第29回HPKI専門家会議　【資料２】ドキュメント確認箇所リスト
過去の専門家会議発言および構成員からの意見聴取シート結果を記載

項番	ドキュメント名	項目	ご意見	現行記載内容	修正案
CA鍵更新に関係するもの					
1		5.6	鍵の切り替えに関する詳細な手順等を示すべき。CPSで詳述するのであれば、その旨を記すべき。	5.6　鍵の切り替え 認証局は、15年に一度ルートCA私有鍵の更新を行う。ルートCA私有鍵は、認証設備室内にて、複数人の立会いのもと、専用の暗号モジュール（HSM）を用いて生成される。 ルートCA私有鍵の更新と共にルートCA証明書の更新も実施される。この更新においてもルートCA私有鍵生成の場合と同様に、複数人の立会いのもと執り行われる。 サブCA証明書については、加入者からの更新依頼がある場合、サブCA私有鍵の有効期間に応じて5年から10年に一度更新を行う。	
2	ルート認証局CP/CPS	6.3.2	公開鍵証明書の有効期間と鍵ペアの使用期間の項は大幅に改訂する必要があります。SubCAの私有鍵の使用期限は１６年になりますし、あくまでもCRL署名に限定する必要があります。	6.3.2　公開鍵証明書の有効期間と鍵ペアの使用期間 私有鍵と公開鍵の有効期間については、表6-1に示す。	
3	ルート認証局CP/CPS	6.3.2	それ以外にARLの発行に関して、「CRL署名が必要でなくなった場合」が必要で、これを記載することがRFC5820に違反しないことも検証が必要です。準拠しているとCPに明記していますから。	表 6-1 鍵の有効期間 | | 私有鍵有効期間 | 公開鍵有効期間 | | 本認証局 | 15 年 | 30 年 | | サブ CA | 10 年以下 | 20 年以下 |	
4	ルート認証局CP/CPS	6.3.2	また６年間ではありますが、同一のSubCA運営者に対して、二つのSubCAに対してRootCAとして証明書を発行する必要がありますが、無条件で複数のSubCAを運用して良いわけではなく、その認証基準を加筆する必要もあると思います。		
5	ルート認証局CP/CPS	6.3.2	上記をすべてやると、大規模改訂になり、OIDの変更も必要で、各SubCAの同意も必要です。		
6	ルート認証局CP/CPS	6.3.2	HPKIとしてRootCAのCPのOIDが変更になるというのは大事件ですので、公知がおよび猶予期間のトラストの扱いも決めなければならないと思います。		
7	認証局署名用証明書ポリシ、認証局認証用（人）証明書ポリシ	6.2.10	CA私有鍵の廃棄についてHSMを完全に初期化するとか物理的破壊と書いてあるが本当にするのか？記載の見直しを行った方がよいのではないか	6.2.10　私有鍵の廃棄方法 CA私有鍵を破棄しなければならない状況の場合、認証局室内でCP「6.2.2　私有鍵の複数人によるコントロール」と同じく、複数名の権限を有する者によって、私有鍵の格納されたHSM を完全に初期化し、又は物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続きによって破棄する。 加入者私有鍵破棄手続きは、CPS又は加入者が入手可能な文書に記述するものとする。	

8	認証局署名用証明書ポリシ、認証局認証用（人）証明書ポリシ	6.3.2	サブCA鍵更新対応、暗号移行対応のため私有鍵の使用期限について10年より後でもCRLに署名できるような記載に修正する必要がある。	6.3.2　公開鍵証明書の有効期間と鍵ペアの使用期間 CA公開鍵証明書の有効期間は20年を越えないものとし、その私有鍵の使用は10年を越えないものとする。ただし、10年の私有鍵有効期間を延長する必要がある場合にはHPKI認証局専門家会議の承認を得て、最大1年の範囲において必要な期間に限り延長することができる。 エンドエンティティの加入者の公開鍵証明書の有効期間は、発行の日後の加入者の5回目（加入者が発行を受けている署名用電子証明書の有効期間が満了する日の前に、CPSで定める更新の期間内に加入者が新たな署名用電子証明書の発行の申請をし、新たな署名用電子証明書の発行を受けるときにあっては6 回目）の誕生日とする。	
