HPKI 証明書の改定に係る要望（提案）

日本医師会電子認証センター
日本薬剤師会認証局

HPKI 証明書ポリシに関して、電子処方箋対応に向けた状況の変化、ならびに実運用の観点から、次の通り改定に係る要望をさせていただきます。

1. 電子処方箋での利便性向上に向けた改定

電子処方箋においては、処方箋という文書の趣旨から、医師等の国家資格が確認できる電子署名が必須とされています。その署名は「医療情報システムの安全管理に関するガイドライン」に規定された電子署名であり、HPKI 電子署名に限られたものではありませんが、現時点において HPKI 電子署名が現場において混乱なく利用できる現実解と考えています。

一方で、現在、HPKI 認証局を運営している団体は、電子証明書を IC カードに格納して提供していることから、そのカードの破損・紛失時に業務が滞ること、また、大規模病院においては、全ての診療端末にカードリーダーを設置する必要があることなどが従前から指摘されていました。

従って、HPKI の普及促進と同時に、電子処方箋を推進するために、リモート型による電子署名に対応できるよう、電子証明書（私有鍵）の預託を可能とするため改定を求めます。

なお、リモート署名そのものは、HPKI に限らず、国内において、そのあり方の議論がなされていると承知しており、HPKI 単独でその議論をすることは結論までに相当の時間を要することが想定されます。一方で、電子処方箋は令和 5 年 1 月から本格運用されることになっており、電子署名が必須であることから、電子処方箋への電子署名という目的を限定してリモート署名を開始することもあり得ると考えています。このことから、預託を可能にするための改定とリモート署名そのものの是非は切り離して検討をお願いします。

【改定内容（預託に係る事項）】

- <u>4.4.1 証明書の受理</u>

  交付された電子証明書のエンドエンティティ（格納媒体）が、IC カードだけでなく、クラウド上（リモート先）の預託先になることから、その場合は「到達確認」するとした追記です。

- <u>4.12 および 4.12.1</u>

  法律によって必要とされる場合に加えて、加入者本人の同意がある場合も預託できるとしました。また、同意取得方法については CPS で規定するとしています。

➢ 6.2.3　私有鍵の預託

1.6 の定義で、「鍵の預託（Key Escrow)」としているので、ここだけ「エスクロウ」という必要もないと思われることから、タイトル含めエスクロウを日本語の「預託」に変更しました。その上で、4.12 に記載を合わせています。

2. 現場の運用の更なる利便性向上に係る要望

HPKI 認証局の運営が始まり 10 年近くが経過する中で、更なる利便性向上および普及促進のために検討をお願いしたい事項です。

➢ 3.2.3　個人の認証

・個人の実在性（持参・郵送共通）

こちらは、元々、前々回の改定時に追記しようとして追記忘れだった、住民票記載事項証明書、戸籍（謄抄）本を、電子署名法施行規則第 5 条に合わせて追記しました。

また、HPKI 専門家会議に持ち回りで検討を依頼した、新規免許登録者の住民票省略を明記しています。省略できる期間については、概ね 3 ヶ月と聞いていましたので、3 ヶ月と明記しました。

なお、郵送の場合にも海外在住者の規定は同じですが、記載が抜けていたので平仄を取って追記しました。

・郵送の場合の、個人の本人性と申請意思

これまでも、利便性向上に向けた改定の検討を依頼する際には、電子署名法等の各種法律も参照していました。今回、改めて電子署名法施行規則第 5 条 1 のハを読んでみると、真偽の確認として、本人限定郵便や予め本人に申請をした旨を確認する通知（手紙等）を送って返送があれば真偽の確認ができるという定めがあります。

電子署名法及び施行規則に定めのある「真偽の確認」は、HPKI の CP で定めている、実在性、本人性、申請の意思を包括しているように読めます。

そのため、これを準用して、郵送申請の場合、その手順を踏めば「申請の意思」で求めている印鑑登録証明書を省略できると考えます。

これは、新規申請のハードルを下げる効果だけでなく、更新時に対面でなく郵送で更新を実施するというケースも想定しています。更新の場合、既に一度、本人確認等が実施されていることからも、改めて印鑑登録証明書を送ることなく、それを省略できれば、申請者の利便性向上、認証局の運用負荷の低減が図れます。

➢ 4.2.1　本人性及び資格確認

・(2) 郵送の場合

実在性を確認した後に送付しているので、ここで改めて実在性確認をするというのは重複での確認になってしまうため、前段の改定案の提案も踏まえて、CPS で定める方法で送付するとしました。

3. その他、軽微な修正

- 3.3.1　通常の鍵更新時の本人性確認及び認証

  現在の「加入者情報の通常の鍵更新は、電子証明書が生成された日から 5 年以内であれば」の記載について、更新した場合も電子証明書が「生成」されるため、永遠に過去の記録でよいと解釈することも不可能ではありません。そのため「加入者情報の通常の鍵更新は、初回の電子証明書が生成された日から 5 年以内であれば」と「初回」を追記して明確化しました。

- 6.1.2、6.1.3、6.2.7

  RFC2510 は廃止されて、RFC4210 になっていると思います。1.1 の概要にある参照文章では、RFC4210 になっているので、修正漏れだと思います。

- 1.5.2　問い合わせ先

  医技室になっているので変更お願いします。

なお、認証用（人）CP については、鍵の預託はありませんので預託に係る部分は変更していません。それ以外は、署名用と合わせてあります。