

LGPKIブリッジCAにおけるCA鍵ペアの更新について

LGPKIブリッジCAでは、CA鍵ペアを有効とした日から5年目を迎えようとしているため、「LGPKIブリッジ認証局CP/CPS 4.7 鍵の更新」に定めるとおり、CA鍵ペアの鍵更新を行います。

鍵更新は、平成20年8月21日に行う予定です。

現在のCA鍵ペアと新しいICA鍵ペアとのリンク証明書を発行し、鍵更新後は、新しいICA秘密鍵で署名されたブリッジCAの自己署名証明書、リンク証明書、証明書失効リストが公開リポジトリに格納されます。現在のブリッジCAの自己署名証明書もそのまま公開リポジトリに格納されます。

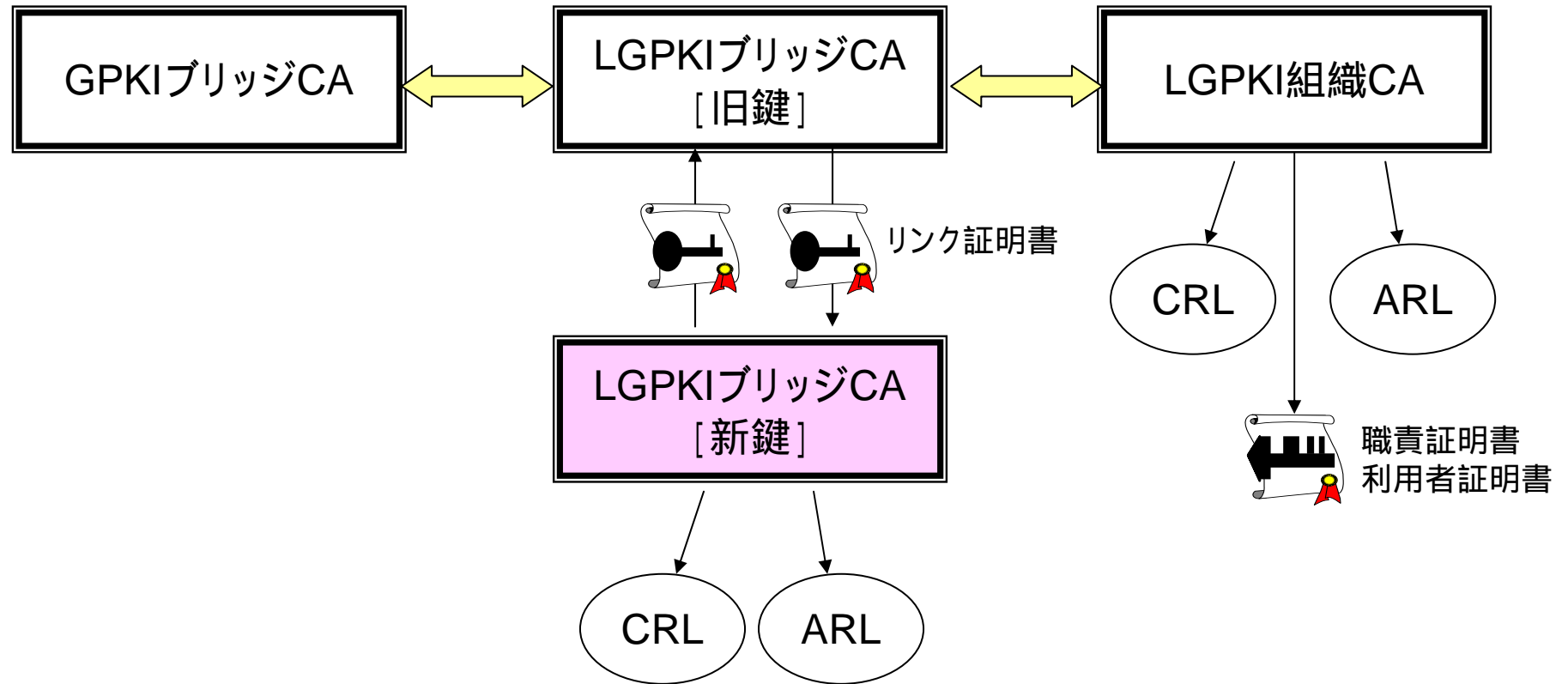
(リンク証明書のプロファイルについては「LGPKI プロファイル設計書 1.1.6. リンク証明書」を参照してください)

なお、政府認証基盤(GPKI)との相互認証証明書に変更はありません。

鍵更新後の各CAとの関連については、次の図のとおりです。

LGPKIブリッジCA鍵更新後の関連について

2008.7



↔ : 相互認証を表す
旧鍵: 鍵更新前(2008.8.20まで)のCA鍵ペア
新鍵: 新しく生成するCA鍵ペア