リモート署名に関係する物					
9	リモート署名サービス評価基準	1.1	また、電子処方箋におけるリモート署名サービスのシステム構成と、図1との関係を同節の図2にて解説した。とあるが、保健医療福祉分野における評価基準に対応するため、新たな適用サービスが出たタイミングで電子処方箋に特化した記載と同様に追記するのか、汎用的な記載を検討するのか。 新たなサービスが評価基準を適用できるよう、予め汎用的な記載を追加することで、適用範囲を拡大できる可能性を検討してみてはいかがか。	1.1 本評価基準の位置づけ 本評価基準は、保健医療福祉分野におけるリモート署名サービスの評価基準を定めるものである。本書で は、1.4 節の図 1 で示すリモート署名サービスを構成する独立した複数のコンポーネントに対してそれぞれの 要求事項を定めているため、評価基準は複数の文書から構成される。また、電子処方箋におけるリモート署 名サービスのシステム構成と、図 1 との関係を同節の図 2 にて解説した。	
10	監査報告書（鍵管理）（デジタル署名生成）	全般	デジタル庁での検討と歩調を合わせるのか、それとも厚生労働省独自の基準の策定を目指すのかを明確にすべき。		
11	監査報告書（鍵管理）	全般	レベルの考え方をどうするか。デジタル庁が公開している基準に関する報告書では、リモート署名サービス事業者の基準として3レベルの保証レベルを規定している。 HPKIとして要求する保証レベルは一つに集約するにしても、デジタル庁の示すレベルとの関係を示す必要があるか。		

12	監査報告書（鍵管理）	18	「ISO/IEC 19790 またはFIPS PUB 140-2レベル3で特定される要件」では今回の実装（分散署名等による）は評価できない。鍵管理の安全性評価のために今回の実装にも適用可能な要件を定める必要がある。	SSASC と証明書生成サービスコンポーネントが別々に管理される場合で、サブジェクトの鍵ペアがCAによって生成されている場合、SSASC は 国に認定された信頼できるCAから直接、安全に署名鍵をインポートするものとする（SHALL)。 （例）CAから直接安全に署名鍵をインポートする手段は、以下が考えられる ・インターネットとの接合点は持たないセキュアな回線を用いる サブジェクトの署名鍵を格納する暗号モジュールは、「保健医療福祉分野PKI 認証局署名用証明書ポリシ1.9版　6.2.11　暗号モジュールの評価」の基準を満たすものとする。 保健医療福祉分野PKI 認証局署名用証明書ポリシ1.9版　6.2.11　暗号モジュールの評価 CA私有鍵を格納する暗号モジュールは、 FIPS 140 2 レベル 3 と同等以上のものを使用する。 エンドエンティティの加入者の私有鍵を格納する暗号モジュールは、FIPS 140 2 レベル 1 と同等以上のものを使用する。	
13	監査報告書（鍵管理）	162	「ISO/IEC 19790 またはFIPS PUB 140-2レベル3で特定される要件」では今回の実装（分散署名等による）は評価できない。鍵管理の安全性評価のために今回の実装にも適用可能な要件を定める必要がある。	― 使用されるSCDevは、ISO/IEC 19790 またはFIPS PUB 140-2レベル3で特定される要件を満たすべきである(SHOULD)。	
その他					
14	ルート認証局CP/CPS	5	最新のJIS Q 27002:2024を引用すべき	5　建物・関連設備、運用のセキュリティ管理 これらは、JIS Q 27002:2006と同等以上の規格、又は認可された認定あるいは免許基準に従うものとする。これは、次の項目をカバーする。	5　建物・関連設備、運用のセキュリティ管理 これらは、JIS Q 27002:2024と同等以上の規格、又は認可された認定あるいは免許基準に従うものとする。これは、次の項目をカバーする。
