経済産業省補助事業

平成１６年度情報基盤対策技術開発等推進事業
（電子商取引（ＥＣ）技術基盤の相互運用性に関する調査研究）

調査報告

公認制度調査

根拠資料　シンガポール編

平成 17 年 3 月

（財）日本情報処理開発協会

注: 日本以外の法規は日本PKIフォーラムによる仮の翻訳である。

目次

シンガポール

[SG/L] 電子取引法

1998.6.2 公布 1999.12.30 改正

	根拠資料	備考
条項番号	条文	

Part 1. 序

1. 略称

SG/L-1.1 本法令は電子取引法として引用できる

2. 解説

SG/L-2.1 本法令は文脈上別の意味を必要としない限り、

「非対称暗号システム」は、デジタル署名を作成するための秘密鍵とデジタル署名を検証する公開鍵から成る安全な鍵ペアを生成できるシステムを意味する

「認定職員」は 50 節で管理者によって認定される者を意味す

	根拠資料	備考
条項番号	条文	
	「認証」は、身元または特定の鍵ペアを持っている者の他の重要な特徴を確認することを意図するデジタル署名を支援するために発行された記録を意味する 「認証局」は認証を発行する者または組織を意味する 「認証業務説明書」は、認証局が認証を発行する際に適用する業務を明記するために認証局により発行された説明書を意味する 「管理者」は、41(1)節で任命された認証局の管理者を意味し、41(2)節で任命された認証局の代理人または副管理者を含む 秘密鍵または公開鍵に関連する「対応」は同様な鍵ペアに属することを意味する 「デジタル署名」は、最初の未変換電子記録を持っている者および署名者の公開鍵が以下を正確に決定できるような非対称暗号システムとハッシュ関数を使用する電子記録の変換から成る電子署名を意味する (a) 署名者の公開鍵に対応する秘密鍵を使って変換されるかどうか。および、 (b) 最初の電子記録が変換後に変更されるかどうか。 「電子記録」は、1 つの情報システムから別のシステムに伝達するためにまたは電子、磁気、光学式、または他の手段により情報システムに生成、通信、受信、または記憶された記録を意味する。 「電子署名」は、電子記録を認証または承認の意図で実行または採用し、電子記録と論理的に結合または付属するデジタル形式のいかなる文字、番号、または他の記号をも意味する	

根拠資料		備考
条項番号	条文	
	「ハッシュ関数」は、一連のビットを、以下のような設定(ハッシュ結果)、一般により小さい別のものにマッピングまたは翻訳するアルゴリズムを意味する (a) アルゴリズムが入力と同じ記録を使用して実行されるたびに、記録は同じハッシュ結果を産出する。 (b) アルゴリズムにより作成されたハッシュ結果から記録を引き出すまたは再構成することが計算上実行不可能である。および、 (c) アルゴリズムを使用して同じハッシュ結果を二つのレコードが産出することは、計算上実行不可能である。 「情報」は、データ、テキスト、イメージ、音、コード、コンピュータプログラム、ソフトウェア、およびデータベースを含む 非対称暗号システムで、「鍵ペア」は秘密鍵とその数学的に関連した公開鍵を意味し、秘密鍵が作成するデジタル署名を公開鍵が検証できる特性を持つ 「認定認証局」は、42 節で作られたあらゆる法令に従う管理者により認定された認証局を意味する 「認証の運用期間」は、認証が認証局により発行される日時から始まり、認証に記載された日時に満了するか、それ以前に中断または取り消される日時に終わる 「秘密鍵」はデジタル署名を作成するために使用される鍵ペアの鍵を意味する 「公開鍵」はデジタル署名を検証するために使用される鍵ペアの鍵を意味する 「記録」は、有形の媒体、あるいは電子または他の媒体に記憶されて感知可能な形式で検索できるものに記入、記憶、または別途固定される情報を意味する 「レポジトリ」は認証または認証に関する他の情報を記憶、検索するためのシステムを意味する 「認証の取り消し」は特定時からの認証運用期間を永久に終わらせることを意味する 「法律の規則」は、成文法を含む	

根拠資料		備考
条項番号	条文	
	「セキュリティプロシージャ」は以下の目的に対するプロシージャを意味する (a) 電子記録が特定の人のものであることを検証する。または、 (b) 特定時点以降の電子記録の通信、コンテンツまたは記憶装置の検出エラーまたは変更。 言葉または番号、暗号化、アンサーバックまたは承認プロシージャ、または同様なセキュリティ装置を識別する、アルゴリズムまたはコードの使用を必要とする。 「署名入り」または「署名」およびその文法上のバリエーションは、電子またはデジタルの方法を含む記録を認証する意図で、実行または採用されたどのような記号、あるいは使用または採用されたどのような方法論またはプロシージャをも含む 「署名者」は、発行された認証において名付けられるかまたは識別された対象であり、その認証に記載された公開鍵と対応する秘密鍵を保有する者を意味する 「認証の中断」は、指定された時間から認証の運用期間を一時的に中断することを意味する 「信頼できるシステム」は、以下のコンピュータハードウェア、ソフトウェア、およびプロシージャを意味する (a) 侵入と悪用に対して適度に安全である。 (b) 妥当なレベルの有用性、信頼性および正しい運用を備える。 (c) 意図されている機能を実行することに合理的に適している。および、 (d) 一般に受け入れられたセキュリティプロシージャを厳守する。 「有効な認証」は、認証局が発行し、そこに記載された署名者が受け取った認証を意味する	

根拠資料		備考
条項番号	条文	
	特定のデジタル署名、記録、および公開鍵に関する「デジタル署名の検証」は、以下を正確に決定することを意味する (a) デジタル署名は、認証に記載された公開鍵に対応する秘密鍵を使用して作成されたこと。および、 (b) そのデジタル署名が作成されてから記録が変更されていないこと。	
	3. 目的と構成	
SG/L-3.1	本法令は、以下の目的を実施するためにその状況下で何が商業的に妥当であるかで一貫して解釈されることとする (a) 信頼できる電子記録によって電子通信を容易にすること。 (b) 電子取引を容易にし、記述と署名要件上の不確定要素に起因する電子取引への障害を取り除き、安全な電子取引を実装するのに必要な法律と業務インフラストラクチャの開発を促進すること。 (c) 政府機関と特殊法人が持つ文書の電子ファイリングを容易にし、信頼できる電子記録によって政府サービスの効率的な配布を促進すること。 (d) 電子記録の偽造、記録の意図的または故意でない変更、およびエレクトロニックコマースと他の電子取引における不正の発生を最小化すること。 (e) 電子記録の認証と整合性に関する規則、法令および標準の一貫性を確立するのに役立てること。および、 (f) 電子記録と電子取引の整合性と信頼性の公的な信頼を促進し、どのような電子媒体での通信においても確実性と整合性に役立つような電子署名の使用を通じた電子取引の開発を助長すること。	

根拠資料		備考
条項番号	条文	

4. 適用

SG/L-4.1 Ⅱ部とⅣ部は、以下のいずれかの問題で法律上必要な記述または署名のどのような規則にでも適用されないこととする

(a) 意図した作成または実行。

(b) 交渉の余地がある手段。

(c) 建設的で結果として生ずる信託を除いた契約書、信託宣言または委任状の作成、実行または施行。

(d) 不動産の販売または他の処置、またはそのような資産のあらゆる利益に関するあらゆる契約。

(e) 不動産の譲渡、または不動産に関するあらゆる利益の移転。

(f) 権利証書。

SG/L-4.2 大臣はあらゆる分野の取引または問題を追加、削除、または改正することによって副節(1)の条項を命令によって修正できる

5. 合意による変更

SG/L-5.1 当事者間で電子記録を生成、送信、受信、記憶、または別途処理することに関わるとき、Ⅱ部またはⅣ部のどのような条項でも協定により変えられる

Part 2.一般的な電子記録と署名

6. 電子記録の法律上の承認

	根拠資料	備考
条項番号	条文	
SG/L-6.1	疑惑の回避のために、電子記録形式の分野に限り情報の法的な効果、妥当性、または強制力を否定されないことが宣言される	
	7. 書類の必要性	
SG/L-7.1	法律の規則が、書面で提出されるように書面に書かれている情報を必要とするか、またはそうではなくて一定の結果に備える場合、もしその中に含まれる情報が次回の参照で使えるようにアクセス可能であるならば電子記録はその法律の規則を満たす	
	8. 電子署名	
SG/L-8.1	法律の規則が署名を必要とするか、または文書が署名されないで特定の結果に備える場合には、電子署名がその法律の規則を満たす	
SG/L-8.2	電子署名は、電子記録が当該当事者のものであることを検証する目的で記号またはセキュリティプロシージャを実行することが、取引をさらに続行するのに、当事者に必要であるためにプロシージャが存在することを示す場合を含むどのような様式でも証明できる	
	9. 電子記録の保存	

根拠資料		備考
条項番号	条文	
SG/L-9.1	法律の規則が特定の文書、記録または情報が記憶されていることを必要とする場合、その要件は、以下の条件が満たされているとき電子記録という形式でそれらを保有することによって満たされる (a) その中に含まれる情報は、次回の参照で使えるようにアクセス可能であり続ける。 (b) 電子記録は、生成、送信、または受信された元の形式、または生成、送信、または受信された元の情報を正確に表示することを実証できる形式で保有されている。 (c) そのような情報は、もしあれば、電子記録の発信元と宛先の識別、および送信、受信された日時を有効にして保有されている。および、 (d) そのような記録を保持するための要件上の監督権を持つ政府省局、州機関または特殊法人の同意は得られた。	
SG/L-9.2	副節(1)(c)に従って文書、記録、または情報を保有するときの義務は、記録が送信または受信されることを可能にするためにだけ必然的および自動的に生成されたいかなる情報にも拡張してはならない	
SG/L-9.3	その副節の段落(a)から(d)の条件に従う者は、どのような他者のサービスでも使用することによって副節(1)において参照された要件を満たす	
SG/L-9.4	この節で以下のことは無いこととする (a) 電子記録という形式で文書、記録、または情報の保持を明確に規定するどのような法律の規則にでも適用する。または、 (b) 当該の政府省局、州機関または特殊法人に属する司法権に制約される電子記録の保持に対する補足的な要件に関して、あらゆる政府省局、州機関、または特殊法人による明記を妨げる。	

Part 3. ネットワークサービスプロバイダの信頼性

	根拠資料	備考
条項番号	条文	

10. ネットワークサービスプロバイダの信頼性

SG/L-10.1 ネットワークサービスプロバイダは、その責任が以下に基づいている場合、単にアクセスを提供する電子記録という形式の第三者の資料についてあらゆる法律の規則におけるいかなる民事または刑事上の責任にも制約されないこととする

(a) そのような資料の制作、発行、普及または配布またはそのような資料で作られたあらゆる説明書。または、

(b) そのような資料または関連するものに存続するあらゆる権利の侵害。

SG/L-10.2 この節は以下に影響しないこととする

(a) 契約に基づくあらゆる義務。

(b) あらゆる成文法に基づいて確立された認定または他の規制制度におけるネットワークサービスプロバイダの義務。または、

(c) あらゆる資料へのアクセスを除去、防止、または否定するために、あらゆる成文法または法廷によって課されたあらゆる義務。

SG/L-10.3 この節の目的に対して、第三者の資料に関連して「アクセスを提供する」は、第三者の資料にアクセスできて、アクセスを提供するために第三者の資料の自動と一時記憶域を含む必要な技術手段の条項を意味する。ネットワークサービスプロバイダに関連して「第三者」は、プロバイダが有効に管理しない者を意味する

Part 3. 電子契約

11. 契約の構成と効力

根拠資料		備考
条項番号	条文	
SG/L-11.1	疑惑の回避のために、契約を構成する文脈で当事者が別途合意しない限り、申し込みおよび申し込みの受理において電子記録によって表現されうることが宣言される	
SG/L-11.2	契約の構成において電子記録が使用される場合、その契約は電子記録がその目的のために使用された分野に限り妥当性または強制力を否定されないこととする	
	12. 当事者間の効力	
SG/L-12.1	電子記録の発信者と受信者の間で、意図の宣言または他の記述は、電子記録形式の分野に限り法的な効力、妥当性または強制力が否定されないこととする	
	13. 帰属	
SG/L-13.1	電子記録は、発信者自身によって送られた場合、発信者のものである	
SG/L-13.2	電子記録の発信者と受信者の間で、以下によって送信された場合、発信者のものであると考えられる (a) その電子記録について、発信者のために行動する権限を持っていた者。または、 (b) 発信者によってまたは発信者のために、自動的に作動するようにプログラムされた情報システム。	

	根拠資料	備考
条項番号	条文	
SG/L-13.3	発信者と受信者の間で、受信者は、電子記録を発信者のものであるとみなして以下の前提で行動する権利を与えられる (a) 電子記録が発信者のものであるかどうかを確かめるために、受信者は、その目的のために発信者が事前に同意したプロシージャを適切に適用した。または、 (b) 受信者により受信されるデータメッセージは、その者が、電子記録を自分のものと認定するために発信者により用いられた方法へのアクセスを得られるようにした発信者または発信者の任意の代理人と関係のある者の行為に起因した。	
SG/L-13.4	副節(3)は以下に適用されない (a) 電子記録が発信者のものでなく、それに応じて行動する妥当な時間があったという発信者からの通知を、受信者が受信した時から。 (b) 副節(3)(b)の場合には、妥当な注意を払い、またはあらゆる合意されたプロシージャを使用し、電子記録が発信者のものではなかったことを受信者が知っていたか、知っていたはずの時点で。または、 (c) その場合のあらゆる状況で、受信者が、電子記録を発信者のものであるとみなすか、またはその前提で行動することが非良心的なとき。	
SG/L-13.5	電子記録が発信者のものであるか、または発信者のものであると考えられる、または受信者がその前提で行動する権利を与えられる場合、発信者と受信者の間で受信者は、受信した電子記録を、発信者がその前提で送信し、行動するつもりであったものであるとみなす権利を与えられる	
SG/L-13.6	受信者が妥当な注意を払ったか、またはあらゆる合意したプロシージャを使用して、電子記録を受信したときに伝達上の任意のエラーが生じたことを受信者が知っていたか、知っていたはずの場合には、受信者はその権利を与えられない	

根拠資料		備考
条項番号	条文	
SG/L-13.7	受信者が別の電子記録を複写し、電子記録が複製であったということを受信者が妥当な注意を払ったか、またはあらゆる合意されたプロシージャを使って受信者が知っていたか、知っていたはずの場合を除いて、受信者は、個々の電子記録を別個の電子記録とみなし、その前提に基づいて行動する権利を与えられる	
SG/L-13.8	この節は政府機関の法律または契約の構成に関する法律に影響しないこととする	
	14. 受信の承認	
SG/L-14.1	副節(2)、(3)および(4)は、電子記録を送信以前に、またはその電子記録によって、発信者が頼んだかまたは電子記録の受信が認められることについて受信者と合意した場合に適用することとする	
SG/L-14.2	承認が特定の形式に、または特定の方法により与えられることについて発信者が受信者と合意しなかった場合には、以下によって承認される (a) 自動またはその他の方法の受信者によるあらゆる通信。または、 (b) 電子記録が受信されたことを発信者に示すのに十分な受信者のあらゆる行為。	
SG/L-14.3	電子記録が承認の受信を条件としていることを発信者が述べた場合、承認が受信されるまでそれが一度も送信されたことがなかったかのように電子記録は扱われる	

根拠資料		備考
条項番号	条文	
SG/L-14.4	電子記録が承認の受信を条件としていることを発信者が述べずに、承認が特定または合意の時間以内に発信者により受信されなかった場合、または時間が妥当な時間以内で特定または合意されていなかった場合、発信者は、 (a) 承認が受信されなかったと述べて、承認が受信されなければならない妥当な時間を明記した通知を受信者に与えることができる。および、 (b) 段落(a)で明記された時間以内に承認が受信されない場合、受信者への通知で、一度も送信されたことがないか、または持ちうるあらゆる他の権利を行使するかのように電子記録を扱える。	
SG/L-14.5	発信者が受信者の受信承認を受信する場合には、反証が提示されない限り、関連した電子記録が受信者によって受信されたけれども、電子記録のコンテンツが、受信された記録のコンテンツに対応していない場合が推定される	
SG/L-14.6	関連した電子記録が適用可能な標準に合意または明記される技術的要件を満たしていたことを受信された承認で述べられている場合、反証が提示されない限り、それらの要件が満たされていたことが推定される	
SG/L-14.7	電子記録の送信または受信と関連する限りを除いて、この部では、その電子記録またはその受信の承認から流出するかもしれない法律の結果を扱うことを意図しない	
	15. ディスパッチの日時と場所および受信	
SG/L-15.1	発信者と受信者の間で別途合意しない限り、電子記録のディスパッチは、発信者のために電子記録を送信した者または発信者の管理外で情報システムに入る時に起こる	

