできない。PCRの中で指定される制限はSSAパーティションと公開パーティションとに適用される。

【0068】

50

公開パーティションには、SSAシステムをホストする装置（例えば、フラッシュカード）に対する通常の読み出しおよび書き込みコマンドでアクセスするか、あるいはSSAコマンドでアクセスする。公開パーティションを制限する権限を有するルートACR（後述）が作成されると、このルートACRはその権限を自身の子に渡すことができる。ACRは、好ましくは通常の読み出しおよび書き込みコマンドによる公開パーティションへのアクセスのみを制限できる。SSAシステムのACRは、好ましくはこれが作成されるときにのみ制限できる。公開パーティションに対する読み出し／書き込み権限をACRが得た後、好ましくはその権限は剥奪できない。

【0069】

鍵IDアクセス

PCRのこの部分には、実体のログインプロセスによってACR方針が満たされた場合に該当する実体からアクセスできる、鍵IDのリスト（ホストからSSAシステムへの提供）と関連付けられたデータが入る。PCRに記載されたパーティション内のファイルには指定された鍵IDが割り振られる。デバイス（例えば、フラッシュカード）の論理アドレスに鍵IDは割り振られないため、ある特定のACRに対して2つ以上のパーティションがある場合、それらのパーティションのいずれかの中にはファイルがある。PCRの中で指定された鍵IDはそれぞれ異なる1組のアクセス権を有することができる。鍵IDによって指示されるデータへのアクセスは、書き込み限定または読み出し限定に制限される場合があったり、あるいは完全書き込み／読み出しアクセス権が指定される場合もある。

【0070】

ACR属性管理（ACAM）

このセクションではACRのシステム属性が変更できる場合について説明する。

SSAシステムで許可され得るACAMアクションは次のとおりである。

1. AGPとACRの作成／削除／更新
2. パーティションと鍵の作成／削除
3. 鍵およびパーティションに対するアクセス権の委譲

父ACRは、好ましくはACAM権限を編集できない。この場合、好ましくはACRの削除と再作成が必要となる。また、ACRによって作成された鍵IDに対するアクセス権限は、好ましくは剥奪できない。

【0071】

ACRには他のACRやAGPを作成する容量があってもよい。ACRを作成するということは、作成元が所有するACAM権限の一部または全部が作成されたACRへ委譲されることを意味する場合がある。ACRを作成する権限を有するということは、次のアクションの権限を有することを意味する。

1. 子の信用証明を設定し編集する－作成元ACRによって一旦設定された認証方法は、好ましくは編集できない。子向けに予め設定された認証アルゴリズムの範囲内で信用証明を変更してもよい。
2. ACRを削除する。
3. 作成権限を子ACRへ委譲する（よって孫ができる）。

【0072】

他のACRを作成する権限を有するACRは、これが作成するACRに遮断解除権限を委譲する権限を有する（しかし、ACRの遮断を解除する権限がない場合もある）。父ACRは解除ACRの参照符を子ACRの中に入れる。

【0073】

父ACRは、自身の子ACRを削除する権限を有する唯一のACRである。ACRが作成した下位ACRを削除すると、この下位ACRから生まれたすべてのACRも自動的に削除される。ACRを削除すると、そのACRによって作成された鍵IDとパーティションはすべて削除される。

例外として、ACRが自身の記録を更新できる場合が2つある。

1. 作成元ACRによって設定されたパスワード／PINでも、それらを含むACRに

10

20

30

40

50

よってのみ更新できる。

2. ルート A C R は自分自身と自身が所属する A G P とを削除できる。

【0074】

鍵・パーティションアクセス権の委譲

A C R とその A G P は階層状のツリーの中で構成され、ルート A G P とその中にある A C R はツリーの最上部に位置する（例えば、図 6 のルート A G P 1 3 0 および 1 3 2）。S S A システムの中には数本の A G P ツリーが存在することがあるが、それらは互いに完全に独立している。A G P の中にある A C R は、自身の鍵に対するアクセス権限を、同じ A G P の中にある全 A C R とそれらによって作成されるこの全 A C R に委譲できる。鍵を作成する権限は、好ましくはその鍵を使用するためのアクセス権限を委譲する権限を含む。

10

【0075】

鍵に対する権限は 3 種類に分かれる。

1. アクセス：鍵に対するアクセス権限、すなわち読み出しと書き込みとを設定する。

2. 所有：当然ながら、鍵の所有者はその鍵を作成した A C R である。この所有権は、ある 1 つの A C R から別の A C R（同じ A G P の中にあるか、あるいは子 A G P の中にある A C R）へ委譲できる。鍵の所有権は、鍵を削除する権限のほかに、鍵に対する権限を委譲する権限を提供する。

3. アクセス権委譲：この権限により、A C R は自身が保持する権利を委譲できる。

A C R は、自身が作成したパーティションのほかに、自身が所有するアクセス権限の対象となる他のパーティションに対するアクセス権限を委譲できる。

20

権限を委譲するには、パーティションの名前と鍵 I D を指定された A C R の P C R に追加する。鍵のアクセス権限を委譲するには、鍵 I D を使っても、あるいは委譲する側の A C R のすべての作成された鍵がアクセス権限の対象となってもよいことを表明する。

【0076】

A C R の遮断と解除

システムによる実体の A C R 認証プロセスが失敗すると、A C R の遮断カウンタが増加する場合がある。一定の最大失敗認証数（M A X）に達すると、S S A システムによって A C R は遮断されることになる。

遮断された A C R は、この遮断された A C R から参照する別の A C R によって解除できる。この解除された A C R に対する参照は、その作成元にたる A C R によって設定される。解除された A C R は、好ましくは遮断された A C R の作成元と同じ A G P の中にあり、「解除」権限を有する。

30

システムの中でこれ以外の A C R は遮断された A C R を解除できない。遮断カウンタがある A C R でも解除 A C R がなければ、遮断された場合に解除できない。

【0077】

ルート A G P - アプリケーションデータベースの作成

S S A システムは複数のアプリケーションを処理し、各アプリケーションのデータを分離するように設計されている。アプリケーションデータを識別し、かつ分離する場合には A G P システムのツリー構造がメインのツールとして用いられる。ルート A G P はアプリケーション S S A データベースツリーの先端に位置し、いくぶん異なる挙動ルールに準拠する。S S A システムでは数個のルート A G P を構成できる。図 6 には 2 つのルート A G P 1 3 0 および 1 3 2 が示されている。当然、これよりも少ない A G P やこれよりも多い A G P が使われる場合があり、本発明の範囲内にある。

40

新規アプリケーションのための装置（例えば、フラッシュカード）の登録および／または装置の新規アプリケーションの信用証明発行は、装置に新たな A G P / A C R ツリーを追加する過程で行う。

【0078】

S S A システムはルート A G P（ならびにルート A G P の全 A C R とその権限）を作成する場合に 3 通りのモードをサポートする。

50

1. オープンモード：いずれのユーザまたは実体でも認証なしで、あるいはシステム A C R（後述）を通じて認証されたユーザ／実体が、新規ルート A G Pを作成できる。オープンモードによるルート A G Pの作成は、セキュリティ対策なしですべてのデータ転送がオープンチャネル（発行機関のセキュア環境内）で行われる場合と、システム A C R 認証（O v e r T h e A i r（O T A）と後発行手順）を通じて確立するセキュアチャネルを通じて行われる場合とがある。

システム A C Rが構成されず（オプションとして）、ルート A G P作成モードをオープンに設定する場合に選べるオプションはオープンチャネルのみである。

2. 制御モード：システム A C Rを通じて認証された実体のみが新規ルート A G Pを作成できる。システム A C Rが構成されなければ、S S Aシステムをこのモードに設定することはできない。

10

3. ロックモード：ルート A G Pの作成は無効になり、さらなるルート A G Pをシステムに加えることはできない。

【0079】

この機能は2つの S S Aコマンドで制御する（これらコマンドはいずれのユーザ／実体でも認証なしで使用できる）。

1. 方法構成コマンド：3通りのルート A G P作成モードのいずれか1つを使用する形に S S Aシステムを構成するために使用する。オプションから制御へ、制御からロックへのモード変更のみが可能である（つまり、S S Aシステムが現在制御モードに構成されている場合、ロックモードにしか変更できない）。

20

2. 方法構成固定コマンド：方法構成コマンドを無効にし、現在選択されている方法で永続的に固定するために使用する。

【0080】

作成されたルート A G Pは特別な初期化モードに入り、A C Rの作成、構成（ルート A G Pの作成に適用されたものと同じアクセス制限を使用）が可能になる。ルート A G P構成プロセスの最後に実体がこれを明示的に作動モードに切り替えると、既存の A C Rは更新できなくなり、A C Rを追加で作成できなくなる。

【0081】

標準モードに入ったルート A G Pを削除するには、その A C Rのうち、ルート A G Pの削除する権限が付与された A C Rを通じてシステムにログインしなければならない。特別の初期化モードのほかに、これもルート A G Pの例外である。これは好ましくは、次のツリーレベルにある A G Pではなく自身の A G Pを削除する権限を有する A C Rを含んでもよい唯一の A G Pである。

30

ルート A C Rと標準 A C Rとの3番目にして最後の違いは、パーティションを作成し削除する権限を有し得るシステム内で唯一の A C Rであるということである。

【0082】

S S Aシステム A C R

システム A C Rは次に記す2つの S S A操作に使用される。

1. 不利な状況の中でセキュアチャネルの保護下で A C R／A G Pツリーを作成する。

2. S S Aシステムをホストする装置を識別し、認証する。

40

好ましくは S S Aの中でシステム A C Rは1つのみであってもよく、いったん設定されたシステム A C Rは好ましくは変更できない。システム A C Rを作成するときシステム認証は必要なく、必要なものは S S Aコマンドのみである。システム A C R作成機能は無効にできる（ルート A G P作成機能と同様）。好ましくは1つのみのシステム A C Rが認められるため、システム A C R作成コマンドはシステム A C Rの作成後には作用しない。

【0083】

システム A C Rはその作成プロセスでは機能しない。作成が完了したら、システム A C Rが作成され準備が整ったことを伝える専用のコマンドを発行する必要がある。好ましくはこの時点でシステム A C Rの更新や差し替えは行えない。

【0084】

50

システム A C R は S S A でルート A C R / A G P を作成する。システム A C R は、ホストがルートレベルに満足し遮断するまでルートレベルを追加／変更する権限を有する。ルート A G P を遮断すると、基本的にはシステム A C R とのつながりは絶たれ、改竄不能となる。この時点でルート A G P とその中にある A C R は誰も変更／編集できない。これは S S A コマンドで果たす。ルート A G P 作成を無効にする作用は永続し、元に戻すことはできない。図 7 には、システム A C R が関わる前述した機能が示されている。システム A C R を使って 3 通りのルート A G P が作成されている。図 7 でシステム A C R をルート A G P に結ぶ点線で示すように、これらのルート A G P が作成された後のある時点で、システム A C R からルート A G P を遮る S S A コマンドがホストから送信され、ルート A G P 作成機能は無効になる。これで 3 つのルート A G P は改竄不能となる。ルート A G P が遮断される前か後に、3 つのルート A G P を使って子 A G P を作ることにより、3 つの別々のツリーが形成されている。

10

【0085】

前述した機能は、コンテンツの所有者がコンテンツを使ってセキュア製品を構成する場合に優れた柔軟性を提供する。セキュア製品は「発行」する必要がある。発行とは、装置がホストを識別しホストが装置を識別するための識別鍵を出すプロセスである。ホストは装置（例えば、フラッシュカード）を識別することにより、この秘密を信用できるかどうかを判断できる。一方、装置はホストを識別することにより、ホストが可能な範囲でのみセキュリティ方針を実施することができる（特定のホストコマンドを許諾し実行する）。

20

【0086】

複数のアプリケーションに対応するように設計された製品は、様々な識別鍵を有することになる。製品は「前発行」するか（出荷に先立つ製造中に鍵を記憶する）、あるいは「後発行」する（出荷後に新たな鍵を追加する）。後発行の場合、ある種の親鍵または装置レベル鍵をメモリ装置（例えば、メモリカード）に入れる必要があり、この鍵は、装置へのアプリケーションの追加が許される実体を識別するために使われる。

【0087】

前述した機能により後発行を有効／無効にするように製品を構成できる。加えて、後発行構成は出荷の後に安全に果たすことができる。装置は、前述した親鍵または装置レベル鍵のほかには鍵のない状態で小売製品として購入され、新たな所有者により、さらなる後発行アプリケーションを有効または無効にするように構成できる。

30

【0088】

このようにシステム A C R 機能は前述した目的を達成するための能力を提供する。

- ・システム A C R がないメモリ装置の場合はアプリケーションを自由に無制限に追加できることになる。

- ・システム A C R がないメモリ装置はシステム A C R の作成を無効にするように構成でき、これは新規アプリケーションの追加を制御できないことを意味する（新規ルート A G P 作成機能も無効にする場合を除く）。

- ・システム A C R があるメモリ装置の場合はシステム A C R 信用証明を使った認証手続きで確立されるセキュアチャネル経由でアプリケーションを追加できる。

40

- ・システム A C R があるメモリ装置は、アプリケーションが追加される前か、あるいは追加された後にアプリケーション追加機能を無効にするように構成できる。

【0089】

鍵 I D リスト

鍵 I D は具体的な A C R 要求に従って作成されるが、メモリシステム 10 でこれを使用するのは S S A システムのみである。鍵 I D の作成時に作成元 A C R から提供されるか、あるいは作成元 A C R へ提供されるデータは次のとおりである。

1. 鍵 I D : この I D はホストを通じて実体から提供され、以降の読み出しアクセスや書き込みアクセスで、鍵と、その鍵を使って暗号化または暗号化されるデータとを参照するために使われる。

50

2. 鍵暗号およびデータ保全モード（後述する前述したブロック、チェーン、およびハッシュモード）

【0090】

ホストから提供される属性に加えて、SSAシステムは次のデータを管理する。

1. 鍵IDの所有者：所有者にあたるACRのID。作成された鍵IDの所有者は作成元ACRである。しかし、鍵IDの所有権は別のACRに譲渡できる。好ましくは、鍵IDの所有権を譲渡し、かつ鍵IDを委譲できるものは鍵IDの所有者のみである。鍵のアクセス権限の委譲とこれらの権利の失効を行えるのは鍵IDの所有者か、または委譲権限を有するその他のACRである。SSAシステムは、これらの操作のいずれかが試みられるときに、操作を要求するACRにその権限が付与されている場合に限り操作を許諾することになる。

10

2. CEK：このCEKの鍵値は、鍵IDが割り振られたコンテンツまたは鍵IDによって指示されるコンテンツの暗号化に使われる。鍵値は、SSAシステムによって生成される128ビットAESランダム鍵であってもよい。

3. MACおよびIV値：連鎖ブロック暗号(CBC)符号化アルゴリズムで使われる動的情報(メッセージ認証コードと開始ベクトル)。

【0091】

図8A～図16のフローチャートを参照しながらSSAの様々な機能を例示するが、これらの図でステップの左側に記された「H」はホストによって実行される操作を意味し、「C」はカードによって実行される操作を意味する。メモリカードを参照しながらSSA機能を例示するが、物理的形態が異なるメモリ装置にもこれらの機能が当てはまることが理解できる。システムACRを作成するため、ホストはメモリ装置10のSSAに向けてシステムACR作成コマンドを発行する(ブロック202)。装置10はこれに応じてシステムACRが既に存在するかどうかをチェックする(ブロック204、菱形206)。装置10はこれが既に存在する場合に失敗ステータスを返し、停止する(長円形208)。メモリ10はこれが既に存在しない場合にシステムACRの作成が許可されるかどうかをチェックし(菱形210)、許可されない場合は失敗ステータスを返す(ブロック212)。従って、例えば、必要なセキュリティ機能が事前に決まるので、システムACRが必要とされない場合等、装置発行者がシステムACRの作成を許可しない場合もある。許可される場合、装置10はOKステータスを返し、ホストからシステムACR信用証明が届くのを待つ(ブロック214)。ホストはSSAステータスをチェックし、システムACRの作成が許可されていることを装置10が伝えているかどうかをチェックする(ブロック216と菱形218)。作成が許可されないか、あるいはシステムACRが既に存在する場合、ホストは停止する(長円形220)。システムACRの作成が許可されていることを装置10が伝える場合、ホストはそのログイン信用証明を設定するSSAコマンドを発行し、装置10へ送信する(ブロック222)。装置10は受信した信用証明でシステムACR記録を更新し、OKステータスを返す(ブロック224)。ホストはこのステータス信号に応じて、システムACRの準備が整っていることを示すSSAコマンドを発行する(ブロック226)。これに応じて装置10はシステムACRをロックするので、システムACRの更新や差し替えはできなくなる(ブロック228)。これによりシステムACRの機能と、ホストに対して装置10を識別するためのアイデンティティとが固定される。

20

30

40

【0092】

新規ツリー(新規ルートAGPおよびACR)の作成手順は、それらの機能が装置でどのように構成されているかによって決まる。図9は、その手順を説明するものである。ホスト24とメモリシステム10はいずれもこの手順をたどる。新規ルートAGPの追加が完全に無効になっている場合、新規ルートAGPは追加できない(菱形246)。これが有効になっているが、システムACRが要求される場合、ホストはルートAGP作成コマンドの発行(ブロック254)に先立ちシステムACRを通じて認証し、セキュアチャネルを確立する(菱形250、ブロック252)。システムACRが要求されない場合(菱

50

形248)、ホスト24は認証なしでルートAGP作成コマンドを発行でき、ブロック254へ進む。ホストは、システムACRが存在する場合、たとえこれが要求されない場合でも、これを使用することがある(フローチャートには示されていない)。装置(例えば、フラッシュカード)は、新規ルートAGP作成機能が無効になっている場合に新規ルートAGPを作成する試みを拒否し、システムACRが要求される場合に認証なしで新規ルートAGPを作成する試みを拒否する(菱形246および250)。ブロック254で新たに作成されるAGPとACRは作動モードに切り替わるので、そのAGPの中にあるACRの更新や変更はできなくなり、AGPへACRを追加することもできなくなる(ブロック256)。ここでオプションとしてシステムはロックされるので、ルートAGPは追加で作成できなくなる(ブロック258)。点線の枠258は、このステップがオプションのステップであることを示す表記法である。本願の図のフローチャートにて点線で示された枠はいずれもオプションのステップである。このように、コンテンツの所有者は正当なコンテンツを含む本物のメモリ装置を装う違法な目的に装置10を利用できないようにすることができる。

10

【0093】

ACR(前述したルートAGPの中にあるACRとは別のACR)を作成するには、図10に示すように、ACRを作成する権利を有するACRから開始できる(ブロック270)。ホスト24を通じて入ることを試みる実体は、入口にあたるACRのアイデンティティと作成したいがための必要となる属性のすべてを含むACRとを提供する(ブロック272)。SSAはACRアイデンティティの一致をチェックし、さらにそのアイデンティティを有するACRにACRを作成する権限があるかどうかをチェックする(菱形274)。要求が証明される場合、装置10のSSAはACRを作成する(ブロック276)。

20

【0094】

図11の2つのAGPは、図10の方法を使用するセキュリティアプリケーションで役に立つツリーを例示するものである。従って、マーケティングAGPの中でアイデンティティm1を有するACRには、ACRを作成する権限がある。ACR m1は、鍵ID「マーケティング情報」と関連付けられたデータと鍵ID「価格リスト」と関連付けられたデータを鍵を使って読み書きする権限も有する。これにより、図10の方法を用いて2つのACR s1およびs2を含む販売AGPを作成する。ACR s1およびs2には鍵ID「価格リスト」と関連付けられた価格データにアクセスするための鍵の読み出し権限のみあるが、鍵ID「マーケティング情報」と関連付けられたデータにアクセスする場合に必要となる鍵の権限はない。このように、ACR s1およびs2を有する実体は、価格データを読み出されてもこれを変更することはできず、さらにマーケティングデータにはアクセスできない。一方、ACR m2にはACRを作成する権限がなく、鍵ID「価格リスト」と鍵ID「マーケティング情報」と関連付けられたデータにアクセスするための鍵の読み出し権限のみを有する。

30

【0095】

従って、アクセス権は前述したやり方で委譲でき、m1は価格データを読み出す権利をs1およびs2に委譲する。これは特に大規模なマーケティング組織や販売組織が関わる場合に有用である。しかし、販売員が1名~少数であれば図10の方法を使う必要はない場合がある。代わりに、図12に示すように、ACRから同じAGPの下位レベルまたは同じレベルに位置するACRにアクセス権を委譲できる。実体はまず、そのAGPのツリーに入るため、ホストを通じてツリーの中のACRを前述したように指定する(ブロック280)。次に、ホストはACRと委譲する権利を指定する。SSAはツリーでこのACRをチェックし、指定された別のACRに権利を委譲する権限がこのACRにあるかどうかをチェックする(菱形282)。権限があるなら権利は委譲され(ブロック284)、そうでないなら停止する。図13はその結果を示す。この場合、ACR m1には読み出し権限をACR s1に委譲する権限があるため、委譲の後、s1は鍵を使って価格データにアクセスできるようになる。これは、m1が価格データにアクセスするための権利ま

