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　韓国編

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

[KR/L] 電子署名法 1
第 1 章 総則 1
1. 目的 1
2. 定義 1
3. 電子署名の効力等 3
第 2 章 公認認証局 3
4. 公認認証局 3
5. 欠格事由 4
6. 公認 CPS 等 4
7. 認証サービスの提供等 5
8. 公認認証局の業務遂行 5
9. 認証業務の譲受等 5
10. 認証業務の休止・廃止等 6
11. 是正命令 6
12. 認証業務の停止及び指定取消等 8
13. 過料の賦課 9
14. 検査等 9
第 3 章 公認証明書 9
15. 公認証明書の発行 9
16. 公認証明書の失効等 10
17. 公認証明書の停止等 11
18. 公認証明書の失効 11
18-2. 公認証明書を利用した本人確認 12
第 4 章 認証業務の安全性及び信頼性の確保 12
18-3. 公認認証局の安全性の確保 12
19. 認証業務に関する設備の運営 12
20. 電子文書の時点確認 13
21. 秘密鍵の管理 13
22. 認証業務に関する記録の管理 14
22-2. 公認証明書の管理等 14
23. 電子署名生成情報の保護等 15
24. 個人情報の保護 15
25. 電子署名認証管理業務 15
25-2. 信頼者の遵守事項 16
25-3. 公認認証局証明書のみの要求禁止 17
26. 賠償責任 17
26-2. 電子署名認証制度発展のための施策の樹立等 17
26-3. 電子署名の相互連動 18
26-4. 電子署名技術の開発及び人材の養成 19
26-5. 電子署名モデル事業の推進 19
26-6. 電子署名利用促進のための支援 20

第 6 章 補則 20
27. 加入者及び利用者の保護 20
27-2. 相互認定 20
28. 料金の賦課 21
29. 聴聞 21
30. 権限の委任 21
第 7 章 罰則 22
31. 罰則 22
32. 罰則 22
33. 両罰規定 22
34. 過料 23
付則 24
施行日 24
賠償責任に関する経過措置 24
罰則の適用に関する経過措置 24
他の法律の改正 25
[KR/E] 電子署名法施行令 1
1. 目的 1
2. 公認認証局の指定規準 1
3. 公認認証局指定の手続き 3
3-2. 指定の有効期間 4
3-3. 更新指定 4
3-4. 認証業務の停止及び指定取消の告示 5
4. 認証業務の独立性 5
5. 権限の委任 5
6. 過料 5
[KR/R] 電子署名法施行規則 1
1. 目的 1
2. 公認認証機関指定申請書 1
3. 公認認証機関指定書 1
4. 協議 2
4-2. 公認認証局指定等の告示 2
5. 公認 CPS の変更の届出の期間 3
6. 譲受及び合併の届出等 3
7. 認証業務の休止・廃止の届出 3
8. 加入者証明書等の引継不能事由の届出 4
9. 行政処分 4
10. 準用規定 4
11. 過料を賦課する違反行為等 5
12. 過料の賦課及び納付 5
13. 過料の督促及び徴収 6
13-2. 実在性確認の基準及び方法 6

13-3. 実在性証明書 8
13-4. 保護措置 9
13-5. 定期検査 9
13-6. 代行費用の支援 10
13-7. モデル事業 10
14. 過怠料の徴収手続き 11
付則 11
施行日 11
定期点検に関する経過措置 11
他の法令の改正 11

[KR/CP] 実在性確認及び本人確認に関する告示 1

1. 目的 1
2. 定義 1
3. 適用範囲 2
4. 実在性認証の原則 2
5. 代理人による実在性認証 2
6. オンライン実在性認証 3

[KR/CPS] CPS ガイドラインに関する告示 1

1. 総則 1
1.1 目的 1
1.2 定義 1
1.3 適用範囲 3
2. 認定証明書の管理 3
2.4 登録情報の転送 3
2.5 公認証明書の発行申請 4
2.6 公認証明書の生成 4
2.7 公認証明書の停止・停止解除等の申請 5
2.8 公認証明書の停止･失効リスト生成 5
2.9 公認証明書の公開および有効性検証サービス 6
3. 鍵ペアの管理 6
3.10 鍵ペアの生成 6
3.11 秘密鍵の保存 6
3.12 秘密鍵のバックアップ 7
3.13 秘密鍵の破棄 7
3.14 秘密鍵の紛失・き損または盗難・流出 8
3.15 タイムスタンプ検証機能の提供 8
3.16 時刻受信および時刻補正 8
3.17 タイムスタンプ検証記録の保管 8
3.18 電子文書の保管 8
3.10 タイムスタンプ検証の記録等のバックアップ 9
4. その他の運営管理 9
4.1 技術規格の遵守 9

4.2 公認証明書の利用範囲および用途の遵守 9
4.3 公認認証業務手順の遵守 10
4.4 設備に関する事項 10
4.5 公認認証業務記録の管理 11
4.6 監査記録の管理 12
4.7 監査記録の管理 13
4.8 登録局の管理 14
4.9 公認認証業務の試験運営 14
4.10 正確な情報の提供および公開 15
[KR/PR] 認証局が採用する安全対策に関する告示 1
1. 目的 1
2. 定義 1
<別表> 2
1. 認証業務に関する施設を電子的侵害行為から保護するための措置 2
1.1 ネットワーク保護 3
1.1.1 構成 3
1.1.2 管理 3
1.2 システム保護 4
1.2.1 構成 4
1.2.2 管理 4
2. 認証業務に関する施設に対する入退管理等、防護措置 5
2.1 入退管理 5
2.1.1 構成 5
2.1.2 管理 6
2.2 物理的侵入の検知/監視 7
2.2.1 構成 7
2.2.2 管理 7
3. 火災・水害等、各種の脅威から認証業務に関する施設の継続的/安定的運営を保障するための措置 8
3.1 災害防止 8
3.1.1 構成 8
3.1.2 管理 8
3.2 システム障害防止 9
3.2.1 構成 9
3.2.2 管理 9
4. その他認証業務に関する施設の安全性確保のための管理的措置 11
4.1 人的セキュリティ 11
4.1.1 構成 11
4.1.2 管理 11
4.2 危機管理 12
4.2.1 構成 12
4.3 記録の保管 13
4.3.1 管理 13

4.4 監査 13
4.4.1 管理 13
[KR/F] 公認認証局の施設設備基準に関する告示 1
第 1 章 総則 1
1.1 目的 1
1.2 定義 1
1.3 適用範囲 2
第 2 章 施設及び設備 2
2.1 加入者登録情報管理設備 2
2.2 電子署名キー生成･管理設備 4
2.3 公認証明書生成･発行･管理設備 7
2.4 タイムスタンプ検証設備 15
2.5 保護設備 17
2.6 加入者設備 25
第 3 章 内部規程 27
3.2 公認認証局鍵ペア管理に関する事項 28
3.3 公認証明書管理に関する事項 28
3.4 施設及び設備の管理等に関する事項 28
3.5 災害復旧に関する事項 29
付則 29
[別表] 30
1. 証明書プロファイル 30
2. 証明書の停止･失効リストプロファイル 30
3. 証明書申請形式 30
4. 証明書 DN 規格 30
5. 証明書 OID 規格 30
6. 相互連動技術規格 31
7. 公認証明書の表示のための技術規格 31
8. 証明書の有効性検証技術規格 31
9. 証明書検証技術規格 31
10. 電子署名アルゴリズム 31
11.ハッシュアルゴリズム 31
12. 暗号アルゴリズム 31
13. 証明書管理プロトコル 32
14. タイムスタンプ検証プロトコル 32
15. タイムスタンプ検証プロトコル 32
16. ディレクトリ関連プロトコル(LDAP) 32
17. 本人確認技術規格 32
18. 官民相互連携技術規格 32

韓国

[KR/L] 電子署名法

1999.2.5 公布 2001.12.31 改正

	根拠資料	備考
条項番号	条文	
	第 1 章 総則	
	1. 目的	
KR/L-1.1	この法律は、電子文書の安全性と信頼性を確保し、その利用を活性化するために、電子署名に関する基本的な事項を定めることにより、国家社会の情報化を促進し、国民生活の利便性を増進することを目的とする	
	2. 定義	
KR/L-2.1	この法律において使用する用語の定義は次のとおりである	

	根拠資料	備考
条項番号	条文	
	1) 「電子文書」とは、情報処理システムにより電磁的形態で作成され、送信または受信され、または保存された情報をいう 2) 「電子署名」とは、署名者を確認し、署名者が当該電子文書に署名したことを明示するのに利用するために当該電子文書に添付し、または論理的に結合した電磁的形態の情報をいう 3) 「公認電子署名」とは、次の各項の要件を満たし、公認証明書に基づいた電子署名をいう a) 秘密鍵が加入者にのみ属していること b) 署名当時、加入者が秘密鍵を支配・管理していること c) 電子署名が行われた後、当該電子署名に対する変更の有無を確認することができること d) 電子署名が行われた後、当該電子文書の変更の有無を確認することができること 4)「秘密鍵」とは、電子署名を生成するために利用する電磁的情報をいう 5)「公開鍵」とは、電子署名を検証するために利用する電磁的情報をいう。 6)「認証」とは、秘密鍵が加入者にのみ属しているという事実を確認し、これを証明する行為をいう 7)「証明書」とは、秘密鍵が加入者にのみ属しているという事実を確認し、これを証明する電磁的情報をいう 8)「公認証明書」とは、**KR/L-15** の規定により公認認証局が発行する証明書をいう。 9)「認証業務」とは、公認証明書の発行、認証関連記録の管理等、公認認証サービスを提供する業務をいう 10)「公認認証局」とは、公認認証サービスを提供するために **KR/L-4** により指定された者をいう 11)「加入者」とは、公認認証局より秘密鍵の認証を受けた者をいう 12)「署名者」とは、秘密鍵を保有し、本人が直接、または他人の代理として署名を行う者をいう	

根拠資料		備考
条項番号	条文	
	13)「個人情報」とは、生存する個人に関する情報で、氏名･住民登録番号等により当該の個人と確認することのできる符号・文字・音声・音響・映像及び身体特性等に関する情報 (当該情報のみでは特定の個人を確認することのできない場合にも､他の情報と容易に結合して確認することができるものを含む)をいう	
	3. 電子署名の効力等	
KR/L-3.1	他の法令において､文書または書面に署名､署名捺印または記名捺印を要する場合､電子文書に公認電子署名があるときにはこれを満たしたものとみなす	
KR/L-3.2	公認電子署名がある場合には､当該電子署名が署名者の署名､署名捺印または記名捺印であり､当該電子文書が電子署名された後はその内容は変更されていないものと推定する	
KR/L-3.3	公認電子署名以外の電子署名は､当事者間の約定に基づく署名､署名捺印または記名捺印としての効力を持つ	
	第 2 章 公認認証局	
	4. 公認認証局	
KR/L-4.1	情報通信省長官は、公認認証業務(以下「認証業務」という)を安全性かつ信頼性をもって遂行する能力があると認められる者を公認認証局に指定することができる	
KR/L-4.2	公認認証局の指定を受けることのできる者は､国家機関･地方公共団体または法人に限る	
KR/L-4.3	公認認証局の指定を受けようとする者は、大統領令(**KR/E**)の定める技術能力･財政能力･施設及び設備その他必要事項を備えていなければならない	

根拠資料		備考
条項番号	条文	
KR/L-4.4	公認認証局の指定手続きその他必要事項は、大統領令(**KR/E**)で定める	
	5. 欠格事由	
KR/L-5.1	次の各号のいずれかに該当する者は、公認認証局の指定を受けることができない	
KR/L-5.1.1	役員に次の各項のいずれかに該当する者がいる法人 a) 禁治産者・限定治産者または破産者で復権していない者 b) 禁固以上の実刑の宣告を受け、その執行が終了し(執行が終了したものとみなす場合を含む)、または執行が免除された日から 2 年が経過していない者 c) 禁固以上の刑の執行猶予宣告を受け、その執行猶予期間中にある者 d) 裁判所の判決または他の法律により資格を喪失し、または資格を停止された者 e) **KR/L-12** の規定により指定を取り消された法人の取消当時、役員だった者(取消の日から 2 年が経過していない者に限る)	
KR/L-5.1.2	**KR/L-12** の規定により指定が取り消されてから 2 年が経過していない法人	
	6. 公認 CPS 等	
KR/L-6.1	公認認証局は、認証業務を開始する前に次の各号の事項が含まれる公認 CPS(以下「CPS」という)を作成し、情報通信省長官に届け出なければならない 1) 認証業務の種類 2) 認証業務の遂行方法及び手続き 3) 公認認証サービス(以下 「認証サービス」という)の利用条件及び利用料金 4) その他認証業務の遂行に関して必要な事項	

根拠資料		備考
条項番号	条文	
KR/L-6.2	公認認証局は、**KR/L-6.1** の規定により届け出た事項を変更する場合、情報通信省令の定める期間内に、これを情報通信省長官に届け出なければならない	
KR/L-6.3	情報通信省長官は、**KR/L-6.1** の規定により届け出た CPS の内容が認証業務の安全性と信頼性の確保に支障をきたし、または加入者の利益を害する恐れがあると判断する場合には、相当の期間を定め、当該公認認証局に CPS の変更を命ずることができる	
KR/L-6.4	公認認証局は、CPS の定める事項を誠実に遵守しなければならない	
	7. 認証サービスの提供等	
KR/L-7.1	公認認証局は、正当な事由なしに認証サービスの提供を拒否してはならない	
KR/L-7.2	公認認証局は、加入者または認証サービスの信頼者を不当に差別してはならない	
	8. 公認認証局の業務遂行	
KR/L-8.1	情報通信省長官は、認証業務の安全性と信頼性の確保のために、公認認証局が認証業務の遂行において守るべき具体的な事項を、CPS ガイドライン(**KR/CPS**)として定め告示することができる	
	9. 認証業務の譲受等	
KR/L-9.1	公認認証局は、他の公認認証局の認証業務を譲受け、または他の公認認証局である法人を合併しようとする場合には、情報通信省令の定めるところにより情報通信省長官に届け出なければならない	

根拠資料		備考
条項番号	条文	
KR/L-9.2	**KR/L-9.1** の規定により認証業務を譲り受けた公認認証局、または合併した場合の合併後存続する法人または合併により設立された法人は、従前の公認認証局の地位を承継する	
	10. 認証業務の休止・廃止等	
KR/L-10.1	公認認証局が認証業務の全部または一部を休止しようとするときには、休止期間を定め、休止する日の 30 日前までにこれを加入者に通知し、情報通信省長官に届け出なければならない。この場合休止期間は 6 ヶ月を超過することはできない	
KR/L-10.2	公認認証局が認証業務を廃止しようとするときには、廃止する日の 60 日前までにこれを加入者に通知し、情報通信省長官に届け出なければならない	
KR/L-10.3	**KR/L-10.2** により届け出た公認認証局は、加入者の公認証明書とその効力の停止及び廃止に関する記録(以下 「加入者認証書等」という)を他の公認認証局に引継がなければならない 但し、やむをえない事由により加入者証明書等を引継ぐことができない場合には、その事実を情報通信省長官にすみやかに届け出なければならない	
KR/L-10.4	情報通信省長官は、**KR/L-10.3** 但し書きの規定により届出を受けたときは、情報通信網利用促進及び情報保護等に関する法律第 52 条の規定による **KISA** に対し、当該公認認証局の加入者証明書等を引き受けるよう命ずることができる	
KR/L-10.5	**KR/L-10.1** から **KR/L-10.4** による認証業務の休止または廃止の届出及び加入者証明書等の引継・引受等に関し、必要な事項は情報通信省令で定める	
	11. 是正命令	

根拠資料		備考
条項番号	条文	
KR/L-11.1	情報通信省長官は、公認認証局が次の各号のいずれかに該当する場合には、期間を定めて、是正措置を命ずることができる 1) 公認認証局の業務遂行方法が不適当で、公認電子署名の安全性と信頼性の確保に支障をきたす恐れがある場合 2) 公認認証局の指定を受けた後、**KR/L-4.3** の規定により公認認証局が備えるべき事項を備えていない場合 3) 役員が **KR/L-5.1** の各項に該当することになった場合 4) **KR/L-6** による届出または変更の届出を行わず、または届出た CPS を遵守しなかった場合 5) **KR/L-7** に違反して認証業務の提供を拒否し、または加入者または認証サービスの信頼者を不当に差別した場合 5-2) **KR/L-8** に違反して CPS ガイドライン(**KR/CPS**)の定める事項を遵守しなかった場合 6) **KR/L-9.1** に違反して認証業務の譲受または公認認証局合併の届出を行わなかった場合 7) **KR/L-10** に違反して認証業務休止または廃止の通知または届出を行わず、または認証業務廃止時に加入者証明書等を引継がなかった場合 8) **KR/L-12.2** に違反して指定を取り消された公認認証局が加入者証明書等を引継がず、または届出を行わなかった場合 9) **KR/L-14.1** による資料を提出しなかった場合 10) **KR/L-17** に違反して公認証明書の停止または回復せず、またはその事実を確認することのできる措置を取らなかった場合 11) **KR/L-18** に違反して公認証明書を失効せず、またはその事実を確認することのできる措置を取らなかった場合 または	