	根拠資料	備考
条項番号	条文	
SG/L-15.2	発信者と受信者の間で別途合意しない限り、電子記録の受信の時間は次の通り決定される (a) 電子記録を受信するために、受信者が情報システムを明示した場合、受信は以下の時点で起こる。 (i) 電子記録が明示された情報システムに入る時点。または、 (ii) 電子記録が、明示された情報システムではない受信者の情報システムに送信された場合、電子記録が受信者により検索される時点。または、 (b) 受信者が情報システムを明示しなかった場合、電子記録が受信者の情報システムに入る時に、受信が起こる。	
SG/L-15.3	情報システムの配置場所が、電子記録が副節(4)で受信されると考えられている場所と違うかもしれないにもかかわらず、副節(2)は適用することとする	
SG/L-15.4	発信者と受信者の間で別途合意しない限り、電子記録は、発信者がその事務所を持っている場所でディスパッチされると考えられ、受信者がその事務所を持っている場所で受信されると考えられる	
SG/L-15.5	この節の目的に対して、 (a) 発信者または受信者が、複数の事務所を持っている場合、事務所は基本的な取引に最も近い関係を持っている場所か、または基本的な取引が全然ない場合、主たる事務所である。 (b) 発信者または受信者が、事務所を持っていない場合、照会は通常の所在地にされる必要がある。および、 (c) 法人に関する「通常の所在地」は、法人組織のある、または別途法律上構成されている場所を意味する。	
SG/L-15.6	この節は、大臣が法令によって規定することができるような状況に適用されないこととする	
	Part 4. 電子記録と署名の安全確保	

根拠資料		備考
条項番号	条文	

16. 電子記録の安全確保

SG/L-16.1 特定の時点以降電子記録が変更されていないことを検証するために、関係する当事者が合意する規定セキュリティプロシージャまたは商業的に妥当なセキュリティプロシージャが電子記録に適切に適用された場合、そのような記録は、その特定の時点から検証の時点まで安全な電子記録とみなされることとする

SG/L-16.2 この節と 17 節の目的に対して、以下を含めて、セキュリティプロシージャが商業的に妥当であるかどうかは、プロシージャが使用された時にプロシージャの目的と商業環境に注意を払いながら決定することとする

(a) 取引の性質。

(b) 当事者の高度化。

(c) どちらかまたはすべての当事者が関わった同様な取引量。

(d) 提案したが、いずれの当事者によっても退けられた選択肢の可用性。

(e) 代替プロシージャの費用。および、

(f) 同様な形式の取引に対する一般使用のプロシージャ。

17. 電子署名の安全確保

	根拠資料	備考
条項番号	条文	
SG/L-17.1	関係する当事者が合意した規定セキュリティプロシージャまたは商業的に妥当なセキュリティプロシージャを適用して、以下が行われた時に電子署名だったという検証ができる (a) それを使用した者の特定。 (b) そのような者を識別する可能性。 (c) それを使用した者だけが管理する様式での、またはその手段を使用しての作成。および、 (d) 記録が変更された場合に電子署名を無効にするような様式に関連する電子記録へのリンク。以上のような署名は安全な電子署名とみなされることとする。	
	18. 電子記録と署名の安全確保に関する推定	
SG/L-18.1	安全な電子記録に関するどのような行為においても、反証が提示されない限り、安全な状態が関連した特定の時点以降安全な電子記録が変更されていないことが推定されることとする	
SG/L-18.2	安全な電子署名に関係するどのような行為においても、反証が提示されない限り、以下が推定される (a) 安全な電子署名は、相関している者の署名である。および、 (b) 安全な電子署名は、電子記録に署名または承認する意図で、その者により添付された。	
SG/L-18.3	安全な電子記録または安全な電子署名が無い場合、この部では、電子記録または電子署名の確実性と整合性に関連するどのような推定もしないこととする	
SG/L-18.4	この節の目的に対して、 「安全な電子記録」は、16 または 19 節によって安全な電子記録とみなされる電子記録を意味する。 「安全な電子署名」は、17 または 20 節によって安全な電子署名とみなされる電子署名を意味する。	

	根拠資料	備考
条項番号	条文	

Part 5. 電子署名の効力

19. 電子署名入り電子記録の安全確保

SG/L-19.1 デジタル署名によって署名される電子記録の一部は、デジタル署名が 20 節による安全な電子署名である場合に安全な電子記録とみなされることとする

20. 電子署名の安全確保

根拠資料		備考
条項番号	条文	
SG/L-20.1	電子記録のどのような部分でもデジタル署名によって署名される時、以下の場合に、デジタル署名はそのような記録部分について安全な電子署名とみなされることとする (a) デジタル署名は有効な認証の運用期間中に作成されて、そのような認証に記載された公開鍵への照会によって検証される。および、 (b) 以下の理由によって、本人確認に公開鍵が正確に結び付いているという点で認証は信頼できると考えられる。 (i) 認証は、42 節で作られた法令に従って運用している認定認証局により発行された。 (ii) 認証は、この目的のために、43 節で作られた法令に従う管理者により認められているシンガポール以外での認証局により発行された。 (iii) 認証は法令によって課すか、または明記することができるような条件についての認証局として行動するために大臣により承認された政府省局、州機関または特殊法人により発行された。または、 (iv) 当事者は、当事者間(発信者と受信者)で、セキュリティプロシージャとしてデジタル署名を使用することに明確に合意し、デジタル署名は発信者の公開鍵への照会によって適切に検証された。	
	21. 認証に関する推定	
SG/L-21.1	認証が署名者により受け取られた場合、反証が提示されない限り、認定認証局により発行された認証に記載された情報(検証されなかった署名者情報と認定される情報を除く)の正しさが推定されることとする	
	22. 信頼できない電子署名	

根拠資料		備考
条項番号	条文	
SG/L-22.1	法律または契約によって別途提供されない限り、デジタル署名入り電子記録を信頼している者は、以下の要素への注意を払っている環境下でデジタル署名の信頼が妥当ではない場合、デジタル署名が署名入り電子記録の署名または認証として無効であるというリスクを仮定する (a) デジタル署名入り電子記録を信頼している者が知っているか、あるいは認証に記載されるか、または照会によりそれに加入したすべての事実を含む通知を持っている事実。 (b) デジタル署名入り電子記録の値または重要性(分かっている場合)。 (c) デジタル署名入り電子記録を信頼している者、および署名者、およびデジタル署名を除いた信頼できるまたは信頼できない任意の入手可能な証印の間における取引の経過。および、 (d) 商慣習、特に、信頼できるシステムまたは他の電子手段により実施される取引。	
	Part 6. 電子署名に関する一般的義務	
	23. 予知できる認証の信頼性	
SG/L-23.1	デジタル署名を信頼する者が、デジタル署名を検証できる公開鍵を含む有効な認証も信頼することは予知できる	
	24. 認証発行の前提条件	

根拠資料		備考
条項番号	条文	
SG/L-24.1	誰も認証を発行できないか、さもなければその者が下記を知っている場合、認証または認証に記載された公開鍵に照会して検証できるデジタル署名を信頼する立場にあるとその者が知っている者に利用可能にする (a) 認証に記載された認証局は、それを発行しなかった。 (b) 認証に記載された署名者は、それを受け取らなかった。または、 (c) そのような発行がその中断または取り消しに先がけて作成されたデジタル署名を検証する目的でない限り、認証は中断または取り消された。	
	Part 7. 電子署名に関する一般的義務	
	25. 不正/不法な目的の発行	
SG/L-25.1	故意に作成、発行、またはどのような不正または不法な目的のための認証でも別途入手可能にする者すべてが違反という罪を犯したことになり、有罪判決に基づき、2 万 S＄(130 万円)以下の罰金、または 2 年以下の懲役またはその両方の刑によって処罰されることとする	
	26. 虚偽/無権限の要求	
SG/L-26.1	認証局に、認証または認証の停止または失効を要求する目的で自分の身元または認可を故意に偽り伝えるどのような者でも違反という罪を犯したことになり、有罪判決に基づき、1 万 S＄(65 万円)以下の罰金、または 6 ヶ月以下の懲役またはその両方の刑によって処罰されることとする	

根拠資料		備考
条項番号	条文	

Part 8. 認証局の義務

27. 信頼できるシステム

SG/L-27.1 認証局は、そのサービスを実行する時に、信頼できるシステムを利用しなければならない

28. 公開

SG/L-28.1 認証局は以下を公開することとする

(a) 別の認証にデジタル署名をするためにその認証局により使用された秘密鍵に対応する公開鍵を含むその認証(この節において認証局認証として参照される)。

(b) あらゆる適切な認証業務説明書。

(c) その認証局認証の取り消しまたは中断の通知。および、

(d) 認証局が発行したという認証の信頼性、またはそのサービスを実行する認証局の能力に実質的に悪影響を及ぼすあらゆる他の事実。

SG/L-28.2 認証局の信頼できるシステムまたはその認証局認証に実質的に悪影響を及ぼす出来事の場合には、認証局は以下を行うこととする

(a) その出来事により影響されるまたは予知できて影響されることを知らされているどのような者にでも通知する妥当な努力をすること。または、

(b) その認証業務説明書において明記されたそのような出来事を規定しているプロシージャに従って行動すること。

	根拠資料	備考
条項番号	条文	

29. 証明書の発行

SG/L-29.1 認証局が以下を行った後にだけ認証局は証明書を加入者に発行できる

1) 加入者から発行要求を受け取った。および

2) 以下。

a) CPS を持っている場合、加入者の識別について、手順を含むその認証業務運用規程に記述された業務と手順のうちのすべてに従った。または、

b) CPS が無い場合、**SG/L-29.2** の条件に従った。

SG/L-29.2 CPS が無い場合、認証局または外部委託事業者を通して次を確認しなければならない

a) 加入者は、発行される証明書に記載される個人である。

b) 加入者が複数の代理人を通している場合、加入者は、秘密鍵を保有していること及び対応した公開鍵を記載している証明書の発行を要求していることについて代理人に権限を与えた。

c) 発行される証明書の情報は正確である。

d) 加入者は、証明書に記載される公開鍵に対応する秘密鍵を正当に保有する。

e) 加入者は、デジタル署名を作成できる秘密鍵を保有する。および、

f) 証明書に記載される公開鍵は、加入者が保有する秘密鍵によって添付されたデジタル署名を検証するために使用できる。

30. 認証発行の説明

根拠資料		備考
条項番号	条文	
SG/L-30.1	認証を発行することによって、認証局は、認証の照会により組み入れられたまたは信頼者が通知を持っているどのような適用可能な認証業務説明書にも従って認証局が認証を発行したという認証に記載された公開鍵によって証明可能な認証またはデジタル署名を合理的に信頼しているどのような者にでも説明する	
SG/L-30.2	そのような認証業務説明書が無い場合、認証局は、以下を確認したことを説明する (a) 認証局が認証を発行したか、またはそれを別途そのような信頼者に利用可能にした場合、認証に記載された署名者がそれを受け取ったという認証を発行する時に、認証局は本法のすべての適用可能な要件に従った。 (b) 認証において識別された署名者は、認証に記載された公開鍵に対応する秘密鍵を保有する。 (c) 署名者の公開鍵と秘密鍵は、機能的な鍵ペアになっている。 (d) 認証局が認証で述べないか、または特定情報の精度が確認されないことを認証での照会によって説明書に組み入れない限り、認証のすべての情報は正確であるおよび、 (e) 認証局は、それが認証に含まれていた場合に段落(a)～(d)の表現の信頼性に悪影響を与えるどのような実質的な事実も全然知らない。	
SG/L-30.3	認証の照会により組み入れられた、または信頼者が通知を持っている適用可能な認証業務説明書がある場合、副節(2)は表現が認証業務説明書と矛盾しない程度に適用することとする	

31. 認証の中断

	根拠資料	備考
条項番号	条文	
SG/L-31.1	認証局と署名者が別途合意しない限り、認証を発行した認証局は、認証局が以下であると合理的に信じる者が要求を受け取った後に、認証をできるだけ早く中断することとする (a) 認証に記載された署名者。 (b) その署名者のために代行することについて権限を正式に与えられる者。または、 (c) 利用できないその署名者のために行動する者。	
	32. 認証の取り消し	
SG/L-32.1	認証局は、以下に発行した認証を取り消すこととする (a) 認証に指定する署名によって取り消しの要求を受け取って、取り消しを要求している者が署名者であるか、または取り消しを要求する権限を持つ署名者の代理人であると確認した後。 (b) 署名者の死亡診断書の認証謄本を受け取った、または署名者が死亡したことを他の証拠によって確認した後。または、 (c) 署名者の解約に影響する文書の提示について、または署名者が取り消されたか、または存在することを止めたという他の証拠によって確認することについて。	
	33. 署名者の同意の無い取り消し	

	根拠資料	備考
条項番号	条文	
SG/L-33.1	認証局が以下のことを確認したとき、認証に記載された署名者が同意するかどうかを問わず認証局は認証を取り消すこととする (a) 認証に示されている実質的な事実は間違いである。 (b) 認証の発行要件は満たされていなかった。 (c) 認証局の秘密鍵または信頼できるシステムは、認証の信頼性に実質的に影響のある様式で妥協された。 (d) 個人の署名者は死亡した。または、 (e) 署名者は取り消されたか、整理されたかまたは別途存在することを止められた。	
SG/L-33.2	副節(1)の(d)または(e)を除いてそのような取り消しが有効になったら、認証局は、直ちに、取り消された認証に記載された署名者に通知することとする。	
	34. 中断の通知	
SG/L-34.1	認証局によって認証が中断されたら直ちに、認証局は、中断通知の発行のために認証に明記されたレポジトリで署名入り中断通知を発行することとする	
SG/L-34.2	複数のレポジトリが明記される場合には、認証局は、すべてのそのようなレポジトリで署名入り中断通知を発行することとする	
	35. 取り消しの通知	
SG/L-35.1	認証局によって認証が取り消されたら直ちに、認証局は、取り消しの通知を発行するために認証に明記されたレポジトリで署名入り取り消し通知を発行することとする	
SG/L-35.2	複数のレポジトリが明記されている場合には、認証局は、すべてのそのようなレポジトリで署名入り取り消し通知を発行することとする	

	根拠資料	備考
条項番号	条文	

Part 9. 署名者の義務

36. 鍵ペアの生成

SG/L-36.1 認証局により発行されて、署名者により受け取られた認証に公開鍵が記載される必要がある鍵ペアを署名者が生成する場合、署名者は、信頼できるシステムを使用してその鍵ペアを生成することとする

SG/L-36.2 この節は、認証局により承認されたシステムを使用することで鍵ペアを生成する署名者に適用されないこととする

37. 認証の取得

SG/L-37.1 そのような表現が認証局により確認されるかどうかを問わず、認証に示されていて署名者に既知のすべての情報を含む認証を取得する目的のために、認証局に対して署名者によって行われたすべての実質的な表現は、署名者の最善の知識と信念を駆使して正確、完全であることとする

38. 認証の受理

根拠資料		備考
条項番号	条文	
SG/L-38.1	以下を行った場合、署名者は、認証を受け取ったと考えられることとする (a) 以下のように発行するか、または認証発行の資格を与える。 (i) 複数の者に。または、 (ii) レポジトリで。または、 (b) そのコンテンツの通知を知っているか、または持っている間に、別途認証の承認を示す。	
SG/L-38.2	自身または認証局によって発行された認証を受け取ることによって、認証に記載された署名者は、以下の認証に含まれる情報を合理的に信頼するすべての者に証明する (a) 署名者は、認証に記載された公開鍵に対応する秘密鍵を正当に保有する。 (b) 認証局および実質的に認証に記載された情報に署名者によって行われたすべての表現は真実である。および、 (c) 署名者の知識内にある認証のすべての情報は真実である。	
	39. 秘密鍵の管理	
SG/L-39.1	認証局により発行された認証を受け取ることによって、認証で識別された署名者は、そのような認証に記載された公開鍵に対応する秘密鍵の管理を保有し、署名者のデジタル署名を作成することについて権限を与えられない者に対してその公開を防止するために妥当な配慮をする義務を仮定する	
SG/L-39.2	そのような義務は、認証の運用期間中と認証の中断期間中に続くこととする	
	40. 認証の中断または取り消しの開始	

根拠資料		備考
条項番号	条文	
SG/L-40.1	認証に記載された公開鍵に対応する秘密鍵が妥協して解決された場合、認証を受け取った署名者は、認証を中断または取り消すことを発行元の認証局にできるだけ早く要求することとする	
	Part 10. 認証局規則	
	41. IDA の検査官および職員の任命	
SG/L-41.1	長官は、本法の目的、および特に認証局の活動を認可、証明、監視、及び監督する目的で認証局の検査官を任命することとする	
SG/L-41.2	本法またはその下に作られたあらゆる規則下の IDA の権限と義務のすべてまたは一部を行使、実行するのに必要であると検査官が考えるとき、検査官は、長官と相談して、認証局の代理と副検査官と職員等の何人かを任命できる	
SG/L-41.3	検査官、および **SG/L-41.2** で検査官により任命された代理、および副検査官と職員は、長官が公表する方針に従ってその下に作られた本法またはあらゆる規則で検査官に授与された権限、義務、および機能を行使、履行、実行することとする	
SG/L-41.4	IDA は、本法の下に作られた規則で必要なすべての詳細を含んでいるはずの認可認証局毎の認証局公開記録を含んでいる公然とアクセス可能なデータベースを保守することとする	
SG/L-41.5	IDA により発行された証明書とそれらの証明書への照会によって検証されたデジタル署名への本法の条項の適用において、IDA は認可認証局であると考えられることとする	
	42. 認証局規則	