40

50

たはそれ以上の権利を有し、さらにそれを委譲する権限を有する場合に果たすことができる。m 1 は、一実施形態において、委譲の後にそのアクセス権を保持する。好ましくは、時間やアクセス数を制限するなどにより（永続的にではなく）一定の条件のもとでアクセス権を委譲する。

【0096】

図14は、鍵と鍵IDを作成するプロセスを示す。実体はACRを通じて認証を受ける（ブロック302）。実体は、ホストによって指定されたIDによる鍵の作成を要求する（ブロック304）。SSAは、指定されたACRにその権限があるかどうかをチェックする（菱形306）。例えば、ある特定のパーティションにあるデータにアクセスするために鍵が使われる場合、SSAはそのパーティションにACRがアクセスできるかどうかを10
チェックすることになる。ACRにその権限がある場合、メモリ装置10はホストから提供された鍵IDと関連付けられた鍵値を作成し（ブロック308）、鍵IDをACRに記憶し、鍵値をメモリ（コントローラ関連メモリまたはメモリ20のいずれか）に記憶し、実体から提供された情報に従って権利と権限を付与し（ブロック310）、付与された権利および権限で該当するACRのPCRを修正する（ブロック312）。従って、読み出しおよび書き込み権限、同じAGPの中にある他のACRまたは下位レベルのACRに委譲し共有する権利、鍵の所有権を譲渡する権利等、鍵の作成元はすべての権利を有する。

【0097】

図15に示すように、ACRはSSAシステムの中にある別のACRの権限（またはACRの存在そのもの）を変更できる。実体はこれまでどおりACRを通じてツリーに入る場合がある。この場合は実体の認証が行われ、実体はACRを指定する（ブロック330、332）。実体はターゲットACRの削除またはターゲットACRの権限の削除を要求する（ブロック334）。指定されたACRまたはその時点でアクティブなACRにその権利があるなら（菱形336）、ターゲットACRを削除し、あるいはそのような権限を削除するためにターゲットACRのPCRを変更する（ブロック338）。これが認可されない場合、システムは停止する。20

【0098】

前述したプロセスの後、ターゲットはプロセスの前にアクセスできたデータにアクセスできなくなる。図16に示すように、かつて存在したACR IDはもはやSSAに存在しないため、ターゲットACRに入ることを試みる実体は認証プロセスの失敗に気づくので、アクセス権は拒否される場合がある（菱形352）。ACR IDが削除されていないと仮定した場合、実体はACRを指定し（ブロック354）、鍵IDおよび／または特定のパーティションのデータを指定し（ブロック356）、SSAはそのようなACRのPCRに従って鍵IDまたはパーティションアクセス要求が許可されるかどうかをチェックする（菱形358）。権限が削除されているか、あるいは失効している場合、要求は再度却下される。そうでない場合、要求は許諾される（ブロック360）。30

前述したプロセスは、ACRとそのPCRが別のACRによって変更された場合であれ、あるいは初めからそのように構成されていた場合であれ、被保護データに対するアクセスが装置（例えば、フラッシュカード）によってどのように管理されるかを説明するものである。40

【0099】

セッション

SSAシステムは、同時にログインする複数のユーザを処理するように設計されている。この機能を使用する場合、SSAによって受信されるコマンドには特定の実体が対応し、コマンドは、この実体の認証に用いるACRに要求された動作を行う権限がある場合に限り実行される。

【0100】

複数の実体はセッションのコンセプトによってサポートされる。セッションは認証プロセスで確立し、SSAシステムによってセッションidが割り当てられる。セッションid 50

dはシステムへのログインに使われたACRに内部で関連付けられ、実体へエクスポートされ、それ以降のSSAコマンドで使われる。

【0101】

SSAシステムは、2通りのセッション、すなわちオープンセッションとセキュアセッションとをサポートする。認証プロセスと関連付けられたセッションのタイプはACRの中で設定される。SSAシステムは、認証の施行と同様のやり方でセッション確立を施行する。実体の権限はACRで設定されるため、システム設計者は特定の鍵IDに対するアクセスまたは特定のACR管理操作（新規ACRの作成、信用証明の設定等）の実行にセキュアトンネルを関連付けることができる。

【0102】

オープンセッション

オープンセッションはセッションidで識別されるセッションであるが、バス暗号化は行われなため、コマンドとデータはいずれも暗号化されずに引き渡される。この動作モードは、好ましくは実体が脅威モデルに該当せずバス上で傍受を行わない多数のユーザまたは多数の実体環境に使用される。

【0103】

オープンセッションモードではデータ送信が保護されず、ホスト側のアプリケーション間に効率的なファイアウォールは実施されないが、SSAシステムが認証済みのACRでアクセスできる情報のみにアクセスを許すことができる。

【0104】

オープンセッションはパーティションまたは鍵を保護する必要がある場合にも使用できる。しかし、有効な認証プロセスの後にはホスト側のすべての実体にアクセスが許諾される。ホストアプリケーションはセッションidさえあれば認証済みACRの権限を得ることができる。これは図17Aに例示されている。線400より上のステップはホスト24によって実行されるステップである。ACR1の認証（ブロック402）を終えた実体は、メモリ装置10で鍵ID Xと関連付けられたファイルへのアクセスを要求する（ブロック404、406、および408）。ACR1のPCRがこのアクセスを認める場合、装置10は要求を許諾する（菱形410）。そうでない場合、システムはブロック402まで戻る。認証が完了した後、メモリシステム10はコマンドを発行する実体を（ACR信用証明ではなく）割り当てられたセッションidのみで識別する。オープンセッションでいったんACR1がPCRの鍵IDと関連付けられたデータに到達すると、他のどのアプリケーションまたはユーザでも、ホスト24上の様々なアプリケーションによって共有される正しいセッションidを指定することによって同じデータにアクセスできる。この機能は、一度のみログインし、様々なアプリケーションに対してログインに使われたアカウントに結合されたすべてのデータにアクセスできることがユーザにとって好都合な場合のアプリケーションに有利である。携帯電話機のユーザの場合、記憶されたeメールにアクセスし、ログインを繰り返すことなくメモリ20に記憶された音楽を聞くことができる。一方、ACR1に該当しないデータにはアクセスできないことになる。このため、ゲームや写真等の同じ携帯電話機のユーザにとって貴重となり得るコンテンツは、別のアカウントACR2を通じてアクセスされる。これは、携帯電話機のユーザの電話機を借りる人にアクセスさせたくないデータであるが、携帯電話機のユーザにとって、最初のアカウントACR1でアクセスできるデータなら他人がアクセスしてもよい。データへのアクセスを2つの別々のアカウントに分け、ACR1へのアクセスをオープンセッションで行うことにより、使い易くなるばかりでなく貴重なデータを保護できる。

【0105】

ホストアプリケーション間でのセッションidの共有をさらに簡単にするには、オープンセッションを要求するACRが、セッションに「0（ゼロ）」idを割り当てることを具体的に要求する。このように、アプリケーションは所定のセッションidを使用するように設計できる。当然ながら、セッション0を要求するACRは一度に1つしか認証できない。セッション0を要求する別のACRを認証する試みは拒否されることになる。

10

20

30

40

50

【0106】

セキュアセッション

セキュリティ層を追加するため、セッションidは図17Bに示すように使ってもよい。この場合はメモリ10もアクティブセッションのセッションidを記憶する。図17Bで、例えば鍵ID Xと関連付けられたファイルにアクセスするには、実体もセッションid、例えばセッションid「A」を提供する必要がある、その上でファイルへのアクセスが許可されることになる（ブロック404、406、412、および414）。このように、要求する実体は正しいセッションidを知らない限りメモリ10にアクセスできない。セッションidはセッションが終わった後に削除され、セッションのたびに異なるため、実体はセッション番号を提供できた場合に限りアクセスできる。

10

【0107】

SSAシステムは、コマンドが実際に正しい認証済み実体から届いているかどうかを、セッション番号を使って追跡する。攻撃者がオープンチャネルを使って悪質なコマンドの送信を試みるおそれがある用途や使用がある場合、ホストアプリケーションはセキュアセッション（セキュアチャネル）を使用する。

セキュアチャネルを使用する場合、セッションidとコマンド全体がセキュアチャネル暗号化（セッション）鍵を使って暗号化され、そのセキュリティ水準はホスト側の実施例と同じくらい高くなる。

【0108】

セッションの終了

セッションは次に記すシナリオのいずれか1つで終了し、ACRはログオフされる。

1. 実体が明示的なセッション終了コマンドを発行する。
2. 通信タイムアウトが発生する。ある特定の実体がACRパラメータの一パラメータとして設定された期間にわたってコマンドを発行しなかった。
3. 装置（例えば、フラッシュカード）のリセットおよび／またはパワーサイクルの後にはすべてのオープンセッションが終了する。

20

【0109】

データ保全サービス

SSAシステムは、SSAデータベース（ACR、PCR等を収容）が完全な状態に保たれていることをベリファイする。このほかに、鍵ID機構による実体データのデータ保全サービスも提供される。

30

鍵IDの暗号化アルゴリズムがハッシュモードに設定される場合、CEKおよびIVと併せてハッシュ値がCEK記録に記憶される。書き込み操作中にはハッシュ値の計算と記憶が行われる。読み出し操作のときにも再度ハッシュ値を計算し、前の書き込み操作中に記憶された値と比較する。実体が鍵IDにアクセスするたびに追加のデータが古いデータに（暗号的に）連結され、該当するハッシュ値（読み出しまたは書き込みのため）が更新される。

【0110】

鍵IDと関連付けられた、または鍵IDによって指示される、データファイルを知るのはホストのみであるため、データ保全機能の各態様はホストが明示的に次のように管理する。

40

1. 鍵IDと関連付けられた、または鍵IDによって指示される、データファイルは最初から最後まで書き込まれるか、または読み出される。SSAシステムはCBC暗号方式を使用し、データ全体のハッシュ化メッセージダイジェストを生成するため、ファイルの一部分にアクセスする試みによってファイルは混乱することになる。

2. 中間ハッシュ値はSSAシステムによって管理されるため、連続するストリームの中でデータを処理する必要はない（このデータストリームは他の鍵IDのデータストリームでインターリーブでき、複数のセッションにわたって分割できる）。しかし、実体は、データストリームが再度始まる場合にハッシュ値のリセットをシステムに明示的に指示する必要がある。

50

3. ホストは読み出し操作が完了すると、読み出されたハッシュを書き込み操作中に計算したハッシュ値と比較することによって有効にすることをSSAシステムに明示的に要求する。

4. SSAシステムは「ダミー読み出し」操作も提供する。この機能によりデータは暗号化エンジンを通して、ホストには送出不されることになる。この機能を利用すれば、データが実際に装置（例えば、フラッシュカード）から読み出される前に、データが完全な状態に保たれていることをベリファイすることができる。

【0111】

乱数生成

外部実体はSSAシステムの内部乱数生成器を利用でき、乱数はSSAシステムの外で使用できる。このサービスはいずれのホストでも利用でき、認証は必要ない。

【0112】

RSA鍵対生成

外部ユーザはSSAシステムの内部RSA鍵対生成機能を利用でき、鍵対はSSAシステムの外で使用できる。このサービスはいずれのホストでも利用でき、認証は必要ない。

【0113】

代替の実施形態

階層アプローチを使う代わりに、図18に示すデータベースアプローチを使って同様の結果を達成できる。

図18に示すように、コントローラ12またはメモリ20に記憶されたデータベースにの信用証明リスト、認証方法、最大失敗数、遮断解除に必要な最小信用証明数等は、メモリ10のコントローラ12によって実行されるデータベース内の方針（鍵・パーティションに対する読み出し、書き込みアクセス、セキュアチャネル要件）に結び付いている。鍵・パーティションアクセスに対する制約事項や制限事項もデータベースに記憶される。ホワイトリストにある可能性がある（例えば、システム管理者）はすべての鍵とパーティションにアクセスできる。ブラックリストにある可能性があるによる情報アクセスの試みは阻止される。制限は全域におよぶ場合と鍵および／またはパーティションごとに適用される場合とがある。これは、特定ののみが特定の鍵・パーティションにアクセスでき、特定のはアクセスできないことを意味する。コンテンツのパーティションや、コンテンツの暗号化または復号化に使う鍵にかかわらず、コンテンツ自体に制約を課すこともできる。したがって、データ（例えば、歌）にアクセスする可能性がある最初の5ホスト装置のみにアクセスを許可したり、あるいはデータ（例えば、映画）にアクセスしたりするは問わず、データの読み出し回数を制限することができる。

認証

パスワード保護

・パスワード保護は、被保護領域へアクセスする場合にパスワードの提示が求められることを意味する。パスワードが1つに限られる場合を除き、それぞれのパスワードには読み出しアクセスや読み出し／書き込みアクセス等、別々の権利を割り振ることができる。

・パスワード保護は、ホストから提供されるパスワードを装置（例えば、フラッシュカード）がベリファイできること、すなわち装置もまた装置によって管理され保護されたメモリ領域にパスワードを記憶することを意味する。

問題と限界

・パスワードはリプレー攻撃を被ることがある。提示のたびに変わらないパスワードは同じ状態で再送できる。つまり、保護の対象となるデータが貴重で、通信バスへのアクセスが容易い場合、パスワードを現状のまま使用するべきではない。

・パスワードによって記憶データへのアクセスは保護できるが、（鍵ではなく）データの保護のためにパスワードを使用するべきではない。

・パスワードに関わるセキュリティ水準を上げるため、親鍵を使ってパスワードを多様化すれば、1つのパスワードがハッキングされてもシステム全体が破られることはない。

10

20

30

40

50

パスワードの送信にはセッション鍵方式のセキュア通信チャネルを使用できる。

【0114】

図19は、パスワードを使った認証を示すフローチャートである。実体はアカウントidとパスワードをシステム10（例えば、フラッシュメモリカード）へ送信する。システムは、パスワードが自身のメモリにあるパスワードに一致するかどうかをチェックする。一致する場合は認証済みステータスを返す。そうでない場合はそのアカウントのエラーカウンタが増加し、実体にはアカウントidとパスワードの再入力が求められる。システムはカウンタが一杯になるとアクセス拒否ステータスを返す。

【0115】

対称鍵

10

対称鍵アルゴリズムは、暗号化と復号化の両側で同じ鍵が使われることを意味する。これは、通信に先立ち予め鍵を取り決めておくことを意味する。それぞれの側では相手側の逆のアルゴリズムを実行する。つまり、一方は暗号化アルゴリズムになり、他方は復号化アルゴリズムになる。通信する場合に両側で両方のアルゴリズムを実行する必要はない。

認証

- ・対称鍵認証は、装置（例えば、フラッシュカード）とホストが同じ鍵を共有し、同じ暗号アルゴリズム（ダイレクトおよびリバース、例えばDES、DES-1）を具備することを意味する。

- ・対称鍵認証は、チャレンジ・レスポンス（リプレー攻撃対策）を意味する。被保護装置が他の装置に対する質問を生成し、両方の装置で回答を計算する。認証を受ける側の装置は回答を送り返し、被保護装置はその回答をチェックして真贋を検査する。そして、認証に応じて権利を付与する。

20

認証には次のものがある。

- ・外部認証：装置（例えば、フラッシュカード）が外部を認証する。つまり、装置は特定のホストまたはアプリケーションの信用証明を検査する。

- ・相互認証：両側で質問を生成する。

- ・内部認証：ホストアプリケーションが装置（例えば、フラッシュカード）を認証する。つまり、ホストは、装置がそのアプリケーションにとって真正であるかどうかをチェックする。

システム全体のセキュリティ水準を上げるため（1つが破られてもすべてが破られないようにするため）

30

- ・対称鍵には通常、親鍵を使った多様化を組み合わせる。

- ・質問が真正な質問であることを確認するため、相互認証により両側からの質問を使用する。

暗号化

対称鍵暗号法はすこぶる効率的なアルゴリズムで、暗号処理する場合に強力なCPUを必要としないため、暗号化にも使われる。

【0116】

通信チャネルを安全に使う場合：

- ・チャネルの安全を確保する（つまり、全発信データを暗号化し全着信データを復号化する）ために使うセッション鍵を、両方の装置が知らなければならない。このセッション鍵は通常、事前共有秘密対称鍵を使うか、あるいはPKIを使って設定する。

40

- ・両方の装置が同じ暗号アルゴリズムを知り、実行しなければならない。

署名

対称鍵を使ってデータに署名することもできる。この場合の署名は暗号化の部分的な結果である。このため、鍵値を露出することなく必要に応じて何度でも署名できる。

【0117】

問題と限界

対称アルゴリズムは非常に効率的で安全ではあるが、事前共有秘密を基礎とする。問題は、この秘密を動的に安全に共有することと、（セッション鍵のように）ランダムにする

50

ことである。つまり、共有秘密を長期間にわたって安全に保つのは困難であり、多数の人々と共有することはほぼ不可能である。

この作業を促進するために考案されたのが、秘密を共有せずに交換する公開鍵アルゴリズムである。

【0118】

非対称認証手続き

非対称鍵に基づく認証では、一連のコマンドを使ってデータを受け渡ししながら、最終的にはセキュアチャネル通信のためのセッション鍵を作る。その基本的プロトコルではSSAシステムに対してユーザを認証する。プロトコルのバリエーションにより、ユーザが使用するACRをベリファイする相互認証や二因子認証も可能である。

10

【0119】

SSAの非対称認証プロトコルでは好ましくは、公開鍵基盤(PKI)アルゴリズムとRSAアルゴリズムを使用する。これらのアルゴリズムで規定することで、認証プロセスの各当事者に独自のRSA鍵対を用意することができる。それぞれの対は公開鍵と秘密鍵とからなる。これらの鍵は秘匿の鍵であるためにアイデンティティの証拠を提供することはできない。PKI層では信頼された第三者機関が公開鍵に署名する。この信用機関の公開鍵は、互いを認証する当事者間で事前共有され、当事者の公開鍵をベリファイするために使われる。信用が成立すると(両当事者が相手方から提供される公開鍵を信用できると判断したら)、プロトコルによる認証(各当事者が所有する秘密鍵の一致をベリファイする)と鍵の交換が続行する。これは、後述する図22および23のチャレンジ・レスポンス機構で果たすことができる。

20

【0120】

署名済みの公開鍵を収容する構造を証明書という。証明書に署名した信用機関を証明機関(CA)という。認証を受ける側は公開鍵の信憑性を立証する証明書とRSA鍵対を有する。証明書は、相手方(認証する側)が信用する証明機関によって署名される。認証する側には信用CAの公開鍵の所有が求められる。

【0121】

SSAは証明書チェーンに対応する。これは、識別される側の公開鍵が別のCA、すなわち識別する側が信用するCAとは異なるCAによって署名されることを意味する。この場合の識別される側は、自分自身の証明書のほかに、その公開鍵に署名したCAの証明書を提供する。この第2レベルの証明書さえも相手方によって信用されない(信用CAによって署名されていない)場合、第3レベルの証明書を提供できる。この証明書チェーンアルゴリズムでは、各当事者が公開鍵の認証に必要な証明書の完全なリストを所有する。このことは、図23および24に例示されている。この種のACRによる相互認証に必要な信用証明は、一定の長さを有するRSA鍵対である。

30

【0122】

SSA証明書

SSAは[X.509]バージョン3デジタル証明書を採用する。[X.509]は汎用規格であり、ここで説明するSSA証明書プロファイルは証明書の所定フィールドの内容をさらに指定し、制限する。この証明書プロファイルは、証明書チェーンの管理に用いる信頼階層と、SSA証明書の検査と、証明書失効リスト(CRL)プロファイルも規定する。

40

証明書は公開情報(内部の公開鍵として)とみなされるため、暗号化されない。しかし、証明書はRSA署名を含み、このRSA署名によって公開鍵やその他の情報フィールドが改竄されていないことをベリファイする。

[X.509]はASN.1規格を使った各フィールドのフォーマットを定め、ASN.1規格はデータ符号化にDERフォーマットを使用する。

【0123】

SSA証明書の概要

図20と図21とに示されたSSA証明書管理アーキテクチャの一実施形態は、ホスト

50

の無限階層レベルと装置の3階層レベルからなるが、装置で使用する階層レベルは3レベルより多い場合または3レベルより少ない場合がある。

【0124】

ホスト証明書階層

装置は、2つの要素、すなわち装置に記憶されたルートCA証明書（ACR信用証明としてACRの作成時に記憶）と、装置への（その特定のACRへの）アクセスを試みる実体から提供される証明書／証明書チェーンとに基づき、ホストを認証する。

