健康で豊かな国民生活を保健医療福祉情報システムが支えます

電子処方箋署名共通モジュール仕様案に対する補足

2024年7月19日

JAHIS　セキュリティ委員会　HPKI電子署名規格作成WG

認証局の鍵更新について

- HPKI認証局証明書ポリシ(CP)(※)(以下、HPKI証明書ポリシ)では“認証局は、定期的に CA 私有鍵の更新を行う”と定められており、この度サブCAである日本医師会認証局の方で、CA私有鍵更新が行われるとの情報共有がありました
- 鍵更新に当たっては、第27回HPKI専門家会議にて日本医師会のサブCAについては、鍵の運用切替え（A案）にて実施することが確認されました
  - A案：CAシステムは更新せず、同一のIssuer nameのCAとして、ルート認証局より新たなサブCA証明書を発行、鍵の切換えを行い、旧鍵は廃棄、旧CAで発行済みエンドエンティティ証明書(以下、EE証明書)へのCRLは新CAより発行
  - https://www.mhlw.go.jp/content/10808000/001263338.pdf
- JAHISから要望を出させて頂いた電子処方箋署名共通モジュール仕様案については、参照すべき文書として下記を挙げており、その中でHPKI証明書ポリシ及びRFC5280を参照文書として挙げています
  - JAHIS標準 ID 18-006「JAHISヘルスケアPKIを利用した医療文書に対する電子署名規格Ver.2.0」
- また、RFC5280では、CA私有鍵の更新手順の詳細について、RFC4210を参照しています

（※）厚生労働省が策定している保健医療福祉分野ＰＫＩ認証局署名用証明書ポリシ
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/pki-policy/repository.html

仕様案に対する補足事項

- EE証明書の検証を行う際にはCA私有鍵の更新が行われることを前提として考えるべきです
  - RFC4210 3.1.2 10.に記載
    - 新旧の認証局から発行された証明書は、どちらも検証できなければならない
- 日本医師会のサブCAの鍵更新は、鍵の運用切替えで実施されるため、下記のポイントを踏まえて検証を行う必要があります
  - 鍵切替後は旧サブCAからはCRLは発行されない
  - 新サブCAから発行されるCRLには、旧サブCAで発行したEE証明書の失効情報(シリアル番号)も含まれる
  - トラストアンカーは厚労省ルートCAのまま変わらない
  - 新旧サブCAのSubjectは変わらない
  - EE証明書、CRLのIssuerも変わらない
  - RFC5280の通りEE証明書の検証と、CRLの検証を分けて実施する（詳細は次ページ）
    - EE証明書のパス検証（EE証明書の署名検証を含む）を行う
    - CRLの検証（CRLのパス検証とCRLの署名検証）を行う
- 署名検証モジュールでは、検証のために複数の証明書、複数のCRLが参照することが必要となるケースを想定するべきで、RFC5280に沿って確認がされるべきです

