全銀協認証局について

１．はじめに

全国銀行協会（以下、全銀協という。）では、本年 3 月、日本国内で発行され国内外の広い環境で使用される IC キャッシュカードの金融機関間の相互運用性を確保するとともに、IC カード、関連機器、システムベンダ等の開発コストの低廉化を図り、ひいてはセキュリティ・顧客利便性に優れた IC キャッシュカードの普及を期待して、「全銀協 IC キャッシュカード標準仕様」（以下、標準仕様という。）を制定しました。

標準仕様においては、IC キャッシュカード発行のための関連運用体制整備として、①IC カードおよび金融機関 ATM 等の端末の相互運用性を検証し、認定する「認定制度」と②IC キャッシュカードを発行する金融機関を認証し、公開鍵暗号方式を利用した IC カード・端末の認証処理の要となる「全銀協認証局」の構築が必要不可欠のスキームとされています。

２．認証局の必要性

標準仕様では、オフライン取引（オフラインデビット取引による商品購入等）におけるＩＣカード・端末間の「カード認証」および「端末認証」は、公開鍵暗号方式の採用を原則としており、オンライン取引についても、金融機関ホスト対応やＡＴＭ提携ネットワークの対応を考慮し、経過期間中の措置として、ＩＣカード・端末間の認証を共通鍵暗号方式に代わり公開鍵暗号方式を利用して行うことを認めています。

共通鍵暗号方式とは、平文を暗号化するときに使用した鍵と同じ鍵を使用して暗号文を復号する暗号方式で、公開鍵暗号方式とは、平文を暗号化するときに使用した鍵と異なる鍵を使用して暗号文を復号する暗号方式です。この暗号方式では暗号用の鍵と復号用の鍵が異なり、一方の鍵が見られても、その鍵からもう一方の鍵を見つけ出すことは（暗号強度により）困難な仕組みになっています。一般的に、この公開される方の鍵は「公開鍵」、もう一方の鍵は「秘密鍵」と言われます。

さらに、公開鍵暗号方式は、鍵ペア（公開鍵と秘密鍵）のうち、秘密鍵を必ず本人が持つという前提を利用すると、通信相手が本当に自分が通信したかった相手なのかどうかを確かめる相手認証にも利用が可能となります。

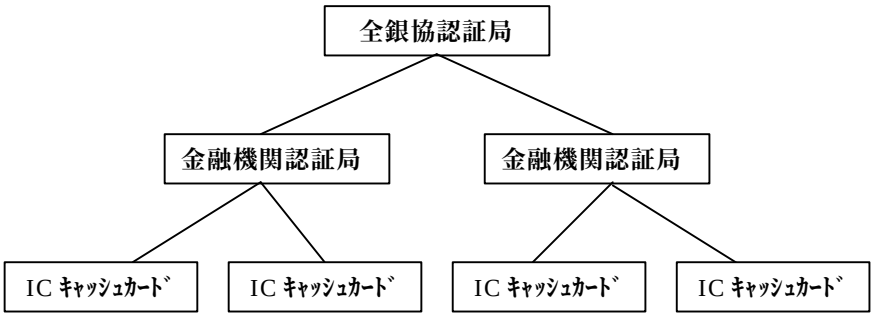
（例）

- Ａは、平文メッセージに自分の秘密鍵でデジタル署名を添付して、Ｂに送付する。
- Ｂは、Ａの公開鍵を使ってＡから来たメッセージの署名を検証し、Ａのメッセージであることを確認することができる。

公開鍵暗号を利用したこの認証においては、認証に使用される公開鍵が正しい鍵であることを証明するため、認証局という証明機関が必要とされます（上記例でいえば、悪意のある第三者がＡになりすます可能性があり、公開鍵が確かにＡの秘密鍵に対応するものであることを信頼できる者に証明してもらうことが必要となります。）。すなわち、認証局は、鍵利用者から信頼され、鍵を保持しているということを公開鍵に署