根拠資料		備考
条項番号	条文	
	11-2) **KR/L-18-3** に違反して認証業務に関連した安全対策の具体的事項(**KR/PR**)を取らなかった場合	
	12. 認証業務の停止及び指定取消等	
KR/L-12.1	情報通信省長官は、公認認証局が次の各号のいずれかに該当する場合には、6ヶ月以内の期間を定め、認証業務の全部または一部の停止を命じ、または指定を取り消すことができる。但し、**KR/L-12.1.1** 及び **KR/L-12.1.2** の場合には、指定を取り消さなければならない	
	1) 詐欺その他の不正な方法により **KR/L-4** による指定を受けた場合	
	2) 認証業務の停止命令を受けた者が、その命令に違反して認証業務を停止しなかった場合	
	3) **KR/L-4** による指定を受けた日から6ヶ月以内に認証業務を開始せず、または 6 ヶ月以上継続して認証業務を休止した場合	
	4) **KR/L-6.3** による CPS 変更命令に違反した場合 または 5) **KR/L-11** による是正命令を正当な事由なしに履行しなかった場合	
KR/L-12.2	**KR/L-12.1** により指定を取り消された公認認証局は、加入者証明書等を他の公認認証局に引継がなければならない	
	但し、やむをえない事由により加入者証明書等を引継ぐことができないときは、その事実を情報通信省長官にすみやかに届け出なければならない	
KR/L-12.3	**KR/L-10.4** は、指定を取り消された公認認証局についてこれを準用する	
KR/L-12.4	**KR/L-12.1** による処分の基準及び手続きと、**KR/L-12.2** 及び **KR/L-12.3** による引継・引受等に関して必要な事項は、情報通信省令で定める	

根拠資料		備考
条項番号	条文	

13. 過料の賦課

KR/L-13.1 情報通信省長官は、**KR/L-12.1** 各号のいずれかに該当する場合で、その業務怠慢が加入者等にいちじるしい不利益を与え、またはその他公益を害する恐れがあるときには、その業務停止処分に代えて 2000 万 W(200 万円)以下の過料を賦課することができる

KR/L-13.2 **KR/L-13.1** による過料を賦課する違反行為の種別とその程度による過料の金額その他必要な事項は、情報通信省令で定める

KR/L-13.3 情報通信省長官は、**KR/L-13.1** による過料を納付すべき者が納付期限までにこれを納付しないときは、国税滞納処分の例によりこれを徴収する

14. 検査等

KR/L-14.1 情報通信省長官は、認証業務の安全性と信頼性の確保及び加入者の保護等のために必要な場合には、公認認証局に対し資料を提出させることができ、関係公務員を公認認証局の事務所・事業所その他必要な場所に立ち入らせ、認証業務に関する施設及び設備・帳簿・書類その他物件を検査させることができる

KR/L-14.2 **KR/L-14.1** により立入・検査を行う公務員は、その権限を明示した証票を関係人に提示しなければならない

第 3 章 公認証明書

15. 公認証明書の発行

	根拠資料	備考
条項番号	条文	
KR/L-15.1	公認認証局は、公認証明書の発行を受けようとする者に公認証明書を発行する。この場合公認認証局は、公認証明書の発行を受けようとする者の実在性を認証しなければならない	
KR/L-15.2	公認認証局が発行する公認証明書には、次の各号の事項が含まれていなければならない 1) 加入者の氏名(法人の場合には名称をいう) 2) 加入者の公開鍵 3) 加入者と公認認証局が利用する電子署名方式 4) 公認証明書のシリアル番号 5) 公認証明書の有効期間 6) 公認認証局の名称等公認認証局であることを確認することのできる情報 7) 公認証明書の利用範囲または用途を制限する場合、これに関する事項 8) 加入者が第三者のための代理権等を持つ場合、または職業上の資格等の表示を要請した場合、これに関する事項 及び 9) 公認証明書であることを明示する表示	
KR/L-15.4	公認認証局は、公認証明書の発行を受けようとする者の申請がある場合には、公認証明書の利用範囲または用途を制限する公認証明書を発行することができる	
KR/L-15.5	公認認証局は、公認証明書の利用範囲及び用途、利用される技術の安全性と信頼性等を考慮し、公認証明書の有効期間を適正に定めなければならない	
KR/L-15.6	公認証明書の発行にともなう実在性確認の手続き及び方法等に関して必要な事項は情報通信省(**KR/CP**)で定める	

16. 公認証明書の失効等

根拠資料		備考
条項番号	条文	
KR/L-16.1	公認認証局が発行した公認証明書は、次の各号のいずれかに該当する事由が発生した場合には、その事由が発生した時点で失効する 1) 公認証明書の有効期間が経過した場合 2) **KR/L-12.1** により公認認証局の指定が取り消された場合 3) **KR/L-17** により公認証明書が停止した場合 4) **KR/L-18** により公認証明書が失効となった場合	
KR/L-16.2	情報通信省長官は、認証業務の安全性と信頼性の確保のために必要な場合には、**KR/L-10** により認証業務を休止または廃止し、または **KR/L-12** により認証業務を停止された公認認証局が発行した公認証明書を停止することができる	
KR/L-16.3	情報通信省長官は、**KR/L-16.2** により公認証明書を停止したときには、その事実をつねに確認することができるようすみやかに **KISA** に必要な措置を取らせなければならない。**KR/L-16.1.2** により公認証明書が失効した場合にもまた同様である	
	17. 公認証明書の停止等	
KR/L-17.1a	公認認証局は、加入者またはその代理人の申請がある場合には、公認証明書を停止し、または停止した公認証明書の効力を回復させなければならない	
KR/L-17.1b	…この場合公認証明書の効力回復の申請は、公認証明書が停止した日から 6 ヶ月以内に行わなければならない	
KR/L-17.2	公認認証局が **KR/L-17.1** により公認証明書を停止し、または回復した場合には、その事実をつねに確認することができるようすみやかに必要な措置を取らなければならない	
	18. 公認証明書の失効	

根拠資料		備考
条項番号	条文	
KR/L-18.1	公認認証局は、公認証明書に関して次の各号のいずれかに該当する事由が発生した場合には、当該公認証明書を失効しなければならない 1) 加入者またはその代理人が公認証明書の失効を申請した場合 2) 加入者が詐欺その他不正な方法で公認証明書の発行を受けた事実を認めた場合 3) 加入者の死亡・失踪宣告または解散の事実を認めた場合 4) 加入者の秘密鍵が紛失・き損または盗難・流出した事実を認めた場合	
KR/L-18.2	公認認証局は、**KR/L-18.1** により公認証明書を失効した場合には、その事実をつねに確認することができるようすみやかに必要な措置を取らなければならない	
	18-2. 公認証明書を利用した本人確認	
KR/L-18-2.1	他の法律において公認証明書を利用して本人であることを確認することを制限または排除していない場合には、この法律の規定によって公認認証局が発行した公認証明書により本人であることを確認することができる	
	第 4 章 認証業務の安全性及び信頼性の確保	
	18-3. 公認認証局の安全性の確保	
KR/L-18-3.1	公認認証局は、認証業務に関する施設の安全性確保のために情報通信省令の定める保護措置を取らなければならない	
	19. 認証業務に関する設備の運営	

根拠資料		備考
条項番号	条文	
KR/L-19.1	公認認証局は、自身が発行した公認証明書が有効であるかどうかを誰もがつねに確認することができるようにする設備等、認証業務に関する施設及び設備を安全に運営しなければならない**(KR/F)**	
KR/L-19.2	公認認証局は、**KR/L-19.1** の施設及び設備の安全な運営が行われているかどうか、**KISA** による定期的な検査を受けなければならない	
KR/L-19.3	公認認証局は、指定後 **KR/L-19.1** の規定による施設及び設備を変更する場合、すみやかに情報通信省長官にこれを届け出なければならない。この場合情報通信省長官は、**KISA** に当該施設及び設備の安全性如何を検査させることができる	
	20. 電子文書の時点確認	
KR/L-20.1	公認認証局は、加入者または公認証明書を利用する者(以下「信頼者」という)の申請がある場合には、電子文書が当該公認認証局に提示された時点を電子署名をもって確認することができる	
	21. 秘密鍵の管理	
KR/L-21.1	加入者は、自身の秘密鍵を安全に保管・管理し、これを紛失・き損または盗難・流出し、またはき損の危険を認めたときには、その事実を公認認証局に通知しなければならない。この場合加入者は、すみやかに信頼者に公認認証局に通知した内容を告知しなければならない	
KR/L-21.2	公認認証局は、**KR/L-21.1** による事実を通知または告知することのできる手段を提供しなければならない	
KR/L-21.3	公認認証局は、加入者の申請がある場合以外には、加入者の秘密鍵を保管してはならず、加入者の申請によりその秘密鍵を保管する場合、当該加入者の同意なくこれを利用し、または流出してはならない	

根拠資料		備考
条項番号	条文	
KR/L-21.4	公認認証局は、自身が利用する秘密鍵を安全に保管・管理しなければならない。この場合当該秘密鍵が紛失・き損または盗難・流出し、またはき損の危険を認めたときには、すみやかにその事実を **KISA** に通知し、認証業務の安全性と信頼性を確保することのできる対策を講じなければならない	
	22. 認証業務に関する記録の管理	
KR/L-22.1	公認認証局は、加入者の公認証明書と認証業務に関する記録を安全に保管・管理しなければならない	
KR/L-22.2	公認認証局は、加入者証明書等を当該公認証明書が失効した日から 10 年間保管しなければならない	
	22-2. 公認証明書の管理等	
KR/L-22-2.1	公認認証局及び加入者は、公認証明書の有効期間内に当該公認証明書の記載事項または公認証明書と結合した情報が正確かつ完全に維持されるよう相当の注意を傾けなければならない	
KR/L-22-2.2	公認認証局は、信頼者が公認証明書により次の各号の事項を確認することができるよう容易な手段を提供しなければならない 1) 公認認証局の名称等公認認証局であることを確認することのできる情報 2) 加入者が当該公認証明書が発行された当時、秘密鍵を支配・管理していた事実 3) 公認証明書の発行前に秘密鍵が有効だった事実	

根拠資料		備考
条項番号	条文	
KR/L-22-2.3	公認認証局は、信頼者が次の各号の事実を確認することができるよう容易な手段を提供しなければならない 1) 署名者の実在性を確認することのできる方法 2) 秘密鍵または公認証明書の使用目的または使用金額に対する制限 3) 公認認証局が負担する責任の範囲または程度	
	23. 電子署名生成情報の保護等	
KR/L-23.1	何人も他人の秘密鍵を盗用または漏洩してはならない	
KR/L-23.2	何人も他人の名義で公認証明書の発行を受け、または発給を受けることができるようにしてはならない	
KR/L-23.3	何人も公認証明書ではない認証書等を公認証明書と混同させ、または混同する恐れのある類似の表示を使用し、または偽って公認証明書の使用を表示してはならない	
	24. 個人情報の保護	
KR/L-24.1	公認認証局は、認証業務の遂行に関連する個人情報を保護しなければならない	
KR/L-24.2	**KR/L-24.1** の個人情報保護に関しては、情報通信網利用促進及び情報保護等に関する法律第 22 条から第 32 条、第 36 条第 1 項、第 54 条、第 55 条、第 62 条、第 66 条及び第 67 条の個人情報に関する規定を準用する。この場合、「情報通信サービス提供者」は「公認認証局」と、「利用者」は「加入者」とみなす	
	25. 電子署名認証管理業務	

根拠資料		備考
条項番号	条文	
KR/L-25.1	**KISA** は、電子署名の安全で信頼のおける利用が可能となるように環境を整え、公認認証局を効率的に管理するために次の各号の業務を遂行する 1) **KR/L-4** により公認認証局を指定する場合、公認認証局の指定を受けようとする者が備えるべき施設及び設備に対する審査の支援 2) **KR/L-14.1** による公認認証局に対する検査の支援 3) **KR/L-18-3** による安全対策に対する審査及び技術の支援 4) **KR/L-19.2** による施設及び設備が安全に運営されているかどうかに関する検査 5) 公認認証局に対する公認証明書の発行･管理等の認証業務 6) 電子署名認証に関連する技術開発･普及及び標準化の研究 7) 電子署名認証に関連する制度の研究及び相互認証等国際協力の支援 8) その他電子署名認証管理業務に関連して必要な事項	
KR/L-25.2	**KR/L-3**、**KR/L-6**、**KR/L-7**、**KR/L-15**から**KR/L-18**、**KR/L-18-2**、**KR/L-18-3**、**KR/L-19.1**及び**KR/L-22**の規定は、**KISA**の電子署名認証管理業務に関してこれを準用する。この場合、「公認認証局」は「**KISA**」と、「加入者」は「公認認証局」とみなす	
KR/L-25.3	**KISA**は、**KR/L-25.1**の規定による審査･技術支援･検査及び公認証明書の発行等電子署名認証管理業務に関連して手数料等を賦課することができる	

25-2. 信頼者の遵守事項

根拠資料		備考
条項番号	条文	
KR/L-25-2.1	信頼者は、**KR/L-15.2.1** から **KR/L-15.2.6** の公認証明書の記載事項等により公認電子署名の真偽を確認するために、次の各項の措置を取らなければならない a) 公認証明書が有効かどうかの確認 b) 公認証明書が停止または失効されていないかどうかの確認 c) **KR/L-15.2.7** 及び **KR/L-15.2.8** の事項の確認	
	25-3. 公認認証局証明書のみの要求禁止	
KR/L-25-3.1	何人も公認証明書を利用して電子署名を確認する場合、正当な理由なく(KISA から LCA に発行される)公認認証局証明書のみを要求してはならない	
	26. 賠償責任	
KR/L-26.1	公認認証局は、認証業務の遂行に関連して加入者または公認証明書を信頼者に損害を与えたときには、その損害を賠償しなければならない。但し、その損害が不可抗力により発生した場合にはその賠償責任が軽減され、公認認証局が過失のないことを立証した場合にはその賠償責任が免除される	
	26-2. 電子署名認証制度発展のための施策の樹立等	

根拠資料		備考
条項番号	条文	
KR/L-26-2.1	政府は、電子署名の安全性と信頼性を確保し、その利用を活性化する等の電子署名及び認証業務の発展のために、次の各号の施策を樹立･施行する 1) 電子署名の安全性と信頼性の確保及び利用の活性化のための基本政策に関する事項 2) 電子署名の円滑な相互連動のための政策及び技術の標準化に関する事項 3) 電子署名に関連する技術開発 4) 電子署名利用の活性化のための教育及び広報に関する事項 5) 電子署名利用の拡大のための制度の改善及び関係法令の整備に関する事項 6) 電子署名関連団体の支援及び関連情報の提供に関する事項 7) 認証業務に関連する加入者と利用者の権益保護に関する事項 8) 外国の電子署名及び認証書に対する相互認定及び国際協力に関する事項 9) 電子署名関連産業の育成及び人材の養成に関する事項 10) 認可認証機関の安全性の確保のための保護措置に関する事項 11) 電子署名利用の活性化のためのモデル事業の推進及び統計･実態調査に関する事項 12) 電子文書の安全性と信頼性の確保のための暗号の使用に関する事項 13) その他電子署名の安全性と信頼性の確保及び利用促進のために必要な事項	

26-3. 電子署名の相互連動

根拠資料		備考
条項番号	条文	
KR/L-26-3.1	情報通信省長官は、電子署名の円滑な相互連動のために、次の各号の事項を推進する 1) 電子署名の相互連動のための国内外標準の調査研究及び開発 2) 電子署名の相互連動に関連する標準の制定及び普及 3) 電子署名の相互連動のための電子署名及び認証政策の調整 4) その他電子署名の相互連動に関連する事項	
KR/L-26-3.2	情報通信省長官は、第 1 項各号の事項を推進するために必要な場合、関連機関及び団体にこれを代行させることができる。この場合情報通信省令の定めるところによりこれに要する費用を支援することができる	
	26-4. 電子署名技術の開発及び人材の養成	
KR/L-26-4.1	情報通信省長官は、電子署名利用の促進に必要な技術の開発及び専門的人材の養成のために、次の各号の事項を推進する 1) 電子署名関連の技術水準の調査、技術の研究･開発及び活用に関する事項 2) 電子署名関連の技術協力及び技術移転に関する事項 3) 電子署名に関する技術情報の提供及び関連機関･団体との協力に関する事項 4) 電子署名関連の専門的人材の需給実態調査及び専門的人材の養成のための支援事項 5) その他電子署名に関する技術開発及び人材養成に必要な事項	
	26-5. 電子署名モデル事業の推進	

根拠資料		備考
条項番号	条文	
KR/L-26-5.1	情報通信省長官は、電子署名の利用拡大のために情報通信省令の定めるところによりモデル事業を実施することができる	
KR/L-26-5.2	政府は、第 1 項の規定によるモデル事業に対して行政的･財政的･技術的支援を行うことができる	
	26-6. 電子署名利用促進のための支援	
KR/L-26-6.1	国又は地方公共団体は、電子署名の利用促進のために金融支援を行うことができる	
KR/L-26-6.2	政府は、電子取引の安全性と信頼性の確保のために認可電子署名を使用する場合、電子取引に伴う手数料等を減免する施策を樹立･施行することができる	
KR/L-26-6.3	政府は、電子署名に関連する法人又は団体が電子署名の利用促進のための事業を実施する場合、予算の範囲内で当該事業費の全部又は一部を支援することができる	
	第 6 章 補則	
	27. 加入者及び利用者の保護	
KR/L-27-1	政府は、加入者及び利用者の不満及び被害を迅速かつ公正に処理することができるよう、必要な措置を講じなければならない	
KR/L-27-2	第 1 項の措置に関する具体的な事項は、情報通信省令で定める	
	27-2. 相互認定	

根拠資料		備考
条項番号	条文	
KR/L-27-2.1	政府は、電子署名の相互認定のために外国政府と協定を締結することができる	
KR/L-27-2.2	第 1 項の規定により協定を締結する場合には、外国の認証機関又は外国の認証機関が発給した認証書に対し、この法律による認可認証機関又は認可認証書と同一の法的地位若しくは法的効力を付与することをその協定の内容とすることができる	
KR/L-27-2.3	情報通信省長官は、第 1 項の規定により外国政府と電子署名の相互認定に関する協定を締結した場合には、その内容を告示しなければならない	
KR/L-27-2.4	第 1 項の規定により外国政府との協定が締結された場合、外国の電子署名又は認証書は、認可電子署名又は認可認証書と同等の効力を持つものとみなす	
	28. 料金の賦課	
KR/L-28-1	認可認証機関は、認可認証書の発給を申請する者又は認証役務の提供を受ける者に、手数料等必要な料金を賦課することができる	
	29. 聴聞	
KR/L-29.1	情報通信省長官は、**KR/L-12.1** により指定取消を行おうとする場合には、聴聞を実施しなければならない	
	30. 権限の委任	
KR/L-30.1	この法律による情報通信省長官の権限は、大統領令**(KR/E)**の定めるところによりその一部を所属機関の長に委任することができる	