【0125】

ホスト証明機関は、それぞれのACRに対してルートCA（ACR信用証明の中にある証明書）の役割を果たす。例えば、ある1つのACRにとってのルートCAは「ホスト1 CA（レベル2）証明書」であり、別のACRにとってのルートCAは「ホストルートCA証明書」である。それぞれのACRに対して、ルートCAによって署名された証明書（またはルートCAを末端実体証明書までつなげる証明書チェーン）を保持するすべての実体が、末端実体証明書の対応する秘密鍵を有している場合、そのACRにログインできる。前述したように、証明書は公知であり、秘密にしない。

【0126】

ルートCAによって発行された証明書（ならびに対応する秘密鍵）の所有者は誰でもそのACRにログインできるということは、ある特定のACRに対する認証がそのACRの信用証明に記憶されたルートCAの発行者によって決まることを意味する。換言すると、ルートCAの発行者がACRの認証方式を管理する実体になる。

【0127】

ホストルート証明書

ルート証明書は、ログインを試みる実体（ホスト）の公開鍵のベリファイを開始するのにSSAが使われるときに使用する信用CA証明書である。この証明書はACRの作成時にACR信用証明の一部として提供される。これはPKIシステムに対する信用の根元にあたるものであるため、信用された実体（父ACR、または製造／構成信頼環境）から提供されることが前提となる。この証明書をベリファイするSSAは、その公開鍵を使って証明書の署名をベリファイする。ホストルート証明書は暗号化された状態で不揮発性メモリ（図1には示されていない）に記憶され、装置の秘密鍵にアクセスできるものは、好ましくは図1のシステム10のCPU12のみである。

【0128】

ホスト証明書チェーン

これらの証明書は認証中にSSAへ提供される。チェーンの処理が完了した後にホストの証明書チェーンを再度集めて装置に記憶することはしない。

【0129】

図20は、多数のホスト証明書チェーンを示す、ホスト証明書レベル階層の概略図である。図20に示すように、ホスト証明書は多数の証明書チェーンを有することがあり、ここでは3つの証明書チェーンのみが例示されている。

- A1. ホストルートCA証明書502、ホスト1 CA（レベル2）証明書504、ホスト証明書506
- B1. ホストルートCA証明書502、ホストn CA（レベル2）証明書508、ホスト1 CA（レベル3）証明書510、ホスト証明書512
- C1. ホストルートCA証明書502、ホストn CA（レベル2）証明書508、ホスト証明書514

【0130】

前述した3つの証明書チェーンA1、B1、およびC1は、ホストの公開鍵が真正であることを証明するために使われてもよい3通りのホスト証明書チェーンを例示するものである。図20と前述した証明書チェーンA1を参照し、ホスト1のCA（レベル2）証明書504の公開鍵はホストルートCAの秘密鍵によって署名され（すなわち、公開鍵のダイジェストを暗号化）、この公開鍵はホストルートCA証明書502にある。したがって

、ホストルートCAの公開鍵を有する実体は、前述した証明書チェーンA1の信憑性をベリファイできることになる。この実体は最初のステップとして、ホストから送信されたホスト1のCA（レベル2）証明書504の署名済み公開鍵を、自身が所有するホストルートCAの公開鍵を使って復号化し、復号化した署名済み公開鍵を、ホストから送信されたホスト1のCA（レベル2）証明書504の署名されていない公開鍵のダイジェストと比較する。2つが一致する場合、ホスト1のCA（レベル2）の公開鍵は認証され、実体は次に、ホストから送信されたホスト証明書506の中にあるホスト1のCA（レベル2）の秘密鍵によって署名されたホストの公開鍵を、ホスト1のCA（レベル2）の認証済み公開鍵を用いて復号化することになる。この復号化された署名済みの値が、ホストから送信されたホスト証明書506の中にある公開鍵のダイジェストの値に一致する場合、ホストの公開鍵も認証される。証明書チェーンB1およびC1を使った認証も同様に行われる。

10

【0131】

チェーンA1に関わる前述したプロセスから分かるように、ホストから送信され実体によってベリファイされる最初の公開鍵は、ホストルートCA証明書ではなくホスト1のCA（レベル2）の公開鍵である。このため、ホストが実体へ送る必要があるものはホスト1のCA（レベル2）証明書504とホスト証明書506であって、ホスト1のCA（レベル2）証明書はチェーンの中で最初に送信される必要があることになる。前述したように、証明書のベリファイ順序は次のとおりである。ベリファイする側の実体、すなわちこの場合のメモリ装置10はまず、チェーンの中で最初の証明書の公開鍵の真性をベリファイし、この場合のものはルートCAの下に位置するCAの証明書504である。この証明書の公開鍵が真正であることをベリファイした後、装置10は次の証明書のベリファイに進み、この場合のものはホスト証明書506である。証明書チェーンが3つ以上の証明書を含む場合のベリファイ順序も同様に、ルート証明書のすぐ下に位置する証明書から始まり、認証の対象となる実体の証明書で終わる。

20

【0132】

装置証明書階層

ホストは2つの要素、すなわちホストに記憶された装置ルートCAと、装置からホストへ提供される（ACRの作成時に信用証明として装置に提供される）証明書／証明書チェーンとに基づき装置を認証する。ホストによる装置の認証プロセスは、前述した装置によるホスト認証プロセスに類似する。

30

【0133】

装置証明書チェーン

これらの証明書はACRの鍵対の証明書である。これらの証明書はACRの作成時にカードに提供される。SSAはこれらの証明書を個別に記憶し、認証のときにはそれらを1つずつホストに提供する。SSAはこれらの証明書を使ってホストの認証を受ける。装置は3つの証明書からなるチェーンを処理できるが、証明書数が3以外になる場合がある。証明書の数はACRによって異なることがある。これはACRが作成されるときに決まる。装置はホストに向けて証明書チェーンを送信できるが、証明書チェーンデータを使用するわけではないので、証明書チェーンを解析する必要はない。

40

【0134】

図21は、SSAを使用する記憶装置等の装置で1～n通りの証明書チェーンを示す、装置証明書レベル階層の概略図である。図21に示されたn通りの証明書チェーンは次のとおりである。

A2．装置ルートCA証明書520、装置1 CA（製造業者）証明書522、
装置証明書524

B2．装置ルートCA証明書520、装置n CA（製造業者）証明書526、
装置証明書528

【0135】

SSA装置は、それぞれ独自の装置CA証明書を有する1～n通りの製造業者によって

50

製造される。したがって、ある特定の装置の装置証明書の公開鍵はその異なる製造業者の秘密鍵によって署名され、製造業者の公開鍵は装置ルートCAの秘密鍵によって署名される。装置の公開鍵をベリファイする方法は、前述したホストの公開鍵の場合の方法に類似する。ホストについて前述した連鎖A1のベリファイの場合と同様に、装置ルートCA証明書を送る必要はなく、連鎖の中で送信すべき最初の証明書は装置i CA（製造業者）証明書であって、その後に装置証明書が続く、iは1～nの整数である。

【0136】

図21に示す実施形態において、装置は2つの証明書、つまり装置i CA（製造業者）証明書と、その後に自身の装置証明書とを送信する。装置i CA（製造業者）証明書は、このような装置を製造し、装置の公開鍵に署名するための秘密鍵を提供する製造業者の証明書である。装置i CA（製造業者）証明書を受信したホストは、自身が所有するルートCAの公開鍵を使って装置i CA（製造業者）公開鍵を復号化し、ベリファイする。ホストはこのベリファイに失敗した場合、プロセスを中断し、認証が失敗したことを装置に伝える。ホストが認証に成功した場合、次の証明書を求める要求を装置へ送信する。そして、装置は自身の装置証明書を送信し、ホストはこれを同様にベリファイする。

10

【0137】

図22および図23は、前述したベリファイプロセスをさらに詳しく示すものである。図22の「SSMシステム」は、本願明細書で説明するSSAシステムと後述するその他の機能とを実行するソフトウェアモジュールである。SSMはソフトウェアまたはコンピュータコードとして具現化でき、メモリ20またはCPU12の不揮発性メモリ（図示せず）にデータベースを記憶し、RAM12aに読み込まれてCPU12によって実行される。

20

【0138】

図22に示すように、装置10のSSMシステム542がホストシステム540を認証するプロセスには3つの段階がある。最初の公開鍵ベリファイ段階では、ホストシステム540がSSMコマンドでホスト証明書チェーンをSSMシステム542へ送信する。SSMシステム542は、ホスト証明書544の真性とホスト公開鍵546の真性を、ACR550のホストルート証明書548にあるルート証明機関公開鍵を用いてベリファイする（ブロック552）。ルート証明機関とホストの間に中間証明機関が介在する場合、中間証明書549もブロック552のベリファイに使われる。ベリファイまたはプロセス（ブロック552）が成功したと仮定し、SSMシステム542は第2段階へ進む。

30

【0139】

SSMシステム542は乱数554を生成し、これを質問としてホストシステム540へ送信する。システム540はホストシステムの秘密鍵547を使って乱数554に署名し（ブロック556）、質問に対する回答として署名済みの乱数を送信する。その回答はホスト公開鍵546を使って復号化され（ブロック558）、乱数554と比較される（ブロック560）。復号化された回答が乱数554に一致したと仮定すると、チャレンジ・レスポンスは成功である。

【0140】

第3段階ではホスト公開鍵546を使って乱数562を暗号化する。この乱数562がセッション鍵となる。ホストシステム540は、SSMシステム542からの暗号化数562を秘密鍵を使って復号化（ブロック564）することによってセッション鍵を得ることができる。このセッション鍵により、ホストシステム540とSSMシステム542との間でセキュア通信を開始できる。図22に示す一方方向非対称認証では、装置10のSSMシステム542によってホストシステム540が認証される。図23は、図22の一方方向認証プロトコルに類似する双方向相互認証プロセスを示すプロトコル図であり、図23ではSSMシステム542もホストシステム540によって認証される。

40

【0141】

図24は、本発明の一実施形態を例示する証明書チェーン590の図である。前述したように、ベリファイする場合に提示の必要がある証明書チェーンは多数の証明書を含むこ

50

とがある。図24の証明書チェーンは全部で9つの証明書を含み、認証する場合にはこれらの証明書をすべてベリファイすることが必要となる場合がある。背景技術の欄で前に説明したように、既存の証明書ベリファイシステムでは、送信される証明書チェーンに不備があったり、信用証明全体が送信されたり、証明書が特定の順序で送信されないと、受信側は証明書を一通り受信し記憶するまで証明書を解析できない。しかし、チェーンに含まれる証明書の数は事前に分からないため、問題が生じることがある。長さが定かでない証明書チェーンを記憶するために大量の記憶容量を確保する必要があることがある。これはベリファイを行う記憶装置にとって問題になることがある。

【0142】

本発明の一実施形態は、証明書チェーンが記憶装置によってベリファイされる順序と同じ順序でホスト装置が証明書チェーンを送信するシステムによってこの問題を軽減できるという認識に基づく。よって、図24に示すように、証明書のチェーン590は、ホストルート証明書のすぐ下に位置する証明書590(1)から始まり、ホスト証明書に相当する証明書590(9)で終わる。したがって、装置10はまず、証明書590(1)で公開鍵をベリファイし、その後に証明書590(2)で公開鍵のベリファイ等を行い、最後に証明書590(9)で公開鍵をベリファイする。これで証明書チェーン590全体のベリファイプロセスは完了する。ホスト装置が証明書チェーン590をベリファイと同じ順序でメモリ装置10へ送信する場合、メモリ装置10は証明書が届くたびにベリファイを開始することができ、チェーン590に含まれる9つの証明書が一通り届くまで待つ必要はない。

【0143】

したがって、ホスト装置は、一実施形態において、メモリ装置10に対してチェーン590の証明書を一度に1つずつ送信する。メモリ装置10は一度に1つの証明書を記憶することになる。チェーンの中の最後の証明書を除き、ベリファイ済みの証明書はホストから送信される次の証明書で上書きできる。このため、メモリ装置10には、1つのみの証明書を随時記憶する容量を確保すればよい。

【0144】

メモリ装置は、チェーン590が一通り届いたことを知る必要がある。このため、好ましくは、最後の証明書590(9)には、これがチェーンの中で最後の証明書であることを伝える標識または標示を入れる。これを例示する図25の表は、ホストからメモリ装置10へ送信される証明書バッファに先行する制御セクタ内の情報を示す。図25に示すように、証明書590(9)の制御セクタには引数名「最終」フラグがある。メモリ装置10は、「最終」フラグが設定されているかどうかをチェックして受信した証明書がチェーンにおける最終証明書であるかどうかを判断することにより、チェーンの中で証明書590(9)が最後の証明書であることをベリファイできる。

【0145】

代替的な実施形態では、チェーン590の証明書を1つずつ送信するのではなく、1つ、2つ、または3つの証明書からなるグループで送信してもよい。当然ながら、グループで使用する証明書の数は異なる場合があったり、あるいは同じになる場合がある。チェーン590には5つの連続する証明書列591、593、595、597、および599がある。それぞれの列は少なくとも1つの証明書を含む。ある1つの証明書の列には、チェーンの中で該当する1列の先行列に隣接する証明書(先頭証明書)と、チェーンの中で該当する1列の後続列に隣接する証明書(終端証明書)と、先頭証明書と終端証明書との間にある全証明書が含まれる。例えば列593の中には、全部で3つの証明書590(2)、証明書590(3)、および証明書590(4)がある。メモリ装置10による5つの証明書の列のベリファイは591、593、595、597の順で行われ、599で終わる。したがって、5つの列がメモリ装置10によるベリファイと同じ順序で送信され、受信される場合、ベリファイ済みの列をメモリ装置で記憶する必要はなくなり、最後の列を除く列はいずれも、ホストから到着する次の列で上書きできる。前の実施形態と同様に、チェーン内の最後の証明書には標識、例えばこれがチェーンにおける最後の証明書である

ことを伝える特定の値に設定されたフラグを入れるのが望ましい。この実施形態の場合、メモリ装置は5つの列のうち、証明書数が最も多い列の証明書を記憶する十分な容量を確保するだけでよい。よって、ホストが送ろうとする列のうちの最も大きい列を事前にメモリ装置10に知らせる場合、メモリ装置10は最も大きい列のための十分な容量を確保するだけでよい。

【0146】

好ましくは、ホストによって送信されるチェーン中の各証明書の長さは、その証明書によって証明される公開鍵の長さの4倍以下である。同様に、メモリ装置の公開鍵を証明するためにメモリ装置10からホスト装置へ送信される証明書の長さは好ましくは、その証明書によって証明される公開鍵の長さの4倍以下である。

10

【0147】

図26のフローチャートは、前述した証明書チェーンベリファイの実施形態を示すものであり、ここでは簡潔を図るため、各グループ内の証明書数を1と仮定する。図26に示すように、ホストはカードに向けてチェーン内の証明書を順次送信する。チェーンの中の第1の証明書（前述したように、通常はルート証明書の後続証明書）から始まって、カードは、認証の対象となるホストから証明書チェーンを順次受信する（ブロック602）。そして、カードは受信する証明書の各々をベリファイし、証明書のいずれかでベリファイに失敗した場合はプロセスを中止する。カードは、証明書のいずれかでベリファイに失敗した場合、ホストに通知する（ブロック604、606）。次に、カードは、最後の証明書が受信されベリファイされたかどうかを検出する（菱形608）。最終証明書の受信とベリファイとがまだであれば、カードはブロック602まで戻り、ホストからの証明書の受信とベリファイを続行する。最終証明書を受信し、ベリファイしたら、カードは証明書ベリファイの後に続く次の段階へ進む（610）。図26とそれ以降の図の内容は例としてメモリカードを参照するが、物理的形態がメモリカードではないメモリ装置にもこれらの内容が当てはまることが理解できる。

20

【0148】

図27は、カードがホストを認証する場合にホストによって実行されるプロセスを示す。図27に示すように、ホストはチェーンの中の次の証明書をカードに送信する（ブロック620）（通常はルート証明書の後続証明書から始まる。ホストは、認証の失敗を伝える中止通知がカードから届いているかどうかを判断する（菱形622）。中止通知が届いているならホストは停止する（ブロック624）。中止通知が届いてなければ、ホストは送信された最後の証明書で「最終フラグ」が設定されているかどうかをチェックすることにより、チェーンの最終証明書が送信済みかどうかを確認する。最終証明書が送信済みであれば、ホストは証明書ベリファイの後に続く次の段階へ進む（ブロック628）。図22および23に示すように、次の段階はチャレンジ・レスポンスであり、その後にセッション鍵の作成が続いてもよい。チェーンの最終証明書が送信済みでなければ、ホストはブロック620まで戻り、チェーン内の次の証明書を送信する。

30

【0149】

図28および図29は、カードが認証される場合にカードとホストがとる動作を示す。図28に示すように、カードは開始後、チェーンの中で証明書の送信を求めるホストからの要求を待つ（ブロック630、菱形632）。ホストから要求が届かなければ、カードは菱形632へ戻る。ホストから要求が届く場合、カードはチェーンの中の次の証明書を送信することになり、これは送信すべき最初の証明書から始まる（通常はルート証明書の後続証明書から始まる）（ブロック634）。カードは、ホストから失敗通知が届いたかどうかを判断する（菱形636）。失敗通知が届いた場合、カードは停止する（ブロック637）。失敗通知が届かない場合、カードは最終証明書が送信済みかどうかを判断する（菱形638）。最終証明書が送信済みでなければ、カードは菱形632まで戻り、チェーン内の次の証明書の送信を求める次の要求をホストから受け取るまで待つ。最終証明書が送信済みであれば、カードは次の段階へ進む（ブロック639）。

40

【0150】

50

図29は、カードが認証される場合にホストがとる動作を示す。ホストは、チェーン内の次の証明書を求める要求をカードへ送り、これは送信されるべき最初の証明書に対する要求から始まる（ブロック640）。ホストは受信するそれぞれの証明書をベリファイし、ベリファイに失敗した場合はプロセスを中止し、カードに通知する（ブロック642）。ベリファイに合格した場合、ホストは最終証明書が受信済みでベリファイに成功したかどうかをチェックする（菱形644）。最終証明書の受信とベリファイがまだであれば、ホストはブロック640まで戻り、チェーン内の次の証明書を求める要求を送る。最終証明書が受信済みでベリファイに成功した場合、ホストは証明書ベリファイの後に続く次の段階へ進む（ブロック646）。

【0151】

証明書失効

発行された証明書はその有効期間全体にわたって使われることが予想される。しかし、様々な事情から有効期間の満了に先立ち証明書が無効になる場合がある。名称の変更、対象とCAとの関係の変化（例えば、従業員の退職）、対応する秘密鍵の侵害または侵害の疑い等がこれにあたる。このような場合にはCAが証明書を無効にする必要がある。

【0152】

SSAにおける証明書の失効には別の方法があり、ACRはそれぞれ別々の証明書失効制度で構成できる。まず、失効制度をサポートしない形にACRを構成することができる。この場合の証明書は有効期限まで有効とみなされる。証明書失効リスト（CRL）を使うこともできる。さらに別の代案として、後述するようにある特定のアプリケーションに失効制度を限定する、つまりアプリケーション別にしてもよい。ACRでは、失効値を指定することによって3通りの失効制度のどれが採用されているかを指定する。失効制度なしで作成されたACRでは、そのACRの所有者の失効制度を採用できる。メモリ装置証明書の失効は、SSAセキュリティシステムではなくホストによって執り行われる。ホストルート証明書の失効管理はACRの所有者が担当し、これはACRの信用証明を更新することによって果たされる。

【0153】

証明書失効リスト（CRL）

SSAシステムで失効制度を使用するには、それぞれのCAが証明書失効リスト（CRL）と呼ばれる署名済みデータ構造を定期的に発行する。CRLは失効した証明書を識別するタイムスタンプ付きリストであり、CA（該当する証明書を発行したCA）によって署名され、一般に公開され自由に利用できる。CRLの中では、失効した証明書をそれぞれの証明書シリアル番号で識別する。CRLのサイズは任意なものであって、期限切れ前に失効する証明書の数しだいである。（例えば、ホストのアイデンティティをベリファイするため）証明書を使用する装置は、証明書の署名（ならびに有効性）をチェックするだけでなく、CRLを通じて受け取ったシリアル番号のリストにこれを照らしてベリファイする。証明書の発行元にあたるCAから発行されるCRLでその証明書の識別情報、例えばシリアル番号が見つかる場合、これは、その証明書が失効し、もはや有効でないことを意味する。