名することにより、公開鍵証明書を発行する役割を担うのです。

全銀協認証局は、金融機関の公開鍵（発行者公開鍵および端末公開鍵）を登録し、この登録された公開鍵に対して電子的な証明書を発行する上位認証局、すなわち、ルート認証局です（下図参照）。この証明書がＩＣカード・端末間で提示されることによって認証が可能となります。



３．認証局の運営主体

全銀協認証局の運営は、認証局を事業として行うこと、および後述するように、認証業務の一部外部委託に伴う契約を締結する必要があることから法人格を有する社団法人東京銀行協会（以下、東銀協という。）が行うことにしています。

運営に係る経費については、基盤整備等の運営全般にかかる経費を東銀協が支弁する一方、利用者（金融機関）からは証明書の発行費用を徴収することとしています。これは、一つは、全銀協認証局（ルート認証局）の設置が、ＩＣキャッシュカード発行に際して不可欠な存在であり、銀行界としてその基盤を整備する必要があること、また他方で、全銀協認証局の利用は、ＩＣキャッシュカードを発行する銀行に限られ、受益者負担の原則を勘案することが必要であることの両面を考慮したものです。

４．認証局における鍵・証明書およびその配付先

IC キャッシュカードにかかる認証において必要となる鍵および証明書の生成者ならびにその配付先は下表のとおりです。

〔認証局における鍵・証明書およびその配付先〕

（オフラインデビット（電子マネー・電子財布）業務実施の場合）

鍵の生成者	鍵	配付先
全銀協 ルート認証局 （CA）※1	CA 秘密鍵	CA にて秘匿
	CA 公開鍵	CA⇒金融機関⇒ATM（経過期間）／IC カード ⇒オフデビ加盟店
金融機関認証局 ※2	発行者秘密鍵	金融機関認証局にて秘匿
	発行者公開鍵	金融機関⇒CA にて証明書化⇒金融機関⇒IC カード
	ＩＣカード秘密鍵	IC カード内に秘匿
	ＩＣカード公開鍵	金融機関認証局にて証明書化⇒IC カード
	端末秘密鍵	ATM 内に秘匿
	端末公開鍵	金融機関⇒CA にて証明書化⇒金融機関⇒ATM（経過期間）

※１ルート認証局→金融機関の公開鍵（発行者公開鍵および端末（ＡＴＭ）公開鍵）を登録し、この公開鍵に対してルート認証局が証明書を発行する。この証明書

を提示することで IC カード、端末間の認証が可能となる。
なお、CA は Certified Authority の略。

※２金融機関認証局→IC カード公開鍵に対して発行金融機関認証局が証明書を発行し、IC カードがこれを保持する。IC カードがこの証明書を提示することで取引毎に異なる暗号データによって IC カード発行元の認証が可能となる。

〔公開鍵証明書の種類と配付先等〕

（オフラインデビット業務実施の場合）

証明書	作成場所	署名鍵	配付先	利用する認証処理
発行者公開鍵証明書	ＣＡ	ＣＡ秘密鍵	ＩＣカード	カード認証
IC カード公開鍵証明書	金融機関	発行者秘密鍵	ＩＣカード	カード認証（動的認証）
端末公開鍵証明書	ＣＡ	ＣＡ秘密鍵	ＡＴＭ	端末認証（経過期間）

