【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18年9月21日(2006.9.21)

【公開番号】特開2005-117514(P2005-117514A)
【公開日】平成17年4月28日(2005.4.28)
【年通号数】公開・登録公報2005-017
【出願番号】特願2003-351509(P2003-351509)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｈ０４Ｌ　9/00　６０１Ｆ

【手続補正書】
【提出日】平成18年8月8日(2006.8.8)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
エンドエンティティに対して公開鍵証明書を発行するエンドエンティティ証明書発行認証局を含む，複数の認証局から構成される公開鍵基盤において，前記エンドエンティティが操作するエンドエンティティ装置が生成した署名の検証に用いる，前記エンドエンティティ証明書発行認証局が発行した公開鍵証明書の有効性を，コンピュータが確認する公開鍵証明書の有効性確認方法であって，
前記コンピュータは，
任意の前記認証局を起点認証局とし，
任意の前記起点認証局と前記エンドエンティティ証明書発行認証局との間の有効なパスをデータベースに登録するパス登録ステップと，
前記公開鍵証明書の有効性確認依頼を受け付け，前記データベースに登録されている情報を用いて，前記依頼された公開鍵証明書の有効性を判断し，前記判断結果を出力する有効性確認ステップと，を独立して行い，
前記コンピュータは，前記パス登録ステップにおいて，
前記任意の起点認証局と前記エンドエンティティ証明書発行認証局間のパスを検索するステップ１と，
前記ステップ１により検出したパスを検証するステップ２と，
前記ステップ２による検証に成功したパスを，有効なパスとして前記データベースに登録するステップ３と，を行い，
前記コンピュータは，前記有効性確認ステップにおいて，
前記有効性確認依頼にて特定される，前記有効性確認依頼の依頼元がトラストアンカとする起点認証局からエンドエンティティ証明書発行認証局までのパスが，前記データベースに登録されているか，を調べるステップ４と，
前記ステップ４において，前記特定されるパスが，有効なパスとして前記データベースに登録されている場合は，前記有効性確認依頼の対象となった公開鍵証明書は有効である，と判断し，当該判断結果を出力するステップ５と，
前記ステップ４において，前記特定されるパスが，有効なパスとして前記データベース

に登録されていない場合は，前記特定されるパスを新たに検索するステップ６と，
前記ステップ６において，前記特定されるパスを検出した場合に，前記検出したパスを検証するステップ７と，
前記ステップ７による検証結果に従い，前記有効性確認依頼の対象となった公開鍵証明書の有効性を判断し，当該判断結果を出力するステップ８と，
前記ステップ６において検出し前記ステップ７の検証に成功した，前記パスを，有効なパスとして前記データベースに登録するステップ９と，を行う
ことを特徴とする公開鍵証明書の有効性確認方法。
【請求項２】
請求項１に記載の公開鍵証明書の有効性確認方法であって，
前記コンピュータは，
前記有効性確認ステップの前記ステップ６において，前記特定されるパスを検出しなかった場合に，前記有効性確認依頼の対象となった公開鍵証明書は有効ではない，と判断し，当該判断結果を出力するステップ１０を行う
ことを特徴とする公開鍵証明書の有効性確認方法。
【請求項３】
請求項１または２に記載の公開鍵証明書の有効性確認方法であって，
前記コンピュータは，
前記パス登録ステップの前記ステップ１において，
検出したパスを構成する前記エンドエンティティ証明書発行認証局が発行している，エンドエンティティ証明書に関する失効リストを取得するステップ１１を行い，
前記ステップ３において，
前記ステップ２またはステップ７によるパスの検証に成功した場合に，前記ステップ１２において取得した前記失効リストを，当該エンドエンティティ証明書発行認証局が発行している公開鍵証明書を用いて検証するステップ１２と，
前記ステップ１２による検証に成功した場合は，当該失効リストは有効であると判断し，前記有効なパスと前記有効な失効リストとを前記データベースに登録するステップ１３と，を行う
ことを特徴とする公開鍵証明書の有効性確認方法。
【請求項４】
請求項３に記載の公開鍵証明書の有効性確認方法であって，
前記コンピュータは，
前記有効性確認ステップの前記ステップ５において，前記特定されるパスが，有効なパスとして前記データベースに登録されている場合は，
前記特定されるパスを構成する前記エンドエンティティ証明書発行認証局が発行している公開鍵証明書を用いて、前記有効性確認依頼の対象となった公開鍵証明書の署名検証を行うステップ１４と，
前記ステップ１４による署名検証に成功した場合に，前記特定されるパスに対応づけて登録されている，有効な前記失効リストを用いて，当該公開鍵証明書が失効しているかどうかを調べるステップ１５と，
前記ステップ１５において，前記有効性確認依頼の対象となった公開鍵証明書が失効していなければ，当該公開鍵証明書は有効である，と判断し，失効していれば，当該公開鍵証明書は有効ではない，と判断するステップ１６と，を行う
ことを特徴とする公開鍵証明書の有効性確認方法。
【請求項５】
請求項１ないし４いずれか一に記載の公開鍵証明書の有効性確認方法であって，
前記コンピュータは，
前記有効性確認ステップの前記ステップ５において，
前記データベースの検索の結果，前記特定されるパスが，有効なパスとして前記データベースに登録されている場合に，当該有効性確認依頼の対象となった公開鍵証明書，また

は，前記特定されるパスに含まれる他の前記認証局が発行する他の公開鍵証明書に，制限事項が含まれているかどうかを調べ，
前記制限事項が含まれている場合は，前記特定されるパスが前記制限事項に反しているかどうか，を調べ，
前記特定されるパスが前記制限事項に反していなければ，前記有効性確認依頼の対象となった公開鍵証明書は有効である，と判断するステップ１７を行う
ことを特徴とする公開鍵証明書の有効性確認方法。
【請求項６】
請求項１ないし４いずれか一に記載の公開鍵証明書の有効性確認方法であって，
前記コンピュータは，
前記有効性確認ステップの前記ステップ５において，
前記データベースの検索の結果，前記特定されるパスが，有効なパスとして前記データベースに登録されている場合に，前記有効性確認依頼にポリシが含まれ，当該有効性確認依頼の対象となった公開鍵証明書または前記特定されるパスに含まれる他の前記認証局が発行する他の公開鍵証明書の内容が，前記有効性確認依頼に含まれるポリシを満たしているかどうかを調べ，
前記有効性確認依頼の対象となった公開鍵証明書または前記他の公開鍵証明書の内容が，前記ポリシを満たしている場合に，前記有効性確認依頼の対象となった公開鍵証明書は有効であると判断するステップ１８を行う
ことを特徴とする公開鍵証明書の有効性確認方法。