【0154】

証明書の有効性を検査する目的をCRLで果たすには、CRLについても、これが真正であることをベリファイする必要がある。CRLには、その発行元にあたるCAの秘密鍵を使って署名し、CAの公開鍵を使って署名済みCRLを復号化することによってこれが真正であることをベリファイする。復号化されたCRLが無署名CRLのダイジェストに一致する場合、そのCRLに改竄がなく、真正であることを意味する。CRLのダイジェストを得るためにハッシュアルゴリズムを使って頻繁にCRLのハッシュ計算が行われ、そのダイジェストはCAの秘密鍵で暗号化される。CRLが有効かどうかをベリファイするには、CAの公開鍵を使って署名済みCRL（すなわち、ハッシュ化・暗号化CRL）を復号化して復号化・ハッシュ化CRL（すなわち、CRLのダイジェスト）を得る。そして、これをハッシュ化CRLと比較する。このため、ベリファイプロセスでは、復号化

10

20

30

40

50

・ハッシュ化CRLとの比較のためのCRLのハッシュ計算ステップを頻繁にともなうことがある。

【0155】

CRL方式の一特徴として、(CRLを使った)証明書の妥当性のベリファイはCRLの入手と分けて行うことができる。CRLも証明書の適切な発行元によって署名され、証明書のベリファイと同様に、CRLの発行元に当たるCAの公開鍵を使って前述したようにベリファイされる。メモリ装置は署名がCRLのものであることをベリファイし、さらにCRLの発行元と証明書の発行元との一致をベリファイする。CRL方式の別の特徴として、CRLは証明書自体とまったく同じやり方で、具体的には信頼性のないサーバと信頼性のない通信を通じて、配布できる。X.509規格ではCRLとその特徴が詳述されている。

10

【0156】

CRLのためのSSA基盤構造

SSAは、CRL方式を使ったホスト失効のための基盤構造を提供する。CRL失効制度を採用するRSA方式ACRで認証する場合、ホストはSet Certificateコマンドに対して追加のフィールドとして1つのCRL(発行元CAによって無効にされた証明書がない場合は空のCRL)を加える。このフィールドには、証明書の発行元によって署名されたCRLが入る。このフィールドが存在する場合、メモリ装置10は最初にSet Certificateコマンドで証明書をベリファイする。CRLリポジトリの入手とアクセスは全面的にホストが担当する。CRLが有効であり続ける期間(CRL有効期間、すなわちCET)もCRLと併せて発行される。現在の時間がこの期間から外れていることがベリファイ中に判明すると、そのCRLには不備があるとみなされ、証明書のベリファイに使うことはできない。その結果、証明書の認証は失敗する。

20

【0157】

従来の証明書ベリファイ方法では、認証する側またはベリファイする側の実体が、証明書失効リストを所有しているか、あるいはそうでないかにかかわらず、証明機関(CA)から取り込むことができ、認証のために提示される証明書のシリアル番号をリストに照らしてチェックし、提示された証明書が失効しているかどうかを判断することになっている。認証またはベリファイする側の実体がメモリ装置の場合、そのメモリ装置自体が使われなかったら、CAから証明書失効リストは取り込まれない。予め装置に記憶された証明書失効リストが時間を経て古くなると、インストールされた日より後に失効した証明書はリストに現れない。その結果、ユーザは失効した証明書を使ってその記憶装置にアクセスできることになる。これは望ましくない。

30

【0158】

一実施形態において、認証を受けようとする実体が、認証の対象となる証明書と併せて証明書失効リストを、認証する側の実体、例えばメモリ装置10に提示するシステムによって前述した問題を解決できる。認証する側の実体は、受け取った証明書の真偽と証明書失効リストの真偽をベリファイする。認証する側の実体は、失効リストで証明書の識別情報の有無、例えば証明書のシリアル番号の有無をチェックすることにより、証明書が失効リストに登録されているかどうかをチェックする。

40

【0159】

前述したことを踏まえ、ホスト装置とメモリ装置10との相互認証に非対称認証方式を使うことができる。メモリ装置10の認証を受けようとするホスト装置は、証明書チェーンと対応するCRLの両方を提供する必要がある。一方、ホスト装置は予めCAに接続してCRLを入手しているため、ホスト装置がメモリ装置10を認証する場合、メモリ装置は、証明書または証明書チェーンと併せてCRLをホスト装置に提示する必要はない。

【0160】

種々の内蔵または独立型ミュージックプレーヤ、MP3プレーヤ、携帯電話機、個人用携帯情報端末(PDA)、ノートブックコンピュータ等、近年コンテンツの再生に使える種々の携帯型装置は増えている。証明機関から証明書失効リストへアクセスするため、そ

50

のような装置をワールドワイドウェブに接続することは可能であるが、多数のユーザは通常、ウェブに毎日接続するのではなく、例えば数週間に1度、新たなコンテンツを入手したり契約を更新したりするときに、これを行う。そのようなユーザにとって、証明機関からより頻繁に証明書失効リストを入手するのは面倒な場合がある。そのようなユーザについて、証明書失効リスト、さらに必要であれば被保護コンテンツへアクセスする場合に記憶装置に提示するホスト証明書を、好ましくは記憶装置自体の非保護領域に記憶する。多数の記憶装置（例えば、フラッシュメモリ）で、記憶装置の非保護領域は記憶装置自体によって管理されるのではなくホスト装置によって管理される。これにより、ユーザはより新しい証明書失効リストを入手するため（ホスト装置を通じて）ウェブに接続する必要がある。ホスト装置は記憶装置の非保護領域からそのような情報を検索し、記憶装置またはメモリ装置に証明書とリストを提示して、記憶装置の被保護コンテンツにアクセスできる。被保護コンテンツにアクセスするための証明書とその対応する証明書失効リストは通常であれば一定の期間にわたって有効であるため、それらが有効である限り、ユーザは最新の証明書または証明書失効リストを入手する必要はない。このため、ユーザは、適度に長い期間にわたって有効な証明書と証明書失効リストを容易く入手でき、最新情報を得るために証明機関に接続する必要はない。

10

【0161】

図30および図31のフローチャートには、前述したプロセスが示されている。図30に示すように、ホスト24は、認証のためにメモリ装置に提示する証明書に付随するCRLをメモリ装置10の非保護公開領域から読み出す（ブロック652）。CRLはメモリの非保護領域に記憶されているため、ホストによるCRLの入手より前に認証は必要ない。CRLはメモリ装置の公開領域に記憶されているため、CRLの読み出しはホスト装置24によって管理される。そして、ホストは、CRLをベリファイの対象となる証明書と併せてメモリ装置へ送信し（ブロック654）、メモリ装置10から失敗通知を受け取らなければ次の段階へ進む（ブロック656）。図31を参照し、メモリ装置はホストからCRLと証明書を受信し（ブロック658）、CRLにおける証明書シリアル番号の有無やその他の点（例えば、CRLが失効しているかどうか）をチェックする（ブロック660）。証明書シリアル番号がCRLで見つかるか、あるいはその他の理由で失敗に終わる場合、メモリ装置はホストに失敗通知を送る（ブロック662）。このように同じCRLを異なるホストの認証に使えるため、それぞれのホストはメモリ装置の公開領域に記憶されたCRLを入手する。前述したように、CRLを使ってベリファイする証明書もまた、ユーザの便宜を図るため、好ましくはメモリ装置10の非保護領域に、CRLと併せて、記憶する。しかし、メモリ装置に対して認証する場合に証明書を使えるホストは、証明書の発行を受けたホストのみである。

20

30

【0162】

図32に示すようにCRLのフィールドに次の更新時間が入る場合、装置10のSSAは、現在の時間をこの時間に照らしてチェックし、現在の時間がこの時間を過ぎているかどうかを確認し、過ぎている場合は認証に失敗する。つまり、SSAは好ましくは、現在の時間（またはメモリ装置10でCRLを受信した時間）に照らしてCETをチェックするばかりでなく次回更新の時間もチェックする。

40

【0163】

前述したように、CRLに含まれる失効済み証明書の識別情報のリストが長くなると、リストの処理（例えば、ハッシュ計算）と、ホストによって提示される証明書のシリアル番号の検索とに時間を要し、処理と検索が順次に行われる場合は特に時間がかかる。このプロセスを加速するために処理と検索とを同時に行う。また、CRLの全体を受信した後でないとCRLの処理と検索にかかれない場合にもプロセスに時間がかかる。発明者らは、CRLの一部分を受信の時点で（その都度）処理し検索すれば、CRLの最終部分を受信するときにはプロセスは完了間際となり、プロセスが捗ることに気づいた。

【0164】

図33および図34は、前述した失効制度の特徴を示す。認証する側の実体（例えば、

50

メモ리카ード等のメモリ装置)では、認証を受けようとする実体から証明書とCRLを受信する(ブロック702)。暗号化されていないCRLの一部分を処理し(例えば、ハッシュ化し)、それと同時に、提示された証明書の識別情報(例えば、シリアル番号)をそのような部分で検索する。処理された(例えば、ハッシュ化された)CRL部分を完全なハッシュ化CRLに組み立て、認証を受ける側の実体から受信した部分から復号化されたCRL部分を組み立てることによって形成される完全な復号化・ハッシュ化CRLとこれを比較する。一致しないことが比較で明らかになる場合、認証は失敗に終わる。また、認証する側の実体は、現在の時間に照らしてCETと次回更新時間の両方をチェックする(ブロック706、708)。提示された証明書の識別情報がCRLに記載されていることが判明する場合、あるいは現在の時間がCETの範囲内にある場合、あるいはCRLの次回更新時間が過ぎている場合にも、認証は失敗に終わる(ブロック710)。実行に際して、ハッシュ化CRL部分と復号化・ハッシュ化CRL部分を組み立てるために記憶する場合、大量の記憶容量は必要ない場合がある。

10

【0165】

認証を受けようとする実体(例えば、ホスト)は、その証明書とCRLを認証する側の実体へ送信し(ブロック722)、次の段階へ進む(ブロック724)。これは図34に示されている。

実体が認証のために証明書チェーンを示す場合にも前述したものと同様のプロセスを実施できる。この場合、チェーンの中の各証明書とその対応するCRLにつき前述したプロセスを繰り返すことになる。各々の証明書とそのCRLを受信したらその都度処理でき、証明書チェーンの残りの部分とその対応するCRLの受信を待たずにすむ。

20

【0166】

アイデンティティオブジェクト(I DO)

アイデンティティオブジェクトは、フラッシュメモ리카ード等のメモリ装置10がRSA鍵対またはその他の暗号IDを記憶するための被保護オブジェクトである。アイデンティティの署名とベリファイ、データの暗号化と復号化に使う暗号IDであればどのようなタイプのものでもアイデンティティオブジェクトに入れることができる。鍵対の公開鍵が真正であることを証明するCAの証明書(または複数のCAの証明書チェーン)もアイデンティティオブジェクトに入れる。アイデンティティオブジェクトを使えば、外部実体や内部カード実体(すなわち、アイデンティティオブジェクトの所有者と呼ばれる装置自体、内部のアプリケーション、その他)のアイデンティティの証拠を提出できる。したがって、カードは、チャレンジ・レスポンス機構でホストを認証するためにRSA鍵対またはその他のタイプの暗号IDを使うのではなく、識別情報の証拠としてカードに提示されるデータストリームに署名する。換言すると、アイデンティティオブジェクトはその所有者の暗号IDを収容する。アイデンティティオブジェクトの中の暗号IDにアクセスするにはまず、ホストを認証する必要がある。後述するように、この認証プロセスはACRによって管理される。ホストの認証に成功したら、アイデンティティオブジェクトの所有者は相手方に対して暗号IDを使って自身のアイデンティティを立証できる。例えば、相手方からホストを通じて提示されるデータには暗号ID(例えば、公開-秘密鍵対の秘密鍵)を使って署名できる。アイデンティティオブジェクトの署名済みデータと証明書はアイデンティティオブジェクトの所有者に代わって相手方へ提示される。証明書にある公開-秘密鍵の公開鍵が真正であることはCA(すなわち、信用機関)によって証明されるため、相手方はこの公開鍵が真正であると信用できる。そこで相手方は証明書の公開鍵を使って署名済みデータを復号化し、復号化されたデータを相手方によって送信されたデータと比較できる。復号化されたデータが相手方によって送信されたデータに一致する場合、アイデンティティオブジェクトの所有者は真正の秘密鍵にアクセスできる自称する実体であることが分かる。

30

40

【0167】

アイデンティティオブジェクトの第2の用途は、暗号ID、例えばRSA鍵自体を使って、IDOの所有者に指定されたデータを保護することである。このデータをIDOの公

50

開鍵を使って暗号化する。メモリカード等のメモリ装置 10 は秘密鍵を使ってデータを復号化する。

【0168】

I DO はどのようなタイプの A C R でも作成できるオブジェクトである。A C R は、一実施形態において、1 つのみの I D O オブジェクトを有していてもよい。データの署名と保護はいずれも、A C R の認証を受ける 実体 に対して S S A システムから提供されるサービスである。I D O の保護水準は A C R のログイン認証方式と同じくらい高い。I D O を有することになる A C R には任意の認証アルゴリズムを選ぶことができる。I D O 運用を良好に保護し得るアルゴリズムを評価し決定するのは作成元（ホスト）である。I D O を有する A C R は、I D O 公開鍵取得コマンドに応じて証明書 チェーン を提供する。

10

【0169】

データ保護に I D O を使用する場合でも、カードから出力される復号化データにはさらなる保護が必要になることがある。そのような場合には、いずれかの認証アルゴリズムによって確立されるセキュアチャネルの使用がホストに推奨される。

I D O を作成するときには鍵の長さと P K C S # 1 バージョンを選択する。一実施形態において、P K C S # 1 バージョン 2. 1 が定める（指数、係数）表現を公開および秘密鍵に使用する。

I D O の作成中に盛り込まれるデータは、一実施形態において、選択された長さを有する R S A 鍵対と、公開鍵の信憑性を帰納的に証明する証明書 チェーン である。

【0170】

20

I D O を所有する A C R はユーザデータの署名を許可する。これは 2 つの S S A コマンドを使って果たす。

- ・ S e t u s e r d a t a : 署名の対象となる自由書式のデータバッファを提供する。

- ・ G e t S S A s i g n a t u r e : カードは R S A 署名を提供する（A C R 秘密鍵を使用）。署名の形式とサイズはオブジェクトのタイプに応じて P K C S # 1 バージョン 1. 5 または V 2. 1 に従い設定される。

【0171】

図 3 5 ~ 図 3 7 は I D O を使った操作を示すものであり、ここでメモリ装置 10 はフラッシュメモリカードであり、このカードが I D O の所有者である。図 3 5 は、ホストへ送信されるデータに署名する場合にカードによって実行されるプロセスを示す。図 3 5 を参照し、前述したツリー構造のノードに位置する A C R の管理下でホストが認証された後（ブロック 8 0 2）、カードは証明書を求めるホスト要求を待つ（菱形 8 0 4）。要求を受け取ったカードは証明書を送り、菱形 8 0 4 へ戻り、次のホスト要求を待つ（ブロック 8 0 6）。カードが所有する I D O の公開鍵を証明するために証明書 チェーン を送信する必要がある場合、チェーン の中のすべての証明書がホストへ送信されるまで前述した操作を繰り返す。それぞれの証明書がホストに送信された後、カードはホストから別のコマンドが届くのを待つ（菱形 8 0 8）。所定の期間内にホストからコマンドが届かなければ、カードは菱形 8 0 4 へ戻る。ホストからデータとコマンドを受け取ったカードは、そのコマンドをチェックし、データに署名するためのものであるかどうかを確認する（菱形 8 1 0）。データに署名するためのコマンドである場合、カードは I D O の秘密鍵を使ってデータに署名し、署名したデータをホストへ送信し（ブロック 8 1 2）、菱形 8 0 4 まで戻る。ホストからのコマンドがホストからのデータに署名するためのものでなければ、カードは I D O の秘密鍵を使って受信データを復号化し（ブロック 8 1 4）、菱形 8 0 4 まで戻る。

30

40

【0172】

図 3 6 は、ホストへ送信されるデータにカードが署名する場合にホストによって実行されるプロセスを示す。図 3 6 を参照すると、ホストはカードへ認証情報を送信する（ブロック 8 2 2）。前述したツリー構造のノードに位置する A C R の制御下で認証に成功したら、ホストは証明書 チェーン を求める要求をカードへ送り、チェーン を受け取る（ブロッ

50

ク 8 2 4)。カードの公開鍵のベリファイが終わったら、ホストは署名されるデータをカードへ送信し、カードの秘密鍵で署名されたデータを受信する（ブロック 8 2 6）。

【0 1 7 3】

図 3 7 は、ホストがカードの公開鍵を使ってデータを暗号化し、暗号化したデータをカードへ送信するときにホストによって実行されるプロセスを示す。図 3 7 を参照すると、ホストはカードへ認証情報を送信する（ブロック 8 6 2）。A C R の管理下で認証に成功したら、ホストは I D O の中にあるカードの公開鍵をベリファイする場合に必要な証明書チェーンの要求をカードへ送り（ブロック 8 6 4）、さらにデータを求める要求をカードに送る。I D O の中にあるカードの公開鍵をベリファイした後、ホストはカードのベリファイ済み公開鍵を使ってカードから届いたデータを暗号化し、カードへ送信する（ブ
10
ロック 8 6 6、8 6 8）。

【0 1 7 4】

クエリ

ホストとアプリケーションは、システム操作をの実行する場合に相手方のメモリ装置またはカードについてある種の情報を所有する必要がある。例えば、ホストとアプリケーションは、メモリカードに記憶されたアプリケーションのうち、実行できるアプリケーションがいずれであるかを知る必要がある。ホストにとっての必要情報は公知でない場合があり、これはその情報を所有する権利を有する者とそうでない者があることを意味する。権限を有するユーザと持たないユーザとを区別するには、ホストで使えるクエリを 2 通り用意する必要がある。
20

【0 1 7 5】

一般情報クエリ

このクエリはシステム公開情報を無制限に放出する。メモリ装置に記憶される機密情報は 2 つの部分、すなわち共有部分と非共有部分とからなる。機密情報の一部分には個々の実体にとっての専有情報が入り、それぞれの実体は自身の専有情報に限りアクセスが認められ、他の実体の専有機密情報にはアクセスできない。この種の機密情報は共有されず、機密情報の非共有部位または部分を形成する。

【0 1 7 6】

カードの中にあるアプリケーションの名前とそのライフサイクル状態等、通常であれば公の情報と考えられるものでも、場合によっては機密とみなされることがある。別の例として、公の情報とされるルート A C R 名でも S S A の使用するといった場合によっては機密になることがある。このような場合には、一般情報クエリに応じて情報をすべて認証済みユーザに限って利用させ、認証されていないユーザには利用させないようにするためのオプションをシステムに用意しなければならない。このような情報は機密情報の共有部分を占める。ルート A C R リスト、すなわち装置上に現在存在する全ルート A C R のリストは、機密情報の共有部分の一例となり得る。
30

【0 1 7 7】

一般情報クエリによる公開情報へアクセスする場合、ホスト／ユーザは A C R にログインする必要がない。このため、S S A 規格に精通する者であれば誰でも実行可能であり、情報を受け取ることができる。S S A の規定ではセッション番号なしでこのクエリコマンドが処理される。しかし、機密情報の共有部分へのアクセスを望む実体は最初に、メモリ装置のデータに対するアクセスを制御する制御構造（例えば、A C R）のいずれかを通じて認証を受ける必要がある。認証に成功した実体は、一般情報クエリを使って機密情報の共有部分にアクセスできるようになる。前述したように、認証プロセスの結果としてアクセスのための S S A セッション番号または i d が割り当てられる。
40

【0 1 7 8】

非公開情報クエリ

個々の A C R とそのシステムアクセスおよび資産に関する私的情報は非公開とされ、明確な認証を必要とする。この種の情報クエリで許可を得るには、A C R のログインと認証（認証が A C R で指定されている場合）が事前に必要になる。このクエリには S S A セッ
50

ション番号が必要である。

2種類のクエリを詳述する前に、クエリを実行する現実的な解決策としてインデックスグループの概念を説明することが有益である。

【0179】

インデックスグループ

ポテンシャルSSAホストで実行するアプリケーションには、読み出しの対象となるセクタ数を指定することがシステムドライバとホスト上のオペレーティングシステム(OS)から求められる。これは、ホストアプリケーションがSSA読み出し操作のたびに読み出しセクタ数を把握する必要があることを意味する。

クエリ操作で供給される情報は、一般的にはこれを要求する側にとって未知の情報であるため、ホストアプリケーションがクエリを発行し、その操作に必要なセクタの量を推測するのは困難である。