根拠資料		備考
条項番号	条文	

第 7 章 罰則

31. 罰則

KR/L-31.1 次の各号のいずれかに該当する者は、3 年以下の懲役または 3000 万 W(300 万円)以下の罰金に処する

1) **KR/L-21.3** に違反して加入者の申請なしに加入者の秘密鍵を保管し、または秘密鍵の保管を申請した加入者の承諾なしにこれを利用し、または流出させた者

2) **KR/L-23.1** に違反して他人の秘密鍵を盗用または漏洩した者

3) **KR/L-23.2** に違反して他人の名義で公認証明書の発行を受け、または発行を受けることができるようにした者

32. 罰則

KR/L-32.1 次の各号のいずれかに該当する者は、1 年以下の懲役又は 1000 万 W(100 万円)以下の罰金に処する

1) **KR/L-22.2** に違反して加入者証明書等を保管しなかった者

2) **KR/L-25.3** に違反して特定認可認証局の認可証明書のみを要求した者

33. 両罰規定

根拠資料		備考
条項番号	条文	
KR/L-33.1	法人の代表者または法人、または個人の代理人・使用人その他従業員がその法人または個人の業務に関して **KR/L-31** または **KR/L-32** の違反行為を行ったときには、行為者を罰する以外にその法人または個人に対しても各該当条の罰金刑を課す	
	34. 過料	
KR/L-34.1	次の各号のいずれかに該当する者は、500 万 W(50 万円)以下の過料に処する 1) **KR/L-6.1** または **KR/L-6.2(KR/L-25.2** により準用される場合を含む)に違反して CPS の届出または変更の届出を行わず、又は **KR/L-6.3(KR/L-25.2** により準用される場合を含む)による CPS の変更に関する命令を履行しなかった者 2) **KR/L-7(KR/L-25.2** により準用される場合を含む)の規定に違反して正当な事由なしに認証サービスの提供を拒否し、または加入者または利用者を不当に差別した者 3) **KR/L-9.1** による届出を行わなかった者 4) **KR/L-10.1** による認証業務の休止、又は **KR/L-10.2** による認証業務の廃止事実を加入者に通知せず、または情報通信省長官に届け出なかった者 5) **KR/L-10.3** または **KR/L-12.2** に違反して正当な事由なしに他の公認認証局に加入者証明書等の引継を行わず、または届け出なかった者 6) **KR/L-14.1** による資料を提出せず、又は虚偽の資料を提出した者、又は関係公務員の立入・検査を拒否・妨害若しくは忌避した者 7) **KR/L-21.4** による通知を行わなかった者 または 8) **KR/L-23.3** に違反して公認証明書ではない証明書等を公認証明書と混同させ、又は混同する恐れのある類似の表示を使用し、又は偽って公認証明書の使用を表示した者	

根拠資料		備考
条項番号	条文	
KR/L-34.2	**KR/L-34.1** による過料は、大統領令**(KR/E)**の定めるところにより情報通信省長官が賦課・徴収する	
KR/L-34.3	**KR/L-34.2** による過料処分に不服のある者は、その処分の告知を受けた日から 30 日以内に情報通信省長官に異議を申し立てることができる	
KR/L-34.4	**KR/L-34.2** による過料処分を受けた者が **KR/L-34.3** により異議を申し立てたときには、情報通信省長官は、すみやかに管轄裁判所にその事実を通知しなければならず、その通知を受けた管轄裁判所は、非訟事件手続法による過料の裁判を行う	
KR/L-34.5	**KR/L-34.3** による期間内に異議を申し立てず、過料を納付しなかったときには、国税滞納処分の例によりこれを徴収する	
	付則	
	施行日	
KR/L-付則.1	この法律は 2002 年 4 月 1 日から施行する	
	賠償責任に関する経過措置	
KR/L-付則.2	この法律の施行前に認可認証機関の認証業務遂行に関連し発生した損害に対する賠償責任は、従前の規定による	
	罰則の適用に関する経過措置	
KR/L-付則.3	この法律の施行前の行為に関する罰則の適用においては、従前の規定による	

	根拠資料	備考
条項番号	条文	

他の法律の改正

KR/L-付則.4

情報通信網利用促進及び情報保護等に関する法律のうち次の部分を改正する

第 18 条第 2 項の「電子署名(作成者を確認することができ、文書の変更の有無を確認することができるものをいう)」を「電子署名法第 2 条第 3 号の規定による認可電子署名」とする

電子政府具現のための行政業務等の電子化促進に関する法律のうち次の部分を改正する。第 18 条第 1 項、第 20 条第 1 項及び第 3 項のうち「電子署名法第 2 条第 2 号の規定による電子署名」をそれぞれ「電子署名法第 2 条第 3 号の規定による認可電子署名」とする

韓国

[KR/E] 電子署名法施行令

1999.7.1 施行 2002.6.10 改正

根拠資料		備考
条項番号	条文	
	1. 目的	
KR/E-1.1	この令は電子署名法(以下、「法」という)において委任された事項とその施行に関して必要な事項を規定することを目的とする	
	2. 公認認証局の指定規準	
KR/E-2.1	**KR/L-4.3** により公認認証局として指定を受けようとする者が備えるべき技術能力・財政能力・施設及び設備その他の必要な事項は次の各号のとおりである。ただし、国家機関または地方公共団体が公認認証局として指定を受ける場合には、**KR/E-2.1.2** の財政能力を適用しない	

根拠資料		備考
条項番号	条文	
KR/E-2.1.1	技術能力：公認認証業務(以下、「認証業務」という)に必要な施設及び設備の運営人材として次の要件を備えた者 12 人以上 a) 情報通信技術者・情報処理技術者及び電子計算機システム応用技術者以上の国家技術資格またはこれと同等以上の資格があると情報通信省長官が認める資格を有すること b) 情報通信省長官が定めて告示する情報保護または情報通信運営・管理分野において 2 年以上勤務した経歴を有すること c) 情報通信網利用促進及び情報保護等に関する法律第 52 条の規定による **KISA** において実施する認証業務に関する施設及び設備の運営･非常復旧対策及び侵害事故の対応等に関する教育課程を履修すること	
KR/E-2.1.2	財政能力：資本金 80 億 W(8 億円)以上	
KR/E-2.1.3	施設及び設備：次の設備 a) 加入者の登録情報を管理するための設備 b) 電子署名生成情報及び電子署名検証情報を生成･管理するための設備 c) 公認証明書を生成･発行･管理するための設備 d) 電子文書が公認認証局に提示された時点を確認するための設備 e) 認証業務に関する施設及び設備を安全に運営するための保護設備 f) 公認認証局が公認認証サービスに関連して加入者に提供する設備	
KR/E-2.1.4	**KR/E-2.1.3 a)**から **e)**による設備の管理･運営手続き及び方法を定めた内部規程	
KR/E-2.2	**KR/E-2.1.3** 及び **KR/E-2.1.4** による施設及び設備と内部規程に関する具体的な事項は情報通信省長官が定めて告示する。->**KR/F、KR/CPS**	

根拠資料		備考
条項番号	条文	

3. 公認認証局指定の手続き

KR/E-3.1 **KR/L-4** により公認認証局として指定を受けようとする者は、公認認証局指定申請書に次の各号の書類を添付して情報通信省長官に提出しなければならない

1) 法人の代表者及び役員の戸籍抄本または戸籍謄本

2) 定款及び法人登録証明書

3) **KR/E-2.1** による技術能力・財政能力・施設及び設備その他の必要な事項を備えていることを確認することのできる証明書

4) 事業計画書

KR/E-3.2 情報通信省長官は、**KR/E-3.1** による指定申請があるときには、次の各号の事項を審査しなければならない

1) **KR/E-2.1** による技術能力・財政能力・施設及び設備その他の必要な事項を備えているかどうか

2) 申請人が法人の場合、**KR/L-5** による欠格事由に該当するかどうか

KR/E-3.3 情報通信省長官は、**KR/E-3.2** による審査を行うに当たって必要だと認めるときには、申請人に資料の提出を要求し、または申請人の意見を聞くことができる

KR/E-3.4 情報通信省長官は、**KR/E-3.1** により審査した結果、その申請が同項各号の規定に適合すると認めるときには、申請人に公認認証局指定書を交付しなければならない

KR/E-3.5 情報通信省長官は、国家機関または地方公共団体を公認認証局として指定する場合には、あらかじめ関係機関の長と協議しなければならない

KR/E-3.6 情報通信省長官は、公認認証局を指定したときには情報通信省令の定めるところによりこれを告示しなければならない

根拠資料		備考
条項番号	条文	

3-2. 指定の有効期間

KR/E-3-2.1 公認認証局指定の有効期間は、指定を受けた日から 2 年とする

3-3. 更新指定

KR/E-3-3.1 公認認証局の指定を受けた者がこれを更新しようとする場合には、指定の有効期間満了日の 30 日前までに公認認証局指定申請書に次の各号の書類を添付して情報通信省長官に提出しなければならない

1) **KR/E-3.1.1** 及び **KR/E-3.1.2** の書類

2) 指定または更新指定の有効期間中に定期検査を受けたことを確認することのできる証明書

KR/E-3-3.2 情報通信省長官は、**KR/E-3-3.1** による更新指定申請があるときには、次の各号の事項を審査しなければならない

1) **KR/L-6** による CPS の届出または変更届出を誠実に履行したかどうか

2) **KR/L-19.2** による定期検査を受けたかどうか

3) その他法及びこの令の規定を誠実に遵守したかどうか

KR/E-3-3.3 情報通信省長官は、**KR/E-3-3.2** により審査した結果、その更新申請が同項各号の規定に適合すると認めるときには、有効期間が満了する公認認証局指定書を回収した後、公認認証局指定書を交付しなければならない

KR/E-3-3.4 情報通信省長官は、公認認証局を更新指定したときには、情報通信省令の定めるところによりこれを告示しなければならない

根拠資料		備考
条項番号	条文	

3-4. 認証業務の停止及び指定取消の告示

KR/E-3-4.1 情報通信省長官は、**KR/L-12.1** により公認認証局の認証業務を停止し、または指定を取り消したときには、情報通信省令の定めるところによりこれを告示しなければならない

4. 認証業務の独立性

KR/E-4.1 公認認証局は、認証業務を安全かつ信頼されるべく遂行するために、自身が発給した公認証明書を利用する加入者との関係において独立性を維持しなければならない

5. 権限の委任

KR/E-5.1 情報通信省長官は、**KR/L-30** により次の各号の権限を管轄する逓信庁長官に委任する

1) **KR/L-9.1** による譲受及び合併の届出の受理

2) **KR/L-10.1** 及び **KR/L-10.2** による業務休止・廃止の届出の受理

3) **KR/L-10.3** 但し書きによる加入者証明書等の引継不能事実届出の受理

6. 過料

KR/E-6.1 情報通信省長官は、**KR/L-34.2** により過料を賦課するときには、当該違反行為を調査・確認した後、違反の事実・過料金額等を書面により明示してこれを納付することを過料処分対象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	
KR/E-6.2	情報通信省長官は、**KR/E-6.1** により過料を賦課しようとするときには、10 日以上の期間を定めて過料処分対象者に口述または書面による意見陳述の機会を与えなければならない。この場合、指定された期日までに意見陳述がないときには意見がないものとみなす	
KR/E-6.3	情報通信省長官は、過料の金額を定めるに当たって当該違反行為の動機とその結果等を斟酌しなければならない	
KR/E-6.4	過料の徴収手続きは、情報通信省令において定める	
	付則	
	①(施行日) この令は公布された日から施行する	
	②(他の法令の改正) 電子政府具現のための行政業務等の電子化促進に関する法律施行令のうち、次のとおり改正する	
	第 7 条第 1 項第 1 号のうち、電子署名法第 2 条第 2 号の規定による電子署名(以下、電子署韓国 電子署名法施行令 4 名という)を電子署名法第 2 条第 3 号の規定による公認電子署名(以下、公認電子署名という)とし、第 7 条第 2 項･第 9 条及び第 44 条第 1 項第 4 号のうち、電子署名をそれぞれ公認電子署名とし、第 57 条第 1 項第 2 号のうち、電子署名法第 2 条第 2 号の規定による電子署名間を電子署名法第 2 条第 3 号の規定による公認電子署名間とする	

韓国

[KR/R] 電子署名法施行規則

1999.8.12 施行 2002.7.11 改正

根拠資料		備考
条項番号	条文	
	1. 目的	
KR/R-1.1	この規則は、電子署名法及び同法施行令において委任された事項とその施行に関して必要な事項を規定することを目的とする	
	2. 公認認証機関指定申請書	
KR/R-2.1	電子署名法施行令(以下「令」という)第 3 条第 1 項及び第 3 条の 3 第 1 項の規定による公認認証機関指定申請書は、別紙第 1 号書式のとおりである	
	3. 公認認証機関指定書	

根拠資料		備考
条項番号	条文	
KR/R-3.1	令第 3 条第 4 項及び第 3 条の 3 第 3 項の規定による公認認証機関指定書は別紙第 2 号書式のとおりである	
	4. 協議	
KR/R-4.1	情報通信省長官は、令第 3 条第 5 項の規定により国家機関または地方公共団体を公認認証機関として指定するときには、国家保安政策と合致しているかどうかを国家情報院長官と協議しなければならない	
	4-2. 公認認証局指定等の告示	
KR/R-4-2.1	**KR/E-3.6** による公認認証局の指定の告示、**KR/E-3-3.4** による公認認証局の更新指定の告示または **KR/E-3-4** による公認認証業務(以下 認証業務」という)の停止及び指定取消の告示は、次の各号の事項を官報に掲載する方法により行う 1) 公認認証局の指定及び更新指定の場合 a) 指定を受けた者の名称・住所 b) 指定日 c) 指定の有効期間 d) その他必要な事項 2) 認証業務の停止及び指定取消の場合 a) 処分を受けた者の名称・住所 b) 処分の種類 c) 処分日 d) 認証業務の停止期間(認証業務の停止の場合に限る) e) その他必要な事項	

根拠資料		備考
条項番号	条文	

5. 公認 CPS の変更の届出の期間

KR/R-5.1 **KR/L-6.2** による公認 CPS の変更の届出は、その変更される公認 CPS に基づいて認証業務を遂行する 15 日前までに行わなければならない

6. 譲受及び合併の届出等

KR/R-6.1 **KR/L-9.1** により公認認証局の認証業務の譲受の届出を行おうとする者は、その事由が発生した日から 15 日以内に別紙第 3 号書式の公認認証業務譲受届に次の各号の書類を添付して管轄する逓信庁長官に提出しなければならない

1) 譲渡契約書の写本
2) 譲受人の定款及び法人登記簿謄本
3) 譲受後の事業計画書

KR/R-6.2 **KR/L-9.1** により公認認証局の合併の届出を行おうとする者は、その事由が発生した日から 15 日以内に別紙第 4 号書式の公認認証局合併届に次の各号の書類を添付して管轄する逓信庁長官に提出しなければならない

1) 合併契約書の写本
2) 合併当事者の定款及び法人登記簿謄本
3) 合併後の事業計画書

KR/R-6.3 情報通信省長官は、公認認証局の認証業務の譲受または公認認証局の合併があるときには、その事実を告示しなければならない

7. 認証業務の休止・廃止の届出

根拠資料		備考
条項番号	条文	
KR/R-7.1	**KR/L-10.1** 前段または **KR/L-10.2** により認証業務の休止または廃止の届出を行おうとする者は、別紙第 5 号書式の公認認証業務(休止・廃止)届に次の各号の書類を添付して管轄する逓信庁長官に提出しなければならない 1) 〈削除〉 2) 加入者の公認証明書とその効力停止及び廃止に関する記録(以下 「加入者認証書等」という)を引受けた公認認証局との引継・引受契約書の写本(廃止の場合に限る) 3) 加入者に休止または廃止の事実を通知したことを確認することのできる書類 4) 公認認証局指定書(廃止の場合に限る)	
	8. 加入者証明書等の引継不能事由の届出	
KR/R-8.1	**KR/L-10.3** 但し書きまたは **KR/L-12.2** 但し書きの規定により公認認証局が他の公認認証局に加入者証明書等を引継ぐことができない場合には、別紙第 6 号書式の加入者証明書等の引継不能事由届及び引継ぐ加入者証明書等のリストを管轄する逓信庁長官に提出しなければならない	
	9. 行政処分	
KR/R-9.1	**KR/L-12.1** による認証業務の停止及び指定取消の基準は別表 1 のとおりである	
KR/R-9.2	情報通信省長官は、**KR/L-12.1** により認証業務の停止または指定取消を行った場合には、当該公認認証局に書面によりこれを通知しなければならない	
	10. 準用規定	

根拠資料		備考
条項番号	条文	
KR/R-10.1	**KR/R-6.3** は、次の各号のにこれを準用する 1) **KR/R-7** による認証業務の休止または廃止 2)(削除) 3) **KR/L-10.3** 本文及び **KR/L-12.2** 本文による加入者認証書等の引継・引受	
KR/R-10.2	(削除)	
	11. 過料を賦課する違反行為等	
KR/R-11.1	**KR/L-13.1** により過料を賦課する違反行為の種別とそれに伴う過料の金額は別表 2 のとおりである	
KR/R-11.2	情報通信省長官は、違反行為の程度及び回数等を斟酌し、**KR/R-11.1** による過料の金額の 2 分の 1 の範囲内においてこれを加増し、または減軽することができる。この場合、加増するときであって過料の総額は 2000 万 W(200 万円)を超過することができない	
	12. 過料の賦課及び納付	
KR/R-12.1	情報通信省長官は、**KR/L-13.1** により過料を賦課しようとするときには、その違反行為の種別と当該過料の金額等を明示してこれを納付することを別紙第 7 号書式により通知しなければならない	
KR/R-12.2	**KR/R-12.1** により通知を受けた者は、通知を受けた日から 20 日以内に過料を情報通信省長官が定める受納機関に納付しなければならない。ただし、天災その他のやむをえない事由によりその期間内に過料を納付することができない場合には、その事由が消滅した日から 7 日以内に納付しなければならない	
KR/R-12.3	**KR/R-12.2** により過料の納付を受けた受納機関は、過料を納付した者に別紙第 7 号書式による過料納付領収証を交付しなければならない	