	根拠資料	備考
条項番号	条文	
SG/L-42.1	認証局に関する規則と認可のために、およびデジタル署名が安全な電子署名としての資格を得る時に定義するために、長官は規則(SG/R)を作ることができる	
SG/L-42.2	**SG/L-42.1** の一般性を失うことなく、長官は以下のためにまたは以下について規則を作ることができる 1) 認証局、権限代表者、付随事項の認可あるいは認可更新の申請; 2) 手法、営業の方法/場所、運営、および認可されない認証局の営業禁止事項を含む認証局の業務; 3) 認証局毎の維持される標準; 4) 求職者や職員の資格、経験および教育に関しての適切な基準の規定; 5) 認証局毎の運営条件の規定; 6) デジタル証明書または鍵について個人に配信されるまたは使用されるコンテンツ、書かれた/印刷された/視覚的な資料、広告資料; 7) デジタル証明書または鍵の形式と内容の規定; 8) 認証局が保管する記録/勘定の細則; 9) 監査役の任命および報酬規則、及び規則下で実行される監査費用の準備; 10) 認証局の電子システム(単独であるいは他の認証局と相互に)の設置および規則、及び IDA の要求、条件または制約に関する賦課および変更に関する準備; 11) 認可者とその顧客との取引、認可者と顧客を含む利益相反、およびデジタル証明書に関してのその顧客に対する認可者の義務に関する慣習; 12) 規則の目的に対する形式の規定; および、 13) **SG/L** または規則の目的のために必要なあらゆる問題または物に関して支払われる料金の規定。	
SG/L-42.3	SG/L-42 で作られた規則は、明記された条項の違反が不法であり、5 万 S＄(32 万 5 千円)以下の罰金、または 12 ヶ月以下の懲役またはその両方の刑に処せると規定できる	

	根拠資料	備考
条項番号	条文	

43. 外国の認証局の承認

SG/L-43.1 大臣は、法令によって、管理者が以下の目的のいずれに対しても規定された要件を満たしているシンガポール以外の認証局を認めることができると規定できる

(a) 推奨される信頼限度が、もしあれば、認証局により発行された認証に明記される。

(b) 20(b)(ⅱ)と 21 節において参照された推定。

44. 推奨される信頼限度

SG/L-44.1 認定認証局は、認証を署名者に発行する時に、認証の推奨される信頼限度を明記することとする

SG/L-44.2 適合を考慮して、認定認証局は様々な認証の様々な信頼限度を明記できる

45. 認定認証局の信頼限度

	根拠資料	備考
条項番号	条文	
SG/L-45.1	認定認証局がこの節の申請を放棄しない限り、認定認証局は以下に責任がないこととする (a) 署名者の間違いまたは偽造されたデジタル署名を信頼したことにより起こされたどのような損失額についても、間違いまたは偽造されたデジタル署名について、認定認証局が本法の要件に従った場合。または、 (b) 以下のどちらかのその推奨された信頼限度が認証に明記された額を超えた場合。 (i) 認定認証局が、確認を要求されるというあらゆる事実の認証に不当表示があって信頼を失い生じた損失額。または、 (ii) 認証を発行する場合の 29 と 30 節に従わないとき。	
	46. レポジトリに関する法令	
SG/L-46.1	大臣は、レポジトリと提供サービスの品質を保証するために、レポジトリの標準、認定、または許可の条項を含む法令を作ることができる	
	Part 11. 電子記録と署名の行政用途	
	47. 電子ファイリングの受理と文書発行	

	根拠資料	備考
条項番号	条文	
SG/L-47.1	あらゆる成文法に従うあらゆる政府省局、州機関または特殊法人は、 (a) 文書のファイリングを受け取るか、あるいは文書を作成または保有する必要がある。 (b) あらゆる許可、認定、または承認を発行する。または、 (c) そのような成文法に反するものにもかかわらず支払うことができる方法と様式について準備する。 (i) 電子記録の形式でそのような文書のファイリング、あるいはそのような文書の作成または保持を受け取る。 (ii) 電子記録の形式で許可、認定、または承認を発行する。または、 (iii) 電子形式でそのような支払いをする。	
SG/L-47.2	いかなる場合でも政府省局、州機関または特殊法人が副節(1)(ⅰ)、(ⅱ)または(iii)のあらゆる機能を実行すると決める場合、そのような政府機関は以下に明記できる (a) そのような電子記録がファイル、作成、保有、または発行されるべき様式と形式。 (b) そのような電子記録が署名される必要がある場合、必要な電子署名の形式(適用可能な場合、発信者がデジタル署名または他の安全な電子署名を使用する要件を含む)。 (c) そのような署名が電子記録に添付されるべき様式と形式、および文書をファイルする者により利用される、あらゆる認証局によって満たされるべきその身元または基準。 (d) 電子記録または支払いの適正な整合性、セキュリティ、および機密を保証するために適切な管理処理と手順。および、 (e) 対応する書類文書のために現在明記される電子記録または支払いに必要なあらゆる他の属性。	

根拠資料		備考
条項番号	条文	
SG/L-47.3	電子記録の形式であらゆる文書を受け取り、または発行する、あらゆる政府省局、州機関、または特殊法人を、本法はそれ自体で強制しないこととする	
	Part 12. 一般	
	48. 機密保持の義務	
SG/L-48.1	本法の目的あるいはあらゆる成文法または法廷の命令に対する違反に関するあらゆる起訴を除いて、この部で授与されたあらゆる権限に従って、あらゆる電子の記録、本、登録、通信、情報、文書、または他の資料にアクセスできた者は、そのような電子の記録、本、登録、通信、情報、文書、または他の資料を、どの他者にも公開しないこととする	
SG/L-48.2	**SG/L-48.1** を破るあらゆる者は、違反という罪を犯したことになり、有罪判決に基づき、1 万 S＄(65 万円)以下の罰金、または 12 ヶ月以下の懲役またはその両方の刑によって処罰されることとする	
	49. 両罰	
SG/L-49.1	本法またはその下に作られたあらゆる規則に関する違反が法人によって犯されて、その同意または黙認によって犯された、またはあらゆる所長、理事、秘書、または法人の他の同様な職員、またはそのような能力を演じる意図のあったあらゆる者の一部のあらゆる行為または不履行に起因したと証明される場合、法人だけでなく当事者もその違反という罪を犯し、訴えられて、結果的に罰せられることとする	

根拠資料		備考
条項番号	条文	

50. 認定職員

SG/L-50.1 管理者は書面であらゆる職員または従業員にこの部にある管理者の権限のいずれをも行使する資格を与えられる

SG/L-50.2 管理者およびあらゆるそのような職員は、刑法(224章)の趣旨で公務員であると考えられることとする。

SG/L-50.3 本法の強制権限のいずれかを行使する時に、認定職員は、求めに応じて、管理者が与えた認証局の役を演じている者に演出することとする

51. 管理者による準拠方針

SG/L-51.1 本法またはその下に作られたあらゆる法令の条項への追従を保証する必要がある場合、管理者は、書面での通知によって、認証局またはそのあらゆる職員または従業員に、通知において明記されるような手段を取るか、または活動継続の停止を命じることができる

SG/L-51.2 副節(1)に基づいて発行された通知に明記されたいずれかの指示に従わないあらゆる者は、違反という罪を犯したことになり、有罪判決に基づき、5万S$(325万円)以下の罰金刑、または 12 ヶ月以下の拘禁刑またはその両方の刑によって処罰されることとす。

52. 調査権限

SG/L-52.1 管理者または認定職員は、本法およびその下に作られたあらゆる法令へのその追従に関連して認証局の活動を調査できる

SG/L-52.2 副節(1)の目的のために、管理者は、本法またはその下に作られたあらゆる法令に従ってその調査を進めるかまたは安全にするように、認証局に書面で命令を出せる

根拠資料		備考
条項番号	条文	

53. コンピュータとデータへのアクセス

SG/L-53.1 IDA または任命職員は、以下のことをいつでも与えられることとする

1) 疑う妥当な理由があるまたは本法のあらゆる違反に関連して使用したあらゆるコンピュータシステムおよびあらゆる関連設備の運用または資料にアクセス、検査、確認する。および、

2) そのようなコンピュータシステムに含まれるか、または利用可能などのようなデータでも捜すために、そのようなコンピュータシステムを使用するまたは使用されるようにする。

SG/L-53.2 **SG/L-53.1** の目的のために必要とするかもしれないような妥当な技術、および他の補助を提供するために、IDA または任命職員は、以下に必要な権利を与えられることとする

1) IDA または任命職員が、コンピュータがそのように使われているまたは使われていたことを疑う妥当な理由を持つことによるまたは持つための者。または、

2) コンピュータ、設備、または資料の運用を管理または別途関係するあらゆる者。

SG/L-53.3 以下のあらゆる者は､違反という罪を犯したことになり、有罪判決に基づき、2 万 S＄(130 万円)以下の罰金、または 12 ヶ月以下の懲役またはその両方の刑によって処罰されることとする

1) **SG/L-53.1** の権限の合法な行使を妨害する。または、

2) **SG/L-53.2** の要求に従わない。

54. IDA に対する妨害

根拠資料		備考
条項番号	条文	
SG/L-54.1	本法の機能の実行において、IDA またはあらゆる任命職員に妨害、邪魔、非難、または干渉するどのような者でも違反という罪を犯すことになる	
	55. 文書、データ等の作成	
SG/L-55.1	管理者または認定職員は、本法を実行するために、以下のすべてまたはいずれかを行う権限を持つこととする (a) 認定認証局により管理された記録、勘定、データ、および文書の提示、およびそれらのいずれをも検査、調査、コピーすることを必要とする。 (b) 本法またはその下に作られたあらゆる法令のあらゆる違反に関連したあらゆる者に、あらゆる識別文書の提示を要求する。 (c) 本法の条項またはその下に作られたあらゆる法令に従ったかを確かめるのに必要であるかもしれないような問い合わせをする。	
	56. 一般罰則	
SG/L-56.1	刑罰が明確に課されないで本法またはその下に作られた規則に違反した罪を犯しているあらゆる者は、有罪判決に基づき、2 万 S＄(130 万円)以下の罰金、または 6 ヶ月以下の懲役またはその両方の刑によって処罰されることとする	
	57. 検察官の是認	
SG/L-57.1	本法またはその下に作られたあらゆる法令のあらゆる違反についての起訴は、検察官の是認によるまたは是認がある場合を除いて起こされないこととする	

根拠資料		備考
条項番号	条文	

58. 裁判所の管轄

SG/L-58.1 本法およびその下に作られたあらゆる法令のあらゆる違反を審問、決定するために地方裁判所または治安判事裁判所が司法権を持っていることとし、刑事訴訟法(68 章)に反するものがあるにもかかわらず、本法またはその下に作られたあらゆる法令のあらゆる違反についても、完全な刑罰または処罰を課す権限を持っていることとする

59. 違反の調停

SG/L-59.1 IDA は、自由裁量で、合計 5,000S＄(32 万 5 千円)以下の違反を犯したと合理的に疑われている者から集金することによって和議にされうる違反であると規定されている本法またはその下に作られたあらゆる規則のあらゆる違反でも和議にすることができる

SG/L-59.2 長官は、和議にされうる違反を規定する規則を作ることができる

60. 免除権限

SG/L-60.1 大臣は、適合と考えられるような条件に従って、本法またはその下に作られたあらゆる法令の条項のすべてまたはいずれかからでもあらゆる者または集団を免除できる

61. 法令

SG/L-61.1 大臣は、本法に規定されることを要求されるあらゆるものを規定するために、および一般的に本法の条項を実行するために法令を作ることができる

シンガポール

[SG/R] 電子取引法規則

1999.2.10 施行

根拠資料		備考
条項番号	条文	
	i1. 序	
SG/R-i1.1a	電子取引法およびその規則は、認証局(CAs)に関する任意的資格認可制度を定めた	
SG/R-i1.1b	検査官による認証局の資格認可にかかわる行政的枠組みの定めに加え、規則は、認証局がシンガポールにおいて資格を認可されるための基準および資格認可後の運営に関する継続的な要件を定めるものである。認証局のマイナス評価にかかわる基準には、その財政状態、運営ポリシーおよび手順、ならびに業績が含まれる	
	i2. 資格認定による利益	
SG/R-i2.1	資格認定制度は任意的なものであるが、資格認定を受けた認証機関には次のような利益がある	

	根拠資料	備考
条項番号	条文	
	1)資格認定を受けた認証機関は、その発行する証明書から生成されたデジタル署名につき、証拠上の推定という利益を享受する。そのような推定がなければ、デジタル署名に依拠しようとする当事者は、当該署名が真正でありうる状況下で創出されたことにつき、十分な証拠をもって裁判所を納得させなければならない。この推定に基づけば、当該署名に依拠する当事者は単に当該署名が適正に確認されたことのみを示すだけでよく、署名につきこれに反する主張をする当事者が立証の負担を負うことになる 2)資格認定を受けた認証機関の責任は、電子取引法に基づいて制限される。当該認証機関が電子取引法および規則の要件を満たす限り、利用者の虚偽あるいは偽造されたデジタル署名に依拠した結果生じた損害については、その賠償責任を負わない。資格認定を受けた認証機関がその義務のいくつかを遵守しなかったときは、当該認証機関は、証明書に示された信頼限度までのみ責任を負う 3)監督官がある認証機関に対して資格認定をしたということは、当該認証機関が法定の厳しい要件を満たしたことを示すものである。したがってこれは、当該認証機関が信頼に足るものであることを公に示すものであり、したがって消費者の信頼にもつながる。デジタル署名を利用するにかかわっての証明の容易さともあいまって、資格認定を受けた認証機関がより高い確率をもって利用される可能性がある	
	i3. 資格認定制度	
SG/R-i3.1	資格認定を申請するについては、申請者は申請料として、処理費用を賄うために 5,000 シンガポールドルを支払わなければならない。資格認定がなされた後は、年間資格料金として 1,000 シンガポールドルを徴収する。1 年間有効の資格認定が当初付与される。この産業が成熟しかつ当該認証機関がその業績を積むに至れば、より長い有効期間の資格認定を付与することができる	

	根拠資料	備考
条項番号	条文	

資格認可付与および更新のための要件

i4. 財政的要件等

SG/R-i4.1a	本資格認可制度は、シンガポール内において活動する企業を対象としている
SG/R-i4.1b	申請者は、認証局を運営するために十分な資金を有することおよび主要な責任分野を十分にカバーする保険を付していることを示さなければならない。さらに、申請者は、信用状または銀行保障を差し入れなければならない(罰金/継承用)
SG/R-i4.1c	これは、法令違反に基づく罰金の支払あるいは認証局の過失によって生じた損害に関する責任ならびに是正費用のためのものである
SG/R-i4.1d	これはさらに、当該認証局がその業務を廃止することを決定した場合にその承継者となる認証局への引継ぎ費用に充てることもできる

i5. 運営に関する要件

SG/R-i5.1	資格認可に先立ち、申請者は、これが法および規則の定める要件を満たすものであることを証するための初回監査を受けかつこれに合格しなければならない。加えて申請者は、その CPS に準拠しているか否かについても監査を受ける。CPS は、認証局がその発行する証明書に関するポリシーおよび手続きを規定する書類をいう。資格認可を更新するに先立っても、監査をしなければならない

i6. セキュリティガイドライン

	根拠資料	備考
条項番号	条文	
SG/R-i6.1	検査官は、認証局監査の基準となるセキュリティガイドラインを発表した。このセキュリティガイドラインは、認証局の業務のために特別に作られたものである。したがって、一般的な安全要件に加えて、証明書および鍵の管理等認証局の運営を規制する特別の要件が含まれている	
	i7. 記録保持に関する要件	
SG/R-i7.1	資格認可を受けた認証局は、当該認証局の業務の核となる活動の信頼しうる記録およびログを有しなければならない。これらの活動には、証明書管理、鍵生成およびその計算設備の管理が含まれる。過去の取引の確認を可能とするため、資格認可を受けた認証局は証明書を 7 年以上保存しておかなければならない。認証局は、可能な限り、これをさらに長期間保持しなければならない	
	i8. 証明書の管理	
SG/R-i8.1a	証明書の管理は認証局の中核的機能であり、これについては厳格な要件が定められる。検査官は、認証局が利用者に証明書を付与しあるいはこれを更新するに先立って当該利用者の本人性を確認するために用いられる方法を認可しなければならない	
SG/R-i8.1b	法の定めに従い、資格認可を受けた認証局はさらに証明書停止および失効通知を、証明書停止あるいは失効に関する適法な申請を受領した後直ちに公開しなければならない	
	i9. セキュアなデジタル署名	