【0180】

この問題を解決するため、SSAのクエリ出力バッファは各クエリ要求につき1つのみのセクタ(512バイト)からなる。出力情報の一部をなすオブジェクトはインデックスグループと呼ばれるものに編成される。オブジェクトのバイトサイズはオブジェクトのタイプによって異なり、そこから1セクタに収まるオブジェクトの数が明らかになる。これによってオブジェクトのインデックスグループが決まる。オブジェクトのサイズが20バイトである場合、このオブジェクトのインデックスグループは25オブジェクトまで収容される。そのようなオブジェクトが全部で56個ある場合、それらは3つのインデックスグループに編成され、第1のインデックスグループの先頭はオブジェクト「0」(第1のオブジェクト)となり、第2のインデックスグループの先頭はオブジェクト「25」となり、第3の最終インデックスグループの先頭はオブジェクト50となる。

【0181】

システムクエリ (一般情報クエリ)

このクエリは、装置がサポートするSSAシステムと、ツリー状に構成された現行のシステムと、装置で実行するアプリケーションとについての一般公開情報を提供する。後述するACRクエリ(非公開クエリ)と同様に、システムクエリは種々のクエリオプションを提供するように構成されている。

・General: サポートされたSSAバージョン

・SSA Applications: 現在装置に存在する全SSAアプリケーションのリストで、アプリケーションの実行状態を含む。

【0182】

前述した情報は公開情報である。ACRクエリと同様に、ホストがクエリ出力バッファのための読み出しセクタ数を知らずにすませるため、装置からは1セクタが送り返され、ホストが引き続きさらなるインデックスグループを照会できる。インデックスグループ「0」でルートACRオブジェクトの数が出力バッファサイズの数を超過する場合、ホストは後続のインデックスグループ(「1」)で別のクエリ要求を送ることができる。

【0183】

ACRクエリ (非公開情報クエリ)

SSAのACRクエリコマンドは、鍵ID、アプリケーションID、パーティション、子ACR等、ACRのシステムリソースに関する情報をACRユーザに供給するためのものである。そのクエリ情報はログインされたACRに関するもののみであり、システムツリー上の他のACRに関するものはない。換言すると、アクセスは、機密情報のうち、該当するACRの許可のもとでアクセス可能な部分に限られる。

ユーザが照会できるACRオブジェクトには3通りある。

・パーティション: 名前とアクセス権(所有者、読み出し、書き込み)。

・鍵IDとアプリケーションID: 名前とアクセス権(所有者、読み出し、書き込み)。

。

・子ACR: 直接の子にあたるACRのACRおよびAGP名。

・ I D O とセキュアデータオブジェクト（後述）：名前とアクセス権（所有者、読み出し、書き込み）。

【0184】

A C R に結び付いたオブジェクトの数は様々に異なる場合があり、情報は 512 バイト、すなわち 1 セクタを上回ることがある。オブジェクトの数が事前に分からない限り、ユーザはリストすべてを得るために装置内の S S A システムから読み出される必要があるセクタの数を知らない。そこで前述したシステムクエリの場合と同様に、S S A システムによって提供される各オブジェクトリストはインデックスグループに分割される。インデックスグループはセクタに収まるオブジェクトの数であり、例えば装置内の S S A システムからホストにかけて 1 セクタで送信できるオブジェクトの数である。これにより、装置内の S S A システムは要求されたインデックスグループを 1 セクタで送信できる。ホスト／ユーザは、照会したオブジェクトのバッファ、バッファ内のオブジェクト数を受け取ることになる。バッファが一杯である場合、ユーザは次のオブジェクトインデックスグループを照会できる。

10

【0185】

図 38 は、一般情報クエリをともなう操作を示すフローチャートである。図 38 を参照すると、実体から一般情報クエリを受け取った S S A システムは（902）、その実体が認証済みかどうかを判断する（菱形 904）。認証済みである場合には、システムは公開情報と機密情報の共有部分とを実体に供給する（ブロック 906）。認証済みでなければ、システムは公開情報のみを実体に供給する（ブロック 908）。

20

【0186】

図 39 は、非公開情報クエリをともなう操作を示すフローチャートである。図 39 を参照すると、実体から非公開情報クエリを受け取った S S A システムは（922）、その実体が認証済みかどうかを判断する（菱形 924）。認証済みである場合には、システムは実体に機密情報を供給する（ブロック 926）。認証済みでない場合には、システムは機密情報に対する実体のアクセスを拒否する（ブロック（928））。

【0187】

フィーチャセットエクステンション（F S E）

多くの場合、データ処理活動（例えば、D R M ライセンスオブジェクト検査）をカード上の S S A の内部で実行できることは大変有利である。その結果、データ処理タスクのすべてをホストで実行する代替的な解決策に比べてより安全でより効率的なシステムとなり、ホストへの依存度も低くなる。

30

【0188】

S S A セキュリティシステムは、メモリカードによって記憶され、管理され、保護されるオブジェクトのアクセス、使用、収集を制御する一連の認証アルゴリズムと認可方針とを備える。アクセスを得たホストは、メモリ装置に記憶されたデータに対して処理を行い、メモリ装置に対するアクセスは S S A によって制御される。しかし、データは本質的に用途によって大いに異なるため、装置に記憶されたデータを取り扱うわけではない S S A ではデータ形式またはデータ処理は決まっていない。

【0189】

本発明の一実施形態は、通常であればホストによって果たされる機能の一部をメモリカードで実行する形に S S A システムを強化できるという認識に基づく。そこで、ホストのソフトウェア機能のいくつかは、2つの部分、すなわち引き続きホストによって果たされる部分と、カードによって果たされる部分とに分かれる場合がある。こうすることで多くの用途にとってデータ処理の安全性と効率性が向上する。この目的のため、F S E と呼ばれる機構を加えることによって S S A の能力を高める場合がある。このようにカードによって実行される F S E のホストアプリケーションを、ここでは内部アプリケーションまたは装置内部アプリケーションと呼ぶ場合がある。

40

【0190】

強化 S S A システムは、カードの認証およびアクセス制御を提供する基本 S S A コマン

50

ド群を、カードアプリケーションの導入により拡張する機構を提供する。カードアプリケーションは、SSA以外のサービスを（例えば、DRMスキーム、eコマーストランザクション）を実行することになっている。SSAフィーチャセットエクステンション（FSE）は、独自開発のデータ処理ソフトウェア／ハードウェアモジュールで標準SSAセキュリティシステムを強化する機構である。SSA FSEシステムのサービスにより、ホスト装置は前述したクエリで得られる情報のほかに、カードで使用可能なアプリケーションを照会し、特定のアプリケーションを選択し、これと通信できる。前述した一般クエリと非公開クエリをこの目的に使うこともできる。

【0191】

SSA FSEでカード機能群を拡張するには2つの方法を使う。

- ・サービス提供：認可された実体が通信パイプと呼ばれる独自のコマンドチャネルを使って内部アプリケーションと直に通信することによって実現する。

- ・SSA標準アクセス制御方針の拡張：内部の被保護データオブジェクト（CEK、後述するセキュアデータオブジェクト、すなわちSDO等）に内部カードアプリケーションを関連付けさせることによって実現する。そのようなオブジェクトにアクセスするときに所定の標準SSA方針が満たされる場合は関連付けアプリケーションが起動して、標準SSA方針に加えて少なくとも1つの条件を課す。この条件は好ましくは、標準SSA方針とは対峙しない。この追加条件も満たされる場合に限りアクセスが許諾される。FSEの能力をさらに詳述する前に、FSEの構造的態様と通信パイプとSDOをここで取り上げる。

【0192】

SSAモジュールと関連するモジュール

図40Aは、ホスト装置24へ接続されたメモリ装置10（フラッシュメモリカード等）におけるシステムアーキテクチャ1000の機能ブロック図であり、本発明の一実施形態を例示するものである。カード20のメモリ装置にあるソフトウェアモジュールの主要コンポーネントは次のとおりである。

【0193】

SSAトランスポート層1002

SSAトランスポート層はカードプロトコルに依拠する。これはカード10のプロトコル層でホスト側SSA要求（コマンド）を処理し、処理したものをSSM APIに送る。ホストカードの同期とSSAコマンドの識別はすべてこのモジュールで行われる。ホスト24とカード10との間のSSAデータ転送もトランスポート層がすべて担当する。

【0194】

セキュアサービスモジュールコア（SSMコア）1004

このモジュールはSSAの実施例の重要部分である。SSMコアはSSAアーキテクチャを実装する。より具体的に、SSMコアはSSAツリーと、ACRシステムと、前述したシステムを構成する全ルールを実行する。SSMコアモジュールは暗号ライブラリ1012を使ってSSAセキュリティと暗号化、復号化、ハッシュ計算等の暗号機能を支援する。

【0195】

SSMコアAPI1006

これは、ホストと内部アプリケーションがSSMコアと連絡をとりながらSSA操作を実行するところの層である。図40Aに示すように、ホスト24と内部装置アプリケーション1010はいずれも同じAPIを使用する。

【0196】

セキュアアプリケーション管理モジュール（SAMM）1008

SAMMはSSAシステムの一部ではないが、SSAシステムと連絡をとりながら内部装置アプリケーションを制御するカードの重要モジュールである。

実行する内部装置アプリケーションはいずれもSAMMによって管理される。

1. アプリケーションライフサイクルの監視と制御

2. アプリケーションの初期化

3. アプリケーション／ホスト／SSAインターフェイス

【0197】

装置内部アプリケーション1010

これは、カード側での実行が許可されたアプリケーションである。SAMMによって管理され、SSAシステムにアクセスすることがある。ホスト側アプリケーションと内部アプリケーションとの間の通信パイプはSSMコアから提供される。DRMアプリケーションや以降で詳述する使い捨てパスワード(OTP)アプリケーションは内部実行アプリケーションの一例である。

【0198】

装置管理システム(DMS)1011

これは、カードのシステムおよびアプリケーションファームウェアを更新したり、出荷後(一般的に後発行と呼ばれる)モードでサービスを追加／削除したりするためのプロセスおよびプロトコルを収容するモジュールである。

【0199】

図40Bは、SSMコア1004の内部ソフトウェアモジュールの機能ブロック図である。図40Bに示すように、コア1004はSSAコマンド処理部1022を含む。処理部1022は、ホストまたは装置内部アプリケーション1010から発行されたSSAコマンドを解析した後、SSA管理部1024に引き渡す。AGPやACR等のSSAセキュリティデータ構造や、すべてのSSAのルールと方針はいずれもSSAデータベース1026に記憶される。SSA管理部1024は、データベース1026に記憶されたACRやAGPやその他の制御構造によって制御を実施する。IDOやセキュアデータオブジェクトをはじめとするその他のオブジェクトもSSAデータベース1026に記憶される。SSA管理部1024は、データベース1026に記憶されたACRやAGPやその他の制御構造に制御を実施する。SSAが関与しない非セキュア操作はSSA非セキュア操作モジュール1028によって処理される。SSAアーキテクチャのもとでのセキュア操作はSSAセキュア操作モジュール1030によって処理される。モジュール1032は、モジュール1030を暗号ライブラリ1012へ接続するインターフェイスである。1034は、モジュール1026および1028を図1のフラッシュメモリ20へ接続する層である。

【0200】

通信(またはパススルー)パイプ

パススルーパイプオブジェクトは、SSMコアとSAMMの制御下で認可されたホスト側実体と内部アプリケーションとの通信を可能にする。ホストと内部アプリケーションとのデータ転送はSENDコマンドとRECEIVEコマンドで行われる(後述)。実際のコマンドはアプリケーションによって異なる。パイプを作る実体(ACR)は、パイプ名とチャンネルの開通によってつながるアプリケーションのIDとを提供することが必要になる。他の被保護オブジェクトと同様に、このACRがパイプの所有者になり、標準の委譲ルールおよび制限に従って他のACRに使用権や所有権を委譲できる。

【0201】

認証済みの実体は、そのACAMでCREATE_PIPE権限が設定されている場合にパイプオブジェクトの作成が許可されることになる。内部アプリケーションとの通信は、そのPCRでパイプ書き込み権限またはパイプ読み出し権限が設定されている場合に限り許可される。所有権とアクセス権の委譲は、実体がパイプの所有者か、あるいはそのPCRでアクセス権委譲が設定されている場合に限り許可される。他のすべての権限と同様に、別のACRへ所有権を委譲する当初の所有者は、好ましくはこの装置アプリケーションに対するすべての権限から引き離される。

【0202】

好ましくは、ある特定のアプリケーションにつき1つのみの通信パイプを作成する。第2のパイプを作成し、接続済みのアプリケーションにそれを接続する試みは、好ましくは

10

20

30

40

50

S S Mシステム1 0 0 0によって拒否される。したがって、好ましくは、装置内部アプリケーション1 0 1 0のいずれか1つと通信パイプとの間に1対1の関係がある。しかし、（委譲機構により）複数のA C Rが1つの装置内部アプリケーションと通信する場合がある。（別々のアプリケーションに接続された複数パイプの委譲または所有権により）1つのA C Rが数個の装置アプリケーションと通信する場合がある。通信パイプ間のクロストークをなくすため、別々のパイプを制御するA C Rは、好ましくは全く別個のツリーノードに位置する。

【0 2 0 3】

ホストと特定のアプリケーションとのデータ転送は次のコマンドを使って行う。

- ・書き込みパススルー：ホストから装置内部アプリケーションへ非定型データバッファを転送する。

- ・読み出しパススルー：ホストから装置内部アプリケーションへ非定型データバッファを転送し、内部処理が完了したら非定型データバッファをホストに戻す。

【0 2 0 4】

書き込みパススルーコマンドと読み出しパススルーコマンドでは、ホストが通信しようとする相手方の装置内部アプリケーション1 0 0 8のI Dをパラメータとして提供する。実体の権限をベリファイし、要求される側のアプリケーションにつながるパイプを使用する権限が要求する側の実体（すなわち、この実体が使っているセッションを運営するA C R）にある場合、データバッファを解釈し、コマンドを実行する。

この通信方法により、ホストアプリケーションはS S A A C Rセッションチャンネルを通じて内部装置アプリケーションにベンダー固有／独自のコマンドを引き渡すことができる。

【0 2 0 5】

セキュアデータオブジェクト（S D O）

S D Oは、F S Eと併せて使用できる便利なオブジェクトである。

S D Oは汎用容器として機密情報を安全に記憶する役割を果たす。C E Kオブジェクトと同様に、S D OはA C Rが所有し、アクセス権と所有権はA C R間で委譲できる。S D Oは所定の規制に従って保護され使用されるデータを収容し、オプションとして、装置内部アプリケーション1 0 0 8へ至るリンクを有する。機密データは、好ましくはS S Aシステムによって使用されることも解釈されることもなく、オブジェクトの所有者とユーザがこれを使用し、解釈する。換言すると、S S Aシステムは取り扱うデータの情報を認識しない。このため、オブジェクトの中にあるデータの所有者とユーザは、ホストとデータオブジェクトとの間でデータが受け渡しされるときにS S Aシステムとの結び付きによって機密情報が失われることをさほど心配せずにすむ。S D Oオブジェクトはホストシステム（または内部アプリケーション）によって作成され、C E Kを作成する場合と同様に、文字列I Dが割り当てられる。作成する場合にホストは名前のほかに、S D OへリンクするアプリケーションのアプリケーションI Dと、S S Aによって記憶され、保全性ベリファイが行われ、検索されるデータブロックとを提供する。

【0 2 0 6】

S D Oは、C E Kと同様に、好ましくはS S Aセッションの中でのみ作成される。このセッションを開放するために使われるA C RがS D Oの所有者となり、S D Oを削除する権利や機密データを読み書きする権利を有するほかにも、S D Oの所有権やこれにアクセスする権限を別のA C R（子A C Rまたは同一A G P内のA C R）に委譲する権利を有する。

【0 2 0 7】

書き込み操作と読み出し操作はS D Oの所有者に限定される。書き込み操作は既存のS D Oオブジェクトデータを提示されたデータバッファで上書きする。読み出し操作はS D Oのデータ記録一式を検索する。

【0 2 0 8】

正式なアクセス権限を有する所有者以外のA C Rには、S D Oのアクセス操作が許可さ

10

20

30

40

50

れる。次の操作が定められている。

・ SDO Set、アプリケーションIDの指定：データはこのアプリケーションIDを有する内部SSAアプリケーションによって処理される。アプリケーションはSDOとの関連付けによって起動する。オプションとして、アプリケーションがSDOオブジェクトの書き込みを行う場合がある。

・ SDO Set、アプリケーションIDの不在：このオプションは無効であり、不正コマンドエラーを促す。Setコマンドにはカードで実行する内部アプリケーションが必要となる。

・ SDO Get、アプリケーションIDの指定：要求はこのアプリケーションIDを有する装置内部アプリケーションによって処理される。アプリケーションはSDOとの関連付けによって起動する。出力は、指定がなくとも、要求する側へ送り返される。オプションとして、アプリケーションがSDOオブジェクトの読み出しを行う場合がある。

・ SDO Get、アプリケーションIDの不在：このオプションは無効であり、不正コマンドエラーを促す。Getコマンドにはカードで実行する内部アプリケーションが必要となる。

・ SDO関連の権限：ACRにはSDOの所有者になるものと、アクセス権限（Set、Get、または両方）を有するのみのものがある。ACRには、自身が所有しないSDOに対する自身のアクセス権を別のACRへ譲渡することが許可される。ACAM権限を有するACRにはSDOの作成とアクセス権の委譲が明示的に許可される。

【0209】

内部ACR

内部ACRはPCRを有するACRに類似するが、装置10にとって外部の実体はこのACRにログインできない。代替的に、これの管理下にあるオブジェクトか、あるいはこのオブジェクトと関連付けするアプリケーションが呼び出されるときに、図40BのSSA管理部1024が自動的に内部ACRにログインする。アクセスを試みる実体はカードまたはメモリ装置にとって内部の実体であるため、認証の必要はない。SSA管理部1024は内部通信を可能にするために内部ACRにセッション鍵を渡すことになる。

【0210】

これより使い捨てパスワード生成とデジタル権利管理という2つの例を引いてFSEの能力を例示する。使い捨てパスワード生成の例を説明する前に、二因子認証のテーマを取り上げる。

【0211】

OTP実施形態

二因子認証（DFA）

DFAは、標準のユーザ信用証明（具体的にはユーザ名とパスワード）に追加の秘密、すなわち「第2の因子」を加えることにより、ウェブサービスサーバ等への私的なログインでセキュリティを高める認証プロトコルである。この第2の秘密は通常、ユーザが所有する物理的で安全なトークンに記憶される。ユーザはログインの過程でログイン信用証明の一部として所有の証拠を提供する必要がある。所有の証明には使い捨てパスワード（OTP）がよく使われ、これはセキュアトークンで生成され出力される、1回のログインのみで通用するパスワードである。トークンなしでOTPを計算するのは暗号技術的に不可能であるため、ユーザが正しいOTPを提供できる場合、これをもってトークン所有の十分な証拠とみなされる。OTPは1回のログインのみで通用し、前のログインから得た古いパスワードは通用しないことになるため、ユーザはログインのときにトークンを所有していなければならない。

【0212】

以降のセクションで説明する製品は、SSAのセキュリティデータ構造と、一連のOTPで次のパスワードを計算するFSE設計とを利用しながら、フラッシュメモリでそれぞれ別々のパスワード系列（異なるウェブサイトへのログインに使用）を生成する複数の「仮想」セキュアトークンを実行するものである。図41は、このシステムのブロック図を

示す。

【0213】

システム一式1050は、認証サーバ1052と、インターネットサーバ1054と、トークン1058を有するユーザ1056とを備える。最初のステップでは、認証サーバとユーザとの間で共有秘密を取り決める（シード提供とも呼ばれる）。ユーザ1056は秘密またはシードの発行を要求し、これをセキュアトークン1058に記憶する。次のステップでは、発行された秘密またはシードを特定のウェブサービスサーバに結合する。これを果たしたら認証に取りかかることができる。ユーザはOTPの生成をトークンに指示する。OTPはユーザ名とパスワードと併せてインターネットサーバ1054へ送信される。インターネットサーバ1054は認証サーバ1052にOTPを転送し、ユーザアイデンティティのベリファイを依頼する。認証サーバもOTPを生成するが、これはトークンとの共有秘密から生成されるため、トークンから生成されたOTPに一致することになる。一致が判明する場合、ユーザアイデンティティはベリファイされ、認証サーバがインターネットサーバ1054へ肯定応答を返すとユーザログインプロセスは完了することになる。

10

【0214】

FSEによるOTP生成には次のような特徴がある。

- ・OTPシードは安全な状態で（暗号化されて）カードに記憶される。
- ・パスワード生成アルゴリズムはカードの内部で実行される。
- ・装置10は複数の仮想トークンをエミュレートでき、それぞれの仮想トークンでは異なるシードを記憶し、異なるパスワード生成アルゴリズムを使用できる。
- ・認証サーバから装置10へシードを移すセキュアプロトコルは装置10が提供する。