根拠資料		備考
条項番号	条文	
KR/R-12.4	過料の受納機関は、**KR/R-12.2** により過料を受納したときには、遅滞なく別紙第 7 号書式による過料領収済通知書を情報通信省長官に送付しなければならない	
KR/R-12.5	過料はこれを分割して納付することができない	
	13. 過料の督促及び徴収	
KR/R-13.1	情報通信省長官は、**KR/l-12.1** により過料の納付通知を受けた者が納付期限までに過料を納付しなかった場合には、納付期限が経過した日から 7 日以内に督促状を発布しなければならない。この場合、納付期限は督促状を受けた日から 10 日以内としなければならない	
KR/R-13.2	情報通信省長官は、**KR/R-13.1** により督促を受けた者が納付期限までに過料を納付しなかった場合には、所属公務員をして国税滞納処分の例にならい過料を強制徴収させることができる。この場合、所属公務員はその権限を表示する証票を関係人に提示しなければならない	
	13-2. 実在性確認の基準及び方法	
KR/R-13-2.1	公認認証局は、**KR/L-15.1** 後段の規定により公認証明書の発行を受けようとする者の実在性を認証する場合には、次の各号の区分による名義を基準としなければならない	

根拠資料		備考
条項番号	条文	
KR/R-13-2.1.1	個人の場合 a) 住民登録証明書に記載された氏名及び住民登録番号。ただし、在外国民の場合には旅券に記載されている氏名及び旅券番号(旅券が発行されていない在外国民の場合には在外国民登録法による登録簿に記載されている氏名及び登録番号) b) 外国人の場合には出入国管理法による登録外国人記録票に記載されている氏名及び登録番号。ただし、外国人登録証明書が発行されていない外国人の場合には旅券または身分証に記載されている氏名及び番号	
KR/R-13-2.1.2	法人(国税基本法により法人とみなす法人格のない社団等を含む。以下同じ)の場合 法人税法により交付された法人登録証明書に記載されている法人名及び法人登録番号。ただし、法人登録証明書の交付を受けていない法人の場合には法人税法により納税番号を付与された文書に記載されている法人名及び納税番号	
KR/R-13-2.1.3	法人でない団体の場合 当該団体を代表する者の **KR/R-13-2.1.1** の規定による名義。ただし、付加価値税法により固有番号を付与され、または所得税法により納税番号を付与されている団体の場合にはその文書に記載されている団体名と固有番号または納税番号	
KR/R-13-2.1.4	**KR/R-13-2.1.1** から **KR/R-13-2.1.3** の規定によることが困難な場合 情報通信省長官が定める名義	
KR/R-13-2.2	公認認証局は、公認証明書の発行を受けようとする者の実在性を認証するときには、その者の名義が **KR/R-13-2.1** の規定による名義なのかどうかを認証し、**KR/R-13-3** の規定による実在性証明書により本人であることを確認しなければならない。ただし、申請者が法人の場合には当該法人の代表者に対しても **KR/R-13-2.1.1** 及び **KR/R-13-3.1.1** の規定により実在性認証を行わなければならない。	

根拠資料		備考
条項番号	条文	
KR/R-13-2.3	公認証明書の発行を受けようとする者は、やむをえない事由がある場合には、代理人等を介して **KR/R-13-2.1** 及び **KR/R-13-2.2** の規定による実在性認証を受けることができる。この場合、代理人の許容範囲、実在性認証方法及び手続きに関して必要な事項は情報通信省長官が定めて告示する。	
	13-3. 実在性証明書	
KR/R-13-3.1	**KR/R-13-2.1** の規定による名義人が本人かどうかは、次の各号の区分による実在性認証により確認する	
KR/R-13-3.1.1	個人の場合 a) 住民登録証明書発行対象者は住民登録証明書。ただし、住民登録証明書によることが困難な場合には国家機関、地方公共団体または初･中等教育法及び高等教育法による学校の長が発行したものであって、**KR/R-13-2.1.1** の規定による名義の確認が可能な証明書または書類 b) 住民登録証明書発行対象者でない者は国家機関、地方公共団体または初･中等教育法及び高等教育法による学校の長が発行したものであって、**KR/R-13-2.1.1** の規定による名義の確認が可能な証明書または本人の住民登録証明書謄本と法定代理人の a)の証明書 c) 在外国民は旅券または在外国民登録証明書 d) 外国人は出入国管理法による外国人登録証明書。ただし、外国人登録証明書が発行されていない者の場合には旅券または身分証明書	
KR/R-13-3.1.2	法人の場合 非訟事件手続法による法人登記簿謄本または商業登記簿謄本、法人税法による法人登録証明書、所得税法による納税番号を付与された文書または写し、付加価値税法による法人登録証明書及び固有番号を付与された文書または写し	

根拠資料		備考
条項番号	条文	
KR/R-13-3.1.3	法人でない団体の場合 当該団体を代表する者の実在性を確認することのできる **KR/R-13-3.1.1** の証明書･書類。ただし、**KR/R-13-2.1.3** ただし書の規定による団体の場合には､納税番号または固有番号を付与された文書または写し	
KR/R-13-3.1.4	**KR/R-13-3.1.1** から **KR/R-13-3.1.3** の規定により本人かどうかを確認することが困難な場合 関係機関の長の確認書･証明書等､情報通信省長官が定める実在性認証	
	13-4. 保護措置	
KR/R-13-4.1	公認認証局が **KR/L-18-3** による認証業務に関する施設の安全性確保のために取るべき保護措置は次の各号のとおりである 1) 電子的不正アクセスからの保護措置 2) 外部者の入退管理等の防護措置 3) 火災・水害等の災害に備えた措置 4) その他認証業務に関する施設の安全性確保のための管理的措置	
KR/R-13-4.2	**KR/L-13-4.1** による保護措置に関する細部事項は、情報通信省長官が定めて告示する	
	13-5. 定期検査	
KR/R-13-5.1	公認認証局は、**KR/L-19.2** により認証業務に関する施設及び設備が安全に運営されているかどうかについての定期検査を公認認証局としての指定を受けた日から 6 ヵ月以内に受けなければならず、その後は最初の定期検査日を起点として 1 年に 1 回受けなければならない	

根拠資料		備考
条項番号	条文	
KR/R-13-5.2	**KR/R13-5.1** による定期検査の検査事項は次の各号のとおりである 1) **KR/L-8** による電子署名認証業務指針(KR/CPS)を遵守しているかどうか 2) **KR/R13-4**(KR/PR)による保護措置を履行しているかどうか	
	13-6. 代行費用の支援	
KR/R-13-6.1	法第 26 条の 3 第 2 項後段の規定により電子署名の相互連動に関する事業の推進を代行する関連機関及び団体がこれに要する費用の支援を受けようとする場合には、その代行事業の推進計画及びその所要費用算定内訳を情報通信省長官に提出しなければならない	
KR/R-13-6.2	第 1 項の規定により費用の支援を受けた関連機関及び団体は、別途会計を設定してこれを計理しなければならず、他の用途に使用してはならない	
KR/R-13-6.3	第 1 項の規定による代行費用の支援申請手続き･支援方法･支援金に対する事後監督等に関して必要な事項は情報通信省長官が定めて告示する	
	13-7. モデル事業	
KR/R-13-7.1	情報通信省長官は、法第 26 条の 5 の規定により次の各号の事業をモデル事業として推進することができる 1) 電子署名の利用拡大のための試験的事業 2) 電子署名の相互連動等認証業務の効率化事業 3) 電子署名の相互認定のための国際協力事業 4) 電子署名技術の実用化事業 5) その他電子署名の利用活性化のための事業	

根拠資料		備考
条項番号	条文	

14. 過怠料の徴収手続き

KR/R-14-1 令第 6 条第 4 項の規定による過怠料の徴収手続きに関しては、税収徴収官事務処理規則を準用する。この場合、納入告知書にはこの申請方法及びこの申請期間をともに記載しなければならない

付則

施行日

KR/R-付則-1 この規則は公布した日から施行する

定期点検に関する経過措置

KR/R-付則-2 この規則の施行当時、法第 4 条の規定により指定を受けた公認認証機関は、第 13 条の 5 の改正規定にかかわらず、認証業務に関する施設及び装置が安全に運営されているかどうかについての最初の定期点検を 2003 年 6 月 30 日までに受けなければならない

他の法令の改正

医療法施行規則のうち、次のとおり改正する

第 15 条第 1 項のうち、「電子署名」を「公認電子署名」とする。

韓国

[KR/CP] 実在性確認及び本人確認に関する告示

2002.12.17 施行

根拠資料		備考
条項番号	条文	

1. 目的

この告示は、**KR/L-15.1** 後段および **KR/R-13-2.3** の規定により公認認証局が、代理人等を通じて公認証明書の発行を受けようとする者に対する実在性を認証する場合、その方法と手順等、必要な事項を定めることを目的とする

2. 定義

この告示において使用する用語の定義は、次のとおりである

1. “登録局” とは、公認認証局から公認証明書申請書の受付・処理および実在性認証業務等の委託を受けた者をいう

根拠資料		備考
条項番号	条文	
	2. “金融機関” とは、金融機関電子金融業務監督規定の適用を受ける金融機関をいう	
	3. “電子金融取引” とは、金融機関の加入者が、金融機関が提供する電子金融業務 (単に情報のみを提供する場合、これを除外する) を利用する取引をいう。この場合、電子金融取引の開始から終了時まで、非電子的な手段が介入しない場合に限る	
	3. 適用範囲	
	この告示は、公認認証局および登録局(以下「公認認証局等」という) が公認証明書の発行を受けようとする者に対して遂行する実在性認証業務に適用する	
	4. 実在性認証の原則	
KR/CP-4	公認認証局等は、**KR/L-15** および **KR/R-13-2.1** ないし **KR/R-13-2.2** の規定にしたがい、公認証明書の発行を受けようとする者に対する実在性を認証しなければならない。但し、公認認証局等は、不可避であると判断する場合に限り、自己責任により **KR/CP-5** および **KR/CP-6** の規定にしたがい、代理人による実在性認証またはオンライン実在性認証を行うことができる	
	5. 代理人による実在性認証	
KR/CP-5.1	公認認証局等は、**KR/R-13-2.1.2** の規定による法人が公認証明書の発行を受けようとする場合に限り、KR/CP-4 ただし書の規定により代理人による実在性認証を行うことができる	

根拠資料		備考
条項番号	条文	
KR/CP-5.2	公認認証局等は、代理人により法人の実在性を認証する場合、次の各号の事項を確認しなければならない 1) **KR/R-13-3.1.2** の規定による法人の実在性証明書 2) 法人の代表者の委任状 3) 法人印鑑証明書 4) **KR/R-13-3.1.1** の規定による代理人の実在性証明書	
KR/CP-5.3	法人を代理することができる者は、当該法人の役員または職員に限る	
	6. オンライン実在性認証	
KR/CP-6.1	公認認証局等は、金融実名取引および秘密保障に関する法律にしたがい、金融機関により実地名義が確認された電子金融取引加入者が公認証明書の発行を受けようとする場合に限り、KR/CP-4 但し書の規定によりオンライン実在性認証を行うことができる	
KR/CP-6.2	公認認証局等は、電子金融取引加入者に対してオンライン実在性認証を行う場合、次の各号の事項を確認しなければならない 1) 加入者の勘定 2) 加入者の勘定番号 3) 加入者の口座番号 4) 加入者の住民登録番号 5) ワンタイムパスワードまたは 1)から 4)の事項を除外した加入者本人のみが知り得る 2 つ以上の付加情報	
KR/CP-6.3	公認認証局等は、電子金融取引加入者に対してオンライン実在性認証を行う場合、KR/CP-6.2 の規定にかかわらず、金融機関と加入者間の約定にしたがい発行された公開鍵暗号技術に基づいた証明書を利用して、電子金融取引加入者の実在性を認証することができる	

根拠資料		備考
条項番号	条文	
KR/CP-6.4	公認認証局等は、オンライン実在性認証の安全性と信頼性を検証しなければならない	
KR/CP-6.5	公認認証局等は、KR/CP-6.4 の規定による検証の結果、問題点があると判断するときには、オンライン実在性認証により公認証明書が発行された電子金融取引加入者に対して、遅滞なく対面審査を実施しなければならない	
	付則	
	1. 施行日	
KR/CP-付則.1	この告示は、告示した日から施行する	
	2. 経過措置	
KR/CP-付則.2	この告示施行前に、この告示の規定による代理人等による実在性確認と同様の方法と手順により発給された公認認証書は、この告示にしたがい発給されたものと見なす	
	3. 適用例	
KR/CP-付則.3	第 6 条第 2 項第 5 号の規定は、証券取引加入者に対しては、2003 年 4 月 1 日から、これを適用する	

韓国

[KR/CPS] CPS ガイドラインに関する告示

2002.11.15 施行 2003.11.27 施行

根拠資料		備考
条項番号	条文	
	1. 総則	
	1.1 目的	
KR/CPS-1.1.1	1.1.1 この指針は、**KR/L-8.1** の規定により公認認証業務の安全性と信頼性の確保のために、公認認証局が公開鍵暗号化方式の技術を利用した公認認証業務を遂行するにあたり、守らなければならない具体的事項を定めることを目的とする	
	1.2 定義	

	根拠資料	備考
条項番号	条文	
KR/CPS-1.2.1	1.2.1 この指針において使用する用語の定義は、次のとおりである ア. “認証マネジメントシステム”とは、証明書の発行および認証関連記録の管理等、認証サービスを提供するための体系をいう イ. “認証システム”とは、加入者の登録情報管理、鍵ペアの生成・管理、公認証明書の生成・発行・管理、タイムスタンプ検証機能等をサポートするシステムであって、公認認証サービスのために公認認証局内に設置されたシステムをいう ウ. “非対称暗号化方式”とは、情報を暗号化するために使用するキーと暗号化された情報を復元するために使用するキーが互いに異なる暗号化方式をいう エ. “公開鍵”とは、電子署名を検証するために利用する電子式情報をいう オ. “秘密鍵”とは、電子署名を生成するために利用する電子式情報をいう。 カ. “鍵ペア”とは、秘密鍵とこれに合致する公開鍵をいう キ. “登録局”とは、公認認証局から公認証明書申請書の受付・処理および実在性認証業務等の委託を受けた者をいう ク. “加入者登録情報”とは、公認証明書申請書、申請者が実在性認証のために公認認証局に提出した書類および提示した証明書等の写し、そしてその他公認証明書申請に必要な電子的記録をいう。 ケ. “ネットワークセキュリティシステム”とは、ファイアウォール、IDS、ネットワーク管理システム等、ネットワークを安全に運営するためのシステムをいう コ. “ 更新発行 ”とは、証明書の有効期間の満了により、満了の時点以前に有効期間を延長し、証明書を発行することを言う	

根拠資料		備考
条項番号	条文	
	サ. “ 再発行 ”とは、加入者の秘密鍵が紛失・毀損、または盗難・流出した場合、該当の証明書を失効して新たな鍵ペアを生成し、証明書を発行することを言う シ. “ 変更発行 ”とは、証明書の所有者の識別名称(以下「DN」とする)等、証明書内の加入者の情報が変更した場合、該当の情報を変更し、証明書を発行することを言う	
	1.3 適用範囲	
KR/CPS-1.3.1	1.3.1 この指針は、非対称暗号化方式の電子署名技術を利用した公認認証業務に適用する	
	2. 認定証明書の管理	
	2.4 登録情報の転送	
KR/CPS-2.4.1	認定認証局は、登録局から認定証明書の発行を受けようとする者の登録情報を、ネットワークを通じて転送を受ける場合、当該の登録情報に対し、登録局の認定電子署名かつ認定認証局の施設および装備などに関する規定第 5 条第 1 項第 3 号の暗号アルゴリズムによる暗号化を適用しなければならない。ただし、登録局との約定により、認定電子署名以外の電子署名を利用する場合は、認定認証局の施設および装備等に関する規定第 5 条第 1 項第 1 号の電子署名アルゴリズムを使用しなければならない	

根拠資料		備考
条項番号	条文	

2.5 公認証明書の発行申請

KR/CPS-2.5.1 認定認証局は、認定証明書の発行を受けようとする者または加入者から、認定証明書の新規発行・更新発行・再発行・変更発行等の申請がある場合、法第 15 条第 6 項で定める実在性確認の手続を遵守し、当該の申請内容に不備がないことを確認しなければならない

KR/CPS-2.5.2 認定認証局は、第 1 項の更新発行または変更発行申請の場合、当該の加入者に限り、認定電子署名を利用して実在性確認および申請内容に不備がないことを確認することができる

KR/CPS-2.5.3 第 2 項の規定により、認定電子署名を利用して、変更発行の申請に対する実在性確認および申請内容に不備がないことを確認する場合、住民登録票謄本や法人登記簿謄本等の関連資料を活用し、信頼できる方法で変更された情報の正確性を確認しなければならない

2.6 公認証明書の生成

KR/CPS-2.6.1 公認認証局は、秘密鍵が公認証明書の発行を受けようとする者に属するという事実を確認しなければならないとともに、公認証明書の発行を受けようとする者の公開鍵に対する一意性を有するかどうか確認しなければならない