	根拠資料	備考
条項番号	条文	
SG/R-i9.1	基本的なセキュリティポリシーおよび要件を遵守するのに加えて、規則はさらに、どのような場合にデジタル署名が安全なデジタル署名(すなわち、法的拘束力を有するデジタル署名であって、法に基づく証拠上の推定が働くもの)と認められるかを規定している。申請者は、安全なデジタル署名を生成するためのこれらの要件を満たすシステムを提供しなければならない。これら要件は、たとえば以下のものを含む： 1) デジタル署名の正しく検査された場合、これはすなわち、当該デジタル署名を付した文書あるいは記録が、当該署名を付した以降に不正に改ざんされていないことが確認されるものでなければならない 2) デジタル署名の適性が確認されたときは、その署名者も正確に特定されなければならない 3) 当該署名者以外の者が当該デジタル署名を創出したことは、計算上考えられないこと 4) 署名の創出は、署名者の意思に基づかなければできないことを保障するための措置が採られなければならない 5) 署名者本人の関与あるいはその知識に基づかなければ、当該署名者以外の者が当該署名創出のための一連のステップを複製ししたがってこれにより有効な署名を創出することができないこと	

i10. 証明書の種類

根拠資料		備考
条項番号	条文	
SG/R-i10.1	市場の要請に応じるため、資格認定を受けた認証機関は、確かさの度合いの異なる証明書を発行することができる。資格認定を受けた認証機関は、安全なデジタル署名を創出することのできる信頼性の高い証明書を発行することができ、あるいはたとえば電子メールにおいて単純な真正確認あるいは本人確認のために用いるような、確実性のより低い証明書を発行することもできる。しかしながらこれについては、監督官の承認が前提となり、それぞれのタイプの証明書については、これに関する格別の承認された CPS がなければならない。これにより、資格認定を受けた認証機関により高いフレキシビリティが与えられ、また、その発行しうる証明書のタイプとの兼ね合いで、資格認定を受けていない認証機関に比較した場合の不利益を回避することができる	
	i11. 秘密要件	
SG/R-i11.1	資格認可を受けた認証局は､利用者に関する情報の秘密を保障しなければならない。これは、利用者が証明書を申請するに際しその潜在的にプライベートな情報を提供するについての信頼を害することを防ぐことを目的とするものである	
	i12. 政府認証機関	
SG/R-i12.1	法に基づき、通産大臣は、政府機関につき、資格認定を受けた認証機関と同様の利益のもとに認証機関として行為すべき政府機関を認定することができる。一定の要件(例：財政的要件)を除き、かかる政府認証機関にも規則は適用される	
	i13. 適用除外	

根拠資料		備考
条項番号	条文	
SG/R-i13.1	規則は認証機関一般に適用されるものであるが、監督官は、特別の状況下、とりわけ、クローズド・ネットワーク・コミュニティにおける認証機関につき、規則の定める要件の一部の適用除外を認めることがある	
	i14. 結び	
SG/R-i14.1	法および規則は、国内外のマーケットに寄与するシンガポールの信頼される認証機関サービスを確立するための法的枠組みを提供することを目的とする。これは長期的には、シンガポールが広い範囲でセキュリティ・プロダクトおよびサービスを提供しこれにより信頼される電子取引のハブとなるための基礎をなすことになるものである	
	Part 1 予備的事項	
	1. 略称および発効日	
SG/R-1.1	本規則は「1999 年電子取引(認証局)規則」と呼称することができ、1999 年 2 月 10 日に施行する	
	2. 定義	

	根拠資料	備考
条項番号	条文	
SG/R-2.1	本規則において、文脈上ほかの意味に理解する必要がない以上、 「資格認可」とは、本規則に基づいて与えられた資格認可をいう； 「加入者識別方法」とは、加入者の本人確認のために利用される方法をいう； 「トラステッド・パーソン」とは、以下の者をいう 1) 認証局に関して、法および本規則によって規制されている業務活動の日常の運営、安全および成果について直接の責任を有する者、または、 2) 証明書の発行、更新、停止、失効に直接かかわる義務(資格認可を受けた認証局に対して証明書を請求する者の本人特定を含む)、秘密鍵の創出に直接かかわる義務あるいは認証局の電算施設の管理に直接かかわる義務を負う者	
	Part 2 認証局の資格認可	
	3. 資格認可申請	
SG/R-3.1	認証局にかかわる資格認可申請は、検査官が適宜定める方法によって行い、かつ検査官が要求する資料を添付するものとする	
SG/R-3.2	検査官は、申請者に対し、当該申請にかかわって必要な追加的情報を提出することを求めることができる	
SG/R-3.3	検査官は、資格認可の更新申請について、その要求する要件のもとに電子記録の形式で提出することを認めることができる	
SG/R-3.4	資格認可は、検査官が適宜定めることができる条件、規制および制限の対象となる	

	根拠資料	備考
条項番号	条文	

4. 資格認可の有効期間

SG/R-4.1 資格認可は 1 年間有効とする。ただし、検査官は、これより長い有効期間を定めることができる

5. 資格認可の更新

SG/R-5.1 **SG/R-3** は、資格認可の新規申請に対すると同様に、更新申請に対しても適用する

SG/R-5.2 認証局は、その資格認可の更新申請を、その有効期限の 3 ヶ月前までに提出しなければならない。

SG/R-5.3 認証局がその資格認可を更新する意思がないときは、以下を行わなければならない

1) 検査官に対し、有効期限の 3 ヶ月前までにこれを通知すること

2) 有効期限の 2 ヶ月前までに、すべての加入者に対して書面でこれを通知すること、および

3) 資格認可失効の 2 ヶ月前までに、検査官が定める方法により、日刊新聞にこれを広告すること

6. 資格認可料

SG/R-6.1 資格認可認証局となるための資格認可授与または更新申請をするときは、その度ごとに、検査官に対して、申請料 5,000S＄(32 万 5 千円)を支払わなければならない

SG/R-6.2 前項に定める申請が承認されたときは、検査官に対し、当該資格認可付与につき 1 年当たり 1,000S＄(6 万 5 千円)の料金を支払わなければならない。

	根拠資料	備考
条項番号	条文	
SG/R-6.3	資格認可の更新については、検査官に対し、更新 1 件につき 1 年当たり 1,000S＄(6 万 5 千円)の料金を支払わなければならない	
SG/R-6.4	申請が承認されず、撤回されあるいは廃止されまたは資格認可が停止あるいは取り消された場合でも、検査官は支払済みの料金を返還しない	
	Part 3 資格認可要件	
	7. 資格認可の更新	
SG/R-7.1	資格認可申請者は、以下の要件を満たさなければならない： 1) 申請者は、シンガポール内において運営される会社でなければならない。 2) 申請者は、申請者、その役員または従業員の過誤または懈怠に基づいてなされる各請求につき、保障額が 100 万 S＄(6500 万円)を下らない賠償責任保険に加入していなければならない。 3) 申請者は、 a) 200 万 S＄(1 億 3000 万円)の払込済み資本を有し、かつ b) これに加え、払込済み資本と利用可能資金証明の合計が 500 万 S＄(3 億 2500 万円)以上であること 4) 申請者は、検査官を受益者として、その定める形式により、100 万 S＄(6500 万円)以上の信用状または銀行保証を取得しなければならない。	

	根拠資料	備考
条項番号	条文	
SG/R-7.2	**SG/R-7.1.4** の信用状または銀行保証は、以下の場合にこれを行使することができる： 1) 検査官がなした和解提案に基づく支払 2) 認証局、その役員または従業員の過失に基づく損害賠償および修正費用の支払 3) 当該認証局の資格認可または業務が廃止された場合、当該廃止または資格認可認証局業務の移転に関して生じた費用の支払	
	8. 要員	
SG/R-8.1	申請者は、すべてのトラステッド・パーソンが以下の事項を満たすことを確実に実現するための合理的な方策を講じなければならない 1) 同人が、同人に与えられた義務を遂行するについて、適切な人物であること 2) 同人がシンガポール内あるいは国外において免責前破産者ではなくあるいはその債権者との間で和議または債務整理を行ったこと 3) シンガポール内あるいは国外で、以下の罪につき有罪判決を受けていないこと： a) 詐欺または背任の罪 b) 法または本規則違反	

根拠資料		備考
条項番号	条文	
SG/R-8.2	検査官は、前項 c 号にかかわらず、申請者が同号に言及する罪につき有罪判決を受けたトラステッド･パーソンを置くことを認めることができる。ただし、検査官が以下の事項を認めた場合に限る： 1) 当該トラステッド・パーソンが、現時点においては、その職務を遂行するにつき適切であること、および 2) 以下の時点から 10 年が経過したこと a) 有罪判決の日、または b) 同人が懲役／禁固の刑を受けたときは、釈放の日の遅いほうの時点	
SG/R-8.3	すべてのトラステッド・パーソンは、 1) 法および本規則について十分な知識を有さなければならない。 2) 認証局の CPS につき訓練を受けなければならない。 3) その職務を効率的に遂行するために、関連する技術資格、技能および経験を有さなければならない。	
	9. 運用に関する要件	
SG/R-9.1	申請者は､運営に関する以下の要件を満たさなければならない： 1) 申請者は、IDA が公認した CPS を有さなければならない。 2) 申請者は、IDA によってなされる資格認可付与前の初回監査を受けこれに合格しなければならない。 3) 申請者は、IDA が書面により通知して要求する監査を受け、これに合格しなければならない。	

根拠資料		備考
条項番号	条文	
SG/R-9.2	本条で言及する監査は、 1) **SG/R-10** に示す監査の要件に沿って行われなければならない。 2) 検査官が書面による通知で特定する期間内に完了しなければならない。	
	10. 監査に関する要件	
SG/R-10.1	申請者は、以下に関する適合について **SG/R-9.1** に要求する監査に合格しなければならない 1) **SG/R-26** に言及するセキュリティガイドライン (SG/CA) 2) 資格認可条件 3) CPS および 4) 法および本規則	
SG/R-10.2	すべての監査は、検査官が本規定の目的のために承認した資格ある独立した監査チームにより行う。このチームは、１名の公認会計士および 1 名の公認情報システム監査人で構成され、かつその内の 1 人はデジタル署名および証明書につき十分な知識を有する者でなければならない	
SG/R-10.3	この監査チームが属する企業または会社は監査の対象である認証局から独立していなければならず、また、当該認証局に役務を提供しあるいは設備を供給しまたはしていたソフトウェアまたはハードウエアの販売者であってはならない	
SG/R-10.4	監査料は、認証局の負担とする	
SG/R-10.5	すべての監査につき、検査官に対し、監査終了後 4 週間以内に、監査報告書 1 部を提出するものとする	
SG/R-10.6	監査不合格に基づいて、資格認可を取り消すことがある	

根拠資料		備考
条項番号	条文	

11. 特定の状況における、検査官による資格認可授与または更新の拒絶

SG/R-11.1 以下のいずれかに当たる場合、検査官は、資格認可の授与または更新を拒否することができる

SG/R-11.1.1 1) 申請者が検査官に対し、検査官が要求する以下に関する情報を提供していないとき

a) 申請者またはその従業員あるいは業務上の目的のために関係を有する人員

b) その業務遂行方法に影響を与える可能性のある一切の状況

SG/R-11.1.2 2) 申請者またはその重要な持分所有者が解散または清算中であるとき

SG/R-11.1.3 3) 申請者またはその重要な持分所有者につき、管財人または管財・管理人が選任されたとき

SG/R-11.1.4 4) シンガポール内外にかかわらず、申請者またはその重要な持分所有者が債権者との間で和議または債務整理手続きを開始し、これが決了していないとき

SG/R-11.1.5 5) シンガポール内外を問わず、申請者またはその重要な持分所有者あるいはあらゆるトラステッド・パーソンが、その欺罔または不誠実行為を認定されて有罪判決を受け、あるいは法または本規則の違反について有罪判決を受けたとき

SG/R-11.1.6 6) 申請者の資格認可保有に関連する職務を実施するトラステッド・パーソンの資格または経験について、検査官が十分と認めないとき

SG/R-11.1.7 7) 申請者が資格認可を取得するにつき適性のある者であることまたはそのすべてのトラステッド・パーソンおよび重要な持分所有者も適正な者であることについて検査官を納得させることができないとき

根拠資料		備考
条項番号	条文	
SG/R-11.1.8	8) 申請者またはその重要な持分所有者あるいはトラステッド・パーソンの評判、性格、財政状態および信頼性に鑑み、申請者が加入者、顧客または参加者の最大限の利益のために活動することができない可能性があると信ずる理由を検査官が有するとき	
SG/R-11.1.9	9) 検査官が、申請者またはその重要な持分所有者の財政状態について満足しないとき	
SG/R-11.1.10	10) 申請者がその資格認可保有に関連して行うであろう事業の性質に鑑み、申請者またはトラステッド・パーソンの過去の実績または専門性について検査官が満足しないとき	
SG/R-11.1.11	11) その他、申請者またはその重要な持分所有者あるいはトラステッド・パーソンにつき、その不適切な業務活動をきたしあるいは信頼を害するべき業務の方法を反映するものである可能性のある状況があるとき、または	
SG/R-11.1.12	12) 資格認可拒否が公共の利益に合致すると検査官が認めるとき	
SG/R-11.2	**SG/R-11.1** にいう「重要な持分者」とは、会社である申請者との関係では、会社法(第 50 章)の規定すると同様の者をいう。	
	Part 4 認可の取消と休止	
	12. 認可の取消もしくは休止	
SG/R-12.1	認証局が解散される場合は、認可は取り消されたと見なされるものとする	

根拠資料		備考
条項番号	条文	
SG/R-12.2	検査官は、以下の場合に、認証局の認可の取消または休止を実施しなければならない 1) **SG/R-11** に基づいて検査官が認可の許可を拒否しなければならない任意の理由がある場合 2) **SG/L-51** に定められた検査官の指示に従うことを認証局が怠った場合 3) 認証局が解散するか、解散を予定している場合 4) 認証局がその債権者と任意の示談もしくは和解を開始した場合 5) 認証局が、認可が与えられた業務の遂行を怠った場合 6) 認証局またはその委託人がその義務を効率的に、または誠実もしくは公正に果たしていないと判断する理由が検査官にある場合 7) 認証局が、認可に関して適用可能な任意の条件または制限に違反するか、従わない場合	
SG/R-12.3	検査官は、認証局の依頼があれば、その認証局の認可を取り消さなければならない	
SG/R-12.4	検査官は、認証局に釈明の機会を最初に与えることなしに、**SG/R-12.2** に基づいて認可を取り消してはならない	
	13. 誤行為の場合における検査官の権限	
SG/R-13.1	認証局、その幹部、またはその従業員が、任意の誤行為を犯している、または犯したことがあるとする任意の申し立てについて、または、認証局による業務上の不正行為または営業方法に関する不信につながった、またはつながる恐れがある任意のその他の状況から、認証局、その幹部、またはその従業員は認可を受け続けるにはもはや不適切であるとする任意の申し立てについて、検査官は調査を実施しなければならない	

根拠資料		備考
条項番号	条文	
SG/R-13.2	**SG/R-13.1** に基づく申し立ての調査後、申し立てが立証されたと検査官が判断する場合、検査官は適切と判断すれば以下を実行しなければならない 1) 認証局の認可を取り消す。 2) 検査官が決定を行う期間、または、検査官が決定を行うまで、認証局の認可を休止する。 3) 認証局を懲戒する。	
SG/R-13.3	検査官は、**SG/R-13.1** における認証局への申し立ての調査の審問において、認証局に釈明の機会を与えなければならない	
SG/R-13.4	**SG/R-13.1** に基づき申し立ての調査を実施した後、申し立ては悪意に基づいていたり、不真面目または嫌がらせであると検査官が判断する場合、検査官は申し立てを行った当事者に対し、調査にかかった任意の費用および出費を書面による命令で請求するものとする	
SG/R-13.5	検査官は、調査の結果として、本条例のセクション 51 に定められた承諾に対して、認証局に指示を与えなければならない	
SG/R-13.6	“誤行為”とは、この規則の目的に対して以下を意味する 1) 本条例の要件またはそれらの規則、または、認証局の認証局運用規定の承諾に対する任意の怠慢 2) 公共の利益に反する、または反するような、認証局の業務に関する任意の行為または怠慢	
	14. 認定の取消もしくは停止の効果	
SG/R-14.1	規則 12 または 13 に基づいて認定の取り消しもしくは停止処分を受ける認証局は、この規則の目的に対し、監督官が認定の取り消しもしくは停止を行う日から、場合に応じて、未認定であると見なされるものとする。	

根拠資料		備考
条項番号	条文	
SG/R-14.2	認証局の認定の取り消しまたは停止は、以下の目的で実施されてはならない 1)認証局によって締結された任意の協定、取引または取り決めを無効にすること、またはそれらに影響を与えること。この場合、任意の協定、取引または取り決めの締結が認定の取り消しまたは停止の前に行われたのか後に行われたのかは問わない。 2)こうした任意の協定、取引または取り決めの下で発生する権利、義務、または責任に影響を与えること。	
	15. 認定の拒否に対する訴え	
SG/R-15.1	以下の場合、監督官の決定によって害を受ける任意の当事者は、決定の通知を受けてから 14 日以内に、大臣に訴え出ることができ、その大臣の決定は最終的なものとなる 1)監督官が、規則 11 に基づいて認定の供与または更新を拒否する場合 2)監督官が、規則 12 に基づいて認定を取り消す場合 3)規則 13 に基づいて、認定の取り消しまたは停止が行われるか、認証局が懲戒を受ける場合 4)契約履行保証または銀行保証が、規則 7(2)の下で提示される場合	
SG/R-15.2	監督官の決定に対して訴えが行われた場合、監督官は適切と判断するならば、大臣による決定が下されるまで、または、訴えが撤回されるまで、場合に応じて決定の行使を延期しなければならない	
SG/R-15.3	監督官は、決定の行使を延期するかどうかを検討する際、認証局の任意の加入者、または損害を被る可能性がある任意の第三者の利益に延期が反するかどうかを考慮しなければならない	
SG/R-15.4	大臣の判断を求めて訴えが行われた場合、訴えの写しは監督官に提出されなければならない	