20

【0215】

図42は、SSAのOTPシード提供機能とOTP生成機能を示すものであり、ここで実線の矢印は所有権またはアクセス権を示し、破線の矢印は関連付けまたはリンクを示している。図42に示すように、SSA FSEシステム1100ではN個のアプリケーションACR1106によってそれぞれ管理される1つ以上の通信パイプ1104を通じてソフトウェアプログラムコードFSE1102にアクセスできる。後述する実施形態では1つのみのFSEソフトウェアアプリケーションを例示し、各FSEアプリケーションにつき1つのみの通信パイプがある。しかし、複数のFSEアプリケーションを使えることが理解できる。図42には1つのみの通信パイプが例示されているが、複数の通信パイプを使えることが理解できる。そのような変形例はいずれも可能である。図40A、40B、および42を参照すると、FSE1102はOTP提供に用いるアプリケーションであって、図40Aの装置内部アプリケーション1010の一部をなす場合がある。制御データ構造（ACR1101、1103、1106、1110）はSSAのセキュリティデータ構造の一部であり、SSAデータベース1026に記憶される。IDO1120やSDOオブジェクト1122等のデータ構造と通信パイプ1104もSSAデータベース1026に記憶される。

30

【0216】

図40Aおよび図40Bを参照すると、ACRとデータ構造が関わるセキュリティ関連操作（例えば、セッション中のデータ転送、暗号化、復号化、ハッシュ計算等の操作）は、モジュール1030がインターフェイス1032と暗号ライブラリ1012の支援を受けて処理する。SSMコアAPI1006は、ホストと受け渡しするACR（外部ACR）が関わる操作と、ホストと受け渡ししない内部ACRが関わる操作を区別しないため、ホストが関わる操作と装置内部アプリケーション1010が関わる操作に区別はない。ホスト側実体によるアクセスと装置内部アプリケーション1010によるアクセスは、同じ制御機構によって制御される。このため、ホスト側アプリケーションと装置内部アプリケーション1010とでデータ処理を柔軟に区別できる。内部アプリケーション1010（例えば、図42のFSE1102）は内部ACR（例えば、図42のACR1103）と関連付けし、これの管理のもとで起動する。

40

50

【0217】

さらに、重要情報へのアクセス、例えばSDOの内容またはそのSDOの内容から検索される情報へのアクセスは、好ましくはACRやAGP等のセキュリティデータ構造とSSAのルールと方針とによって管理されるため、外部または内部アプリケーションは、SSAのルールと方針とに従う限りにおいてその内容または情報にアクセスできる。例えば、2名のユーザがデータを処理するために個々の装置内部アプリケーション1010を起動する場合、別々の階層ツリーに位置する内部ACRを使って2名のユーザによるアクセスが制御されるため、アプリケーション間のクロストークはない。両ユーザはデータ処理する場合に共通の装置内部アプリケーション1010にアクセスでき、SDOの内容または情報の所有者の側では、内容または情報制御の喪失を心配せずにすむ。例えば、データを記憶するSDOに対する装置内部アプリケーション1010によるアクセスは別々のツリーに位置するACRによって制御できるため、アプリケーション間のクロストークはない。この制御方法は、前述したデータに対するアクセスをSSAが制御する方法に似ている。これは、データオブジェクトに記憶されたデータのセキュリティを内容の所有者とユーザに提供する。

10

【0218】

図42を参照すると、OTP関連ホストアプリケーションに必要なソフトウェアアプリケーションコードの一部分を、FSE1102のアプリケーションとしてメモリ装置10に記憶（メモリカード発行前に予め記憶、またはメモリカード発行後にロード）することは可能である。そのようなコードを実行する場合、ホストはまずN個の認証ACR1106のいずれか1つを通じて認証を受け、パイプ1104にアクセスする必要がある、Nは正の整数である。ホストは、起動しようとするOTP関連アプリケーションを識別するためのアプリケーションIDを提供する必要もある。認証に成功したら、OTP関連アプリケーションと関連付けられたパイプ1104を通じてそのようなコードにアクセスし、実行できる。前述したように、パイプ1104と、OTP関連内部アプリケーション等のアプリケーションとの間には、好ましくは1対1の関係がある。図42に示すように、複数のACR1106が共通のパイプ1104を制御することがある。1つのACRで複数のパイプを制御する場合がある。

20

【0219】

図42には、データ、例えばOTP生成のためのシードをそれぞれ収容するオブジェクト1114と総称するセキュアデータオブジェクトSDO1、SDO2、およびSDO3が示され、このシードは貴重であって、好ましくは暗号化する。3つのデータオブジェクトとFSE1102との間のリンクまたは関連付け1108はこれらのオブジェクトの一属性であり、いずれか1つのオブジェクトにアクセスするときには、アプリケーションIDがSDO属性に一致するFSE1102のアプリケーションが起動し、このアプリケーションは装置のCPU12によって実行され、さらなるホストコマンドを受け取る必要はない（図1）。

30

【0220】

図42を参照すると、OTPプロセスを制御するためのセキュリティデータ構造（ACR1101、1103、1106、および1110）とそのPCRは、ユーザがOTPプロセスを開始する前に作成済みである。ユーザは、認証サーバACR1106のいずれか1つを通じてOTP装置内部アプリケーション1102を起動するためのアクセス権を得る必要がある。ユーザは、N個のユーザACR1110のいずれか1つを通じてOTPに対するアクセス権を得る必要がある。SDO1114はOTPのシード提供過程で作成できる。IDO1116は、好ましくは作成済みで内部ACR1103によって制御される。内部ACR1103は、作成されたSDO1114も制御する。SDO1114にアクセスするときには、図40BのSSA管理部1024が自動的にACR1103にログインする。内部ACR1103にはFSE1102が関連付けられる。破線1108に示すように、OTPのシード提供過程ではSDO1114にFSEを関連付けさせる。関連付けが成立した後、ホストがSDOにアクセスするときには、ホストからさらなる要求がな

40

50

くとも関連付け1108によってFSE1102が起動する。N個のACR1106のいずれか1つを通じて通信パイプ1104にアクセスするときにも、図40BのSSA管理部1024がACR1103に自動的にログインする。いずれの場合でも(SDO1114とパイプ1104へのアクセス)、SSA管理部はFSE1102にセッション番号を渡し、このセッション番号によって内部ACR1103に至るチャンネルが識別される。

【0221】

OTP操作は2つの段階、すなわち図43に示すシード提供段階と図44に示すOTP生成段階とを伴う。図40～図42も併せて参照することで、この説明に役立つ。図43はシード提供プロセスを示すプロトコル図である。図43に示すように、ホスト24等のホストとカードは様々な動作をとる。SSMコア1004を含む図40Aおよび40BのSSMシステムは、カード側で様々な動作をとる1 実体である。図42に示すFSE1102もカード側で様々な動作をとる 実体である。

10

【0222】

二因子認証ではユーザがシードの発行を要求し、発行されたシードはセキュアトークンに記憶される。この例のセキュアトークンはメモリ装置またはカードである。ユーザはSSMシステムにアクセスするため、図42の認証ACR1106のいずれか1つで認証を受ける(矢印1122)。認証に成功したと仮定し(矢印1124)、ユーザはシードを要求する(矢印1126)。ホストは、シード要求に署名するためのアプリケーション1102を選択してシード要求に署名する要求をカードへ送る。起動すべきアプリケーションIDをユーザが知らない場合、例えば装置に対する非公開クエリにより、この情報を装置10から入手できる。そして、ユーザは起動するべきアプリケーションのアプリケーションIDを入力し、これによりこのアプリケーションに対応する通信パイプも選択される。パススルーコマンドにより、ユーザから該当する通信パイプを通じてアプリケーションIDで指定されたアプリケーションにかけて、ユーザコマンドが転送される(矢印1128)。起動したアプリケーションは、図42のIDO1112等の所定のIDOの公開鍵による署名を要求する。

20

【0223】

SSMシステムはIDOの公開鍵を用いてシード要求に署名し、署名の完了をアプリケーションに通知する(矢印1132)。次に、起動アプリケーションはIDOの証明書チェーンを要求する(矢印1134)。これに応じて、SSMシステムは、ACR1103の制御下でIDOの証明書チェーンを提供する。起動アプリケーションは通信パイプを通じて署名済みシード要求とIDOの証明書チェーンをSSMシステムへ提供し、SSMシステムは同じものをホストへ転送する(矢印1138)。通信パイプにおける署名済みシード要求とIDO証明書チェーンの送信は、図40AのSMM1008とSSMコア1004との間で確立するコールバック関数によって行われるが、このコールバック関数については以降で詳述する。

30

【0224】

ホストが受け取った署名済みシード要求とIDO証明書チェーンは、図41に示す認証サーバ1052へ送信される。署名済みシード要求の出所が信用できるトークンであることはカードから提供される証明書チェーンで証明されているため、認証サーバ1052には秘密シードをカードに提供する用意がある。そこで認証サーバ1052は、IDOの公開鍵で暗号化されたシードをユーザACR情報と併せてホストに送信する。このユーザ情報により、N個のユーザACRのうち、これから生成するOTPにユーザがアクセスするためのユーザACRがいずれであるのかが明らかになる。ホストはアプリケーションIDを提供することによってFSE1102でOTPアプリケーションを起動し、これによりこのアプリケーションに対応する通信パイプも選択され、さらにホストはユーザACR情報をSSMシステムへ転送する(矢印1140)。暗号化されたシードとユーザACR情報は通信パイプを通じて選択されたアプリケーションへ転送される(矢印1142)。起動したアプリケーションは、IDOの秘密鍵を使ってシードを復号化する要求をSSMシステムに送る(矢印1144)。SSMシステムはシードを復号化し、復号化の完了を伝

40

50

える通知をアプリケーションに送る（矢印1146）。起動アプリケーションは、セキュアデータオブジェクトを作成し、そのセキュアデータオブジェクトにシードを記憶することを要求する。起動アプリケーションは、使い捨てパスワードを生成するため、そのSDOにOTPアプリケーション（要求するアプリケーションと同じアプリケーションであってもよい）のIDを割り振ることも要求する。SSMシステムはSDO1114のいずれか1つを作成し、そのSDOの中にシードを記憶し、OTPアプリケーションのIDをSDOに割り振り、完了したらアプリケーションに通知を送る（矢印1150）。アプリケーションは、ホストから提供されたユーザ情報に基づきSDO1114にアクセスするためのアクセス権を内部ACRから該当するユーザACRへ委譲することをSSMシステムに要求する（矢印1152）。委譲が完了したらSSMシステムはアプリケーションに通知する（矢印1154）。アプリケーションは、コールバック関数によりSDOの名前（スロットID）を通信パイプ経由でSSMシステムへ送信する（矢印1156）。SSMシステムは同じものをホストへ転送する（矢印1158）。ホストはSDOの名前をユーザACRに結合し、このため、ユーザはSDOにアクセスできるようになる。

【0225】

今度は図44のプロトコル図を参照しながらOTP生成プロセスを説明する。ユーザは使い捨てパスワードを入手するため、アクセス権があるユーザACRにログインする（矢印1172）。認証に成功したと仮定し、SSMシステムはホストに通知し、ホストは「get SDO」コマンドをSSMへ送信する（矢印1174、1176）。前述したように、シードを記憶するSDOにはOTPを生成するアプリケーションが関連付けられている。したがって、これまでのように通信パイプ経由でアプリケーションを選択する代わりに、矢印1176のコマンドでアクセスするSDOとOTP生成アプリケーションとの関連付けによってOTP生成アプリケーションを起動する（矢印1178）。OTP生成アプリケーションは、SDOから内容（すなわち、シード）を読み出すことをSSMシステムに要求する。好ましくは、SSMはSDOの内容に含まれる情報を認識せず、FSEの指示に従ってSDOのデータを処理するに過ぎない。シードが暗号化されている場合、FSEの指示に従い読み出しを行う前にシードを復号化することが必要となる場合がある。SSMシステムはSDOからシードを読み出し、OTP生成アプリケーションへシードを提供する（矢印1182）。OTP生成アプリケーションはOTPを生成し、これをSSMシステムに提供する（矢印1184）。OTPはSSMによってホストへ転送され（矢印1186）、さらにホストから認証サーバ1052へOTPが転送され、二因子認証プロセスは完了する。

【0226】

コールバック関数

図40AのSSMコア1004とSAMM1008との間では汎用コールバック関数を確立する。そのような関数には様々な装置内部アプリケーションと通信パイプを登録できる。起動した装置内部アプリケーションはこのコールバック関数を使用することにより、アプリケーションへのホストコマンドの引き渡しに使われたものと同じ通信パイプを使って処理後のデータをSSMシステムへ引き渡すことができる。

【0227】

DRMシステム実施形態

図45はDRMシステムを示す機能ブロック図であり、このシステムでは通信パイプ1104'と、FSEアプリケーション1102'に至るリンク1108'を備えるCEK1114'と、DRM機能の実行機能を制御する制御構造1101'、1103'、1106'とを使用する。見て分かるように、図45のアーキテクチャはセキュリティデータ構造として認証サーバACRとユーザACRの代わりにライセンスサーバACR1106'と再生ACR1110'を含み、さらにSDOの代わりにCEK1114'を含む点を除き、図42のものによく似ている。加えて、IDOは関係しないから図45で省かれている。CEK1114'はライセンス提供プロセスの中で作成できる。プロトコル図である図46はライセンス提供とコンテンツダウンロードのプロセスを示すものであり、こ

10

20

30

40

50

ここではライセンスオブジェクトの中で鍵が提供される。O T Pの実施例と同様に、ライセンスの取得を望むユーザはまず、N個のA C R 1 1 0 6 'のいずれか1つとN個のA C R 1 1 1 0 'のいずれか1つのもとでアクセス権を取得する必要がある、そうすることでメディアプレーヤソフトウェアアプリケーション等のメディアプレーヤでコンテンツを再生できるようになる。

【0228】

図46に示すように、ホストはライセンスサーバA C R 1 1 0 6 'による認証を受ける(矢印1202)。認証に成功したと仮定し(矢印1204)、ライセンスサーバはライセンスファイルをC E K(鍵I Dと鍵値)と併せてホストに提供する。ホストは、カード上のS S MシステムにアプリケーションI Dを提供することによって起動すべきアプリケーションも選択する。ホストは、プレーヤ情報(例えば、メディアプレーヤソフトウェアアプリケーションの情報)も送信する(矢印1206)。このプレーヤ情報により、N個の再生A C R 1 1 1 0 'のうち、プレーヤのアクセス権がある再生A C Rがいずれであるのかが明らかになる。S S Mシステムは、選択されたアプリケーションに対応する通信パイプを通じてライセンスファイルとC E KをD R Mアプリケーションへ転送する(矢印1208)。起動したアプリケーションは、ライセンスファイルを非表示パーティションに書き込むことをS S Mシステムに要求する(矢印1210)。ライセンスファイルがそのとおりに書き込まれたら、S S Mシステムはアプリケーションに通知する(矢印1212)。D R MアプリケーションはC E Kオブジェクト1114'の作成を要求し、ライセンスファイルからその中に鍵値を記憶する。D R Mアプリケーションは、提供された鍵に関連するライセンスをチェックするD R MアプリケーションのI DをC E Kオブジェクトに割り振ることも要求する(矢印1214)。S S Mシステムはこれらのタスクを完了し、その旨をアプリケーションに通知する(矢印1216)。アプリケーションは、ホストから送信されたプレーヤ情報に基づきC E K 1 1 1 4 'に対するコンテンツの読み出しアクセス権をプレーヤがアクセスできる再生A C Rへ委譲することを要求する(矢印1218)。S S Mシステムは委譲を行い、その旨をアプリケーションに通知する(矢印1220)。ライセンスの記憶が完了したことを伝えるメッセージがアプリケーションから通信パイプを経由しS S Mシステムへ送信され、S S Mシステムはこれをライセンスサーバへ転送する(矢印1222および1224)。通信パイプ経由のこの操作にはコールバック関数を使用する。この通知を受けたライセンスサーバは、提供されたC E Kの鍵値によって暗号化されたコンテンツファイルをカードに提供する。暗号化されたコンテンツはホストによってカードの公開領域に記憶される。暗号化されたコンテンツファイルの記憶にセキュリティ機能は関与しないため、S S Mシステムは記憶に関与しない。

【0229】

図47は、再生操作を示す。ユーザはホストを通じて該当する再生A C R(すなわち、前述した矢印1152および1154で読み出し権を委譲された再生A C R)による認証を受ける(矢印1242)。認証に成功したと仮定し(矢印1244)、ユーザは鍵I Dと関連付けられたコンテンツの読み出し要求を送る(矢印1246)。要求を受け取ったS S Mシステムは、アクセスされているD R MアプリケーションのI DがC E Kオブジェクトに関連付けられていることに気づき、識別されたD R Mアプリケーションを起動する(矢印1248)。このD R Mアプリケーションは、鍵I Dと関連付けられたデータ(すなわち、ライセンス)の読み出しをS S Mシステムに要求する(矢印1250)。読み出し要求があったデータの情報を認識しないS S Mは、F S Eからの要求を処理してデータの読み出しプロセスを実行するに過ぎない。S S Mシステムは非表示パーティションからデータ(すなわち、ライセンス)を読み出し、そのデータをD R Mアプリケーションに提供する(矢印1252)。D R Mアプリケーションはデータを解釈し、データの中にあるライセンス情報をチェックして、ライセンスが有効かどうかを確認する。ライセンスがなお有効である場合、D R Mアプリケーションはコンテンツの復号化が許可されることをS S Mシステムに知らせる(矢印1254)。S S Mシステムは要求のあったコンテンツをC E Kオブジェクトの鍵値を使って復号化し、復号化されたコンテンツを再生するために

10

20

30

40

50

ホストに提供する（矢印1256）。ライセンスがすでに有効でない場合、コンテンツアクセスの要求は拒否される。

【0230】

ライセンスサーバからのライセンスファイルで鍵が提供されない場合のライセンス提供とコンテンツのダウンロードは、図46に示す場合といくぶん異なる。図48のプロトコル図はそのような別方式を示す。図46および図48で同じステップは同じ数字で識別されている。このため、ホストとSSMシステムはまず初めに認証に取り組む（矢印1202、1204）。ライセンスサーバはホストにライセンスファイルと鍵IDを提供するが鍵値は提供せず、ホストはそれらを、起動しようとするDRMアプリケーションのアプリケーションIDと併せて、SSMシステムへ転送する。ホストはプレーヤ情報も送信する（矢印1206'）。SSMシステムは、選択されたアプリケーションに対応する通信パイプを通じて選択されたDRMアプリケーションへライセンスファイルと鍵IDを転送する（矢印1208）。DRMアプリケーションは、非表示パーティションへのライセンスファイル書き込みを要求する（矢印1210）。ライセンスファイルがそのとおりに書き込まれたら、SSMシステムはDRMアプリケーションに通知する（矢印1212）。DRMアプリケーションは、鍵値を生成することと、CEKオブジェクトを作成することと、そこに鍵値を記憶することと、CEKオブジェクトにDRMアプリケーションのIDを割り振ることとをSSMシステムに要求する（矢印1214'）。要求に応じたSSMシステムはDRMアプリケーションへ通知を送る（矢印1216）。DRMアプリケーションは、ホストからのプレーヤ情報に基づきCEKオブジェクトに対する読み出しアクセス権を再生ACRに委譲することをSSMシステムに要求する（矢印1218）。これが完了すると、SSMシステムはその旨をDRMアプリケーションに通知する（矢印1220）。DRMアプリケーションはライセンスが記憶されたことをSSMシステムに通知するが、この通知はコールバック関数により通信パイプ経由で送信される（矢印1222）。通知はSSMシステムによってライセンスサーバへ転送される（矢印1224）。ライセンスサーバは鍵IDと関連付けられたコンテンツファイルをSSMシステムへ送信する（矢印1226）。SSMシステムは鍵IDによって識別された鍵値でコンテンツファイルを暗号化するが、アプリケーションはこれに一切関与しない。暗号化されたカードに記憶されたコンテンツは、図47のプロトコルを用いて再生できる。

【0231】

前述したOTP実施形態とDRM実施形態で、ホスト装置は様々なOTPアプリケーションとDRMアプリケーションをFSE1102および1102'で選ぶことができる。ユーザは所望の装置内部アプリケーションを選択し、起動できる。しかし、SSMモジュールとFSEとの全体的関係は常に同じであるため、ユーザとデータの提供者はSSMモジュールとの受け渡しやFSEを起動する場合に標準のプロトコル群を使用することができる。ユーザと提供者は、独自に開発されたものを含む様々な装置内部アプリケーションの詳細に関わる必要はない。