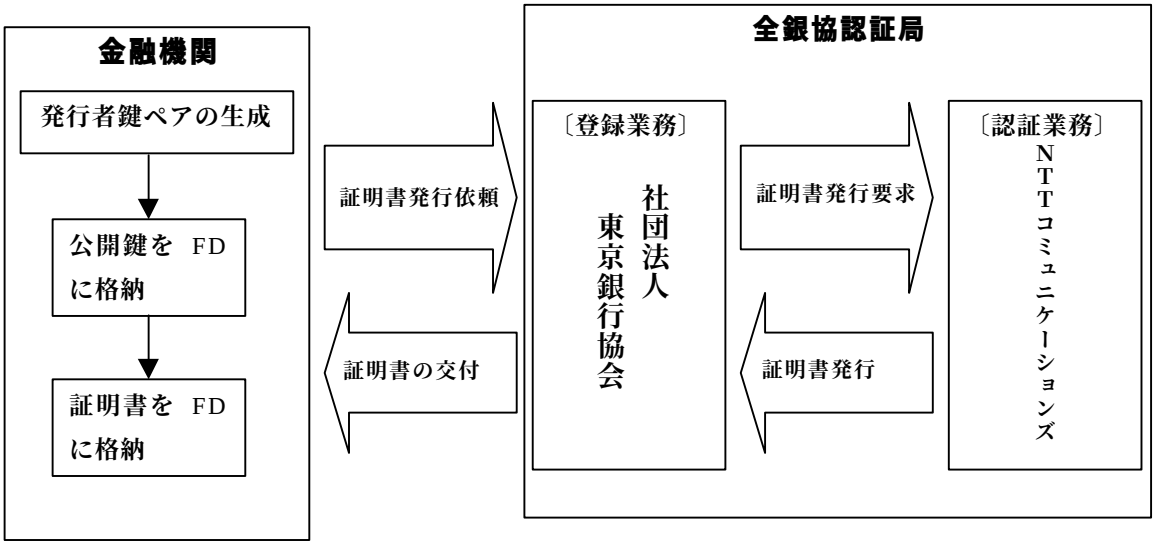
５．全銀協認証局の業務内容

①登録業務と認証業務との区分

全銀協認証局の業務としては、(a)金融機関発行者公開鍵に対する証明書の発行・交付、(b)金融機関端末（ATM）公開鍵に対する証明書の発行・交付、(c)認証局公開鍵の交付、(d)失効情報の管理がありますが、これは金融機関から証明書の発行依頼を受ける登録業務とこれに対して証明書を発行する認証業務とに区分することができます。このうち、認証業務については、その設備を設置する施設の安全性が極めて重要であり、ノウハウを含め外部の専門業者に委託することが認証局全般の安全性を高めることにつながります。

認証業務の委託先については、銀行関係者ならびに外部専門家からなる選定委員会の審議を経てＮＴＴグループ（代表：ＮＴＴコミュニケーションズ株式会社）に内定しています。

一方、登録業務については、金融機関の本人確認、金融機関との間での申請書等の授受など相手先金融機関との関係が重要となることから、東銀協自らが行うこととしています。



②認証局公開鍵暗号アルゴリズム

認証局の公開鍵暗号のアルゴリズムについては、標準仕様において RSA 暗号方式を採用することが必須とされています。

RSA 暗号方式は、現状において、暗号化と復号化とで異なった鍵を使う公開鍵暗号方式の事実上の世界標準であり、十分に大きな２つの素数を掛け合わせた数の素因数分解が難しいことを暗号技術の基礎として利用しています。

③発行者公開鍵証明書および端末公開鍵証明書の有効期限

全銀協認証局の発行する証明書の有効期限は、最長で、検証に使用するＣＡ公開鍵の使用期間終了時としています。

６．認証局のシステム構成

登録業務を担う東銀協には証明書の発行要求を行うための登録用端末を設置し、認証業者の設置するＣＡサーバと専用線により接続します。認証局の署名用秘密鍵の管理は、認証業務における最重要事項であり、公開鍵暗号方式における暗号の安全性・信頼性を確保するには秘密鍵が厳重に管理されていることが大前提となります。この点については FIPS140-1 レベル 4（最高位）[1]相当の機能を備えた耐タンパ装置であるＨＳＭ（Hardware Security Module）を用いて行っています。

７．認証局のセキュリティ基準

認証局のセキュリティ基準については、本年 4 月に施行された電子署名及び認証業務に関する法律に規定されている特定認証業務の認定基準に則して、認証業務委託先および登録局（東銀協）の建物等および業務運営に関するセキュリティレベルとしています。