根拠資料		備考
条項番号	条文	

Part 5 資格認可認証局の業務行為

16. 信頼できる記録の作成および維持管理

SG/R-16.1 資格認定認証機関は、その記録を、紙による書類、電子記録あるいはその他監督官が承認した方法により作成しなければならない

SG/R-16.2 この記録は、索引を付し、正確で完全で判読可能でかつ監督官、監査人あるいは権限を与えられた官吏がアクセスすることのできる状態に保存され、保持されかつ再現されるものとする

17. 信頼に足る取引ログ

SG/R-17.1 すべての資格認定認証機関は、以下に関する記録を信頼に足る方法により作成しかつ保持する：

1)証明書の発行、更新、停止および取消にかかわる活動(資格認定認証機関に対して証明書を要求する者の本人特定の手続きを含む)

2)加入者の鍵ペアの生成あるいは、(関連する場合)資格認定認証機関自らの鍵ペアの生成過程

3)資格認定認証機関の電算設備の管理、および

4)監督官が定める、資格認定認証機関の重要な関連活動

SG/R-17.2 すべての資格認定認証機関は、その発行したすべての証明書の副本を保存し、かつ 7 年以上の間この証明書にアクセスすることができるメカニズムを維持する

SG/R-17.3 すべての資格認定認証機関は、第 1 項の要求するすべての記録および前項に定める証明書の副本記録作成に関するすべてのログを 7 年以上の間保持する

根拠資料		備考
条項番号	条文	

18. 証明書の種類

SG/R-18.1 監督官が承認したときは、資格認定認証機関は、以下の異なるレベルの確実性を有する証明書を発行することができる：

1)法 20 条(b)(i)にいう信頼に足る証明書と認められるもの、および

2)法 20 条(b)(i)にいう信頼に足る証明書と認められないもの

SG/R-18.2 資格認定認証機関は、その発行するそれぞれの種類の証明書について、監督官が承認した特定の CPS を関連付けなければならない

SG/R-18.3 資格認定認証機関は、法 20 条(b)(i)の意味における信頼に足る証明書であると認められない証明書を使用しあるいはこれに依拠することの効果について、加入者およびこれに依拠する者の注意を喚起しなければならない

19. 証明書の発行

SG/R-19.1 法 29 条に規定する要件に加え、すべての資格認定認証機関は本条の定める証明書発行に関する要件を満たさなければならない

SG/R-19.2 証明書は、当該証明書が停止されまたは取り消された場合にこれに関する取消または停止通知が記録される 1 つまたは複数のレポジトリの場所を確認しあるいはこれを特定するのに十分な情報を含みあるいはこれに言及することによってこれと一体をなすものでなければならない

SG/R-19.3 資格認定認証機関の CPS に定める活動および手続きは、法 29 条(2)に規定する条件よりも高い基準の条件を含むものでなければならない

根拠資料		備考
条項番号	条文	
SG/R-19.4	証明書発行に用いられる加入者識別方法は、これをCPS に明示しなければならず、かつ、資格認定申請の際の監督官の承認を受けなければならない	
SG/R-19.5	ある者に対し、ある証明書(本条においては、「新証明書」という。)が、同一人が所有する別の有効な証明書(本条においては、「原証明書」という。)に基づいて発行され、その後原証明書が停止されまたは取り消されたときは、当該新証明書を発行した認証機関は、当該新証明書を停止しまたは取り消すことが必要であるか否かを決定するために調査を実施しなければならない	
SG/R-19.6	資格認定認証機関は、加入者に対し、証明書を受容する前にその内容を確認する合理的な機会を与えなければならない	
SG/R-19.7	加入者が発行された証明書を受容するときは、資格認定認証機関は、当該証明書の署名付き写しを第 2 項に定めるレポジトリに公表するものとする	
SG/R-19.8	前項の定めにかかわらず、資格認定認証機関は加入者との間の契約により、証明書を公開しない旨合意することができる	
SG/R-19.9	加入者が証明書を受容しないときは、資格認定認証機関はこれを公開しない	
SG/R-19.10	資格認定認証機関により証明書が発行されかつこれが加入者によって受容されたときは、資格認定認証機関は、当該証明書の有効性または信頼性に重要な影響を及ぼす事実であって当該資格認定認証機関が知るものを合理的な期間内に加入者に対して通知するものとする	
SG/R-19.11	証明書の発行に関連する一切のやり取りの日時は、そのログを記録し、かつこれを信頼に足る方法により保管しなければならない	
	20. 証明書の更新	
SG/R-20.1	前条の規定は、これが証明書の発行に適用されると同様に、証明書の更新についても適用する	

根拠資料		備考
条項番号	条文	
SG/R-20.2	加入者の本人特定の方法は、監督官によって承認された CPS に定めるものによるものとする	
SG/R-20.3	証明書の更新に関する一切のやり取りの日時は、そのログを記録しかつこれを信頼に足る方法で保管しなければならない	
	21. 証明書の停止	
SG/R-21.1	本条は、加入者による証明書停止申請を認める資格認定認証機関のすべてに対してのみ適用される	
SG/R-21.2	加入者が書面により同意したときは、資格認定認証機関は停止に代わり即時の取消を定めることができる	
SG/R-21.3	法 31 条に基づく証明書停止申請を受領したときは、資格認定認証機関は、当該証明書を確実に停止し、かつ法 34 条に従って停止通知をレポジトリに確実に公開しなければならない	
SG/R-21.4	資格認定認証機関は、その発行した証明書が信頼性を欠くと認める合理的な理由があるときは、当該加入者がこれに同意するか否かを問わず、当該証明書を停止することができる。ただし資格認定認証機関は、当該証明書の信頼性に関する調査を完了した上で、法 32 または 33 条に基づいて当該証明書を復活させるかあるいはこれを取り消すかを合理的な期間内に設定しなければならない	
SG/R-21.5	ある証明書が停止されているか否かを確認することは、当該証明書に依拠しようとする者の責任とする	
SG/R-21.6	資格認定認証機関は、有効な停止申請を受領したときは、証明書を停止する(法 31 条による)。ただし、当該認証機関が、その入手可能な一切の証拠に基づいて取消を相当と判断したときは、当該証明書は法 32 または 33 条に基づいて取り消さなければならない	
SG/R-21.7	資格認定認証機関は、加入者およびその権限ある代理人に対し、証明書を取り消すべきか否かおよび停止後これを復活させるか否かについて確認しなければならない	

根拠資料		備考
条項番号	条文	
SG/R-21.8	資格認定認証機関は、申請に基づいて行われた停止について、当該停止申請が当該加入者またはその権限ある代理人の授権なしになされたものであることを発見しかつこれを確認したときは、停止を終了しなければならない	
SG/R-21.9	停止に基づいて証明書の取消が行われるときは、取消に関する要件が適用される	
SG/R-21.10	証明書の停止に関連する一切のやり取りの日時は、そのログを記録しかつこれを信頼に足る方法により保管しなければならない	
SG/R-21.11	資格認定認証機関は、停止申請をいつ何時においても受領しかつこれに基づいて行為するための施設を維持しなければならない	
	22. 証明書の取消	
SG/R-22.1	法 32 条(a)に従って取消申請を行う加入者またはその権限ある代理人の本人特定のため、資格認定認証機関は、CPS にこれを目的とするものとして定めた加入者識別方法を用いなければならない	
SG/R-22.2	資格認定認証機関は、取消申請を受領したときは、これを検認し、当該証明書を取り消しかつ法 35 条に従って通知を公表しなければならない	
SG/R-22.3	資格認定認証機関は、いつ何時においても取消申請を受領しかつこれに基づいて行為するための施設を維持しなければならない	
SG/R-22.4	資格認定認証機関は、証明書を取り消したときは、これを直ちに当該加入者に通知するものとする	
SG/R-22.5	証明書の取消に関連する一切のやり取りの日時は、そのログを記録しかつ信頼に足る方法により保管しなければならない	
	23. 証明書の失効の日	

根拠資料		備考
条項番号	条文	
SG/R-23.1	証明書には、それが失効する日を表示しなければならない	
	24. CPS	
SG/R-24.1	すべての資格認定認証機関は、その CPS 作成のガイドとして、インターネットエンジニアリングタスクフォースが承認し監督官がそのインターネットウェブサイトに再現する「インターネット X.509 公開鍵インフラストラクチャー証明ポリシーおよび証明業務の枠組み」のインターネットドラフトを使用するものとする	
SG/R-24.2	資格認定期間中の CPS の一切の変更については、監督官の事前の承認を必要とする	
SG/R-24.3	すべての資格認定認証機関は、その加入者に対し、その責任制限について明確に示し、かつ、とりわけ、加入者の証明書の信頼限度額が有する意義についてその注意を喚起しなければならない	
SG/R-24.4	証明書の発行、停止、取消および更新のための加入者識別方法は、これを CPS に定めなければならない。	
SG/R-24.5	最新の CPS は、これにその発効日を付してこれを監督官に提出しかつ一般公衆がアクセス可能な当該認証機関のインターネットウェブサイトにおいて公開しなければならない	
SG/R-24.6	発効日後は、監督官に提出された最新バージョンが特定の証明書につき効力を有するものとする	
SG/R-24.7	すべての資格認定認証機関は、CPS の一切の変更についてそのそれぞれの発効日を付してそのログを記録しなければならない	
SG/R-24.8	資格認定認証機関は、CPS の各バージョンを、その発効日および失効日を付して信頼に足る方法で保管しなければならない	
	25. セキュアなデジタル署名	

根拠資料		備考
条項番号	条文	
SG/R-25.1	法 20 条の要求を技術的に実施するについては、当人の証明書に示されている公開鍵と照らし合わせることによって検証されるデジタル署名を、当該署名が対応する者以外の者が創出することが計算上実現不可能であることが確実に実現されるようにしなければならない	
SG/R-25.2	署名それ自体としては、 1)当該署名が対応する人物の名前あるいはその他の固有の者として特定可能な特徴が署名の一部をなすものとしてこれに含まれかつ代替または改ざんが不可能であることを確実に実現するものでなければならない。また、 2)当該署名に依拠しようとする者に対し、これらの識別要素を明確に示すものでなければならない。	
SG/R-25.3	技術的実施においては、 1)署名創出に向けて採られる手順は、当該署名が対応する者の指図に基づくものであり、かつ 2)当該署名が対応する者の関与あるいはその知識なしには、他者が当該署名を創出するための手順の連続を復元ししたがって有効な署名を創出することができないことを確実に実現するものでなければならない。	
SG/R-25.4	技術的実施においては、署名に依拠する者に対し、当該署名が対象とする文書または記録が何らかの変改を受けたか否かを示し、かつこの摘示が署名の確認手続き中で表示されなければならない	
	26. セキュリティガイドライン	
SG/R-26.1	すべての資格認定認証機関は、その業務の実施が、監督官が決定しかつそのインターネットウェブサイトに公開されたセキュリティガイドラインを本質的に満たすことを確実に実現しなければならない	

根拠資料		備考
条項番号	条文	
SG/R-26.2	監査人は、セキュリティガイドラインからの違背が本質的なものであるか否かを決定するについては、ガイドラインに厳格に合致していない条件が本質的なものであるか否かについて、当該状況およびシステム全体を考慮しつつ、合理的な専門的判断をしなければならない	
SG/R-26.3	監査人が本質的と認めることができる状況が広範なものであるということとは別に、以下の違背はこれを本質的なものとみなす： 1)証明書の有効性にかかわる一切の違背 2)トラステッド・パーソンの機能を、これに不適格な者により行ったこと、または 3)資格認定認証機関が信頼できるシステム以外のシステムを使用すること	
SG/R-26.4	セキュリティガイドラインは、システムが使用される状況との関連において合理的にかつ他の法律との整合性をもって解釈されなければならない	
SG/R-26.5	セキュリティガイドラインの違背が本質的であるか否かに関する監査人の評価にかかわらず、監督官はその自らの評価をなしかつ第 1 項の目的のために監査人のそれとは異なる結論に至ることができる	
SG/R-26.6	すべての資格認定認証機関は、そのすべての加入者に対し、その鍵ペアを生成するための信頼できるシステムを提供しなければならない	
SG/R-26.7	すべての資格認定認証機関は、デジタル署名を信頼に足る方法によって生成し確認するメカニズムを提供しかつそのメカニズムは署名の有効性を示すものでなければならない	
SG/R-26.8	デジタル署名が有効でないときは、提供されたこのメカニズムは、その無効が文書の完全性によるものかあるいは署名によるものかを示しかつ証明書の状況をも示すものでなければならない	
SG/R-26.9	資格認定認証機関以外の第三者によって提供されたメカニズムについては、これによる署名は、資格認定認証機関がその証明書との関連でこのメカニズムの実施を受容する場合にのみセキュアなものとみなす	

根拠資料		備考
条項番号	条文	
SG/R-26.10	すべての資格認定認証機関は、鍵(加入者の鍵および資格認定認証機関自らの鍵を含む)を信頼に足る方法により保管する責任を負う	
SG/R-26.11	監督官は、適宜、そのインターネットウェブサイトにおいて、すべての資格認定認証機関による遵守のために、セキュリティガイドラインにかかわるその他の事項を公開することができる	
	27. 危機管理	
SG/R-27.1	資格認可認証局は、少なくとも以下の事象の管理を定める危機管理計画を実施しなければならない： 1) 鍵の危殆化 2) 認証局のシステムおよびネットワークへの侵入 3) インフラストラクチャーの使用不能および 4) 欺罔による登録および証明書、その停止および失効に関する情報の生成	
SG/R-27.2	**SG/R-27.1** に定める事象が生じたときは、これを 24 時間以内に検査官に報告しなければならない	
	28. 秘密保持	
SG/R-28.1	法第 12 部の目的によるものあるいは成文法に基づく訴追または裁判所の命令による場合を除き、すべての資格認可認証局およびその権限ある代理人は、個々の加入者にかかわる情報を秘密に保たなければならない	
SG/R-28.2	個々の加入者にかかわる情報を資格認可認証局またはその代理人が開示するについては、必ず当該加入者の授権を得なければならない	

根拠資料		備考
条項番号	条文	
SG/R-28.3	本条は、個々の加入者に関する以下の情報には適用しない： 1) 一般に公開される証明書中に含まれているもの 2) 同様の目的のために、当該加入者が資格認可認証局に提供するもの、または 3) 証明書の失効または停止の事実に関連するもの	
	29. マネージメントの変更	
SG/R-29.1	資格認可認証局は、その役員、代表者または代表者と同等の権能を行う者に変更が生じたときは、これを検査官に対し同人の任命後 3 日以内に通知しなければならない	
	Part 6 レポジトリに関する要件	
	30. 一般レポジトリの利用可能性	
SG/R-30.1	1) 一般レポジトリは、通年いつでも利用可能でなければならない。 2) 一般レポジトリは、その合計ダウン時間がどの１ヶ月の期間をとってもその 0.3%を超えないことが保証されなければならない。 3) いかなるダウン時間も、これが予定されたものか否かにかかわらず、1 度に 30 分を超えてはならない。	
	31. 特別レポジトリ	
SG/R-31.1	監督官が承認したときは、特別の目的のためのレポジトリを設けることができ、これについては、その運営時間を制限することも認められる	

根拠資料		備考
条項番号	条文	

Part7. 政府および法定法人に関する適用

32. 政府および法定法人に関する適用

SG/R-32.1 法 20 条(b)(iii)の目的のために、政府省庁、国家機関または同条に基づいて大臣が認証機関として行為することを承認した法定法人は、第三部(7 条および 11 条を除く)、四部(第 12、14 および 15 条を除く)、五部(29 条を除く)、六、七および八部(第 36 条および 37 条を除く)を、資格認定認証機関と同様に遵守しなければならない。

SG/R-32.2 前項に定める規定は、必要な修正およびその他監督官が定める修正を経た上で、政府省庁、国家機関または法 20 条(b)(iii)に基づいて大臣が承認した法定法人にこれを適用する。

Part 8 管理

33. 適用除外

SG/R-33.1 本規則に定める要求事項の適用除外を求めようとする資格認定認証機関は、資格認定申請時にこれを監督官に対して書面で申請することができる

SG/R-33.2 当該申請には申請の理由を付しかつ必要な裏付け書類を添付しなければならない

34. 開示

根拠資料		備考
条項番号	条文	
SG/R-34.1	資格認可認証局は、検査官に対し、半年ごとに業務および財政報告を提出しなければならない。	
SG/R-34.2	半年ごとの業務報告には、以下の情報を記載しなければならない： 1) 加入者数 2) 証明書発行数、停止数、失効数、有効期限切れ数ならびに更新数 3) システムの稼働時間および停止時間ならびに異常事態を含むシステム・パフォーマンス 4) 認証局の組織構成の変更 5) 前回の業務報告または資格認可申請以降に生じた変更、および 6) 検査官に対する前回の提出以降に生じたトラステッド・パーソンに関する事項の変更。ただし、その氏名、識別番号、住所、役職、権能および雇用の日を含む。	
SG/R-34.3	資格認可認証局は、検査官に対し、提出した情報にかかわる一切の変更につき、これを開示する継続的義務を負う	
SG/R-34.4	資格認可認証局の効力を有する最新の CPS のバージョンは、その発効日と共に、当該資格認可認証局のインターネットウェブサイト上で公開されなければならない	
	35. 資格認定認証機関の業務の廃止	
SG/R-35.1	資格認定認証機関がその業務を廃止しようとするときは、その加入者が他の資格認定認証機関に再加入するように手配することができる	
SG/R-35.2	当該資格認定認証機関は、その記録および証明書について、信頼に足る方法で複製が作られるように手配することができる	
SG/R-35.3	記録が他の資格認定認証機関に移転されるときは、信頼に足る方法によりなされなければならない	