15	ルート認証局CP/CPS	5.2	最新のJIS Q 27002:2024を引用すべき	5.2 手続的管理 手続的管理は、JIS Q 27002:2006 と同等以上の規格に従うものとする。	5.2 手続的管理 手続的管理は、JIS Q 27002:2024 と同等以上の規格に従うものとする。
16	ルート認証局CP/CPS	5.4	最新のJIS Q 27002:2024を引用すべき	5.4 監査ログの取扱い セキュリティ監査手続きは、JIS Q 27002:2006と同等以上の規格に従うものとする。	5.4 監査ログの取扱い セキュリティ監査手続きは、JIS Q 27002:2024と同等以上の規格に従うものとする。
17	ルート認証局CP/CPS	5.8	終了後であってもかつて生成された署名の検証が可能となるような情報（トラストアンカーの履歴、CRL/ARL等）の保存が必要。また、それらの情報の保存期間を明示すべき。	5.8　認証局又は登録局の終了 1. 本認証サービスの廃止日までに有効期間の残っている全てのサブCA証明書を失効し、その失効リストはリポジトリに5年間公開する。 2. 本認証サービスを廃止する場合、廃止日の90日前までに加入者に書面で通知するとともに、リポジトリに廃止理由を公開する。 3. 廃止時には、ルートCA私有鍵を完全に初期化し、そのバックアップ媒体を物理的に完全に破壊する。	

18	ルート認証局CP/CPS	6.1.5	2030年問題を配慮した鍵長を採用できるように記載すべき。 RSA2048ビットは2030年以降の使用は望ましくなく、エンドエンティティのRSA1024ビットは既に利用が推奨されない状況である。	6.1.5　鍵のサイズ 本認証局で生成する鍵のサイズは、下記のとおりとする。 本認証局の鍵のサイズは、RSAアルゴリズムの2048ビット サブCAの鍵のサイズは、RSAアルゴリズムの2048ビット ＜認証局ポリシの記述＞ 6.1.5 鍵のサイズ 鍵の最小サイズは、使用されるアルゴリズムに依存する。CA 証明書の鍵の最小サイズ は、RSA アルゴリズムの場合、2048 ビットとする。他のアルゴリズムを使用する CA 証 明書の鍵の最小サイズは、同等のセキュリティを提供するサイズとする。 エンドエンティティの証明書の鍵の最小サイズは、RSA アルゴリズム又は技術的に同 等のアルゴリズムの場合、1024 ビットとする。他のアルゴリズムを使用するエンドエン ティティの証明書の鍵の最小サイズは、同等のセキュリティを提供するサイズとする。	
19	ルート認証局CP/CPS	6.2.1	FIPS 140-3 への対応も含めるべき。	6.2.1　暗号モジュールの標準及び管理 ルートCA私有鍵の格納モジュールは、US FIPS 140-2レベル3と同等以上の規格に準拠するものとする。	
20	ルート認証局CP/CPS	6.2.11	FIPS 140-3 への対応も含めるべき。	6.2.11 暗号モジュールの評価 ルート CA 私有鍵を格納する暗号モジュールは、FIPS 140-2 レベル 3 と同等以上のも のを使用する。	
21	ルート認証局CP/CPS	4.9.5	予期間（その考え方も含めて）が記載されていない。	4.9.5　認証局による失効申請の処理期間 証明書の失効要求の結果として取られる処置は、受領後直ちに開始されるものとする。	
22	認証局署名用証明書ポリシ、認証局認証用（人）証明書ポリシ	6.1.2	鍵の受渡について「又は同様に安全な方法によって」とあるが、具体的に明記されておらず、どのような方法を指しているのか不明確	6.1.2　加入者への私有鍵の送付 エンドエンティティの加入者の私有鍵が認証局で生成される場合は、IETF RFC 4210「証明書管理プロトコル」に従ってオンライントランザクションで、又は同様に安全な方法によって、加入者に引き渡されるものとする。認証局はオリジナルの私有鍵を引き渡した後は私有鍵のコピーを所有していないことの証明ができるものとする。	