８．金融機関との授受データ

①授受データとその形式

(a)登録局（東銀協）への提出データ

金融機関が登録局に対して提出する発行者公開鍵および端末公開鍵に対する証明書発行要求のデータフォーマットはＰＫＣＳ＃10形式[2]としています。ＰＫＣＳ＃10形式は、データの改竄防止・内容検証を行うことのできる署名が含まれた、公開鍵証明書の発行要求として一般的な形式です。

(b)利用金融機関への交付データ

---

[1] FIPS とは米国連邦政府情報処理標準（Federal Information Processing Standards）のことで、140-1 は暗号技術に関するセキュリティ要件を規定している。最低レベルの１から最高レベルの４までのセキュリティレベルが設定されている。

[2] PKCS（Public Key Cryptography Standards）は米国 RSA 研究所が提唱する公開鍵暗号技術をベースとした規格群で、#10 では証明書要求に関する形式標準を定めている。

金融機関に配付する発行者公開鍵証明書および端末公開鍵証明書のフォーマットについては、標準仕様に規定されています。

また、ＣＡ公開鍵については、Ｘ.509形式[3]による自己署名証明書方式を採用しています。

②授受方法

利用金融機関の職員が東銀協に来訪のうえ磁気媒体により授受を行います。

③証明書発行事務フロー

証明書発行の事務については、セキュリティ確保の観点から以下のとおり厳格に定めることとしています。

(a)利用開始の申請

金融機関は、全銀協認証局による公開鍵証明書の発行を受けようとする場合には、あらかじめ、金融機関認証局運営に係るセキュリティ対応など必要事項を記載した利用開始の申請書面を登録局である東銀協に提出します。

東銀協は、受理した書面の内容を審査のうえ、問題がない場合には、申請を受理し、証明書発行等の手続きにかかる事務取扱要領を交付します。

(b)証明書発行の申請

公開鍵証明書の発行を受けようとする金融機関（利用開始の申請に係る手続きを完了している先に限る）は、証明書発行申請書の提出に先立って、東銀協に対し申請を行う旨を電話または書面により届け出ます。

東銀協は、当該金融機関があらかじめ届け出ている金融機関認証局担当部署に対して、申請に要する公開鍵証明書発行申請書、日程表等の書面を送付します。

申請金融機関は、東銀協から提示された日程に従い、東銀協から送付された書面（公開鍵証明書発行依頼書）およびＦＤにより東銀協に申請を行います。提出方法は持参に限るものとし、提出に際して持参者は申請金融機関の社員証等を提示します。

東銀協は、提出を受けた書面等を確認し、受け付けます。

(c)証明書発行処理・証明書の受領

東銀協は、登録用端末により証明書の発行処理を行います。

申請金融機関は、東銀協から提示された日程に従い、受領書と引き換えに証明書および認証局公開鍵を受領します（東銀協に来訪のうえ受領することに限るこ

[3] X.509 は国際通信連合の通信標準セクター（ITU－T）で作成された標準で、公開鍵証明書や公開鍵証明書廃棄リスト（CRL：Certificate Revocation List）のデータ構造等を定めている（現在有効な公開鍵証明書の形式はバージョン 3)。X.509 は、ISO/IEC においても国際標準として規定されており、ISO/IEC9594-8 として登録されている。

ととし、受領に際し受領者は申請金融機関の社員証等を提示します)。

証明書を受領した金融機関は、すみやかに証明書の内容を確認します。

９．利用金融機関の責務

認証局を利用する金融機関は、全銀協の定める認証局運営規則や事務取扱要領を遵守することが求められています。

この場合、利用金融機関には、①金融機関認証局の鍵管理等セキュリティ対策や、②届出・報告義務などが課されることになります。

また、公開鍵証明書の利用範囲についても、現状では、IC キャッシュカード関係業務に限定されています。

以 上