	根拠資料	備考
条項番号	条文	
SG/R-35.4	資格認定認証機関は、監督官に対し、 1)3 ヶ月以上前に書面でその業務を廃止する意思を通知しなければならない。 2)その加入者に対し、2 ヶ月前以上にその業務を廃止する意思を通知しなければならない。さらに、 3)監督官が定める日刊新聞にその定める方法により、2 ヶ月以上前までにその業務を廃止する意思を広告しなければならない。	
	36. 罰則	
SG/R-36.1	何らの合理的理由なく、**SG/R-16.2**、**SG/R-17**、**SG/R-19.2** または **SG/R-19.11**、**SG/R-20.3**、**SG/R-121.10**、**SG/R-22.5**、**SG/R-24.7** または **SG/R-24.8** または **SG/R-28** に違反する者は、罪を犯したものとし、5,000S＄(32 万 5 千円)以下の罰金に処し、2 回目以降については、1 万 S＄(65 万円)以下の罰金に処する	
	37. 違反の宥恕	
SG/R-37.1	本規則に関するいかなる違反についても、法 59 条に基づいて、監督官が宥恕することができる	

シンガポール

[SG/CA] 認証局セキュリティガイドライン

1999.9V1.0, 2003.9V2.0

根拠資料		備考
条項番号	条文	

1. 概要

1.1. 目的

本書の目的は、認証局の管理、システム、運用のセキュリティガイドラインを規定することである。このガイドラインは、認証サービス、データ、システムの完全性、機密性、利用可能性を保護するためのものである

根拠資料		備考
条項番号	条文	

セキュリティガイドラインは、主体の存在を確認し保証する信頼される第三者機関としての役割を持つ認証局に適用される。認証局は以下の証明書管理機能を実行する

(1) 登録、停止、および失効要求の確認

(2) 証明書の生成、発行、停止、および失効

(3) 証明書、停止および失効の情報の公開と保管

1.2. 範囲

本書は、認証局の基本的役割および機能、すなわち存在認証と証明書管理をカバーしている。電子公証や委託タイムスタンプサービスのような拡張機能は扱っていない

本書は、認証局の階層(たとえば、認証局と上位認証局との関係や相互認証主体)の要件は扱っていない。セキュリティガイドラインは、認証局にわたる相互動作性要件(たとえば、証明書フォーマットおよび証明書管理プロトコル)はカバーしていない

1.3. PKI の枠組み

本書は、図 1 に示した一般的な公開鍵基盤(PKI)の機能、システム、運用についてのセキュリティガイドラインを規定する

1.4. 用語

ガイドラインで使われている以下の用語は次の通りに解釈される

(1) 「しなければならない」：規定されたガイドラインは必須要件であり、したがってこれを遵守する必要がある

	根拠資料	備考
条項番号	条文	
	(2) 「すべきである」: 規定されたガイドラインは推奨要件である。遵守しない場合は、それを文書化し管理職から承認を受けなければならない。適切なら、補償制御を実施しなければならない (3) 「してよい」: 規定されたガイドラインはオプション要件である。このガイドラインを実施するかどうかは認証局の要件に応じて決定される	
	1.5. 用語の定義	
	(1) CA 秘密鍵：証明書、停止および失効情報に署名するのに使われる認証局の秘密鍵 (2) 認証局操作者：認証局の機能に対応したシステムを運転する技術要員 (3) 認証システム：認証局の登録、認証、およびリポジトリの機能を実行またはサポートするシステム (4) 証明書：公開鍵と指定された主体との間の対応を確認するデジタル文書。これには、主体の識別情報、公開鍵、鍵の用途範囲や目的、認証局の名前など、デジタル署名が施された特定の情報が含まれている (5) 証明書生成：ユーザの登録要求を承認し、その要求に対応した証明書を作成するプロセス (6) CP：証明書が特定の集団に適用可能かどうか、または共通のセキュリティ要件を持つアプリケーションのクラス(またはその両方)を示すルールの集合 (7) 証明書失効：証明書の失効には主に 2 つのカテゴリーがある (8) 許可失効：証明書は有効期限内であるが、加入者または加入者から権限を与えられている代表者からの要求があったため証明書を無効とすること	

	根拠資料	備考
条項番号	条文	
	(9) 必要失効：証明書は有効期限内であるが、以下の理由で無効にされること a) 証明書の情報が有効でなくなった b) 証明書に対応した秘密鍵、または秘密鍵を保有する媒体が危殆化となった、または危殆化が疑われる c) 加入者が、CP の対象となっている集団のメンバーではなくなった d) 証明書が証明書やその他の適用可能な実務文書にしたがって正しく発行されていなかったと発行者が判断した e) 認証局が営業を停止した。この場合、営業停止に先立ち、認証局から発行された全ての証明書が失効されなければならない (10) 認証：個人、企業、装置等のための証明書、停止および失効情報の生成/署名プロセス (11) 認証局：証明書の発行、公開、停止、失効を行う依存された主体。認証局の基本的役割は、加入者の存在を確認し証明することと、証明書管理サービスを提供することである。認証局は、登録および公開の機能を登録局またはリポジトリサービスプロバイダに委任することができる。特に指定がないかぎり、認証局への言及は登録局およびリポジトリサービスプロバイダにも当てはまる (12) CPS：証明書の発行および管理、一般的な業務責任やサービス利用の取扱いに認証局が用いている実務内容を記載したもの (13) 認証システム：認証または認証局署名機能を実行するために使われるシステム (14) 危殆化：秘密鍵および関連セキュリティ情報が盗難または漏洩にあった、またはその可能性がある場合、または第三者の解読により秘密が紛失した、またはその可能性がある場合 (15) 鍵ペア：特に暗号化および復号化のために生成された暗号鍵ペア	

根拠資料		備考
条項番号	条文	
	(16) 証明書期限切れ：発行者が規定した特定の有効期限が過ぎた時に証明書を無効にすること。期限切れになった証明書は再び有効にすることはできない (17) 証明書発行：認証局が確認し署名した内容の証明書を証明書申請者に発行するプロセス (18) 証明書発行者：証明書を認証局申請者に発行する主体。オープン PKI モデルでは、証明書発行者は多くの場合認証局であり、外部委託モデルでは、証明書発行者はバックエンド認証業務を他の主体に外部委託することができる (19) 鍵管理者：認証局業務の秘密鍵の管理を委託された人物。その人物は、認証局業務の遂行に直接関与してはならない (20) 鍵生成システム：暗号鍵を生成するのに使われるシステム (21) 鍵の実装：鍵は手動でまたは電子的に安全暗号装置を転送するプロセス (22) 物理的通知：物理的通知は、手渡しまたは書留郵便で配達した書面を含むことができる (23) ポリシー管理局：ポリシー管理局は、PKI に関連したポリシーに権限を持ち、CP の作成を担当する (24) 登録局操作者：登録機能に関連するシステムを操作する要員 (25) 登録局：証明書申請者の識別情報を確認するなど、登録機能を遂行する主体 (26) 登録システム：登録機能を遂行するのに使われるシステム (27) 規則：1998 年電子取引法および 1999 年電子取引(CA)規則条項 (28) 信頼者：証明書の受取人で、その証明書で確認されたデジタル署名やその証明書に依存して行動する人	

	根拠資料	備考
条項番号	条文	
	(29) リポジトリ：ユーザ側が証明書、証明書停止および失効情報に関連する情報を取り出すことができるようにするシステム (30) 署名鍵ペア：デジタル署名の作成および署名確認の目的に生成された暗号鍵ペア (31) 複数人管理：複数の人が共同で重要な機能または情報を保護するプロセス。保護された主体に単独の人でアクセスすることはできない (32) 加入者：認証局が証明書を発行した相手の主体(たとえば、個人、組織)。本書では、特に指定がないかぎり、加入者は単にユーザの意味である (33) 停止：有効期限内にある証明書を一時的に無効にすること。証明書情報が有効であり、その証明書に対応した秘密鍵が危殆化にあっていないことが判明した場合、停止の証明書を再び有効にすることができる (34) ユーザ側：認証サービスのユーザ。多くの場合、ユーザ側には証明書加入者および信頼者が含まれる (35) 有効性：次の場合、証明書は有効と見なされる a) 期限切れでない b) 停止になっていない c) 失効になっていない (36) 検証：加入者および信頼者が使う証明書の真正性を確認するプロセス (37) 仮想通知：非安全：ファクスや署名の入っていない電子メールのような、安全でない電子的配布方法	

根拠資料		備考
条項番号	条文	
	(38) 安全：デジタル署名が入ったメッセージのような、安全な電子的方法による通知。全ての当事者への通知には、これを主な手段とすべきである。認証局ポリシーは、当事者が登録済み電子メールアドレスを取得することを要求すべきである。このようなアドレスは、全ての関係者と通知を送受信する場として安全で信頼できると見なすことができる。登録済み電子メールアドレスが使われている場合、認証局は、登録済み電子メールアドレスに送信されたメッセージを受信済みと見なすことができる	
	2. 管理ガイドライン 認証局は、デジタル証明書に合法性を与える機関として、PKI の中で重要な役割を持っている。認証局を適切かつ安全に管理することが非常に重要である。管理ガイドラインの範囲には、要員、資材、財務、情報の管理ガイドラインが含まれる	
	2.1. 義務	
SG/CA-2.1.1	外部委託される認証局の業務またはサービスは、セキュリティガイドラインに準拠していなければならない。外部委託される認証局業務またはサービスは、ガイドラインに準拠しているかどうかを監査しなければならない	
SG/CA-2.1.2	認証局の業務および運用に関連した記録や取引ログは、常にもれがなく正確でなければならない。記録およびログは、適用法で定められた最低期間の間、保管されなければならない	
SG/CA-2.1.3	CPS またはその他の契約合意等で、コントロール不可能な出来事が発生した場合に認証局の義務を免除する「不可抗力」条項にユーザ側の注意を引きつけるようにしなければならない	

根拠資料		備考
条項番号	条文	
SG/CA-2.1.4	証明書の登録、発行、停止、および失効の手続きに関して、ユーザ側に情報を与えなければならない	
SG/CA-2.1.5	加入者の証明書が発行されたら、その中の情報が正確どうかを確かめる責任があることを、加入者に通知しなければならない	
SG/CA-2.1.6	認証局は、加入者の証明書をリポジトリで公開する前に、その加入者から明示的な同意を得なければならない	
SG/CA-2.1.7	加入者の秘密鍵を保護する方法に関して、適切な情報を加入者に提供しなければならない。異なる保護手段にどのような違いがあるかについても、加入者の注意を引きつけるようにしなければならない	
SG/CA-2.1.8	加入者の記録は最新のものを保存するようにし、加入者の証明書の情報に変更があれば迅速に更新しなければならない	
SG/CA-2.1.9	信頼者には、証明書の真正性および有効性を確認するための妥当な手順に関して、情報が与えられなければならない。この手順では、証明書の以下の情報についての確認が含まれていなければならない (1) ポリシーのパラメータ (2) 用途のパラメータ (3) 有効性のパラメータ (4) 失効または停止の情報	
SG/CA-2.1.10	証明書の失効および停止情報の更新時間間隔について、ユーザ側に情報を与えなければならない。そのような情報の公開は、指定された時間間隔に準拠していなければならない	
	2.2. 責務	
SG/CA-2.2.1	証明書に含まれる情報の信頼度に関して、認証局の責務の範囲と制限をユーザ側に情報を与えなければならない	

根拠資料		備考
条項番号	条文	

2.3. CP/CPS

SG/CA-2.3.1	認証局の CP と CPS およびその後の更新状況について、ユーザ側に情報を与えなければならない。CP および CPS の重要性と内容がユーザ側の注目を引くようにしなければならない
SG/CA-2.3.2	CP は、共通の保証レベルおよび使用条件を持つ証明書クラスごとに定義しなければならない
SG/CA-2.3.3	各 CP は、IDA から承認を受けた一意オブジェクト識別子(OID)によって参照されなければならない

2.4. セキュリティ管理

(BS7799-1：2000 のセクション 3 で定義されている追加ガイドラインを参照のこと。)

SG/CA-2.4.1	認証局組織の IT セキュリティポリシーは、上級管理職によって定義され承認されなければならない。このポリシーは、要員がポリシーを意識し思い出せるようにするため、全ての要員に伝達し、組織全体にわたって公開しなければならない
SG/CA-2.4.2	要員には、雇用時に、情報セキュリティポリシーを提供しなければならない。それを読み理解するのは各要員の責任でなければならない。セキュリティ通知、パンフレット、ポスター、記号を使って、セキュリティポリシーの存在や更新を知らせるようにしなければならない
SG/CA-2.4.3	認証局の運用およびシステムに潜在的なセキュリティリスクや情報流出の可能性があることを全ての要員に知らせるために、情報セキュリティ意識向上プログラムを実施しなければならない。特に、第一線のサービスに従事している要員には、典型的な技術的アタックおよびそれらに対する防御手段について情報を与えなければならない

根拠資料		備考
条項番号	条文	
SG/CA-2.4.4	基本 IT 原則および保護について、全ての要員を教育しなければならない。セキュリティ分野を担当する要員(たとえばシステム・運用セキュリティ管理者)は、高度な IT セキュリティ原則および保護の訓練を受けなければならない。セキュリティ要員は、システムおよび運用のセキュリティ機能や弱点について訓練を受けなければならない	
SG/CA-2.4.5	要員または請負人の地位、業務、配置に異動がある場合、それに従って IT システム、情報、資産へのアクセス権の見直し、変更、または取消を行えるように、そのための手続きを文書化し実施しなければならない	
SG/CA-2.4.6	登録ユーザー全員のアクセス権、アクセスのレベル、および継続的アクセス要求を定期的にチェックできるような手段またはメカニズムを確立し実施しなければならない(再認証)	
SG/CA-2.4.7	信頼できる情報源からセキュリティの弱点やアタックが報告された場合、それを積極的に追跡し、対抗手段を開発するか迅速に是正できるようなメカニズムを確立しなければならない。このメカニズムには、セキュリティ侵害やアタックに対して積極的に防御や是正処置が実施できるような事故対応機能を組み込むべきである	
SG/CA-2.4.8	必要に応じて法廷弁論などその後のアクションの根拠となるよう、出来事を文書化する事故対応メカニズムを確立しなければならない	
	2.5. リスク管理	
	(BS7799-1：2000 のセクション 4.2 および 4.3 で定義されている追加ガイドラインを参照のこと。)	

	根拠資料	備考
条項番号	条文	
SG/CA-2.5.1	認証局基盤のコンポーネント(たとえば、暗号アルゴリズムおよびその主要パラメータ、物理的なセキュリティ、システムセキュリティ、オペレーティングシステム等)は、新しいテクノロジーリスクについて毎年見直しを行い、そこで特定されたリスクに関して適切なコンポーネントのアクションプランを作成しなければならない	
SG/CA-2.5.2	認証局が業務を行う環境(物理的または業務的)に対してハードウェアの構成変更、ソフトウェア(オペレーティングシステムまたは階層化製品)の更新、ネットワークの変更(ハードウェア、ネットワークオペレーティングシステムソフトウェア、または構成)、アプリケーションの更新(新規アプリケーションまたは修正された既存アプリケーション)または変更が行われた場合、定期的に認証局システムの包括的な点検を実施しなければならない	
SG/CA-2.5.3	包括的なリスク管理アプローチの一環として、リスク管理のポリシーおよび手続きを定期的に見直さなければならない	
SG/CA-2.5.4	自動監査ツールを使ってネットワークおよびシステムセキュリティ監査を定期的に実施し、新しいセキュリティ弱点を特定できるようにしなければならない	
SG/CA-2.5.5	半年毎にネットワーク侵入試験を実施し、ネットワーク境界線防御に隙間ができていないかどうかを検査すべきである	
SG/CA-2.5.6	侵入検出システムを使って、ネットワークアタックに対してリアルタイムに防御できるようにしなければならない	
SG/CA-2.5.7	全ての事故(実際のまたはその疑いがある)に対して、あるいは知覚脅威レベル(技術的、物理的、または人事的)が変更された場合には、定期的にリスク分析および保護ポリシーを見直さなければならない	
SG/CA-2.5.8	正当な資格を持つ独立機関によって実施される定期的なセキュリティ監査およびネットワーク侵入試験の結果やそれをもとに作成されたアクションプランは、毎年 CCA に提出しなければならない	

	根拠資料	備考
条項番号	条文	

2.6. 要員の管理

(BS7799-1：2000 のセクション 6 で定義されている追加ガイドラインを参照のこと。)