KR/CPS-2.6.2 公認認証局は、公認証明書を生成する場合、ネットワーク利用の促進および情報保護等に関する法律第 52 条の規定による **KISA** から証明を受けた公開鍵に合致する秘密鍵により当該公認証明書に公認電子署名しなければならない

KR/CPS-2.6.3 公認認証局は、認定証明書を加入者に発行する場合、これをリポジトリに公開しなければならない

根拠資料		備考
条項番号	条文	

2.7 公認証明書の停止・停止解除等の申請

KR/CPS-2.7.1 公認認証局は、加入者から公認証明書の停止・失効・定期更新、個人情報の変更、鍵ペアの交換等の申請がある場合、公認電子署名を利用して、加入者の本人確認および申請内容の真偽を確認しなければならない。ただし、公認認証局は、加入者の本人確認および申請内容の真偽を確認するにあたって、公認電子署名の利用が困難な場合、情報通信省長官が認める他の方法によることができる

KR/CPS-2.7.2 公認認証局は、加入者が秘密鍵の紛失・き損等により公認証明書の失効を申請するときには、信頼し得る方法を通じて当該加入者の本人であるかどうかを確認し、該当申請を処理しなければならない

KR/CPS-2.7.3 公認認証局は、加入者の公認証明書の停止解除申請がある場合、停止された日から 6 ヵ月以内に申請したものであるかどうか確認しなければならない。また、公認認証局は、加入者の公認証明書が、停止された日から 6 ヵ月を過ぎた場合、これを失効しなければならない

2.8 公認証明書の停止･失効リスト生成

KR/CPS-2.8.1 公認認証局は、加入者の公認証明書を停止、停止解除、失効する場合、公認証明書の停止･失効リストを生成しなければならない。この場合、公認認証局は、**KISA** から証明を受けた公開鍵に合致する秘密鍵により当該停止･失効リストに公認電子署名して、これをリポジトリに公開しなければならない

KR/CPS-2.8.2 公認認証局は、加入者の公認証明書を停止・停止解除・失効したときには、その事実を検証することができるように、遅滞なく必要な措置を取らなければならない

根拠資料		備考
条項番号	条文	

2.9 公認証明書の公開および有効性検証サービス

KR/CPS-2.9.1 公認認証局は、**加入者**が公認証明書と公認証明書の停止･失効リストを常に検証することができるように、リポジトリを運営しなければならない

KR/CPS-2.9.2 公認認証局は、**加入者**が公認証明書の有効性を検証することができるように、公認証明書の有効性検証サービスを提供しなければならない

3. 鍵ペアの管理

3.10 鍵ペアの生成

KR/CPS-3.10.1 公認認証局は､利用者が認定証明書と認定証明書の一時停止･失効リストを常に検証することができるように、リポジトリを運営しなければならない

KR/CPS-3.10.2 公認認証局は、認証局鍵ペアを生成する場合、3 人以上の権限のある職員が共同でこれを遂行しなければならない

KR/CPS-3.10.3 公認認証局が公認証明書の加入者鍵ペアを生成する場合、2 人以上の権限のある職員が共同でこれを遂行しなければならない

3.11 秘密鍵の保存

KR/CPS-3.11.1 公認認証局は、FIPS 140-1(または 140-2)level 3 を満足する暗号モジュール利用して、CA 秘密鍵を管理しなければならない

根拠資料		備考
条項番号	条文	
KR/CPS-3.11.2	公認認証局は、公認証明書の発行を受けようとする者の秘密鍵を生成した場合、安全性が確認された暗号アルゴリズムにより、これを暗号化して保存装置に保存し、秘密鍵の真正性保障のために、メッセージ認証コード(MAC)等の情報をともに保存して、これを加入者に直接、伝達しなければならない。この場合、公認認証局は、鍵ペアの生成・管理設備の記憶場所または臨時ファイルに残っている秘密鍵および関連情報をただちに削除しなければならない	
KR/CPS-3.11.3	公認認証局は、秘密鍵を鍵ペアの生成・管理設備から保存装置に通信して保存する場合、安全な通信手段を利用しなければならない	
	3.12 秘密鍵のバックアップ	
KR/CPS-3.12.1	公認認証局は、秘密鍵き損等から公認認証業務提供の持続性を保障するために、秘密鍵をバックアップしなければならない	
KR/CPS-3.12.2	公認認証局は、秘密鍵をバックアップする場合、3.2.1 および 3.2.3 において規定する安全性を保障しなければならない	
KR/CPS-3.12.3	公認認証局は、バックアップされた秘密鍵を秘密鍵の原本と分離して保存し、公認認証業務を遂行する施設から 10km 以上の遠隔地保存設備に安全に保管しなければならない	
	3.13 秘密鍵の破棄	
KR/CPS-3.13.1	公認認証局は、管理責任者および保安管理者の立会いのもとに、バックアップされた秘密鍵とその原本を安全に破棄しなければならない	

根拠資料		備考
条項番号	条文	

3.14 秘密鍵の紛失・き損または盗難・流出

KR/CPS-3.14.1 公認認証局は、CA 秘密鍵が紛失・き損または盗難・流出した場合、すべての信頼者がこの事実を知り得るように、ホームページ掲示等、適切な措置を取らなければならない

3.15 タイムスタンプ検証機能の提供

KR/CPS-3.15.1 認定認証局は加入者または利用者が電子文書に対するタイムスタンプ検証を申請する場合、タイムスタンプ検証サービスを提供することができる

3.16 時刻受信および時刻補正

KR/CPS-3.16.1 認定認証局はタイムスタンプ検証の時、正確な時刻情報を提供するため、正確な時刻を受信する装備を運営し、タイムスタンプ検証システムの時刻補正機能を持続的に使用しなければならない。あわせて、時刻補正機能に誤動作が発生した場合は、タイムスタンプ検証サービスを即刻中断しなければならない

3.17 タイムスタンプ検証記録の保管

KR/CPS-3.17.1 認定認証局はタイムスタンプ検証トークン等、タイムスタンプ検証業務と関連した記録を安全に保管しなければならない

3.18 電子文書の保管

根拠資料		備考
条項番号	条文	
KR/CPS-3.9.1	認定認証局はタイムスタンプ検証の申請者から要請がある場合、タイムスタンプ検証の対象となる電子文書、または電子署名を保管することができる	
KR/CPS-3.9.2	第 1 項の規定によりタイムスタンプ検証の対象となる電子文書を保管する場合、該当の電子文書を認定認証局の施設および装備等に関する規定第 5 条第 1 項第 3 号の暗号アルゴリズムにより暗号化し、権限のない使用者が内容を閲覧できないようにしなければならない	
	3.10 タイムスタンプ検証の記録等のバックアップ	
KR/CPS-3.10.1	認定認証局は第 17 条および第 18 条の規定によりタイムスタンプ検証の記録等を保管する場合、該当の記録をバックアップした後、認定認証業務を遂行する施設から 10km 以上の遠隔地にある保存設備に、安全に保管しなければならない。第 20 条(その他の付加業務) 認定認証局は、タイムスタンプ検証以外にも、認定電子署名を利用して付加業務を遂行することができる	
	4. その他の運営管理	
	4.1 技術規格の遵守	
KR/CPS-4.1.1	公認認証局は、公認認証業務の遂行時、**KR/F** 別表の電子署名認証管理体系技術規格を遵守しなければならない	
	4.2 公認証明書の利用範囲および用途の遵守	

根拠資料		備考
条項番号	条文	
KR/CPS-4.2.1	公認認証局は、**KISA** から発行を受けた公認証明書の使用時、該当公認証明書に明示された利用範囲および用途に従い公認証明書を使用しなければならない	
	4.3 公認認証業務手順の遵守	
KR/CPS-4.3.1	公認認証局は、公認認証業務の手順および方法が変更された場合、これを公認 CPS および内部規定に反映しなければならないとともに、次の各号の事項を含めた改定関連記録を維持・管理しなければならない ア. 改定事由 イ. 制定・改定されたすべての規定	
KR/CPS-4.3.2	公認認証局が次の各号のシステムを設置・運営および維持・保守する場合には、2 人以上の職員が共同でこれを遂行しなければならない ア. 加入者登録情報の管理機能をサポートするシステム イ. 公認証明書の生成・発行・管理機能をサポートするシステム ウ. タイムスタンプ検証機能をサポートするシステム	
	4.4 設備に関する事項	
KR/CPS-4.4.1	公認認証局は、公認認証局の指定時に審査を受けた設備を利用して、公認認証業務を遂行しなければならない	

根拠資料		備考
条項番号	条文	
KR/CPS-4.4.2	公認認証局は、公認認証業務遂行のための設備を変更した場合、遅滞なく情報通信省長官にこれを申告しなければならない。ただし、侵害事故・自然災害・システムの誤動作などにより緊急措置が必要な場合は、変更内容を事前に適用することができ、適用後7 日以内に申告しなければならない。ただし、次の事項と関連する設備の変更については、申告対象から除外する ア. 定期的な運営体制パッチまたはアップグレード イ. 既存設備の負荷分散および性能向上のためのCPU、ハードディスク、メモリ等のハードウエア追加または交換 ウ. 公認認証業務の安全性を害さない範囲内において、電気設備、防音設備等の物理的設備の追加または交換	
KR/CPS-4.4.3	公認認証局は、公認認証業務遂行のための設備を変更した場合、変更を記録し維持しなければならない	
KR/CPS-4.4.4	公認認証局は、次の各号の設備について資産管理を行わなければならない ア. 認証システムおよび加入者ソフトウエア イ. ネットワーク構成および設備 ウ. ネットワークセキュリティシステムおよびサーバ管理システム エ. 入退管理システム オ. その他運営システム	
KR/CPS-4.4.5	公認認証局は、加入者ソフトウエア配布時、当該ソフトウエアについて真正性を保証し得る電子署名またはハッシュ値等を管理しなければならない	

4.5 公認認証業務記録の管理

根拠資料		備考
条項番号	条文	
KR/CPS-4.5.1	公認認証局は、次の各号の記録を公認証明書が失効した日から 10 年間保管しなければならない ア. 公認証明書の申請(発行/停止/停止解除/失効)および処理に関する記録 イ. 申請者が実在性認証のために、公認認証局に提出した書類および提示した証明書等の写し ウ. 公認証明書 エ. 公認証明書の停止･失効リスト オ. 公認証明書失効に関する情報 ･公認証明書失効が法第 18 条第 1 項第 2 号ないし第 4 号の規定により発生した場合、これを決定した者の氏名、住民登録番号が記載された証明書失効事由に関する記録 カ. 公認認証局が加入者の電子署名生成キーを生成した場合、電子署名生成キーの生成に関する記録と加入者の秘密鍵受領書 キ. 公認認証局の秘密鍵生成および管理に関する記録	
KR/CPS-4.5.2	4.5.1 の各号資料は、マイクロフィルム・光ディスク等、資料伝達媒体により保管することができる	
KR/CPS-4.5.3	公認認証局がネットワークを通じて、認定証明書の更新発行・変更発行・一時停止および失効の申請を受ける場合は、第 1 項第 1 号の認定証明書の申請記録を加入者の認定電子署名が添付された電子文書として保管することができる	
KR/CPS-4.5.4	認定認証局は、第 1 項の規定による記録を、認定認証業務を遂行する施設と当該施設から 10km 以上の遠隔地保存設備にそれぞれ一部ずつ保管しなければならない	

4.6 監査記録の管理

根拠資料		備考
条項番号	条文	
KR/CPS-4.6.1	公認認証局は、次に挙げる各号の監査対象記録の異常有無を確認しなければならない ア. 公認認証業務の運営と関連する記録 イ. 認証システム、入退管理システム、ネットワークセキュリティシステムにおいて生成される記録	
KR/CPS-4.6.2	第 1 項の規定により、第 25 条第 1 項第 1 号および第 2 号の記録を登録局で保管する場合、認定認証局は次の各号の情報を登録局の認定電子署名が添付された電子文書として転送され、第 25 条に基づいて保管しなければならない。ただし、登録局との約定により、認定電子署名以外の電子署名を利用する場合は、認定認証局の施設および装備等に関する規定第 5 条第 1 項第 1 号の電子署名アルゴリズムを使用しなければならない ア.実在性確認の情報 1)加入者の名前(姓名または法人名) 2)加入者の識別番号(住民登録番号または事業者登録番号など) 3)その他必要な情報 イ.証明書発行のための基本情報 1)申請証明書の種類 2)申請区分(新規/更新/再発行、一時停止/一時停止解除または失効) 3)その他必要な情報	
KR/CPS-4.6.3	第 1 項の規定により、認定認証局が登録局に記録の保管を委任する場合、認定認証局は登録局に、記録保管のために事務の空間と分離して、入退管理装置が設置されている別途の空間に、ロック機能があるキャビネットまたは金庫を具備させなければならない	

4.7 監査記録の管理

根拠資料		備考
条項番号	条文	
KR/CPS-4.7.1	認定認証局は、次に挙げる各号の監査対象記録の異常有無を確認しなければならない ア.認定認証業務の運営と関連する記録 イ.認定認証システム、入退管理システム、ネットワークセキュリティシステムにおいて生成される記録	
	4.8 登録局の管理	
KR/CPS-4.7.1	公認認証局は、登録局を運営する場合、次の事項を6ヵ月ごとに1回以上検査しなければならない ア. 公認証明書申請者の実在性認証業務 イ. 公認証明書申請書の受付・処理業務 ウ. 公認認証局に加入者登録情報を安全に伝達 エ. 登録システムの管理 ・公認証明書発行政策にともなうDN付与 ・公認認証局において生成した参照番号および許可コードの出力 ・登録システムのアクセス統制等、セキュリティ機能 オ. 登録業務遂行と関連した個人情報の保護 カ. その他認証業務と関連して公認認証局が委託した業務	
	4.9 公認認証業務の試験運営	
KR/CPS-4.8.1	公認認証局は、公認認証業務開始前に、**KISA** が定めるところにしたがい、試験運営を実施しなければならないとともに、該当試験運営の結果を **KISA** に提出しなければならない	
KR/CPS-4.8.2	**KISA** は、4.8.1の規定により受け付けた試験運営の結果に対する検討意見を情報通信省長官と該当公認認証局の長に送付する	

根拠資料		備考
条項番号	条文	
KR/CPS-4.8.3	**KISA** は、公認認証局が試験運営の結果、正常的な運営が可能であると判断される場合、公認認証業務遂行のための公認証明書を発行する	
	4.10 正確な情報の提供および公開	
KR/CPS-4.9.1	公認認証局は、**KISA** に次の各号の情報を申請する場合、該当申請書式に正確な情報および事実を記載しなければならない ア. 公認証明書の発行申請 イ. 公認証明書の停止および失効申請 ウ. 公認証明書の停止解除申請	
KR/CPS-4.9.2	公認認証局は、**加入者**に対して、公認証明書の信頼性または有効性に影響を及ぼす可能性のある次の各号の情報を、誰でも常に確認することができるように、遅滞なく公開しなければならない ア. 公認認証局の指定 イ. 公認認証局の認証業務休止・停止または廃止 ウ. 公認認証局の指定取消 エ. 公認認証局の譲渡・譲受または合併 オ. 公認証明書に対する情報 ・加入者の公認証明書 ・加入者の公認証明書停止・失効リスト生成等 カ. その他公認認証業務遂行関連の情報	

根拠資料		備考
条項番号	条文	
KR/CPS-付則	付則 ①(施行日) この指針は、告示した日から施行する。 ②(経過措置) 指針 3.2.1 の暗号モジュール利用の規定は、公認証明書生成・発行・管理設備の場合には、告示後 1 年、その他の設備の場合には、告示後 2 年が経過した日から施行する。 ③(遠隔地保存設備に関する経過措置) 3.3.3 および 4.5.3 の規定が定める遠隔地保存設備基準のうち、10km 以上に対する事項は、この指針告示後 1 年が経過した日から施行する。	

韓国

[KR/PR] 認証局が採用する安全対策に関する告示

2002.11.15 施行

根拠資料		備考
条項番号	条文	

1. 目的

この規程は、電子署名法 第 18 条の 3 および同法施行規則 第 13 条の 4 の規定により公認認証業務に関する施設の安全性確保のために、公認認証局が取らなければならないセキュリティ対策の具体的事項を定めることを目的とする

2. 定義

この規定において使用する用語の定義は、次のとおりである

1. “公認認証業務施設” とは、電子署名法 第 2 条第 9 号の規定による公認認証サービスを提供する公認認証業務に必要な諸般施設をいう

根拠資料		備考
条項番号	条文	
	2. “認証システム” とは、公認認証サービスを提供するために必須的なシステムであって、鍵生成機能、証明書生成機能、加入者証明書登録機能、証明書および証明書失効リスト公告機能、タイムスタンプ検証機能等を備えたシステムをいう 3. “ネットワークセキュリティシステム” とは、ファイアウォール、IDS 等、ネットワークを安全に運営するためのシステムをいう **3. 保護措置** 公認認証業務に関する施設の安全性確保のために、公認認証機関が取らなければならない保護措置に関する具体的事項は、別表のとおりである **付則** ①(施行日) この規定は、告示した日から施行する。 ②(経過措置) 別表 2 の認証業務に関する施設に対する入退管理等、防護措置のうち保安警備要員と関連する事項は、この規定告示後 6 ヵ月が経過した日から施行する **<別表>** **1. 認証業務に関する施設を電子的侵害行為から保護するための措置**	