23	認証局署名用証明書ポリシ、認証局認証用（人）証明書ポリシ	9.6.1	CP内の他の項目と言葉と統一し最低を加える。11年以上保管したらダメと解釈されるのを防ぐため。	9.6.1認証局の表明保証 ～中略～ ・ 申請者の申請内容の真偽の確認において利用した書類を含む、各種の書類の滅失、改ざんを防止し、10 年間保管すること。	9.6.1認証局の表明保証 ～中略～ ・ 申請者の申請内容の真偽の確認において利用した書類を含む、各種の書類の滅失、改ざんを防止し、最低10 年間保管すること。
24	認証局署名用証明書ポリシ、認証局認証用（人）証明書ポリシ	9.6.2	CP内の他の項目と言葉と統一し最低を加える。11年以上保管したらダメと解釈されるのを防ぐため。	9.6.2登録局の表明保証 ～中略～ ・ 将来の検証のため、また証明書がどのように、何故生成されたかを管理可能なように、証明書の作成要求又は失効要求などのイベントを、認証局に移管した場合を除き、証明書の有効期間満了後 10 年間保管すること。	9.6.2登録局の表明保証 ～中略～ ・ 将来の検証のため、また証明書がどのように、何故生成されたかを管理可能なように、証明書の作成要求又は失効要求などのイベントを、認証局に移管した場合を除き、証明書の有効期間満了後 最低10 年間保管すること。

25	認証局署名用証明書ポリシ、認証局認証用（人）証明書ポリシ	3.2.3.1	登録日から最長3ヶ月とすると、医師国家試験実施（合格）後、直ちに医籍登録しなかった場合（数ヶ月後など）でも、登録日から3ヶ月であれば書類の省略が可能となる。そもそも、この規定は国家試験に合格した新卒医師を対象として、合格後、直ちに医籍登録を行うことを想定している。そのため、そこから短期間であれば登録時に提出している住民票の写しの提出を省略できることとして書類準備の負担軽減を目的とした規定である。従って、現在の登録日から最長3ヶ月では趣旨に合わないケースが発生するため、国家試験実施から半年として、現在の規定で想定している登録日から最長3ヶ月（登録が遅れた場合も考慮した7月一杯程度）となるように記載を修正する。	3.2.3　個人の認証 1. 個人の実在性 ～中略～ 。なお、4 に定める国家資格を有する者が国家資格情報を含んだ証明書を申請する場合、官公庁で当該資格の登録時に上記書類のいずれかを提出し、発行された国家資格を証明する書類（以下、国家資格免許証等という）の登録日が明記されていれば、CPS で定める期間（登録日から最長 3 ヶ月）の間は、それら の書類を省略できる。	3.2.3　個人の認証 1. 個人の実在性 ～中略～ なお、4 に定める国家資格を有する者が国家資格情報を含んだ証明書を申請する場合、官公庁で当該資格の登録時に上記書類のいずれかを提出し、発行された国家資格を証明する書類（以下、国家資格免許証等という）の登録日が明記されていれば、CPS で定める期間（国家試験実施後、最長6ヶ月）の間は、それらの書類を省略できる。
26	認証局署名用証明書ポリシ、認証局認証用（人）証明書ポリシ	3.2.3.2	運転経歴証明書は有効期間が永久となっているが、平成24年3月31日以前に発行された証明書は、住所、氏名、生年月日、顔写真の変更ができないので、公的身分証明書としての有効期限の概念がない。記載事項の変更の場合には新しい運転経歴証明書に切替が必要となっている。 そのため、犯罪による収益の移転防止に関する法律施行規則により、金融機関等で本人確認書類として有効としているのは、平成24年4月1日以降発行の運転経歴証明書としている。 従って、「運転免許証（平成24年4月1日以降発行の運転経歴証明書を含む、以下、合わせて運転免許証とする。）」と規定するのが望ましい。	3.2.3　個人の認証 ～中略～ 2.個人の本人性 ～中略～ 【1点で確認できる書類】 本人確認書類の 1 つに「運転免許証（運転経歴証明書を含む、以下、合わせて運転免許証とする。）」と記載されている。	3.2.3　個人の認証 ～中略～ 2.個人の本人性 ～中略～ 【1点で確認できる書類】 本人確認書類の 1 つに「運転免許証（平成24年4月1日以降発行の運転経歴証明書を含む、以下、合わせて運転免許証とする）」と記載されている。
27	準拠性審査実施規則	全般	監査報告書の記載方法の明確化（赤字、認証局名、報告書等）		