【0232】

さらに、図46および図48がそうであるように、提供プロトコルはいくぶん異なることがある。図46の場合、ライセンスオブジェクトは鍵値を収容するが、図48の場合は鍵値を収容しない。このような違いから、前述したような若干異なるプロトコルが必要となる。しかし、図47における再生は、ライセンス提供のあり方にかかわらず同じである。したがって、この違いが問題となるのは通常であればコンテンツの提供者と配布者のみであって、再生段階にしか通常かわらない消費者には関係ない。このアーキテクチャは、プロトコルのカスタマイズする場合にコンテンツの提供者や配布者に多大な柔軟性を提供しつつ、消費者にとっては扱いやすい状態のままである。当然、3つ以上の提供プロトコル群によって提供されるデータから検索される情報でも、第2のプロトコルを用いてアクセスできる。

【0233】

前述した実施形態から提供される別の利点として、ユーザ等の外部実体と装置内部アプ

リケーションはいずれもセキュリティデータ構造によって制御されるデータを利用するが、ユーザがアクセスできるものは装置内部アプリケーションによって記憶データから検索される結果のみである。O T P実施形態の場合、ホスト装置を通じてユーザが入手できるものはO T Pのみであって、シード値は入手できない。D R M実施形態の場合、ホスト装置を通じてユーザが入手できるものは再生されたコンテンツのみであって、ライセンスファイルまたは暗号鍵のいずれにもアクセスできない。このため、セキュリティを損なうことなく消費者の便宜を図ることができる。

【0 2 3 4】

D R Mの一実施形態において、装置内部アプリケーションもホストも暗号鍵にアクセスせず、セキュリティデータ構造のみがこれにアクセスする。別の実施形態において、セキュリティデータ構造以外の実体も暗号鍵にアクセスできる。鍵が装置内部アプリケーションによって生成され、セキュリティデータ構造によって制御される場合もある。

10

【0 2 3 5】

装置内部アプリケーションと情報（例えば、O T Pや再生コンテンツ）へのアクセスは同じセキュリティデータ構造によって制御される。これは、制御システムの複雑さとコストを抑える。

装置内部アプリケーションに対するアクセスを制御する内部A C Rから、装置内部アプリケーションを起動することによって得られる情報に対するホストのアクセスを制御するA C Rへ、アクセス権を委譲する能力を提供することにより、前述した特徴および機能が実現可能となる。

20

【0 2 3 6】

アプリケーション別失効制度

セキュリティデータ構造のアクセス制御プロトコルは装置内部アプリケーションの起動時に修正することもできる。例えば、証明書失効プロトコルには、C R Lを使用する標準のプロトコルまたは独自のプロトコルのいずれでもよい。そこで、F S Eを起動することにより、標準のC R L失効プロトコルをF S E独自プロトコルに差し替えることができる。

【0 2 3 7】

S S AはC R L失効制度をサポートするほか、装置内部アプリケーションとC A、あるいはその他の取消機関との私的通信チャネルを通じて装置の内部アプリケーションからホストを無効にすることができる。内部アプリケーション独自の失効制度はホストアプリケーションの関係に限定される。

30

【0 2 3 8】

アプリケーション別失効制度が構成される場合、S S AシステムはC R L（提供される場合）を拒絶することになり、そうでない場合には証明書と独自のアプリケーションデータ（アプリケーション別通信パイプを通じて提供済みのデータ）を用いて証明書が失効済みか否かを判断する。

【0 2 3 9】

前述したように、A C Rでは失効値を指定することによって3通りの失効制度（失効制度なし、標準C R L制度、アプリケーション別失効制度）のどれを採用するかを指定する。アプリケーション別失効制度を選ぶ場合、その失効制度を担当する内部アプリケーションI DもA C Rで指定し、C E T / A P P _ I Dフィールドの値は失効制度を担当する内部アプリケーションI Dに一致することになる。装置を認証する場合、S S Aシステムは内部アプリケーション独自の制度に準拠する。

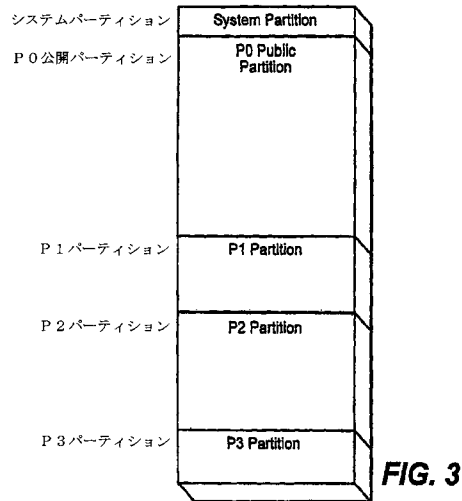
40

【0 2 4 0】

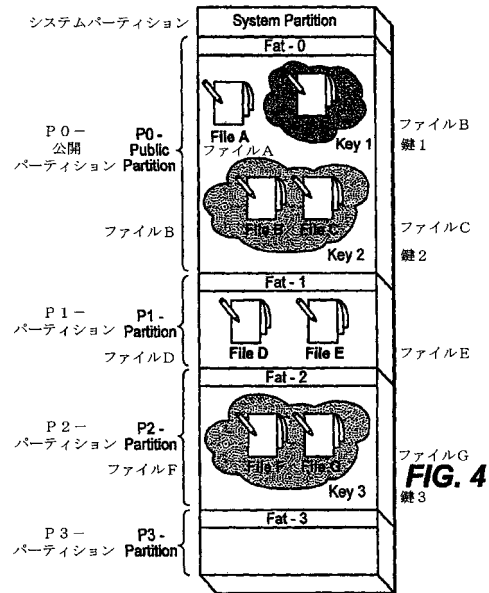
1組のプロトコルを別のものに差し替える代わりに、装置内部アプリケーションを起動する場合、S S Aによって既に施行されているアクセス制御に追加のアクセス条件を設けることもできる。例えば、C E Kの鍵値に対するアクセス権をF S Eでより綿密に調べることができる。鍵値のアクセス権がA C Rにあると判断したS S Aシステムは、F S Eと相談のうえでアクセスを許諾する。これは、コンテンツへのアクセスを制御する場合にコ

50

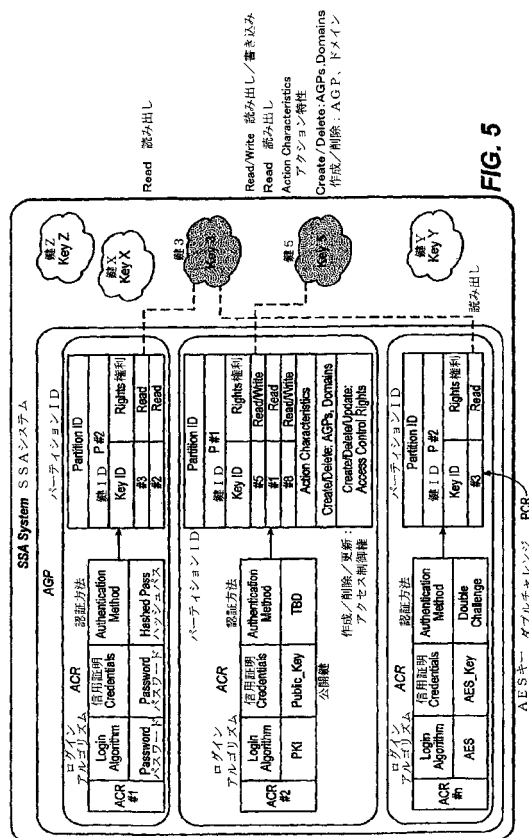
【図 3】



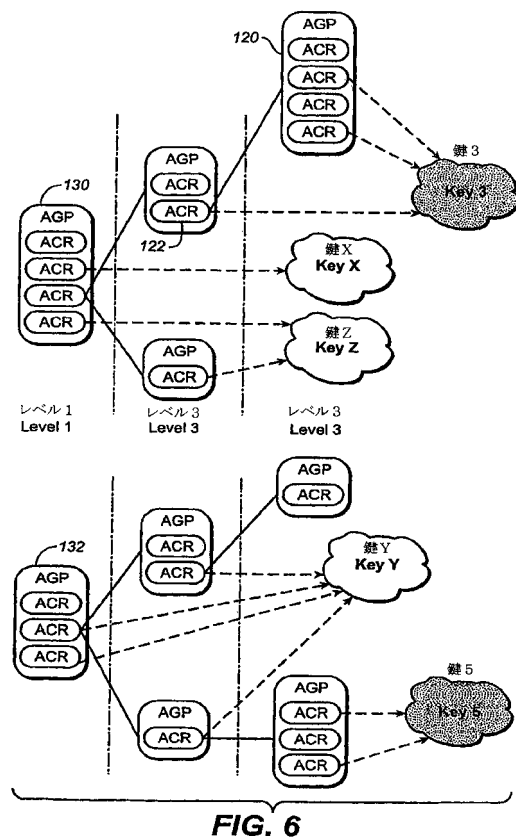
【図 4】



【図 5】



【図 6】



【図 7】

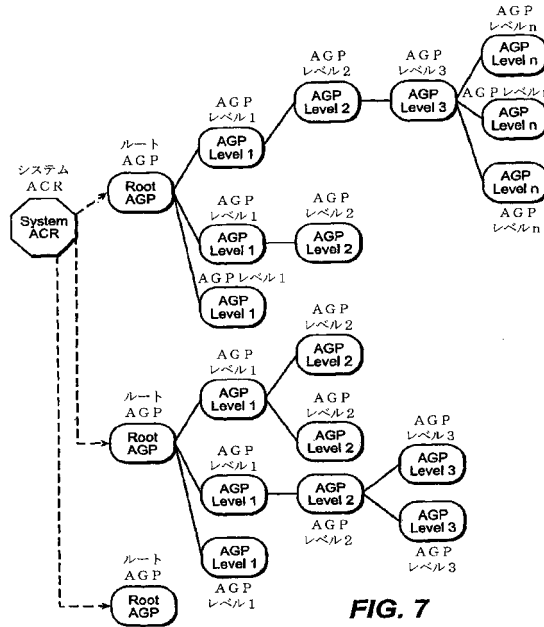


FIG. 7

【図 8 A】

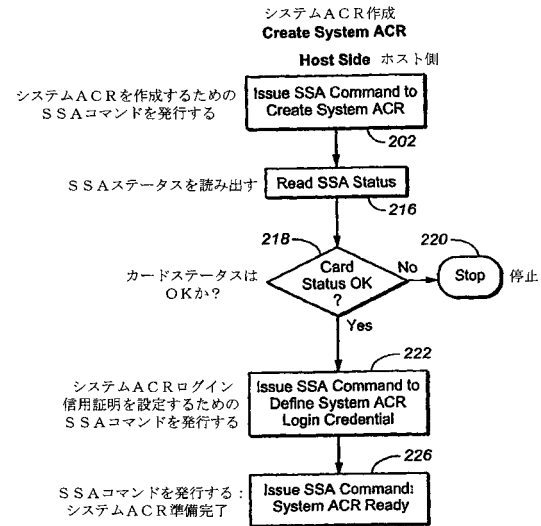


FIG. 8A

【図 8 B】

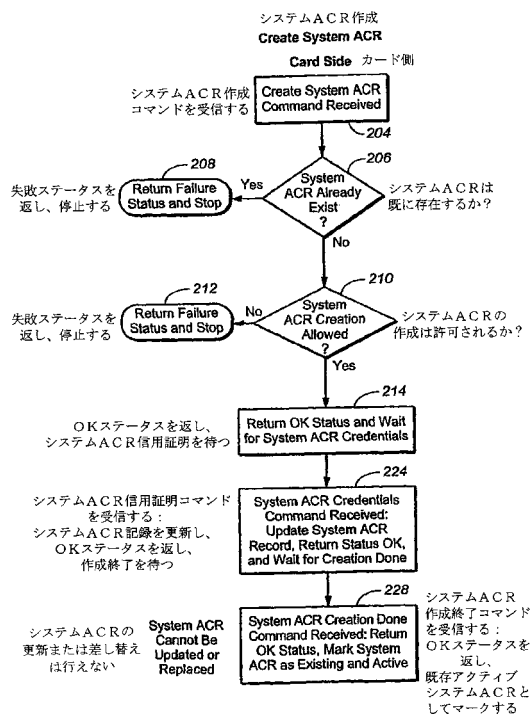


FIG. 8B

【図 9】

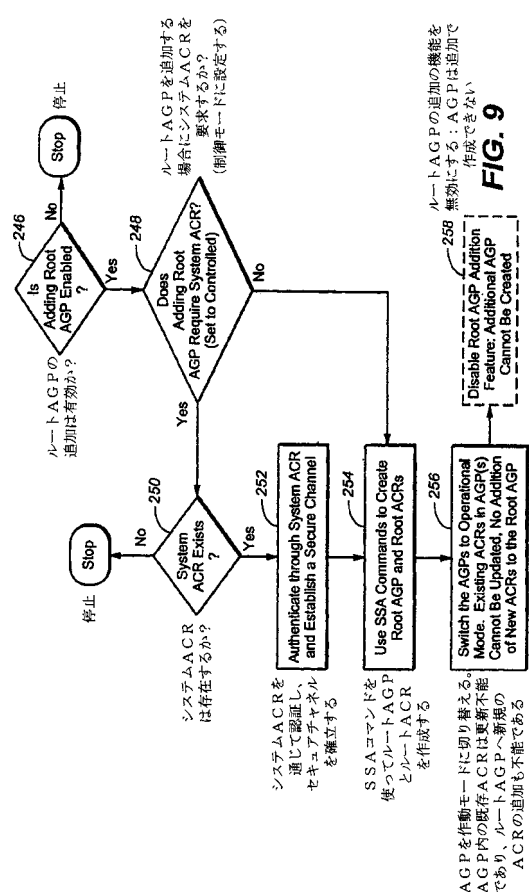
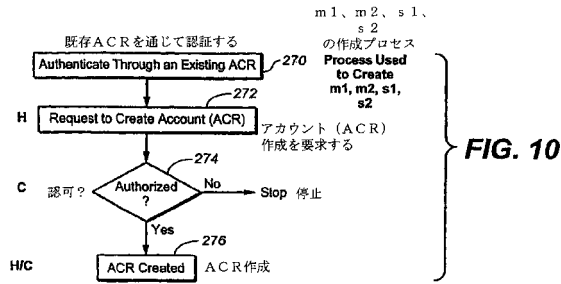
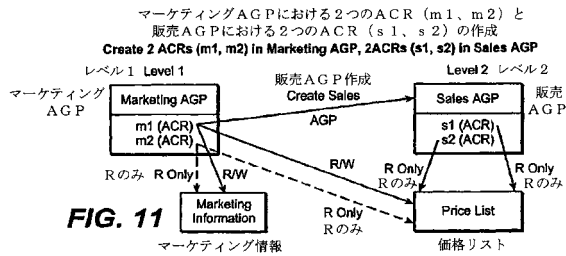


FIG. 9

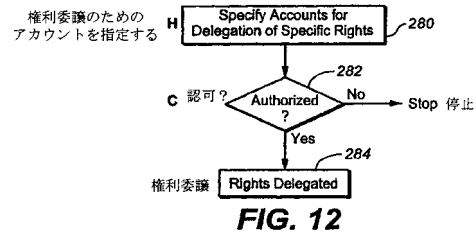
【図 10】



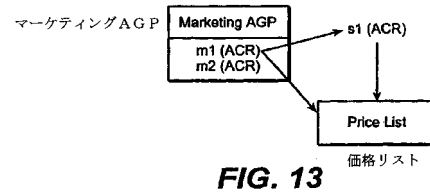
【図 11】



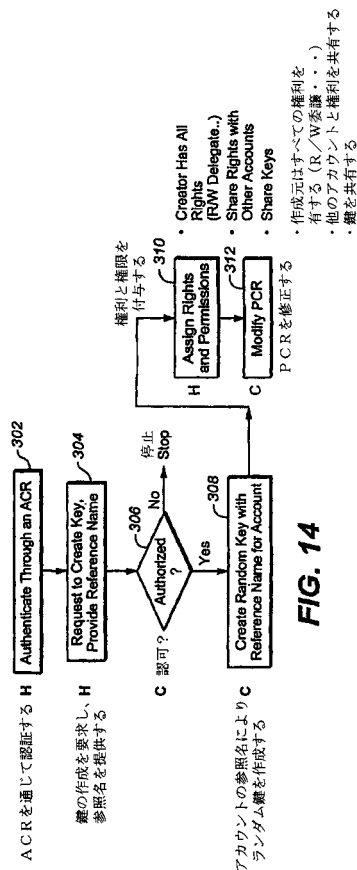
【図 12】



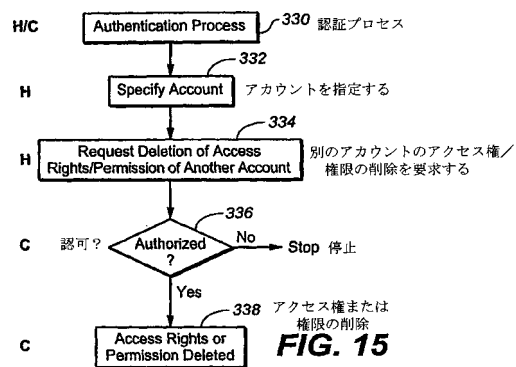
【図 13】



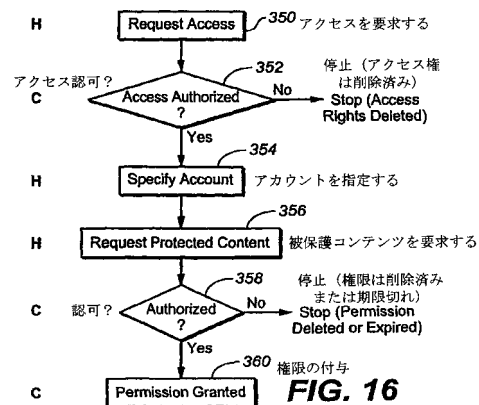
【図 14】



【図 15】



【図 16】



【图 17 B】

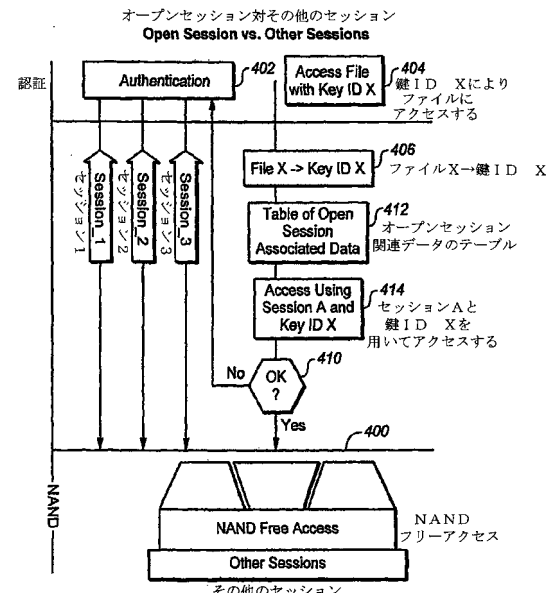
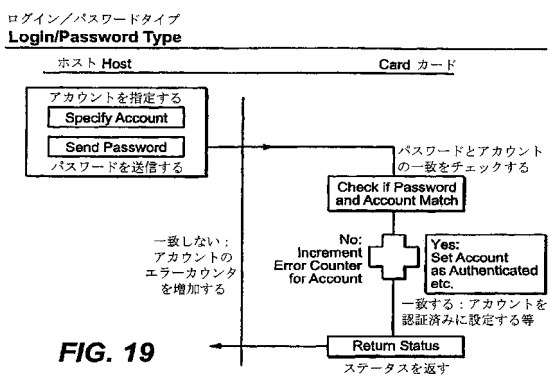