	根拠資料	備考
条項番号	条文	

1.1 ネットワーク保護

1.1.1 構成

KR/PR-t1.1.1.1

1.1.1.1 ネットワークセキュリティシステム

ネットワークセキュリティシステムは、**KR/F** に従い設置すること

1.1.2 管理

KR/PR-t1.1.2.1

1.1.2.1 ネットワーク回線

ネットワーク回線は、公認認証サービス提供のために、別途の回線を使用すること

KR/PR-t1.1.2.2

1.1.2.2 ネットワークセキュリティシステム

ネットワークセキュリティシステムは、本機能のソフトウエアのみ設置すること

ネットワークセキュリティシステムは、安全に設定して運営すること

ファイアウォールの侵入遮断規則は、運営に必須的な事項に対してのみ許可すること

IDS のデータベースは、定期的に更新すること

ネットワーク管理システムは、継続的にモニタリングすること

ネットワークログ記録は、定期的に分析して侵入試行、ネットワーク負荷等を把握し、これに適切に対処すること

ネットワークセキュリティシステムに対する論理的なアクセス制御を設定すること

	根拠資料	備考
条項番号	条文	
KR/PR-t1.1.2.3	1.1.2.3 ネットワーク回線 ネットワークセキュリティシステムの 追加/廃棄/変更(ルーターアクセスリスト、ファイアウォールルールセット変更等)に関する事項は、管理台帳に記録し、維持すること ネットワークセキュリティシステムの 追加/廃棄/変更に関する手順を設けること	
	1.2 システム保護	
	1.2.1 構成	
KR/PR-t1.2.1.1	1.2.1.1 サーバ管理システム 公認認証業務と関連する主要プログラムまたはプロセスの動作可否を検査できるシステムを設置すること	
KR/PR-t1.2.1.2	1.2.1.2 ルート権限制限 ルート管理者の権限を制限できるソフトウエアを設置すること	
	1.2.2 管理	

根拠資料		備考
条項番号	条文	
KR/PR-t1.2.2.1	1.2.2.1 システム管理 システムには、システム運営に必要なプログラムのみを設置すること システム運営体制に不必要な事項は、削除すること システム運営体制の問題点解決のための最新のパッチを設置して運営すること 認証システムは、施錠機能が装着されたラックに保管し、施錠機能の鍵は、別途の保管箱を設けて管理すること システムに対する論理的なアクセス制御を設定すること	
KR/PR-t1.2.2.2	1.2.2.2 追加/廃棄/変更 システムの追加/廃棄/変更/(運営体制の変更、パッチ等)に関する事項は、管理台帳に記録し、維持すること システムに設置されるすべてのソフトウエアのソフトウエア名、設置目的等 システムの追加/廃棄/変更に関する細部手順を設けること	
	2. 認証業務に関する施設に対する入退管理等、防護措置	
	2.1 入退管理	
	2.1.1 構成	

	根拠資料	備考
条項番号	条文	
KR/PR-t2.1.1.1	2.1.1.1 入退管理システム ・入退管理システムおよび入退管理設備は、**KR/F** に従い、設置すること	
KR/PR-t2.1.1.2	2.1.1.2 保安警備要員 ・24 時間警備業務を遂行する専門担当保安警備要員を置くこと	
	2.1.2 管理	
KR/PR-t2.1.2.1	2.1.2.1 職員以外の入退管理 ・保安警備要員に、職員以外のすべての出入を 24 時間 CCTV または肉眼を通じて把握し、管理させること ・職員以外のすべての出入事項は、出入台帳に記録し、維持すること ・職員以外のすべての出入は、1 人以上の職員が同行すること ・適切な認可措置なしに職員以外が認証システム室に接近できないようにすること	
KR/PR-t2.1.2.2	2.1.2.2 職員の入退管理 ・保安警備要員に、職員のすべての出入を 24 時間 CCTV または肉眼を通じて把握し、管理させること ・適切な認可措置なしに職員が認可されていない認証システム室に接近できないようにすること	
KR/PR-t2.1.2.3	2.1.2.3 入退管理システム ・入退管理システムの入退許可は、各職員の任務に合わせて設定して運営すること ・入退管理システムの入退管理設備の設定および制御機能は、権限のある管理者のみがアクセスできるようにすること	

根拠資料		備考
条項番号	条文	

2.2 物理的侵入の検知/監視

2.2.1 構成

KR/PR-t2.2.1.1

2.2.1.1 侵入検知および警報設備

・侵入検知および警報設備は、**KR/F** に従い設置すること

・窓および壁面の侵入検知設備は、24 時間作動するようにすること

KR/PR-t2.2.1.2

2.2.1.2 侵入監視設備

・侵入監視設備は、**KR/F** に従い設置すること

2.2.2 管理

KR/PR-t2.2.2.1

2.2.2.1 侵入検知警報発生

・警報が発生した場合、保安警備要員に、即刻、警報発生の原因を把握して、セキュリティ管理者に報告させ、セキュリティ管理者の指示に従い適切な措置を取らせるようにすること

・侵入検知警報は、保安警備要員またはセキュリティ管理者以外の者が解除できないようにすること

・侵入検知警報発生の事実は、台帳に記録し、維持すること

KR/PR-t2.2.2.2

2.2.2.2 侵入監視

・CCTV モニタリングシステムの CCTV 設定および制御機能は、権限のある管理者のみがアクセスできるようにすること

・CCTV システムの録画記録は、月 1 回以上バックアップすること

根拠資料		備考
条項番号	条文	

3. 火災・水害等、各種の脅威から認証業務に関する施設の継続的/安定的運営を保障するための措置

3.1 災害防止

3.1.1 構成

KR/PR-t3.1.1.1

3.1.1.1 火災

・火災検知設備および消火設備は、**KR/F** に従い設置すること

KR/PR-t3.1.1.2

3.1.1.2 その他

・火災以外の防災関連設備は、**KR/F** に従い設置すること

3.1.2 管理

KR/PR-t3.1.2.1

3.1.2.1 火災

・消火設備は、分期別 1 回以上検査すること

・火災検知設備の受信盤、制御盤等は、分期別 1 回以上検査すること

・ガス式消火設備の消火用剤は、定期交換すること

・職員が携帯用消火器の使用方法を熟知すること

KR/PR-t3.1.2.2

3.1.2.2 水害

・認証システムは、水害から保護できるように、床から 30cm 以上の高さに保管すること

根拠資料		備考
条項番号	条文	
KR/PR-t3.1.2.3	3.1.2.3 地震 ・認証システムは、地震から保護できるように、ラックに保管すること	
KR/PR-t3.1.2.4	3.1.2.4 その他 ・各種電源設備に対する接地施設は、年 1 回以上検査すること	
	3.2 システム障害防止	
	3.2.1 構成	
KR/PR-t3.2.1.1	3.2.1.1 停電 ・無停電電源供給設備は、**KR/F** に従い、設置すること ・自家発電設備は、**KR/F** に従い、設置すること	
KR/PR-t3.2.1.2	3.2.1.2 恒温・恒湿 ・恒温恒湿設備は、**KR/F** に従い、設置すること	
KR/PR-t3.2.1.3	3.2.1.3 ネットワーク二重化 ・ネットワーク回線およびネットワーク設備は、**KR/F** に従い、二重化して設置すること	
KR/PR-t3.2.1.4	3.2.1.4 システム二重化 ・認証システムは、**KR/F** に従い二重化して設置すること	
	3.2.2 管理	

	根拠資料	備考
条項番号	条文	
KR/PR-t3.2.2.1	3.2.2.1 停電 ・無停電電源供給設備は、分期別 1 回以上検査すること ・無停電電源供給設備のバッテリーは、定期的に交換すること	
KR/PR-t3.2.2.2	3.2.2.2 恒温・恒湿 ・恒温恒湿設備は、分期別 1 回以上検査すること	
KR/PR-t3.2.2.3	3.2.2.3 ネットワーク二重化 ・二重化されたネットワーク回線は、障害発生時、自動的に転換されるようにすること ・内部ネットワーク設備および経路は、障害発生時、自動的に転換されるようにすること	
KR/PR-t3.2.2.4	3.2.2.4 システム二重化 ・二重化により構成された認証システムは、同一の運営体制、同一のパッチ、同一のソフトウエア設置等、同一の機能を遂行することができるようにすること ・二重化されたシステム間の資料またはデータベースは、一貫性をもって維持すること	
KR/PR-t3.2.2.5	3.2.2.5 バックアップ ・認証システムは、定期的にハードディスクを除外した保存媒体でバックアップすること ・認証システム中、オンラインシステムは、週 1 回以上バックアップすること ・認証システム中、オフラインシステムとその他システムは、月 1 回以上バックアップすること ・バックアップされた資料は、メーンサイトおよび 10km 以上の遠隔地(またはバックアップサイト)に 1 部ずつ保管すること	

根拠資料		備考
条項番号	条文	

4. その他認証業務に関する施設の安全性確保のための管理的措置

4.1 人的セキュリティ

4.1.1 構成

KR/PR-t4.1.1.1

4.1.1.1 管理責任者

・すべてのセキュリティ対策を計画、監督、統制する管理責任者を指定すること

KR/PR-t4.1.1.2

4.1.1.2 セキュリティ管理者

・すべてのセキュリティ対策の実行を担当するセキュリティ管理者を指定すること

KR/PR-t4.1.1.3

4.1.1.3 セキュリティ実務者

・主要施設の維持・管理のために、システム管理、ネットワーク管理等を担当する専門人員(関連分野 2 年以上の経歴者)を 1 人以上確保すること

4.1.2 管理

根拠資料		備考
条項番号	条文	
KR/PR-t4.1.2.1	4.1.2.1 教育 ・管理責任者は、セキュリティ対策について所属職員が関連内容を熟知できるように、内部教育等の必要な措置を取ること ・管理責任者は、セキュリティ管理者およびセキュリティ実務者、認証システムを管理する職員が年 1 回以上情報保護関連内部または外部教育を履修すること	
KR/PR-t4.1.2.2	4.1.2.2 人事 ・認証システムを管理する職員に対して、業務上知得した機密事項の遵守に関する誓約書を作成すること ・管理責任者は、業務環境の変化等により、セキュリティ対策の修正・補完が必要な場合、これを遅滞なく検討・補完すること ・認証システムを管理する職員が人事異動または退職する場合には、内部規定に従いアカウント削除および保存媒体返納等の適切な措置を取ること	
	4.2 危機管理	
	4.2.1 構成	
KR/PR-t4.2.1.1	4.2.1.1 危機管理計画 ・災害、侵害事故等、非常事態の発生に効果的に対処できる危機管理計画および災害復旧手順を策定すること	
KR/PR-t4.2.2.1	4.2.2 管理 4.2.2.1 危機対応 ・認証システムを管理する職員は、災害、侵害事故等、非常事態の発生時、策定された危機管理計画に従い即刻、緊急対応措置を取ること	

	根拠資料	備考
条項番号	条文	

4.3 記録の保管

4.3.1 管理

KR/PR-t4.3.1.1

4.3.1.1 ログ記録

･次のログ記録は、バックアップした日から 2 年以上保管すること

・ネットワークログ記録

・入退管理システムの出入関連監査記録

・侵入監視警報発生事実に対する記録

・CCTV システムの記録

KR/PR-t4.3.1.2

4.3.1.2 管理台帳

･次の管理台帳は、記録した日から 2 年以上保管すること

・ネットワークシステム管理台帳

・認証システム管理台帳

・職員以外の入退台帳

4.4 監査

4.4.1 管理

	根拠資料	備考
条項番号	条文	
KR/PR-t4.4.1.1	4.4.1.1 監査記録 ・管理責任者は、認証システムの監査記録を毎月 1 回以上ハードディスクを除外した保存媒体によりバックアップすること ・バックアップされた監査記録の完全性を保障すること	

韓国

[KR/F] 公認認証局の施設設備基準に関する告示

2002.11.15 施行

根拠資料		備考
条項番号	条文	
KR/F-1.1.1	**第 1 章 総則** **1.1 目的** 1.1.1 この規程は、非対称暗号化方式の電子署名技術に関して、電子署名法施行令第 2 条第 1 項第 3 号の規定による施設及び設備と同項第 4 号の規定による内部規程に関する具体的事項を定めることを目的とする	
KR/F-1.2.1	**1.2 定義** 1.2.1 この規程において使用する用語の定義は次のとおりである	
KR/F-1.2.1.1	ア. 秘密鍵とは、電子署名を生成するために利用する電子的情報をいう	
KR/F-1.2.1.2	イ. 公開鍵とは、電子署名を検証するために利用する電子的情報をいう	
KR/F-1.2.1.3	ウ. 鍵ペアとは、秘密鍵とこれに合致する公開鍵をいう	

根拠資料		備考
条項番号	条文	
KR/F-1.2.1.4	エ. 電子署名認証管理体系(以下、PKI という)とは、公認証明書の発行及び認証関連記録の管理等、公認認証サービスを提供するためのシステムをいう	
KR/F-1.2.1.5	オ. 認証システムとは、加入者の登録情報管理、鍵ペアの生成･管理、公認証明書の生成･発行･管理、タイムスタンプ検証機能等を支援する諸システムであって、公認認証サービスのために公認認証局内に設置された諸システムをいう	
KR/F-1.2.1.6	カ. 監査管理者とは、認証システムの監査記録を検証し管理する者をいう	
KR/F-1.2.1.7	キ. 運営管理者とは、認証システムの運営を担当する者をいう	
KR/F-1.2.1.8	ク. ポリシー管理者とは、認証システムに関連する方針を樹立し、これを管理する者をいう	
KR/F-1.2.1.9	ケ. 登録情報とは、加入者の登録受付番号･名義･住所･電話番号･電子メールアドレス･DN、公認証明書の利用範囲･用途等をいう	
KR/F-1.2.2	1.2.2 この規程において使用する用語の定義は、2.1 において定めるものを除いては、電子署名法において定めるところによる	
KR/F-1.3.1	**1.3 適用範囲** 1.3.1 この規程は、非対称暗号化方式の電子署名技術を利用する公認認証業務に適用する	
KR/F-2.1.1	**第 2 章 施設及び設備** **2.1 加入者登録情報管理設備** 2.1.1 加入者登録情報管理システム 公認認証局は、次の機能を持つ加入者登録情報管理システムを備えていなければならない	
KR/F-2.1.1.1	2.1.1.1 加入者識別機能 ア. PKI 技術規格のうち、証明書 DN 規格([別表]の第 4 号)に基づいて Distinguished Name(以下「DN」という)を付与する機能	

	根拠資料	備考
条項番号	条文	
KR/F-2.1.1.2	2.1.1.2 加入者登録情報管理機能 ア. 登録情報を入力･アクセス･変更･削除する機能 イ. ネットワークによって伝送される登録情報に対する暗号化及び電子署名機能	
KR/F-2.1.1.3	2.1.1.3 監査及びセキュリティ機能 ア. 登録情報を入力･アクセス･変更･削除した事実、時刻、行為者に関する内訳についての監査記録を生成･保存する機能 イ. 次のおそれに対処することのできる機能 ・ 監査記録の偽造･変造及び削除のおそれに対処する機能 ‐監査記録を変更できないようにする保護機能 ‐権限のない者が監査記録を削除できないようにする保護機能 ‐監査記録をバックアップする機能 ・ 登録情報管理ソフトウエアの偽造･変造及び削除のおそれに対処する機能 ・ 登録情報管理ソフトウエアの不法な使用に対処する機能 ‐運営管理者及び監査管理者に対する役割区分及びアクセス制御機能 ‐その他の管理者がいる場合、これに対する役割区分及びアクセス制御機能 ・ 登録情報に対する偽造･変造､削除及び流出のおそれに対処する機能 ‐権限のある者のみがアクセスすることができるようにするアクセス制御機能 ‐登録情報に対する不法な変更を検知することのできる機能	

根拠資料		備考
条項番号	条文	
KR/F-2.1.2.1	2.1.2 加入者登録情報保管設備 2.1.2.1 公認認証局は、加入者登録情報を保管するために公認認証局内に事務空間と分離され、入退管理設備が設置されている別途の空間に施錠付きキャビネットまたは金庫を備えていなければならない。	
KR/F-2.2	**2.2 電子署名キー生成･管理設備** 2.2.1 公認認証機関は、電子署名キー及び電子署名を安全に生成･管理するために次の事項を確保しなければならない。	
KR/F-2.2.1	2.2.1 アルゴリズム ア. 電子署名アルゴリズム ・ PKI 技術規格のうち、電子署名アルゴリズム([別表]の第 10 号)に明示された電子署名アルゴリズム ・ 電子署名アルゴリズムの鍵ペア生成機能 ‐RSA、KCDSA 電子署名アルゴリズムの場合 ・1024 ビット以上の鍵ペアを生成する機能 ・PKI 技術規格のうち、電子署名アルゴリズム([別表]の第 10 号)に提示された標準を満たす乱数、小数及び鍵ペアを生成する機能 ‐楕円曲線基盤の電子署名アルゴリズムの場合 ・160 ビット以上の鍵ペアを生成する機能 ・PKI 技術規格のうち、電子署名アルゴリズム([別表]の第 10 号)に提示された標準を満たすドメイン媒介変数(Domain Parameter)及び鍵ペアを生成する機能 ‐その他の電子署名アルゴリズムの場合 ･RSA1024 ビット以上の安全性に準じる鍵ペアを生成する機能 イ. ハッシュアルゴリズム ・ PKI 技術規格のうち、ハッシュアルゴリズム([別表]の第 11 号)に明示されたハッシュアルゴリズム ・ ハッシュアルゴリズムは SHA-1 160 ビット以上の安全性に準じるハッシュ値生成機能	

根拠資料		備考
条項番号	条文	
	ウ. 暗号アルゴリズム ・ PKI 技術規格のうち、暗号アルゴリズム([別表]の第 12 号)に明示された暗号アルゴリズム ・ 暗号アルゴリズムは SEED 128 ビット以上の安全性に準じる暗号アルゴリズム	
KR/F-2.2.2	2.2.2 公認認証局鍵ペア生成･管理設備 ア. 鍵ペア生成機能 ・ 2.2.1 のアにおいて規定した電子署名アルゴリズムの鍵ペア生成機能 ‐アルゴリズムの種類、鍵の長さ、用途といった鍵ペア生成関連情報を設定･確認することのできる機能 イ. 鍵ペア保護機能 ・ FIPS140-1(または 140-2)レベル 3 を満たす機能 ウ. 電子署名生成機能 ・ 2.2.1 のアにおいて規定した電子署名アルゴリズムを使用して署名する機能 エ. 監査及びセキュリティ機能 ･鍵ペアの生成及び電子署名に関する内訳についての監査記録を生成･保存する機能 ・ 次のおそれに対処することのできる機能 ‐監査記録の偽造･変造及び削除のおそれに対処する機能 ・監査記録を変更できないようにする保護機能 ・権限のない者が監査記録を削除できないようにする保護機能 ・監査記録をバックアップする機能 ‐鍵ペアソフトウエアの不法な使用に対処する機能 ・運営管理者及び監査管理者に対する役割区分及びアクセス制御機能 ・その他の管理者がいる場合、これに対する役割区分及びアクセス制御機能	