厚労省HPKIでのEE証明書検証とCRL検証のポイント

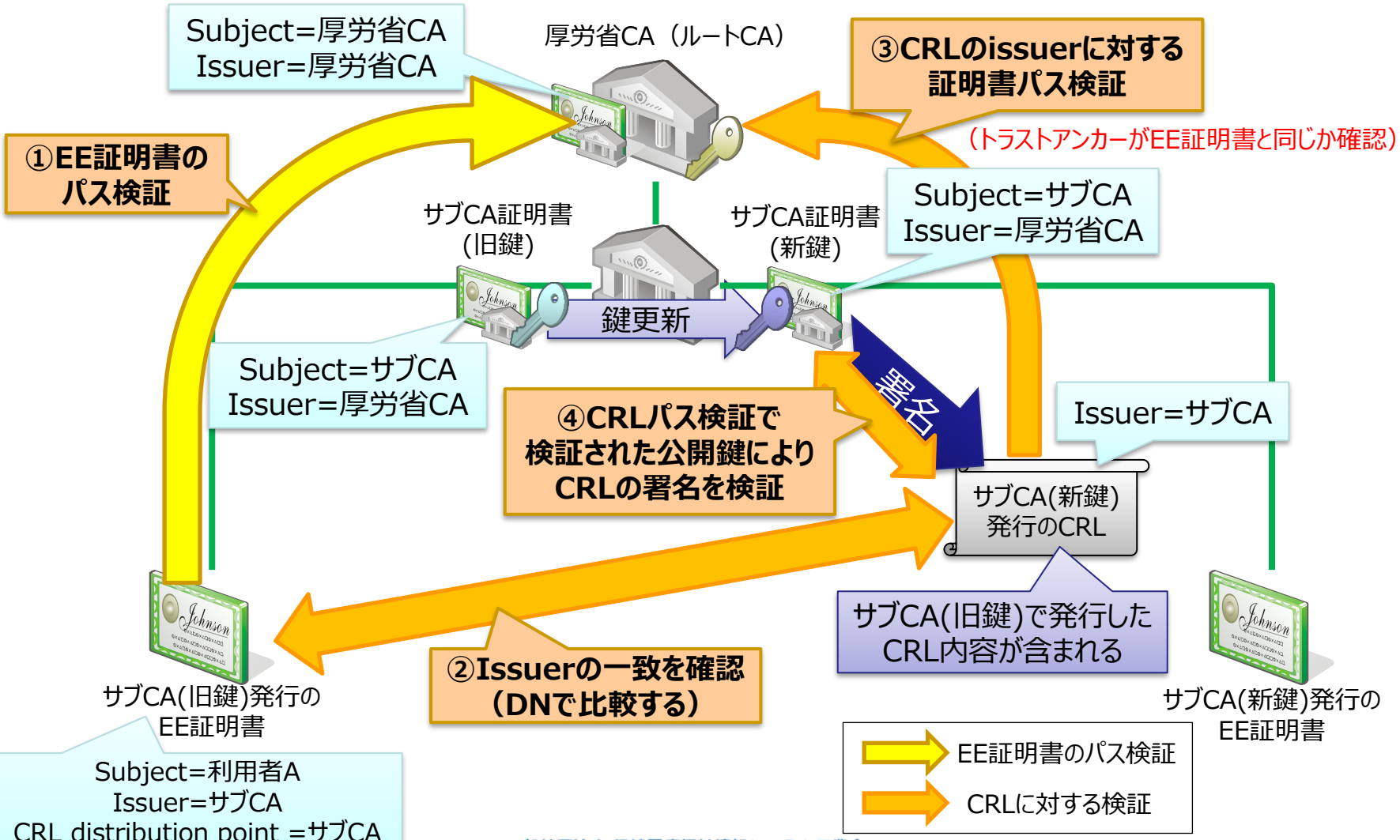
（前提）専門家会議における資料にも記載の通り、Entityの識別は、X.500シリーズが定めるDirectory Name（以下、DN）で示され、認証局自体の名前もこちらで決定されます

- issuerの一致を確認する際は、DNの一致を確認する

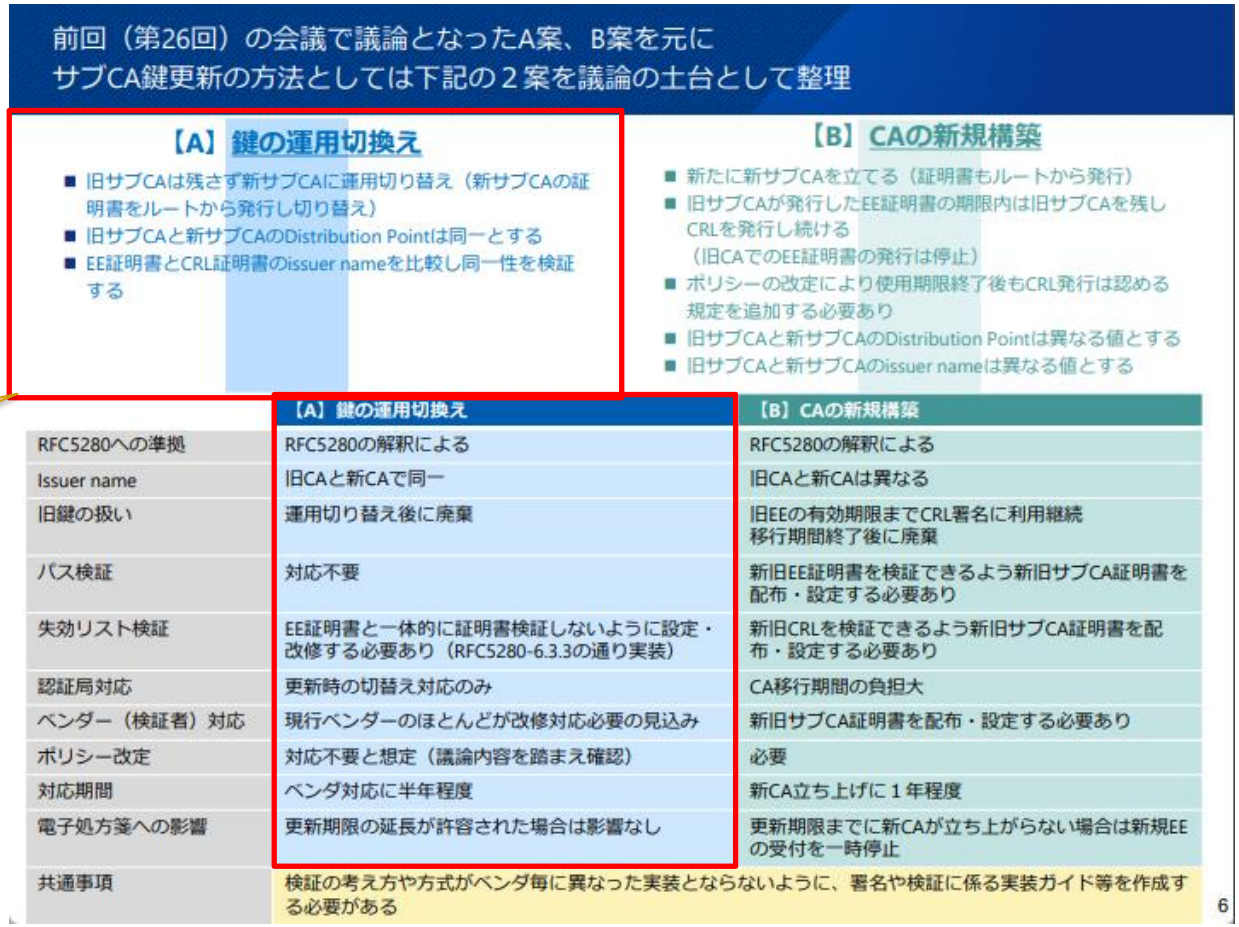
- EE証明書のパス検証とCRLの検証は分けて考え、実施すべきです
  - EE証明書のパス検証を実施【6.1】
    - トラストアンカーは厚労省CA
  - CRLの検証を実施、その際のポイントは以下となる【6.3】
    - 「CRL issuer【3】」を別に構築しないモデルであるため、CRLのissuerとEE証明書のissuerのDNが一致することを確認【6.3.3(b)(1)】
    - CRLのissuerに対する証明書パスを検証して、トラストアンカーがEE証明書と同じ厚労省CAであるかを確認【6.3.3(f)】
    - CRLのissuerに対する証明書パスを検証した際の公開鍵で、CRLに付された署名の検証を行う【6.3.3(g)】
    - 複数のCRLが存在する場合、Issuer、CRLNumber、CRLの発行日等を用い、適切なCRLを選択する