FIG. 17B

【図 19】



【図 20】

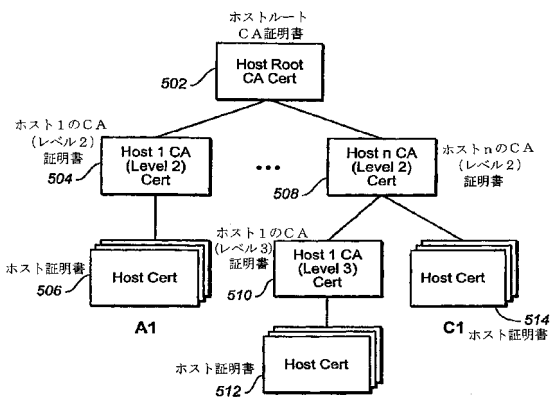


FIG. 20

【図 21】

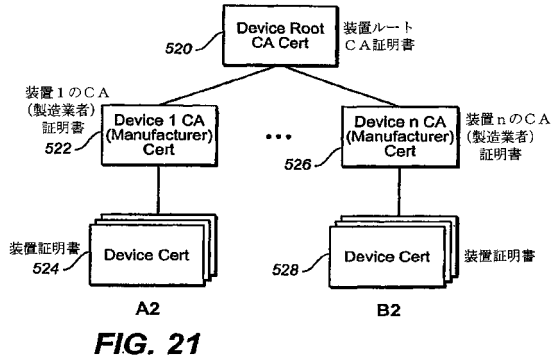


FIG. 21

【図 22】

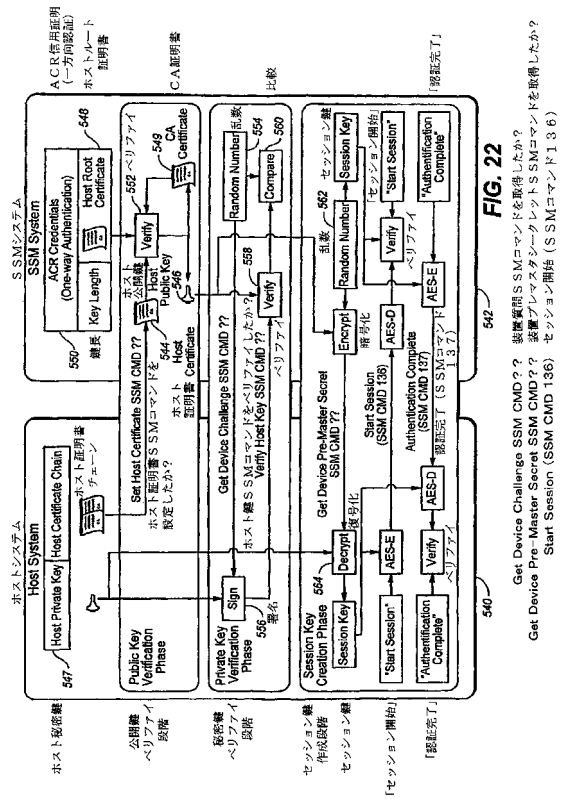


FIG. 22

【図 23 A】

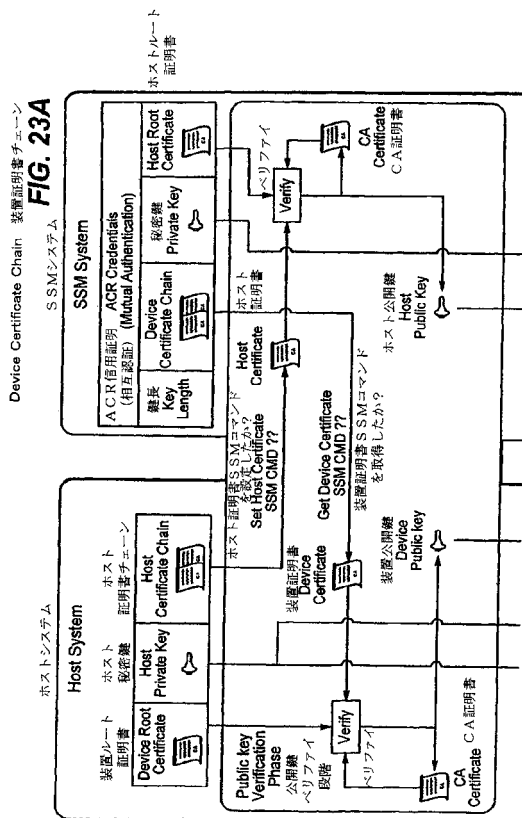


FIG. 23A

【図 23 B】

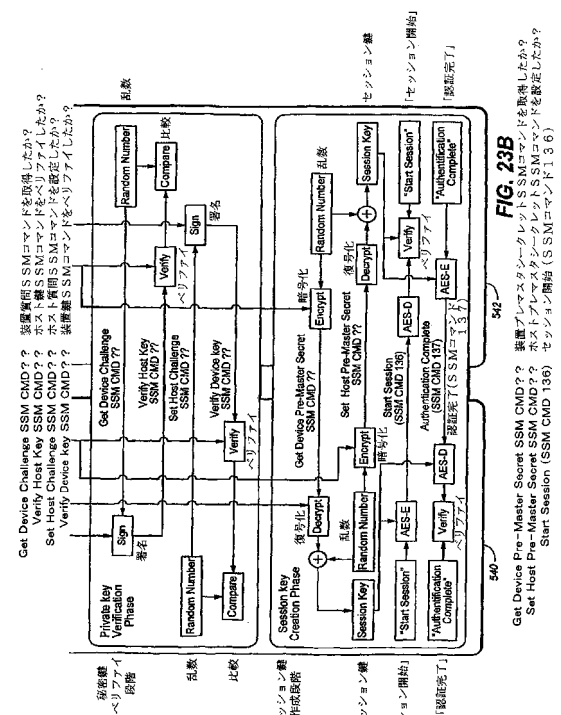
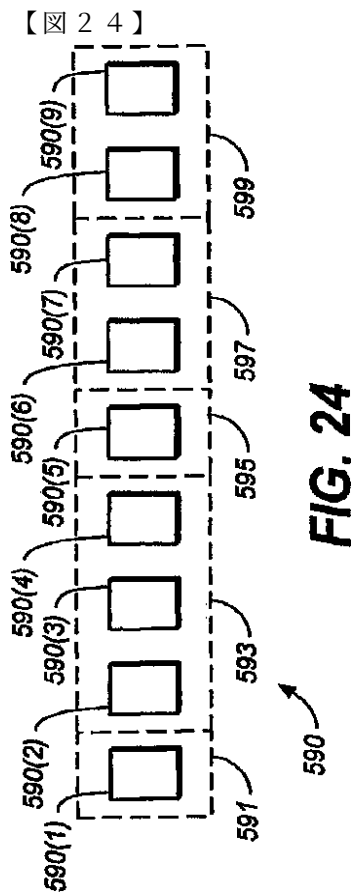


FIG. 23B

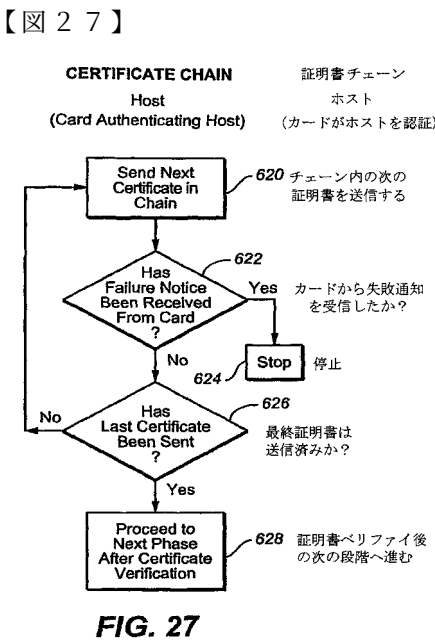
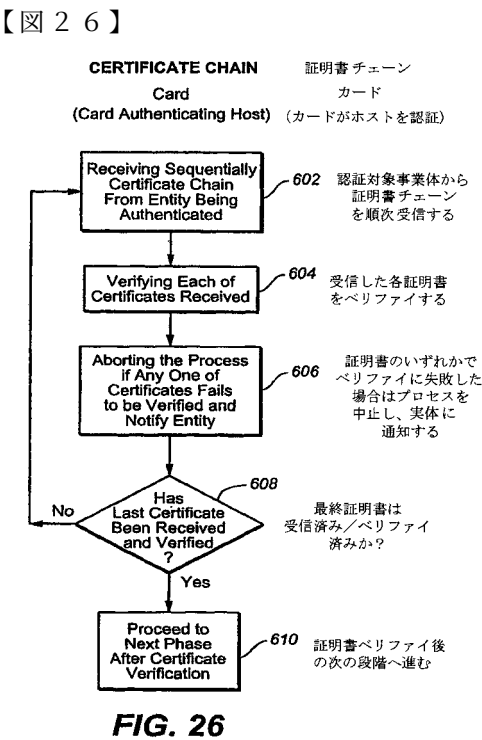


【図 25】

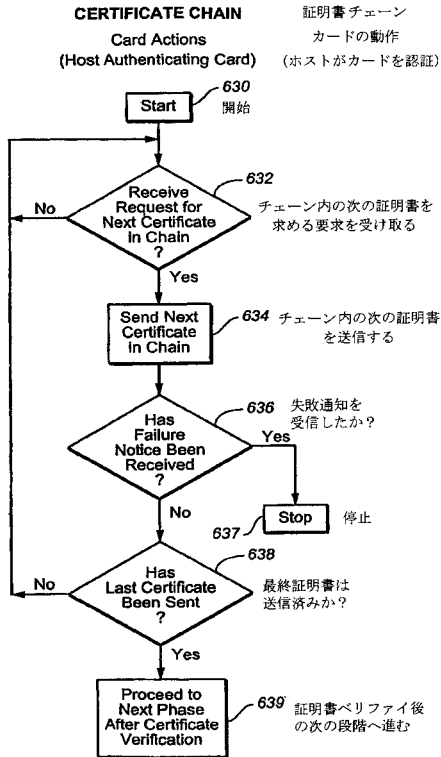
バイト オフセット	引数長さ	引数名	引数型	注釈
0 - 1	2	バイト単位の 証明書サイズ	整数	バイト単位の証明書鍵の 長さ
2	1	「最終」 フラグ	離散	このフラグはチェーンに おける現在の証明書が最終 証明書かどうかを指示する

Byte Offset	Arg. Length	Argument Name	Arg. Type	Comments
0-1	2	Certificate Size in Bytes	Integer	Length of Certificate Key in Bytes
2	1	"Is Final" Flag	Discrete	This Flag Indicates if Current Certificate in the Chain is the Last One

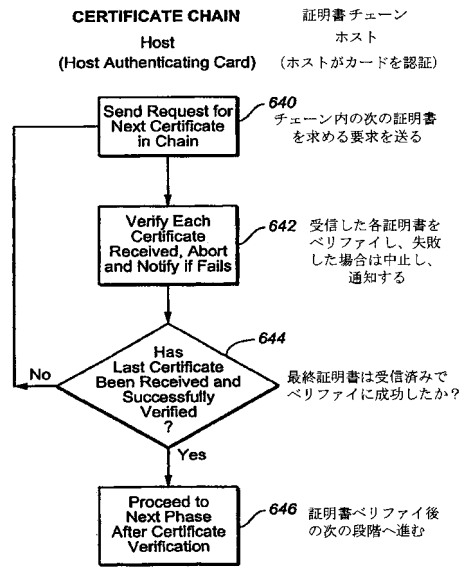
FIG. 25



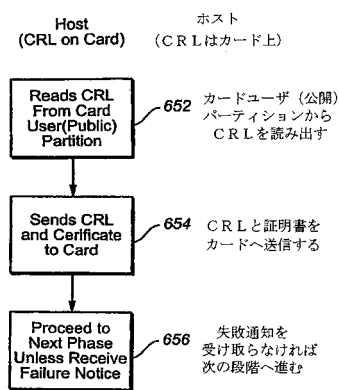
【図 28】



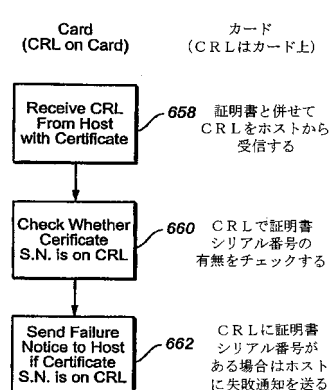
【図 29】



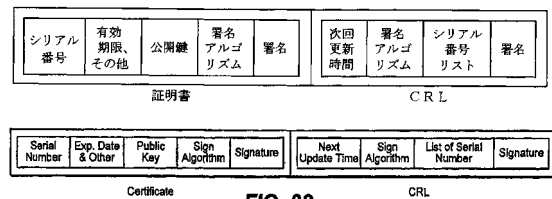
【図 30】



【図 31】



【図 32】



【図 33】

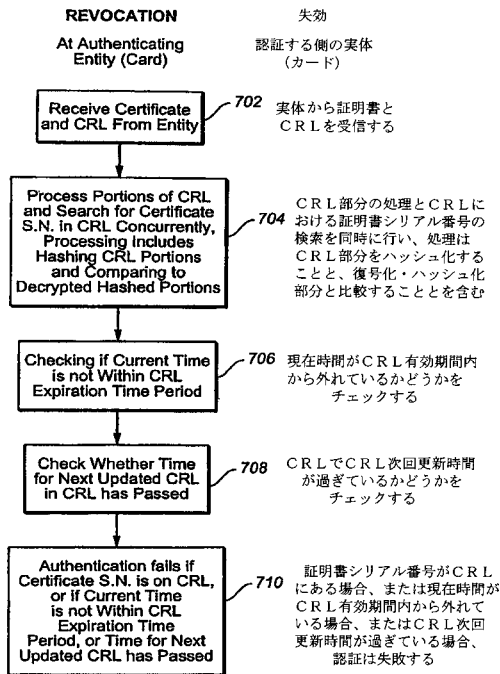


FIG. 33

【図 34】

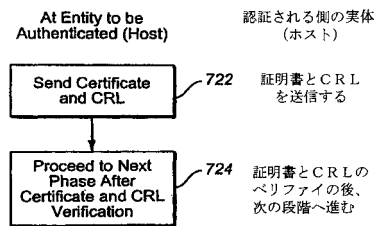


FIG. 34

【図 35】

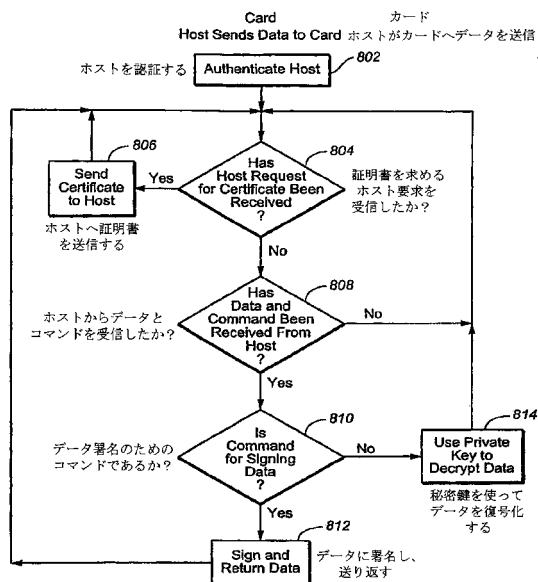


FIG. 35

【図 36】

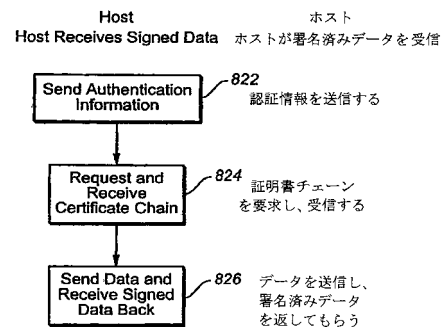


FIG. 36

【図 3 7】

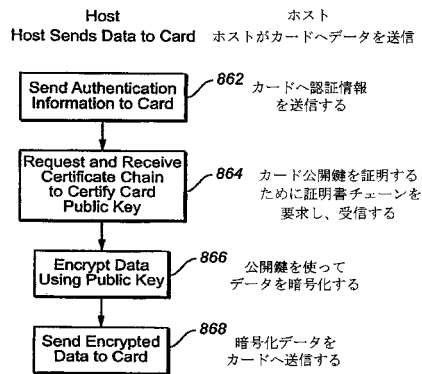


FIG. 37

【図 3 8】

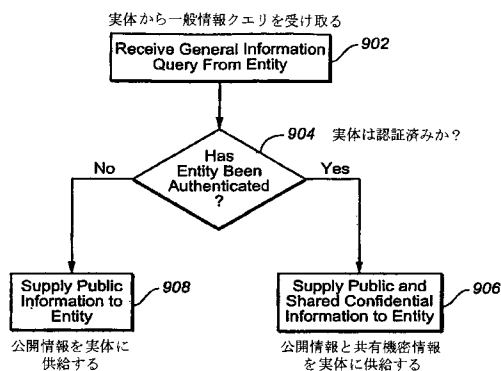
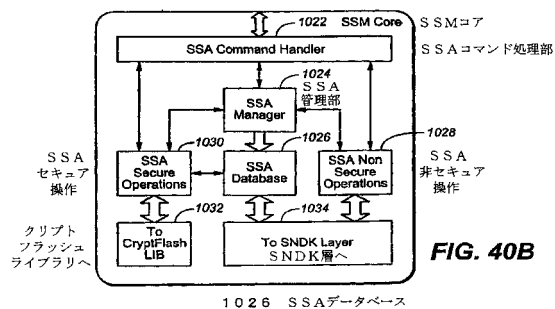


FIG. 38

【図 4 0 B】



【図 4 1】

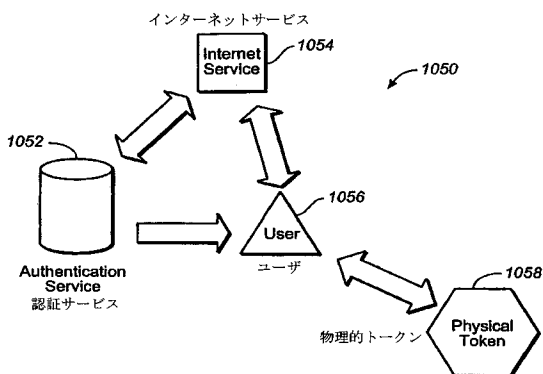


FIG. 41

【图 3 9】

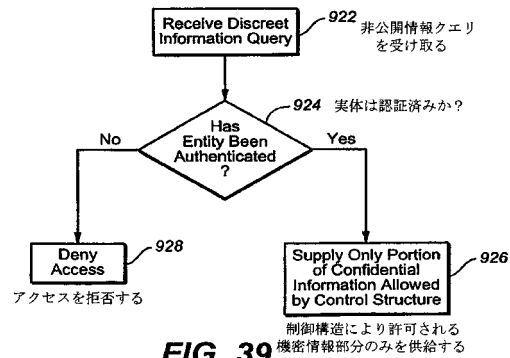


FIG. 39

【図 4 0 A】

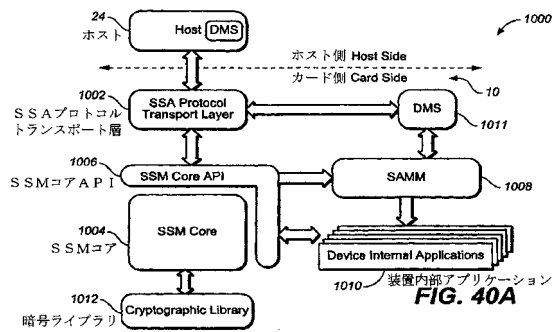
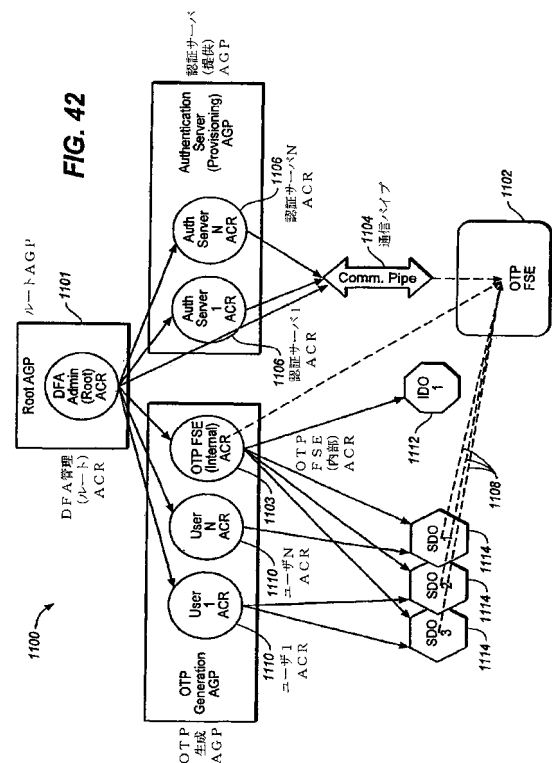


FIG. 40A

【図 4 2】



【图 4 4】



【図 4 6】



```

1178 SDOに割り振られたFSE IDと併せて転送
1180 SDOからのシード読み出しを要求
1182 SDOから読み出されたシード

```



フロントページの続き

(51)Int.Cl. F I
H 0 4 L 9/00 6 7 5 B

(31)優先権主張番号 11/557,041

(32)優先日 平成18年11月6日(2006.11.6)

(33)優先権主張国 米国(US)

(72)発明者 ジョガンドークーロン, ファブリス
アメリカ合衆国、9 4 0 7 0、カリフォルニア州、サン カルロス、バックランド アベニュー
8 5 5

審査官 和田 財太

(56)参考文献 国際公開第2 0 0 6 / 0 6 9 2 7 4 (WO, A 1)
米国特許第0 6 5 8 4 4 9 5 (US, B 1)
再公表特許第2 0 0 6 / 0 8 5 6 4 7 (JP, A 1)

(58)調査した分野(Int.Cl., DB名)
G06F 21/20-21/24
G06F 12/00
G06K 19/073
H04L 9/32