根拠資料		備考
条項番号	条文	
	オ. 3 人以上の権限のある職員が共同で鍵ペアを生成･管理する機能 ・ パスワード、ハードウエアトークン、生体認識といったアクセス制御機能により、3 人以上の権限のある職員を識別･確認する機能 カ. 同一の機能を持つ公認認証局鍵ペア管理設備の二重化	
KR/F-2.2.3.1	2.2.3 加入者鍵ペア生成･管理設備 2.2.3.1 公認認証局が加入者鍵ペアを生成･配布する場合、次の機能を持つ加入者鍵ペア生成･管理設備を備えていなければならない ア. 鍵ペア生成機能 ・ 2.2.1 のアにおいて規定した電子署名アルゴリズムの鍵ペア生成機能 ‐アルゴリズムの種類、鍵の長さ、用途といった鍵ペア生成関連情報を設定･確認することのできる機能 イ. 鍵ペア保護機能 ･秘密鍵保存装置 ‐ディスク、スマートカード、USB トークン等といった保存媒体を使用することのできる機能 ‐ディスクに秘密鍵を保存する場合、秘密鍵を安全性が確認された暗号アルゴリズムにより暗号化して保存する機能 ‐暗号化された秘密鍵を保存装置に保存した後、システムの記憶場所(memory)または臨時ファイルに残された秘密鍵及び関連情報をただちに削除する機能 ‐秘密鍵の無欠性を保証するためにメッセージ認証コード(MAC)等の情報を秘密鍵とともに保存する機能	

根拠資料		備考
条項番号	条文	
	ウ. 監査及びセキュリティ機能 ・鍵ペアの生成及び電子署名に関する内訳についての監査記録を生成・保存する機能 ・ 次のおそれに対処することのできる機能 ‐監査記録の偽造・変造及び削除のおそれに対処する機能 ・監査記録を変更できないようにする保護機能 ・権限のない者が監査記録を削除できないようにする保護機能 ・監査記録をバックアップする機能 ‐鍵ペア管理ソフトウエアの不法な使用に対処する機能 ・運営管理者及び監査管理者に対する役割区分及びアクセス制御機能 ・その他の管理者がいる場合、これに対する役割区分及びアクセス制御機能 エ. 2 人以上の権限のある職員が共同で鍵ペアを生成する機能 ・ パスワード、ハードウエアトークン、生体認識といったアクセス制御機能により、2 人以上の権限のある職員を識別・確認する機能	
KR/F-2.3.1	**2.3 公認証明書生成・発行・管理設備** 2.3.1 公認証明書生成・発行設備 公認認証局は、公認証明書と公認証明書の停止・失効リストを安全に生成・発行するために、次の機能を持つ公認証明書生成・発行設備を備えていなければならない	

根拠資料		備考
条項番号	条文	
KR/F-2.3.1.1	2.3.1.1 公認証明書生成･発行機能 ア. 加入者の公認証明書の発行申請処理機能 ・ PKI 技術規格のうち、証明書申請形式([別表]の第 3 号)処理機能 ･秘密鍵が加入者に属しているという事実を確認する機能 ・ 加入者公開鍵に対する秘密鍵保有証明機能 ・ ネットワークによる公認証明書の発行申請時に、PKI 技術規格のうち、証明書管理プロトコル([別表]の第 3 号)を遵守して処理する機能 イ. PKI 技術規格のうち､証明書プロファイル([別表]の第 1 号)を遵守する公認証明書発行機能 ウ. 次の事項についての公認証明書生成ポリシーの設定機能 ・ 電子署名アルゴリズム(2.2.1 のアの電子署名アルゴリズム) ・ 公認証明書の有効期間 ・ 利用範囲または用途 ・ 公認証明書拡張フィールド エ. 公認証明書生成ポリシーの設定機能と公認証明書生成機能を区分して動作する機能 ・ 機能によって別途の管理者を置き、それぞれに対するアクセス制御を遂行する機能 オ. 公認証明書を生成する機能 ・ 設定された生成ポリシーに基づいて公認証明書を生成する機能 ･鍵ペア管理設備の電子署名機能(2.2.2 のウ)を利用して公認証明書を生成する機能	

根拠資料		備考
条項番号	条文	
	カ. 公認証明書について次の事項を検証する機能 ・ 電子署名アルゴリズム ・ 公認証明書の有効期間 ・ 加入者及び発行者の DN ・ 利用範囲または用途 ・ 公認証明書拡張フィールド ・ 公認証明書の停止及び失効の有無 キ. 公認証明書を DER(X.690)形式により発行する機能	
KR/F-2.3.1.2	2.3.1.2 公認証明書の停止･失効リスト生成･管理機能 ア. 加入者の公認証明書の停止、停止解除及び失効の申請を処理する機能 ・ 停止、停止解除及び失効の区分、申請日、事由等を記録する機能 ・ 対象公認証明書の状態が申請の処理に適切かどうかを確認する機能 ・ ネットワークによる公認証明書の停止及び失効の申請･処理時に、PKI 技術規格のうち、証明書管理プロトコル([別表]の第 13 号)を遵守して処理する機能 ・ ネットワークによる公認証明書の停止及び失効の申請･処理時の送受信情報に対する保護機能 イ. 公認証明書の停止･失効リストプロファイルは、PKI 技術規格のうち､証明書の停止･失効リストプロファイル([別表]の第 2 号)を遵守する公認証明書の停止･失効リストの発行機能 ウ. 次の事項について公認証明書の停止･失効リストの生成ポリシーを設定する機能 ・ 電子署名アルゴリズム(2.2.1 のアの電子署名アルゴリズム) ・ 次の発行日 ・ 公認証明書の停止･失効リスト拡張フィールド ・ 次の発行日以前の自動更新または通知機能	

根拠資料		備考
条項番号	条文	
	エ. 公認証明書の停止･失効リストの生成ポリシー設定機能と、公認証明書の停止･失効リストの生成機能を区分して動作する機能 ・ 機能によって別途の管理者を置き、それぞれに対するアクセス制御を遂行する機能 オ. 公認証明書の停止･失効リストを生成する機能 ・ 設定された生成ポリシーに基づいて公認証明書の停止･失効リストを生成する機能 ･鍵ペア管理設備の電子署名機能(2.2.2 のウ)を利用して公認証明書の停止･失効リストを生成する機能 カ. 公認証明書の停止･失効リストについて次の事項を検証する機能 ・ 電子署名アルゴリズム ・ 発行日及び次の発行日 ・ 停止及び失効された公認証明書の一連番号 ・ 停止及び失効された公認証明書の停止及び失効日時、事由 ・ 公認証明書の停止･失効リスト拡張フィールド キ. 公認証明書の停止･失効リストを DER(X.690)形式により発行する機能 ク. 公認証明書が停止された日から 6 カ月後にこれを失効する機能	
KR/F-2.3.1.3	2.3.1.3 加入者証明書等の保管 ア. 加入者の公認証明書とその停止及び失効に関する記録を当該公認証明書が失効した日から 10 年間保管する設備	

根拠資料		備考
条項番号	条文	
	イ．遠隔地保存設備に関する事項 ・ 加入者の公認証明書とその停止及び失効に関する記録を保管する 10km 以上の遠隔地保存設備 ・ 遠隔地保存設備に対する物理的な入退管理設備とキャビネット等の施錠設備 ・ 遠隔地保存設備に対するアクセス内訳を監査記録し、これを保管する機能 ・ 遠隔地保存設備に対する侵入監視設備	
KR/F-2.3.1.4	2.3.1.4 監査及びセキュリティ機能 ア．公認証明書の発行･停止･停止解除･失効･ポリシー設定に関する内訳についての監査記録を生成･保存する機能 イ．次のおそれに対処することのできる機能 ・ 監査記録の偽造･変造及び削除のおそれに対処する機能 ‐監査記録を変更できないようにする保護機能 ‐権限のない者が監査記録を削除できないようにする保護機能 ‐監査記録をバックアップする機能 ・ 公認証明書生成･管理ソフトウエアの偽造･変造及び削除のおそれに対処する機能 ・ 公認証明書生成･管理ソフトウエアの不法な使用に対処する機能 ‐ポリシー管理者、運営管理者及び監査管理者に対する役割区分及びアクセス制御機能 ‐その他の管理者がいる場合、これに対する役割区分及びアクセス制御機能	
KR/F-2.3.1.5	2.3.1.5 公認証明書生成･発行設備の二重化 ア．同一の機能を持つ公認証明書生成･発行設備の二重化 イ．二重化された公認証明書生成･発行設備を利用した非常時の復旧機能	

根拠資料		備考
条項番号	条文	
KR/F-2.3.2	2.3.2 公認証明書公開･有効性検証設備 公認認証局は、公認証明書の公開及び有効性検証のための設備として次の事項を確保しなければならない	
KR/F-2.3.2.1	2.3.2.1 公認証明書、公認証明書の停止･失効リストを公開する機能 ア. 公認証明書、公認証明書の停止･失効リストを登録･削除する機能 イ. 公認証明書、公認証明書の停止･失効リストをLDAP 等の標準化されたプロトコルを利用してつねに検索することができるようにする機能 ・ 当該機能の具現時に、PKI 技術規格のうち、ディレクトリ関連プロトコル([別表]の第 16 号)を遵守	

根拠資料		備考
条項番号	条文	
	ウ. 監査及びセキュリティ機能 ・ 公認証明書、公認証明書の停止･失効リストを登録･管理した事実、時刻、行為者に関する内訳についての監査記録を生成･保存する機能 ・ 次のおそれに対処することのできる機能 ‐監査記録の偽造･変造及び削除のおそれに対処する機能 ・監査記録を変更できないようにする保護機能 ・権限のない者が監査記録を削除できないようにする保護機能 ・監査記録をバックアップする機能 ‐公認証明書、公認証明書の停止･失効リスト公開ソフトウエアの偽造･変造及び削除のおそれ等に対処する機能 ‐公認証明書、公認証明書の停止･失効リスト公開ソフトウエアの不法な使用に対処する機能 ・運営管理者及び監査管理者等に対する役割区分及びアクセス制御機能 ・その他の管理者がいる場合、これに対する役割区分及びアクセス制御機能 ‐公認証明書、公認証明書の停止･失効リストの削除のおそれに対処する機能 ・権限のある者のみがアクセスすることができるようにするアクセス制御機能 エ. 公認証明書、公認証明書の停止･失効リスト公開設備の二重化 ・ 同一の機能を持つ公認証明書、公認証明書の停止･失効リスト公開設備の二重化 ・ 二重化された公認証明書、公認証明書の停止･失効リスト公開設備を利用した非常時のリアルタイム復旧機能	

根拠資料		備考
条項番号	条文	
KR/F-2.3.2.2	2.3.2.2 公認証明書の有効性検証機能 ア. 公認証明書の有効性の有無確認を提供する機能 ・ 当該機能の具現時に、PKI 技術規格のうち、証明書の有効性検証技術規格([別表]の第 8 号)を遵守 イ. 監査及びセキュリティ機能 ・ 公認証明書の有効性検証を行った事実、時刻、申請者に関する内訳についての監査記録を生成･保存する機能 ・ 次のおそれに対処することのできる機能 ‐監査記録の偽造･変造及び削除のおそれに対処する機能 ・監査記録を変更できないようにする保護機能 ・権限のない者が監査記録を削除できないようにする保護機能 ・監査記録をバックアップする機能 ‐公認証明書の有効性検証ソフトウエアの偽造･変造及び削除のおそれ等に対処する機能 ‐公認証明書の有効性検証ソフトウエアの不法な使用に対処する機能 ・運営管理者及び監査管理者に対する役割区分及びアクセス制御機能 ・その他の管理者がいる場合、これに対する役割区分及びアクセス制御機能 ‐公認証明書の有効性検証システムの秘密鍵を流出･複製するおそれに対処する機能 ・権限のある者のみがアクセスすることができるようにするアクセス制御機能 ウ. 公認証明書の有効性検証設備の二重化 ・ 同一の機能を持つ公認証明書の有効性検証設備の二重化 ・ 二重化された公認証明書の有効性検証設備を利用した非常時のリアルタイム復旧機能	

根拠資料		備考
条項番号	条文	
KR/F-2.4	**2.4 タイムスタンプ検証設備** 公認認証局は、信頼できるタイムスタンプ検証サービスのために次の事項を確保しなければならない。	
KR/F-2.4.1.1	2.4.1 タイムスタンプ受信機能 2.4.1.1 タイムスタンプ受信装置がタイムスタンプソースからタイムスタンプを受信する機能 ア. PKI 技術規格のうち、タイムスタンプ検証プロトコル([別表]の第 15 号)に基づいてタイムスタンプを受信する機能 イ. 千分の 1 秒まで時間を表現する機能 ウ. タイムスタンプ受信装置に問題が発生した場合、これを管理者に知らせる機能 エ. タイムスタンプソースからのタイムスタンプ受信が中止しても 24 時間以上正確な時間を提供する機能	
KR/F-2.4.1.2	2.4.1.2 タイムスタンプ検証システムの時間を保証する機能 ア. タイムスタンプ受信装置が提供する時間を利用してタイムスタンプ検証システムのタイムスタンプを保証する機能 ・ タイムスタンプ検証システムの時間に対して正確なタイムスタンプ保証がなされた後、タイムスタンプ検証サービスが始まる機能 ・ 継続的にタイムスタンプ保証機能を提供する機能 イ. タイムスタンプ保証機能にエラーが発生した場合、これについてのエラーメッセージ出力機能 ・ タイムスタンプ保証機能にエラーが発生した場合あるいは正確なタイムスタンプ提供が不可能な場合、ただちにタイムスタンプ検証サービスが自動的に中止する機能	

	根拠資料	備考
条項番号	条文	
KR/F-2.4.2.1	2.4.2 タイムスタンプ検証サービス 2.4.2.1 電子文書のタイムスタンプを確認することのできるタイムスタンプ検証サーバプログラム ア. PKI 技術規格のうち、タイムスタンプ検証プロトコル([別表]の第 14 号)を遵守してタイムスタンプ検証サービスを提供する機能 イ. 2.2.1 のア及びイにおいて規定したアルゴリズムを利用してタイムスタンプ検証サービスを提供する機能 ウ. 使用者が受信したタイムスタンプ検証トークンに記録されたタイムスタンプが発行記録時間と一致するかどうかを確認する機能 エ. 鍵ペア管理設備の電子署名機能を利用したタイムスタンプ検証サービスの提供	
KR/F-2.4.2.2	2.4.2.2 監査及びセキュリティ機能 ア. 次の事項についての監査記録を生成･保存する機能 ・ タイムスタンプ保証の内容についての記録 ・ タイムスタンプ検証の事実、タイムスタンプ、行為者、申請者 ・ タイムスタンプ非同期等の問題発生の事実、タイムスタンプ ・ タイムスタンプ検証サービス提供の遅延の事実、タイムスタンプ、申請者	

根拠資料		備考
条項番号	条文	
	イ. 次のおそれに対処することのできる機能 ・ 監査記録の偽造･変造及び削除のおそれに対処する機能 ‐監査記録を変更できないようにする保護機能 ‐権限のない者が監査記録を削除できないようにする保護機能 ‐監査記録をバックアップする機能 ・ タイムスタンプ検証ソフトウエアの偽造･変造及び削除のおそれ等に対処する機能 ・ タイムスタンプ検証ソフトウエアの不法な使用に対処する機能 ‐運営管理者及び監査管理者に対する役割区分及びアクセス制御機能 ‐その他の管理者がいる場合、これに対する役割区分及びアクセス制御機能 ‐タイムスタンプ検証システムの管理者であっても時間を変更する機能を使用できないように制限する機能	
KR/F-2.5.1	**2.5 保護設備** 2.5.1 ネットワーク及びシステムのセキュリティ設備 公認認証局は、公認認証業務を提供するネットワーク及び認証システムを保護するために次の事項を確保しなければならない。	

	根拠資料	備考
条項番号	条文	
KR/F-2.5.1.1	2.5.1.1 ネットワークのセキュリティ機能 ア. 二重化されたネットワーク設備 ・ 2 回線以上のネットワーク回線 ‐物理的に分離された 2 回線以上のネットワーク回線を使用 ‐相互に異なる 2 回線以上の ISP(または IX)からの回線を使用 ‐1 回線に障害が発生しても公認認証サービスを持続して提供することのできる機能 ‐ネットワーク回線を公認認証業務専用に使用 ・ 2 系統以上の経路(path)を提供する内部ネットワークの構成 ‐1 経路に異常が発生しても公認認証サービスを持続して提供 ・ ルータを二重化して使用 ‐パケットフィルタリング機能を支援するルータを使用 ・ 監査記録･保存機能 ‐ネットワーク設備及びシステムにおいて生成するネットワーク関連の主要情報に関する内訳 イ. ネットワークのセキュリティ設備 ・ 侵入遮断システムの運営 ‐侵入遮断システムの二重化 ‐K4 等級以上の侵入遮断ソフトウエアの使用 ‐公認認証業務に限定されたアクセス制御ルールを設定して使用	