【 】内はRFC5280の章節番号

参考)サブCA(旧鍵)のEE証明書をサブCA(新鍵)のCRLで検証例



(参考)HPKI専門家会議でのサブCA鍵更新の方法



前回（第26回）の会議で議論となったA案、B案を元に
サブCA鍵更新の方法としては下記の２案を議論の土台として整理

【A】鍵の運用切換え

- 旧サブCAは残さず新サブCAに運用切り替え（新サブCAの証明書をルートから発行し切り替え）
- 旧サブCAと新サブCAのDistribution Pointは同一とする
- EE証明書とCRL証明書のissuer nameを比較し同一性を検証する

【B】CAの新規構築

- 新たに新サブCAを立てる（証明書もルートから発行）
- 旧サブCAが発行したEE証明書の期限内は旧サブCAを残しCRLを発行し続ける（旧CAでのEE証明書の発行は停止）
- ポリシーの改定により使用期限終了後もCRL発行は認める規定を追加する必要あり
- 旧サブCAと新サブCAのDistribution Pointは異なる値とする
- 旧サブCAと新サブCAのissuer nameは異なる値とする

	【A】鍵の運用切換え	【B】CAの新規構築
RFC5280への準拠	RFC5280の解釈による	RFC5280の解釈による
Issuer name	旧CAと新CAで同一	旧CAと新CAは異なる
旧鍵の扱い	運用切り替え後に廃棄	旧EEの有効期限までCRL署名に利用継続 移行期間終了後に廃棄
パス検証	対応不要	新旧EE証明書を検証できるよう新旧サブCA証明書を配布・設定する必要あり
失効リスト検証	EE証明書と一体的に証明書検証しないように設定・改修する必要あり（RFC5280-6.3.3の通り実装）	新旧CRLを検証できるよう新旧サブCA証明書を配布・設定する必要あり
認証局対応	更新時の切替え対応のみ	CA移行期間の負担大
ベンダー（検証者）対応	現行ベンダーのほとんどが改修対応必要の見込み	新旧サブCA証明書を配布・設定する必要あり
ポリシー改定	対応不要と想定（議論内容を踏まえ確認）	必要
対応期間	ベンダ対応に半年程度	新CA立ち上げに１年程度
電子処方箋への影響	更新期限の延長が許容された場合は影響なし	更新期限までに新CAが立ち上がらない場合は新規EEの受付を一時停止
共通事項	検証の考え方や方式がベンダ毎に異なった実装とならないように、署名や検証に係る実装ガイド等を作成する必要がある	

6

日本医師会サブCAで選択した方式

第27回保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議
【資料１】第27回保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議・専門作業班合同会議から引用、加工
https://www.mhlw.go.jp/content/10808000/001263338.pdf