【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成16年9月30日(2004.9.30)

【公開番号】特開2003-158517(P2003-158517A)
【公開日】平成15年5月30日(2003.5.30)
【出願番号】特願2001-356851(P2001-356851)
【国際特許分類第７版】
　ＨＯ４Ｌ　9/32
　ＨＯ４Ｌ　9/08
【ＦＩ】
　ＨＯ４Ｌ　9/00　６７５Ｚ
　ＨＯ４Ｌ　9/00　６０１Ｆ
　ＨＯ４Ｌ　9/00　６７５Ｂ

【手続補正書】
【提出日】平成15年9月18日(2003.9.18)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
公開鍵基盤における、登録機関側装置と発行機関側装置とによる公開鍵証明書の生成方法であって、
前記登録機関側装置は、公開鍵証明書への登録内容と、当該登録内容のうち当該登録機関側装置が保証する情報と、を添付した証明書発行依頼を、前記発行機関側装置に送り、
前記発行機関側装置は、前記証明書発行依頼に記載された前記登録内容と、前記登録機関が保証する情報と、当該発行機関での発行内容と、当該発行内容に対する署名とからなる公開鍵証明書を生成する
ことを特徴とする公開鍵証明書の生成方法。
【請求項２】
請求項１記載の公開鍵証明書の生成方法であって、
前記公開鍵証明書に記載される情報を指定する識別子を予め定め、
前記登録機関側装置は、前記登録機関側装置が保証する情報に対する署名と、前記保証する情報を指定する識別子とを、前記登録機関側装置が保証する情報に含める
ことを特徴とする公開鍵証明書の生成方法。
【請求項３】
請求項１記載の公開鍵証明書の生成方法であって、
前記登録機関側装置は、当該登録機関が保証する情報にハッシュ関数を作用させたハッシュ値を求め、当該ハッシュ値に対する署名を生成し、前記ハッシュ値と前記署名とを、前記登録機関が保証する情報に含める
ことを特徴とする公開鍵証明書の生成方法。
【請求項４】
請求項１に記載された公開鍵証明書の生成方法に従って生成された公開鍵証明書の検証方法であって、
検証者側装置は、前記公開鍵証明書全体に対して付与された前記発行機関の署名と、前記登録機関の署名とを検証し、
前記登録機関側装置が署名した登録内容と前記発行機関側装置が署名した発行内容とを確

認する
ことを特徴とする公開鍵証明書の検証方法。
【請求項５】
請求項２に記載された公開鍵証明書の生成方法に従って生成された公開鍵証明書の検証方法であって、
検証者側装置は、
前記識別子に従い、前記登録機関が署名対象とした情報を公開鍵証明書から取得し、
取得した前記情報のハッシュ値を求め、
前記登録機関が保証する情報に含まれる前記登録機関の署名を当該登録機関の公開鍵で復号化し、
前記ハッシュ値と前記復号化した値とが等しいかどうかを調べ、前記登録機関が保証対象とする情報の検証を行う
ことを特徴とする公開鍵証明書の検証方法。
【請求項６】
請求項３に記載された公開鍵証明書の生成方法に従って生成された公開鍵証明書の検証方法であって、
検証者側装置は、
前記公開鍵証明書に記載された情報のハッシュ値を求め、
前記登録機関が保証する情報に含まれるハッシュ値と、前記求めたハッシュ値とを比較し、
前記登録機関が保証対象とする情報の識別と識別した情報の検証とを行う
ことを特徴とする公開鍵証明書の検証方法。
【請求項７】
請求項４に記載された公開鍵証明書の検証方法であって、
前記検証者側装置は、
前記検証者が信頼する認証局から、前記公開鍵証明書までのパス構築と当該パスの検証を行い、
前記公開鍵証明書に記載された、前記登録機関の署名を、当該登録機関の公開鍵で検証し、
前記検証者が信頼する前記認証局から前記登録機関の公開鍵証明書までのパス構築と検証を行う
ことを特徴とする公開鍵証明書の検証方法。
【請求項８】
請求項７に記載の公開鍵証明書の検証方法であって、
前記認証局から前記登録機関の公開鍵証明書までのパス構築において、
前記検証者側装置は、
は、検証対象の公開鍵証明書に記載された登録機関名に基づいて、当該発行機関側装置の公開鍵証明書データベースから、前記登録機関の公開鍵証明書を取得する
ことを特徴とする公開鍵証明書の検証方法。
【請求項９】
請求項７に記載の公開鍵証明書の検証方法であって、
前記認証局から前記登録機関の公開鍵証明書までのパス構築において、
前記検証者側装置は、前記検証対象の公開鍵証明書の拡張領域に記載された前記登録機関の公開鍵証明書を取得する
ことを特徴とする公開鍵証明書の検証方法。
【請求項１０】
請求項１に記載された公開鍵証明書の生成方法に従って生成された公開鍵証明書の失効方法であって、
前記登録機関側装置は自身の公開鍵証明書の発行機関側装置へ証明書失効要求を送付し、
前記発行機関側装置は、前記証明書失効要求を受け取り、前記登録機関の公開鍵証明書を

失効させ、
前記登録機関側装置が登録を行った公開鍵証明書を失効させる
ことを特徴とする公開鍵証明書の失効方法。