根拠資料		備考
条項番号	条文	
	・ 侵入検知システムの運営	
	‐K4 等級以上の侵入検知ソフトウエアの使用	
	‐サービス妨害攻撃検知機能	
	‐すべてのトラフィックに対する検査及び侵入検知機能	
	‐新たなパターンの侵入類型に対する追加機能	
	‐侵入検知された場合、これを管理者に知らせる機能	
	ウ. ネットワーク及びシステム管理設備	
	・ リアルタイムでネットワーク及びシステムの状態を検査することのできるシステムまたは設備の運営	
	･公認認証業務に関連する主要プログラムまたはプロセスの動作の有無を検査することのできるシステムまたは設備の運営	
	エ. その他の設備	
	･公認認証業務に関連して運営しているその他の設備に対する管理方針の整備	
KR/F-2.5.1.2	2.5.1.2 システムのセキュリティ機能	
	ア. 安全で信頼できる認証システムの運営	
	・ 管理者別にアカウントの分離設定及びアクセス制御	
	・ 必要最小限のユーザ登録	
	・ 公認認証業務に必要なソフトウエアのみ実装･運営	
	･公認認証業務に必要なプログラムまたはプロセスのみ実行	
	・ プログラムに対するパッチの遂行	
	・ 運営体系(OS)に対するパッチの遂行	
	・ システム及び関連ソフトウエアに対する維持保守契約の確認	

根拠資料		備考
条項番号	条文	
	イ．認証システム運営に関する情報についての監査記録を生成･保存する機能 ・ システムの始動／停止 ・ ルート及びユーザのログイン／ログアウト ・ ユーザカウントの追加／削除、権限の変更	
KR/F-2.5.2	2.5.2 物理的セキュリティ設備 公認認証局は、認証システム及び主要設備を保護するために次の事項を確保しなければならない	

	根拠資料	備考
条項番号	条文	
KR/F-2.5.2.1	2.5.2.1 認証システム運営室 ア. 認証システムを安全に運営することのできる別途の管理区域の設置 ・ 次の認証システムを別途の運営室に分離 ‐加入者登録情報管理機能を提供する設備、公認認証局鍵ペア管理、証明書生成･発行機能を提供する設備は同一運営室に設置することができるが、他の設備とは別途の運営室に分離 ‐証明書公開機能を提供する設備は他の設備とは別途の運営室に分離 ‐証明書の状態確認機能を提供する設備、タイムスタンプ検証機能を提供する設備は同一運営室に設置することができるが、他の設備とは別途の運営室に分離 ・ 認証システム運営室の外壁(認証システム運営室の外部と接する面)は外部からの侵入から公認認証業務の提供に必須の認証システムを保護することができるように設計 ‐外壁の材質は、煉瓦または鉄筋コンクリートで築造されており、または鉄骨構造物に 3T 以上の鉄板で溶接 ‐外壁は天井、床まで完全に接合 ・ 運営室を分離することができるように認証システム運営室の内壁(認証システム運営室の内部壁面)を設計 ‐認証システム運営室の内壁及び廊下と接する内壁の材質は、煉瓦で築造されており、または鉄骨構造物に 1.8T 以上の鉄板で溶接 ‐内壁は天井、床まで完全に接合(消防法上の換気口は許容可能) ・ 認証システム運営室の出入口の物理的な入退管理機能 ‐ガラスドアの場合、強化ガラス ‐一般のドアの場合、強化及び防火機能	

根拠資料		備考
条項番号	条文	
	イ. 強化ガラスの窓、通風窓の遮蔽板	
	・ 窓が設置されている場合	
	‐窓は強化ガラスまたは強化フィルムでコーティングしたガラスを使用	
	‐窓を利用して廊下、またはある運営室から他の運営室に侵入できないよう、運営室をつなぐ窓及び窓外部の支持台の除去	
	‐建物外部から内部が覗き込まれないよう、コーティング等の処理	
	・ 通風窓が設置されている場合	
	‐通風窓の大きさが人間が通り抜けられる場合、遮蔽板を設置	
KR/F-2.5.2.2	2.5.2.2 多重入退管理設備	
	ア. 認証システム運営室への入出を管理し、監査記録機能を持つ入退管理設備	
	・ 無許可者が認証システム運営室に接近できないようにする物理的な入退管理	
	・ 入退管理設備は次の情報についての監査記録	
	‐当該レコード識別者	
	‐事件の類型、成功／失敗いずれか及び失敗時の原因	
	‐日付及び時刻	
	‐行為者	
	イ. 生体特性と所持品による本人確認機能を結合して使用する入退管理設備	
	・ 生体特性による本人確認(指紋認識、虹彩認識等)	
	・ 所持品による本人確認(鍵、カード等)	
	ウ. 認証システム運営室に接近時、他の人間が代わりに立ち入り、または後について立ち入る行為を防止する設備	
	エ. 停電時にも入退管理及び監査記録を可能にする機能	

根拠資料		備考
条項番号	条文	
KR/F-2.5.2.3	2.5.2.3 侵入検知･警報及び監視･管理設備 ア. 認証システム運営室に対して物理的な侵入を検知し、これを警報する設備 ・ 侵入検知及び警報機能 ‐運営室内に振動検知設備、音響検知設備等の侵入検知設備の設置 ‐侵入検知設備に異常が発生したとき、これを検知する機能 ‐侵入検知設備が侵入を検知した場合、管理者にただちに知らせる機能 ・ 侵入検知･警報設備と連動する侵入発生位置確認機能 イ. 認証システム運営室を監視･管理し、これについての監査記録機能を持つ設備 ・ 侵入監視機能 ‐CCTV の設置 ‐監視設備は、24 時間リアルタイムで監視する機能 ‐CCTV システムは、すべての立入行為について録画する機能 ‐CCTV システムに対するアクセス制御機能 ‐CCTV システム管理用パスワードに対する保護機能 ・ 多重入退管理設備からの立入現況情報確認機能 ‐正当な管理者のみが監査記録を検証 ‐時間別、行為者別、事件の種類等の多様な条件による監査記録の検索機能 ‐入退管理システム監査記録の保存空間消尽に対する対策 ‐入退管理システムに対するアクセス制御機能 ‐入退管理システム管理用パスワードに対する保護機能 ‐監査記録をバックアップする機能	

根拠資料		備考
条項番号	条文	
KR/F-2.5.2.4	2.5.2.4 物理的施錠設備 ア. 管理区域内の認証システム、侵入遮断システム及びネットワーク設備等への接近を物理的に制御するセキュリティキャビネット イ. 秘密鍵、加入者の公認証明書等の重要資料への接近を物理的に制御する金庫または施錠設備が設置されたキャビネット ウ. 施錠設備の鍵を別途の保管容器に管理	
KR/F-2.5.2.5	2.5.2.5 災害予防設備 ア. 火災発生時にこれを早期に検知し鎮火する設備 ・ 火災警報設備 ‐煙検知設備、温度検知設備等の火災警報設備の設置 ・ 火災消火設備 ‐小規模及び大規模火災に対処することができるよう設置 ‐誤動作に対処することのできる機能 ‐火災消火設備動作時にシステムに悪影響を及ぼさないにすること イ. 水害予防設備 ・ 認証システム、侵入遮断システム及びネットワーク設備等が水に露出しないように床から 30cm 以上高いところに設置 ・ コンセント等の電源接続設備は、床から 30cm 以上高いところに設置 ウ. 停電発生時に持続して認証業務の遂行が可能なように、一定期間電源を供給する電源供給設備 ・ 自家発電設備及び無停電電源供給設備 ‐停電発生時に持続して認証業務の遂行が可能なように、30 分以上電源を供給することのできる設備 ‐自家発電設備の場合、追加の燃料の補充なしに 2 時間以上発電し電源を供給することのできる機能	

根拠資料		備考
条項番号	条文	
	エ. 温度及び湿度を一定に維持するための恒温恒湿設備の設置 オ. その他 ・ 各種電源設備に対するアース施設 ・ 非常時に備えた全地域の誘導灯及び誘導標識の設置	
KR/F-2.6	**2.6 加入者設備** 公認認証局は、公認認証業務に関連して加入者に次の事項を満たすソフトウエアを提供しなければならない。	
KR/F-2.6.1	2.6.1 鍵ペア管理機能 ア. 2.2.1 のアにおいて規定した電子署名アルゴリズムを使用して鍵ペアを生成する機能 イ. 秘密鍵を暗号化して秘密鍵保存装置に保存する機能 ･秘密鍵を PKCS#5 により暗号化する機能 ･秘密鍵を暗号化する際、2.2.1 のウにおいて規定した暗号アルゴリズムを使用して秘密鍵を暗号化し保存する機能 ・ PKCS#5 により暗号化された秘密鍵を PKCS#8 により保存する機能 ･秘密鍵の保存に関連する事項は､PKI 技術規格のうち、相互連動技術規格([別表]の第 6 号)を遵守 ウ. 秘密鍵を生成して別途の保存装置に保存した後､秘密鍵をただちに記憶場所(memory)または臨時ファイルから削除する機能	

根拠資料		備考
条項番号	条文	
KR/F-2.6.2	2.6.2 公認証明書管理機能 ア. 公認証明書管理プロトコル機能 ・ 公認証明書の申請形式生成時に、PKI 技術規格のうち、証明書申請形式([別表]の第 3 号)を遵守 ・ ネットワークによる公認証明書の発行、再発行、更新、停止、失効の申請時に、PKI 技術規格のうち、証明書管理プロトコル([別表]の第 13 号)を遵守 ・ 公認認証局から受信した応答メッセージを処理することのできる機能 イ. 公認証明書保存機能 ・ 加入者公認証明書の保存に関連する事項は、PKI 技術規格のうち、相互連動技術規格([別表]の第 6 号)を遵守 ウ. 公認証明書検証機能 ・ 公認証明書を検証する機能 ・ 公認証明書であることを表示する機能は、PKI 技術規格のうち、公認証明書の表示のための技術規格([別表]の第 7 号)を遵守 ・ 公認証明書の停止･失効リストを検証する機能 エ. 鍵ペアと公認証明書の伝達機能 ･鍵ペアと公認証明書を PKCS#12 形式により送る機能 ･鍵ペアと公認証明書を PKCS#12 形式により読み込む機能 オ. 最上位認証局の証明書の信頼性を確認する機能 ・ PKI 技術規格のうち、相互連動技術規格([別表]の第 6 号)を遵守	
KR/F-2.6.3	2.6.3 電子署名及び公認証明書検証機能 ア. 公認証明書検証機能 ・ 公認証明書の経路構築機能 ・ 公認証明書の状態確認機能 ・ PKI 技術規格のうち、証明書検証技術規格([別表]の第 9 号)を遵守	

根拠資料		備考
条項番号	条文	
	イ. 電子署名生成及び検証機能 ・ 電子署名機能(PKCS#7 等) ・ 電子署名を検証する機能	
KR/F-2.6.4	2.6.4 タイムスタンプ検証機能 使用者がタイムスタンプ検証サービスの提供を受ける場合、次の機能を満たさなければならない ア. タイムスタンプ検証サービスを申請し応答を保存、検証することのできる機能 ・ タイムスタンプ検証サービスを申請する機能 ‐タイムスタンプ検証すべき文書に対するハッシュ値を生成 ‐PKI 技術規格のうち、タイムスタンプ検証プロトコル([別表]の第 14 号)を遵守するタイムスタンプ検証申請形式データの生成機能 ・ 当該申請に対するタイムスタンプ検証トークンを受信する機能 ・ タイムスタンプ検証トークンを検証する機能 ・ 原本ファイルとタイムスタンプ検証トークンを保管、検索することのできる機能 ‐タイムスタンプ検証トークンを原本ファイルとリンクして検索することのできる機能	
KR/F-2.6.5	2.6.5 加入者ソフトウエアのバージョン管理 ア. 公認認証局が提供する加入者ソフトウエアを利用時に、ソフトウエアのバージョンを加入者が確認することのできる機能 イ. 加入者ソフトウエアの変更時に、加入者に変更後のソフトウエアを配布する機能	
KR/F-3.1	**第 3 章 内部規程** 3.1 公認認証局は、公認認証業務を遂行するに当たって次の事項に該当する施設及び設備の管理･運営手続き及び方法を整備しなければならない	

条項番号	根拠資料 条文	備考
KR/F-3.2	**3.2 公認認証局鍵ペア管理に関する事項** ア．公認認証局の鍵ペアに対する生成･バックアップ･破棄に関する事項 イ．公認認証局の秘密鍵の紛失及びき損時の対応に関する事項 ウ．公認認証局の鍵ペア管理台帳の配備に関する事項	
KR/F-3.3	**3.3 公認証明書管理に関する事項** ア．公認証明書発行のための加入者登録手続き及び提出書類に関する事項 イ．加入者登録情報及び提出書類の管理に関する事項 ウ．公認証明書の発行･再発行･失効･有効期間の更新及び公開に関する事項 エ．公認証明書の停止及び失効情報の生成･公開に関する事項	
KR/F-3.4	**3.4 施設及び設備の管理等に関する事項** ア．ソフトウエア･システム･ネットワーク･物理的設備等のアクセス制御に関する事項 イ．ソフトウエア･システム･ネットワーク･物理的設備等の変更及び維持保守に関する事項 ウ．監査ログの記録･バックアップ･管理に関する事項 エ．各種管理台帳の整備に関する事項 ・ スマートカード等のハードウエアトークン管理台帳 ・ パスワード管理台帳 ・ 鍵管理台帳 ・ メディア管理台帳 ・ (外部者) 入退管理台帳	

条項番号	根拠資料 条文	備考
KR/F-3.5	**3.5 災害復旧に関する事項** ア. 障害及び災害発生時の非常計画 ・ 非常連絡網 ・ 非常対応手続き ・ 非常対応マニュアル イ. 運営データ、ソフトウエア、システム、設備に対するバックアップ計画 ・ バックアップ周期、手続き及び場所 ・ バックアップが必要なリソースの定義 ・ リソースに対するバックアップの優先順位及び責任者 ・ 遠隔地バックアップ ウ. 運営データ、ソフトウエア、システム及び設備に対する復旧計画 ・ リソース別の復旧の優先順位、手続き及び復旧責任者	
KR/F-付則	**付則** ①(施行日) この規程は告示した日から施行する ②(経過措置) 2.2.2 のイ(鍵ペア保護機能)の規定は、公認証明書生成･発行･管理設備の場合には告示後 1 年、それ以外の設備の場合には告示後 2 年が経過した日から施行し、2.2.2 のウ(電子署名生成機能)の楕円曲線基盤の電子署名アルゴリズムを使用して電子署名を生成する場合の規定は告示後 2 年が経過した日から施行する	

根拠資料		備考
条項番号	条文	
KR/F- 別表.1	**[別表]** 電子署名 PKI 技術規格 **1. 証明書プロファイル** 有線　・TTAS.KO-12.0012、「証明書プロファイル標準」 無線　・TTAS.KO-12.0016、「無線電子署名証明書プロファイル標準」	
KR/F- 別表.2	**2. 証明書の停止･失効リストプロファイル** 有線　・TTAS.KO-12.0013、「証明書の停止･失効リストプロファイル標準」 無線　・TTAS.KO-12.0017、「無線電子署名証明書の停止･失効リストプロファイル標準」	
KR/F- 別表.3	**3. 証明書申請形式** 有線　オンライン オフライン 無線　オンライン　・KCAC.WCRMF、「無線証明書申請形式プロトコル規格 v1.31」 オフライン	
KR/F- 別表.4	**4. 証明書 DN 規格** 有線　・KCAC.DN、「証明書 DN 規格 v1.00」 無線　・KCAC.WDN、「無線電子署名証明書 DN 規格 v1.21」	
KR/F- 別表.5	**5. 証明書 OID 規格** ・KCAC.OID、「電子署名 PKI OID 規格 v1.10」	

根拠資料		備考
条項番号	条文	
KR/F- 別表.6	**6. 相互連動技術規格** ・KCAC.IACA、「公認認証局間の相互連動技術規格 v1.00」 ・KCAC.UI、「公認認証局間の相互連動のためのユーザインタフェース技術規格 v1.00」 ・KCAC.SC、「PKI 関連スマートカード技術規格 v1.00」	
KR/F- 別表.7	**7. 公認証明書の表示のための技術規格** ・KCAC.NSACA、「公認証明書の表示のための技術規格 v1.00」	
KR/F- 別表.8	**8. 証明書の有効性検証技術規格** ・KCAC.OCSP、「リアルタイム証明書状態確認技術規格 v1.00」	
KR/F- 別表.9	**9. 証明書検証技術規格**	
KR/F- 別表.10	**10. 電子署名アルゴリズム** RSA KCDSA ・TTAS.KO-12.0001/R1、「付加型電子署名方式標準‐第 2 部：証明書基盤電子署名アルゴリズム」 ECDSA ・TTAS.KO-12.0021、「無線電子署名アルゴリズム標準」	
KR/F- 別表.11	**11.ハッシュアルゴリズム** SHA-1 HAS-160 ・TTAS.KO-12.0011/R1、「ハッシュ関数標準‐第 2 部：ハッシュ関数アルゴリズム標準(HAS-160)」	
KR/F- 別表.12	**12. 暗号アルゴリズム** 3-DES SEED ・TTAS.KO-12.0004、「128 ビットブロック暗号アルゴリズム標準」	

根拠資料		備考
条項番号	条文	
KR/F- 別表.13	**13. 証明書管理プロトコル** 有線 無線　・KCAC.WCMP、「無線証明書管理プロトコル規格 v1.31」	
KR/F- 別表.14	**14. タイムスタンプ検証プロトコル**	
KR/F- 別表.15	**15. タイムスタンプ検証プロトコル**	
KR/F- 別表.16	**16. ディレクトリ関連プロトコル(LDAP)** LDAP 運営プロトコル LDAP の属性形式定義 DN の UTF-8 表記 LDAP 検索フィルタのストリーミング表現 LDAP の URL 形式 LDAP スキーマ	
KR/F- 別表.17	**17. 本人確認技術規格** ・KCAC.SIVID、「識別番号を利用した本人確認技術規格 v1.11」	
KR/F- 別表.18	**18. 官民相互連携技術規格** ・KCAC.CTL、認証局間の相互連動のための CTL 技術規格 v1.01	