SG/CA-2.6.1	全ての就職志願者は採用する前にセキュリティ審査をしなければならない。この審査により、望ましくないバックグラウンドを持つ志願者や、認証局業務の信用を傷つけるおそれのある活動に従事している志願者がいないことを確認しなければならない
SG/CA-2.6.2	全ての要員は、最初の雇用条件の 1 つとして、認証局のサービスおよびプロセス施設へのアクセスを許可する前に機密保持契約を結ばなければならない
SG/CA-2.6.3	機密保持または非開示契約は、雇用や契約条件に変更が生じた場合、特に要員の退職あるいは契約の終了時には見直さなければならない
SG/CA-2.6.4	全ての要員は、認可を受けた認証局で再認可を受ける際にセキュリティ再審査を受け、継続して信用できる人物であることを確認しなければならない
SG/CA-2.6.5	委託された役割またはセキュリティに関わる業務を遂行する要員は、厳密なセキュリティ審査(たとえば、性格プロフィール等)を受けなければならない
SG/CA-2.6.6	重要な認証局サービスやプロセスには、重複管理や義務分離を実施しなければならない。特に認証システムの監督者や運転員といった重要な認証局サービスやプロセスに携わる技術的要員には、セキュリティに関わる職務を与えてはならない
SG/CA-2.6.7	セキュリティ関連の役割は､利害の対立なしに職務を遂行するための適切な訓練を受けた専門要員に与えられなければならない

根拠資料		備考
条項番号	条文	
SG/CA-2.6.8	業務責任やアクセス権は毎年任命し、業務機能(すなわち証明書の登録、発行、停止、失効)へのアクセス権割り当てや義務分離が適切となるように見直さなければならない。さらに、相容れない義務や利益(内部的または外部的)に対して要員が行う信頼にもとづく役割やセキュリティ上注意を要する職務に関しては、定期的に照合確認を行わなければならない	
SG/CA-2.6.9	全ての要員は、任命された仕事や業務について適切な訓練を受けなければならない。適切な訓練を受けていない要員は、訓練を受けた要員の立ち会いまたは監視なしに認証局機能を個別に操作することを許してはならない	
	2.7. 加入者のデータの保守	
SG/CA-2.7.1	認証局の管理下にある加入者データのプライバシーや機密を守るための手続きおよびセキュリティ管理を実施しなければならない。加入者から提供された機密情報は、シンガポール共和国法または裁判所命令で情報を開示する必要がある場合を除き、その加入者の同意なしに第三者に開示してはならない	
SG/CA-2.7.2	加入者が証明書をどのような用途に使ったかのデータ、および認証局の運用中に生成された加入者の行動に関するその他の取引データは、加入者のプライバシーを守るために保護しなければならない	
SG/CA-2.7.3	情報資源を監視し、データのオーバーフローや破壊、および不正なアクセス、変更、削除のリスクを最小にしなければならない	
SG/CA-2.7.4	データベース管理ツールを使って、情報資源およびマスターファイルを管理し監視しなければならない	
	2.8. 危機管理	

根拠資料		備考
条項番号	条文	
SG/CA-2.8.1	事故管理プランは管理職によって作成され承認されなければならない。このプランには以下の分野が含まれていなければならない (1) 登録局鍵の危殆化 (2) 認証局秘密鍵の危殆化 (3) ユーザ証明書の危殆化 (4) システムやネットワークへの侵入 (5) 物理的セキュリティの違反 (6) 基盤の利用可能性 (7) 証明書、証明書失効および一時停止に関する偽の情報を登録および生成	
SG/CA-2.8.2	事故対応アクションプランを作成し、認証局がすぐに事故に対応できるようにしなければならない。このプランには以下の分野が含まれていなければならない (1) 危殆化の管理 (2) ユーザ側への通知(適用可能の場合) (3) 影響を受けた証明書の失効(適用可能の場合) (4) 要員事故の処理責任 (5) サービス中断の手続きおよび調査 (6) 監視および監査証跡の分析 (7) メディアおよび広報	
SG/CA-2.8.3	CA 秘密鍵またはその保存装置の紛失または危殆化があった場合、認証局の証明書はすぐに失効しなければならない。認証局の秘密鍵を使って署名された全ての証明書も失効しなければならない	
SG/CA-2.8.4	全ての事故は 24 時間以内に IDA に報告しなければならない	

2.9. 事業継続計画

根拠資料		備考
条項番号	条文	
	(BS7799-1：2000 のセクション 11 で定義されている追加ガイドラインを参照のこと。)	
SG/CA-2.9.1	業務継続プランニングを作成し、定期的に試験して、災害やコンピュータ故障があっても重要サービスを継続可能であることを確認しなければならない	
SG/CA-2.9.2	このプランニングには、CA 秘密鍵の紛失および危殆化が発生した場合の継続プランが含まれていなければならない	
SG/CA-2.9.3	復元チームの要員は、危機を取り扱うことができるように適切な訓練を受けなければならない	
SG/CA-2.9.4	認証局はバックアップ手続きを設定し、認証局の義務から免除されていない「不可抗力」によりサービスが停止しないようにしなければならない	
SG/CA-2.9.5	重要サービスの運用を継続できるように、情報なシステムや設備をタイムリーに利用できるようにしなければならない	
SG/CA-2.9.6	障害回復の「重要度の高い」箇所では、常に適切なセキュリティが確保されていなければならない	
SG/CA-2.9.7	事業継続計画の適合性および妥当性について半年毎に見直しを行い、万一の緊急時においても確実に事業を継続できるようにしなければならない。見直しの内容は文書化して、管理職のレビューを受けなければならない	

3. 認証業務ガイドライン

認証業務プロセスには、証明書、証明書停止、失効の情報の公開だけでなく、証明書の登録、生成、発行、更新、停止、失効が含まれる。ガイドラインの目的は、認証業務プロセスおよび証明書を完全で説明可能なものにすることである

根拠資料		備考
条項番号	条文	
	3.1.証明書の属性	
SG/CA-3.1.1	証明書はコミュニティの中で一意に識別可能でなければならない	
SG/CA-3.1.2	証明書は CP および用途パラメータを記載し、信頼者が証明書の用途を確認できるようにしなければならない	
SG/CA-3.1.3	証明書は期限切れパラメータを記載し、信頼者が証明書の有効性を確認できるようにしなければならない	
SG/CA-3.1.4	証明書はポリシーマップの制約と同様にポリシーマッピングに宣言しているパラメータを含めるべきである	
SG/CA-3.1.5	潜在的な社会的技術侵害からユーザのプライバシーを保護するため、認証ユーザに関する機密性の高い個人情報は、識別名フィールドなどの証明書属性には提供すべきでない	
SG/CA-3.1.6	証明書の拡張領域に重要というラベルを付けることができる。信頼者には、証明書の重要拡張領域を確認し処理するための、または証明書を拒絶するためのアプリケーションが提供されなければならない	

根拠資料		備考
条項番号	条文	
SG/CA-3.1.7	証明書の拡張領域は以下の用途に使われるべきである (1) 証明書発行のポリシーを特定する (2) 同等のポリシーを異なるコミュニティまたはドメインにマッピングする (3) 証明書パスにおいて後続の証明書が特定のポリシー識別子またはポリシーマッピングを含むように要求する (4) 証明書パスにおいて後続の証明書の所有者名スペースを制限する (5) 鍵の用途を規制する (6) 後続の証明書数を制限する (7) 認証局証明書とユーザ証明書を区別する	
	3.2. 登録	
SG/CA-3.2.1-1	a) 申請者の存在を確認するための認証方法は、証明書で与えられた保証レベルに見合うものでなければならない	
SG/CA-3.2.1-2	b) 可能なら、申請者の対面認証が用いられるべきである	
SG/CA-3.2.1-3	c) 登録局と申請者の間に以前から存在する信頼関係も利用することができる	
SG/CA-3.2.2	申請者の属性情報の真正性は、権限のある組織が発行する公文書に照らして確認しなければならない	
SG/CA-3.2.3	毎回の登録に関する適切な文書およびログを保管し、後から証明書申請を確認できるようにしなければならない	
	3.3. 生成	

根拠資料		備考
条項番号	条文	
SG/CA-3.3.1	生成された加入者の証明書が CP に準拠していることを確認するための手続きを定義しなければならない	
SG/CA-3.3.2	証明書の正確性(たとえば、証明書の情報が正しい)および完全性(たとえば、鍵ペアと証明書情報との間が正しく対応している)を確保しなければならない	
	3.4. 発行	
SG/CA-3.4.1	認証局とその加入者との間に安全な通信経路を確立し、証明書発行プロセスにおいて、やりとり(たとえば証明書、パスワード、秘密鍵の送信)の真正性、完全性、機密性を確保するようにしなければならない	
SG/CA-3.4.2	認証局は、発行後すぐに証明書の受領と受入を明示的に通知するよう加入者に要求しなければならない	
	3.5. 公開	
SG/CA-3.5.1	認証局は、定評があり信頼できる経路(たとえば、安全なオンラインメカニズムまたは定評のある新聞)を使って、自分の証明書および、自分の CPS およびリポジトリの場所をユーザ側へ公開しなければならない	
SG/CA-3.5.2	認証局は、少なくとも以下の情報を公開し、認証局を運用している組織が真正であることをユーザ側が確認できるようにしなければならない (1) 会社名および登録番号 (2) X.500 名 (3) インターネットアドレス (4) ホットライン電話番号 (5) 認証局証明書(または証明書の指紋) (6) リポジトリの場所	

根拠資料		備考
条項番号	条文	
SG/CA-3.5.3	リポジトリにある加入者の証明書情報は、加入者の明示的な同意を得た上で公開しなければならない	
SG/CA-3.5.4	リポジトリの内容は、不正な変更、挿入、および削除から保護されていなければならない。リポジトリの内容を修正する当事者の存在を確認するために、強力な認証メカニズムが使用されなければならない。必要なら、ユーザ側のアクセスを規制するか、または加入者のプライバシーを保護するために、リポジトリの内容への適切なアクセス制御を実施しなければならない	
SG/CA-3.5.5	証明書リポジトリの利用可能度が、保証レベルに見合うようにするために、適切なバックアップおよび冗長手段を実施しなければならない	
	3.6. 更新	
SG/CA-3.6.1	認証局は、証明書の有効期限に関して事前に加入者に通知を行い、加入者が更新または終了を申請できるだけの十分な時間を持てるようにしなければならない	
SG/CA-3.6.2	証明書の更新要求は、安全な通信経路を使って提出しなければならない。安全な通信経路には、証明書が有効であるかぎり、加入者がデジタル署名したオンライン更新要求も含めることができる	
SG/CA-3.6.3	本セクションの証明書生成および発行ガイドラインは、期限切れの証明書を交換するために新しい証明書を発行し生成する場合に適用しなければならない	
	3.7. 停止	
SG/CA-3.7.1	加入者の秘密鍵の危殆化が疑われる時は証明書を停止にしなければならない。停止の証明書は、危殆化がなかったことが調査で判明した場合しか再び有効にしないようにすべきである	

	根拠資料	備考
条項番号	条文	
SG/CA-3.7.2	証明書の停止要求は、要求者の存在を確認できるような安全な通信経路を使って提出され、不正なサービス中断や悪意のある一時停止要求による破壊行為のリスクを最小限にしなければならない	
SG/CA-3.7.3	証明書停止情報には、停止の事由と時刻が含まれ、どの時点で証明書が有効でなくなったのかを信頼者が判断できるようにしなければならない	
SG/CA-3.7.4	証明書の停止情報は認証局がデジタル署名を行い、信頼者がその情報の真正性および完全性を確認できるようにしなければならない	
SG/CA-3.7.5	証明書の停止情報は、停止要求が有効であることが確認されたら、公開しなければならない	
SG/CA-3.7.6	証明書の停止情報は、不正な変更や削除から保護されていなければならない	
SG/CA-3.7.7	証明書が停止になった加入者は、停止が実施された時点でそれが通知されなければならない	
	3.8. 失効	
SG/CA-3.8.1	永続的な失効は、加入者が何らかの理由で失効を要求した場合に発生する。認証局は、CP にしたがって発行された証明書の失効を要求できるのはポリシー作成団体か、または CP を遵守する必要のある団体のメンバーかを、CP に記載しなければならない。たとえば、登録局は証明書の失効を要求できるようにすることができる	

根拠資料		備考
条項番号	条文	
SG/CA-3.8.2	正当な理由にもとづいて証明書が信頼できないと当事者が判断した場合、失効が必要となる。証明書は、以下の状況では失効としなければならない (1) 証明書に関する重要情報が正確でなくなった時 (2) 証明書に対応する秘密鍵または秘密鍵を保持する媒体が危殆化となったか、または危殆化が疑われる時 (3) 加入者が、CP を遵守する必要のある団体のメンバーでなくなった時(たとえば、雇用の中止または死亡) (4) 加入者から要求があった時 (5) 証明書が CPS にしたがって正しく発行されなかったと認証局が判断した時 (6) 証明書発行者または認証局が営業を止めた時 (7) CA 秘密鍵が危殆化となった時	
SG/CA-3.8.3	証明書の失効要求は、要求者の存在を確認できるような安全な通信経路を使って提出され、不正なサービス中断による破壊行為のリスクを最小限にしなければならない	
SG/CA-3.8.4	証明書の失効情報は、少なくとも以下の内容を含んでいなければならない (1) 失効の理由コード (2) 失効の日付および時刻	
SG/CA-3.8.5	証明書の失効情報は認証局がデジタル署名を行い、信頼者がその情報の真正性および完全性を確認できるようにしなければならない	
SG/CA-3.8.6	証明書の失効情報は、失効要求が有効であることが確認されたら、公開しなければならない。この情報は以下の条項を含むべきである (1) オンライン証明書失効確認 (2) 証明書失効情報の配布ポイント	
SG/CA-3.8.7	証明書の失効情報は、不正な変更や削除から保護されていなければならない	

根拠資料		備考
条項番号	条文	
SG/CA-3.8.8	証明書が失効になった加入者は、失効が実施された時点でそれが通知されなければならない	
SG/CA-3.8.9	失効になった証明書は再び有効にしてはならない	
	3.9. 保管	
SG/CA-3.9.1	証明書の失効および停止の情報、証明書、およびその登録文書はすべて、当該規制要件にしたがって最小保持期間、保管しなければならない。規制要件がない場合、認証局の管理職が、期限切れ証明書に対応するデジタル署名を確認しやすいように適当な保持期間を決定しなければならない	
SG/CA-3.9.2	デジタルアーカイブは、正確で、完全で、判読可能で、権限のある人だけにアクセス可能となるようにインデックス付け、格納、維持が行われなければならない。デジタルアーカイブは完全な状態でいつでも利用可能でなければならない	
	3.10. 監査証跡	
SG/CA-3.10.1	証明書の登録、生成、発行、更新、停止および失効に関する監査証跡は保存しなければならない	
SG/CA-3.10.2	監査証跡は完全な状態でいつでも利用可能でなければならない	
SG/CA-3.10.3	運用監視の役割を与えられたレビューアーは定期的に証明書管理監査証跡を見直して正常運用を確認し、疑わしい行為を調査しなければならない	
SG/CA-3.10.4	監査証跡は、当該規制要件にしたがって最小保持期間、保管しなければならない。規制要件がない場合、認証局の管理職が、調査しやすいように適当な保持期間を決定しなければならない	

	根拠資料	備考
条項番号	条文	

4. 鍵管理ガイドライン

本セクションは、鍵管理の各フェーズにおいてリスクを管理し、暗号鍵の機密性および完全性を確保するためのガイドラインを記載する。暗号鍵の危殆化リスクを管理するための技術上および管理上のセキュリティ要件を網羅する。認証局(登録局の業務も含む)およびユーザが使う暗号鍵も、対象に含まれる。複数人管理の原則は認証局鍵の取扱いに適用される

4.1. 生成

SG/CA-4.1.1 加入者の鍵ペアは、加入者が生成するか、または鍵生成システム上で生成しなければならない。加入者が自分の鍵ペアを生成する場合、使われる鍵生成システムの承認は認証局が行わなければならない

SG/CA-4.1.2 認証局鍵は、認証システムおよび運用の設立や保守に関与していない当事者の複数人管理よって生成し保存しなければならない

SG/CA-4.1.3 デジタル署名および機密保持には別々の鍵ペアを生成すべきである

SG/CA-4.1.4 鍵生成プロセスは、強力な(一意の)鍵を生成するために、統計的にランダムな鍵値を生成しなければならない

4.2. 配布

SG/CA-4.2.1 鍵は、機密性と完全性を確保した安全なメカニズムを使って、鍵生成システムから記憶装置(鍵が鍵生成システム上に保存されない場合)に転送しなければならない

根拠資料		備考
条項番号	条文	

4.3. 保存

SG/CA-4.3.1	認証局は、加入者の秘密鍵を暗号化形式で安全に保存するための装置およびプログラムを加入者に提供すべきである
SG/CA-4.3.2	認証局鍵は不正操作できない装置内に保存し、認証局システムおよび運用の設立や保守に関与していない当事者の複数人管理でしか有効にすることはできないようにしなければならない。認証局鍵は、不正操作できない暗号モジュールに格納するか、または複数のサブ鍵に分割し管理者の管理下にある不正操作できない装置に格納することができる
SG/CA-4.3.3	認証局鍵管理者は、認証局鍵コンポーネントまたは起動コードが常に自分一人の管理下にあるようにしなければならない。鍵管理者を変更する場合、認証局管理職から承認を受け、文書化しなければならない。鍵管理者が不在の場合には、認証局はチェックシステムを整備して、シングルポイント障害がないようにすべきである

4.4. 活性化

SG/CA-4.4.1	認証局鍵の活性化の前に、システムおよびソフトウェアの完全性確認を実行しなければならない
SG/CA-4.4.2	認証局鍵の管理および認証局鍵へのアクセスは複数人管理下で行われなければならない。特に、認証局鍵の活性化は複数人管理下で実行しなければならない

4.5. バックアップ

	根拠資料	備考
条項番号	条文	
SG/CA-4.5.1	CA 秘密鍵は、鍵を誤って削除したり破壊した時に認証局業務が継続できるようにするため、バックアップを行わなければならない	
SG/CA-4.5.2	CA 秘密鍵のバックアップは、CA 秘密鍵の保存と同じガイドラインを使って保護しなければならない	
SG/CA-4.5.3	バックアップ鍵の各コンポーネントを保護するには、別々の CA 秘密鍵管理者を割り当てなければならない	
SG/CA-4.5.4	CA 秘密鍵のバックアップは、オリジナル鍵の格納場所から離れた、安全な保存設備に保存すべきである	
	4.6. 鍵更新	
SG/CA-4.6.1	認証局および加入者鍵は定期的に変更しなければならない	
SG/CA-4.6.2	鍵の変更は、鍵生成ガイドラインにしたがって処理しなければならない	
SG/CA-4.6.3	有効期間はガイドライン 4.10.5 にしたがって定義しなければならない	
SG/CA-4.6.4	認証局は、認証局証明書署名用の鍵が新しい鍵ペアに変更された場合、加入者の信頼者にも十分に通知しなければならない	
SG/CA-4.6.5	認証局は、鍵生成をどのように連結するか(たとえば、新しい鍵のハッシュを古い鍵で署名する)を示すことで、認証局鍵変更プロセスの信頼性を確保できるようにプロセスを定義しなければならない	
SG/CA-4.6.6	安全なアプリケーションプログラムによる場合でも、あるいは外部委託による場合でも、自動的に鍵の変更が行われた場合には、それがいかなる形態であろうと、認証局は加入者またはデジタル証明書の所有者に通知しなければならない	

根拠資料		備考
条項番号	条文	

4.7. 廃棄

SG/CA-4.7.1 認証局秘密鍵の利用が終わったら、秘密鍵の全てのコンポーネントおよび全てのバックアップコピーを安全な場所に安全な方法でアーカイブおよび保管しなければならない

4.8. 危殆化

SG/CA-4.8.1 CA 秘密鍵の危殆化が発生した場合、それを処理するための手順を事前に設定しなければならない。(セクション 2.8「事故管理」を参照のこと。)

SG/CA-4.8.2 CA 秘密鍵の危殆化が発生した場合、認証局は、関連する全ての加入者証明書をすぐに失効しなければならない

SG/CA-4.8.3 加入者秘密鍵の危殆化が発生した場合、認証局は関連する鍵および証明書をすぐに失効すべきである

4.9. 認証局公開鍵と加入者暗号鍵の保存

SG/CA-4.9.1 CA 公開鍵は、監査または調査の要件を簡単に満たせるように、永続的に保管しなければならない

SG/CA-4.9.2 全ての加入者暗号鍵は十分な期間アーカイブし、ユーザ自身のサービス拒否の原因となり得るあらゆる鍵の危殆化や紛失からユーザを保護すべきである

SG/CA-4.9.3 認証局公開鍵と加入者暗号鍵のアーカイブは、不正な変更から保護されていなければならない

4.10. 暗号技術

根拠資料		備考
条項番号	条文	
SG/CA-4.10.1	認証局業務用の暗号プロセスは、少なくとも FIPS 140-1 セキュリティレベル 3、または FIPS 140-2 セキュリティレベル 3 に準拠したハードウェア暗号モジュール内で実行しなければならない	
SG/CA-4.10.2	登録局の業務を認証局から切り離している場合、その暗号プロセスは少なくとも FIPS 140-1 セキュリティレベル 2、または FIPS 140-2 セキュリティレベル 2 に準拠していなければならない	
SG/CA-4.10.3	加入者が操作するための暗号プロセスは少なくとも FIPS 140-1 セキュリティレベル 1、または FIPS 140-2 セキュリティレベル 1 に準拠していなければならない	
SG/CA-4.10.4	全ての暗号アルゴリズム、プロトコル、およびその実施方法は、正当な資格を持つ独立機関によって見直し、暗号コンポーネントが十分に安全であり正しく実施されているように確保しなければならない。証明を必要とするコンポーネントは、鍵生成、鍵保存、鍵移送、および鍵利用に関わる全てのモジュールおよびコンポーネントである	
SG/CA-4.10.5	暗号鍵および使われているアルゴリズムは、鍵の寿命の間、暗号の結果(たとえばデジタル署名)をアタックから守るだけの強さを十分に持っていなければならない	
SG/CA-4.10.6	使われている非対称暗号アルゴリズムは、公開鍵暗号方式の IEEE 標準仕様(IEEE1363)に準拠すべきである	

5. システム及び運用ガイドライン

	根拠資料	備考
条項番号	条文	
	システムおよびネットワークの設計、構成、運用、保守は IT 対応のビジネスのセキュリティにとって重要である。特に認証局では、中核ビジネスがコンピュータシステムおよびネットワークを利用してデジタル証明書の委託サービスを提供している。ここで列挙したガイドラインは、認証局サービス特有のものであり、NCB IT セキュリティガイドライン(NCB9909)で扱っている一般的な IT セキュリティを補足することを目的としている。重要な認証システムおよび運用に関する利用可能性、機密性、完全性、アクセス制御が範囲に含まれる	
	5.1. 物理的セキュリティ	
	(BS7799-1：2000 のセクション 7 で定義されている追加ガイドラインを参照のこと。)	
SG/CA-5.1.1	認証システムの物理セキュリティに関する責任を定義し、指定した個人に割り当てなければならない	
SG/CA-5.1.2	認証システムの場所は、一般に特定可能であってはならない	
SG/CA-5.1.3	入退管理システムを設置し、認証システムへのアクセスを制御し監査しなければならない	
SG/CA-5.1.4	アクセスカード/鍵および資産一覧の複数人管理を実施しなければならない。カード/鍵を所有する要員の最新リストを維持しなければならない	
SG/CA-5.1.5	鍵管理者の管理下にある暗号鍵は、不正アクセス、利用、および偽造から物理的に保護されていなければならない	
SG/CA-5.1.6	アクセスカード/鍵の紛失があれば、すぐにセキュリティ管理者に報告しなければならない。管理者は不正アクセスを防止するための適切な処置をとるものとする	
SG/CA-5.1.7	認証システムは、強い磁気源や無線周波数干渉がある場所から離れた場所に置かなければならない	

根拠資料		備考
条項番号	条文	
SG/CA-5.1.8	認証機能を実行するシステムは、専用の部屋または仕切り内に置かれ、物理アクセス制御を強化できるようにしなければならない	
SG/CA-5.1.9	部屋および仕切りへの入退場はタイムスタンプ付きで自動的に記録され、認証局セキュリティ管理者が毎日確認しなければならない	
SG/CA-5.1.10	電源制御パネル、通信機器、配線など、認証システムの機能に不可欠な基盤コンポーネントは、権限を与えられた要員しかアクセスできないようにしなければならない	
SG/CA-5.1.11	通常の物理セキュリティ取り決めを一時的にバイパスまたは無効にする必要がある場合(たとえば、緊急事態)、適切な承認手続きおよび補償管理を適時実施できるようにしなければならない	
SG/CA-5.1.12	通常の物理セキュリティ取り決めのバイパスまたは無効化は、セキュリティ要員が許可し記録しなければならない	
SG/CA-5.1.13	プロフェッショナル規格に合わせてインストールされ、定期的にテストを受けている適切な侵入検出システムを利用して、勤務時間後の認証システムへの物理アクセスを監視し、記録しなければならない。人のいない場所は常に警戒するようにし、それ以外の場所は全て保護するようにすべきである	
	5.2. システムおよびソフトウェアの完全性および制御	
	(BS7799-1：2000 のセクションセクション 8.7、9 および 10 で定義されている追加ガイドラインを参照のこと)	
SG/CA-5.2.1	認証機能を実行するシステムはその機能専用であり、他の目的(たとえばウェブサーフィン、ワードプロセシング)に使ってはならない	
SG/CA-5.2.2	システムおよびアプリケーションソフトウェアは、実行前に、それぞれの完全性を確認しなければならない	

根拠資料		備考
条項番号	条文	
SG/CA-5.2.3	システムおよびアプリケーションソフトウェアは、少なくとも共通基準 EAL4、ITSEC E3、またはそれと同等のセキュリティレベルに適合していなければならない	
SG/CA-5.2.4	システムは、予測、辞書アタック、または再生を許さない強力な認証メカニズムを持っていなければならない	
SG/CA-5.2.5	秘密モジュールが埋め込まれたソフトウェアなどセキュリティ上重要なソフトウェアは、正当な資格を持つ独立機関が見直さなければならない	
SG/CA-5.2.6	要員は、認証アプリケーションを安全で正しく運用するための適切な教育を受けなければならない	
SG/CA-5.2.7	ターミナルの非作動時には自動的にタイムアウトとなるように設定すべきである。機密上重要なシステムの場合､タイムアウト時間は 10 分以内に設定すべきである	
	5.3. 変更および構成管理	
	(BS7799-1：2000 のセクション 10.5 で定義されている追加ガイドラインを参照のこと。)	
SG/CA-5.3.1	不審なソースの、あるいは信頼性が確認できないような実行可能プログラムは認証局システムに実装または実行してはならない	
SG/CA-5.3.2	ソフトウェア更新およびパッチは、実施する前にセキュリティの観点から見直さなければならない	
SG/CA-5.3.3	重要システムのセキュリティ弱点を修正するためのソフトウェア更新およびパッチは、迅速に見直して実施しなければならない	
SG/CA-5.3.4	ソフトウェア更新およびパッチやその実施方法に関する情報は、明確および適切に文書化しなければならない	

根拠資料		備考
条項番号	条文	

5.4. ネットワークおよび通信セキュリティ

(BS7799-1：2000 のセクション 8 で定義されている追加ガイドラインを参照のこと。)

SG/CA-5.4.1	認証システムは、他のシステムから重要システムおよびサービスへのネットワークアクセスを制御して保護しなければならない
SG/CA-5.4.2	認証システムから外部ネットワーク(必要な場合)へのネットワーク接続は、認証局機能プロセスおよびサービスを簡単にするのに不可欠な接続だけに限定しなければならない
SG/CA-5.4.3	ネットワーク接続(必要な場合)は、認証機能を実行するシステムが開始し、登録およびリポジトリ機能を実行するシステムへ接続すべきであり、その逆は許可すべきでない。これが不可能な場合、補償制御(たとえばプロキシの利用)を実施し、認証機能を実行するシステムをアタックから保護しなければならない
SG/CA-5.4.4	外部ネットワークへの接続を可能にする前に、認証システムのセキュリティの検査およびネットワークアクセス制御の評価について、正当な資格を持つ独立機関が見直さなければならない。リスクが見つかったら、それを軽減するよう制御しなければならない
SG/CA-5.4.5	CA 秘密鍵は不正アクセスから保護し、機密性および完全性を確保しなければならない
SG/CA-5.4.6	認証局秘密鍵は不正アクセスから保護し、機密性および完全性を確保しなければならない
SG/CA-5.4.7	5.4.6 ネットワーク上の認証システム間の通信は、機密性および完全性が確保されるくらい安全でなければならない。たとえば、ネットワーク上の認証システム間の通信は暗号化されデジタル署名を付けるべきである

根拠資料		備考
条項番号	条文	
SG/CA-5.4.8	5.4.7 重要なネットワークおよびネットワーク境界を監視し、ネットワークへの侵入や侵害の試みがあればタイムリーに管理者に通報するために、侵入検出ツールを導入しなければならない	
	5.5. 監視及び監査ログ	
SG/CA-5.5.1	認証局は、いつでもどこでもセキュリティ状況を統合的に表示できるような自動化されたセキュリティ管理・監視ツールを利用することを検討すべきである	
SG/CA-5.5.2	以下の業務取引の記録を維持しなければならない (1) 登録 (2) 認証 (3) 公開 (4) 停止 (5) 失効	
SG/CA-5.5.3	記録およびログファイルは、以下の行動について定期的に見直さなければならない (1) 乱用 (2) 誤り (3) セキュリティ違反 (4) 特権的な機能の実行 (5) アクセス制御リストの変更 (6) システム構成の変更 (7) ソフトウェアモジュールの変更	
SG/CA-5.5.4	監査証跡の見直しは、特に監督的立場にある要員が実行しなければならない	
SG/CA-5.5.5	監査ログは、不正アクセス、変更、削除から適切に保護し、そして適切なタイミングで定期的にバックアップを取って保管しなければならない	

根拠資料		備考
条項番号	条文	
SG/CA-5.5.6	システムのアクセス記録(たとえば、システムログ、セキュリティ関連ログ等)の監査証跡は、ハードコピーまたは電子形式のいずれかで、少なくとも 12 カ月以上保存しなければならない。犯罪行為に対する訴訟または捜査の参考物件として必要な記録の場合、恒久的に、または関連の法律の規定に従って保存しなければならない	
SG/CA-5.5.7	アプリケーショントランザクションおよび重大な出来事の記録は、当該規制要件に従って、少なくとも 12 カ月以上保存しなければならない	
	6. アプリケーション統合ガイドライン	
	本セクションは、認証局用アプリケーションツールキットを安全に実施し運用するためのガイドラインを規定している。認証局がユーザと開発者側に提供するツールキットが範囲に含まれる。証明書の検証は本セクションで扱うが、証明書管理は認証局機能ではなくユーザ側が使うアプリケーションの機能なので、ここでは扱わない。	
	6.1. 署名機能および検証機能の完全性	
SG/CA-6.1.1	秘密鍵が有効になったら、アプリケーションはユーザに通知しなければならない	
SG/CA-6.1.2	発行者が規定した受入可能な用途とは異なる目的に秘密鍵が使われようとしている場合、ユーザに警報を出すべきである	
SG/CA-6.1.3	不正な変更がなかったかどうかアプリケーションの完全性を確認するメカニズム、特に署名および確認機能の完全性を確認するメカニズムを利用可能にすべきである	

根拠資料		備考
条項番号	条文	
SG/CA-6.1.4	認証局のソフトウェアインフラストラクチャに関しては、アプリケーションセキュリティリスク評価を毎年実施して、証明書の管理、発行、および失効に利用する認証局ソフトウェアを、特定されたリスクが管理できるように改善していくべきである	
SG/CA-6.1.5	アプリケーションは正当な資格を持つ独立機関が見直し、安全な運用を確保すべきである	
	6.2. 秘密鍵の保護	
SG/CA-6.2.1	登録局秘密鍵は不正操作できない装置内に保存し、不正な使用や複製から保護しなければならない	
SG/CA-6.2.2	認証局秘密鍵は不正操作できない装置内に保存し、不正な使用や複製から保護しなければならない	
SG/CA-6.2.3	アプリケーションは、処理用に一時的に保存される秘密鍵を安全に消去し、秘密鍵の機密漏れを最小限に抑えるべきである	
	6.3. 証明書の検証	
SG/CA-6.3.1	アプリケーションは、証明書の有効期限と真正性を確認しなければならない	
SG/CA-6.3.2	検証プロセスでは、認証パスにおける全てのコンポーネントに対する追跡および検証を行わなければならない	
SG/CA-6.3.3	検証者に対しては、個々の保証レベルが示す意味、証明書に対応する秘密鍵の保存方法、コンポーネントの検証方法、および発行プロセスを通知すべきである	

	根拠資料	備考
条項番号	条文	
SG/CA-6.3.4	有効期限と真正性の確認のために、次のことを確認する必要がある (1) 証明書発行者の署名が有効である (2) 証明書が有効である(すなわち、期限切れでない、停止または失効でない) (3) 重要のフラグの付いた証明書拡張領域が適切である	

7. 参考文献

デジタル署名条例 S16(6)によるデジタル署名のドイツ技術カタログ v2.0a　1998 年 4 月

http;//www.iid.de/rahmen/iukdge.html

ECOM 認証局ガイドライン v1.0　1998 年 6 月

http;//www:ecom.or.jp/ecom_e/cag-smry.html

IEEE P1363 公開鍵暗号方式用標準仕様(ドラフト)

http://grouper.ieee.org/groups/1363/index.html

イタリアデジタル署名技術カタログ　1997 年 11 月

http://www.notariato.it/forum

ITU 勧告 X.509 証明書フォーマット

http://www.itu.ch/itudoc/itu-t/rec/x/x500up/x509_27505.html

ITU 勧告 X.509 証明書失効リストリスト バージョン 2

http://www.itu.ch/itudoc/itu-t/rec/x/x500up/x509_27505.html

NCB 情報技術セキュリティガイドライン(バージョン 1.0)、1999 年 9 月

IETF PKIX CP および CPS

http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-03.txt

NIST 連邦情報処理標準 (FIPS) Publication 140-2

http://csrc.nist.org/cryptval/140-2.htm

根拠資料		備考
条項番号	条文	
	BS 7799-1:2000 (情報技術 － 情報セキュリティ管理履行規則) http://www.bsi-global.com	