【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30年3月15日(2018.3.15)

【公開番号】特開2015-154491(P2015-154491A)
【公開日】平成27年8月24日(2015.8.24)
【年通号数】公開・登録公報2015-053
【出願番号】特願2015-21707(P2015-21707)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/64　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０９Ｃ　1/00　６４０Ｄ
Ｈ０４Ｌ　9/00　６７５Ｄ
Ｈ０４Ｌ　9/00　６０１Ｆ
Ｇ０６Ｆ　21/64　３５０

【手続補正書】
【提出日】平成30年2月1日(2018.2.1)
【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】
セキュアアプリケーションの開発に使用するための機密情報を提供する方法であって、前記方法は、
セキュア開発プラットフォーム（ＳＤＰ）により、セキュリティ情報をエンドユーザーから受信することであって、前記ＳＤＰが、ＳＤＰプロセッサを含む、セキュリティ情報をエンドユーザーから受信することと、
セキュリティトークンを前記セキュリティ情報に基づきユーザー装置と交換することと、
前記ユーザー装置から、デジタル証明書に対する要求を受信することと、
ＰＫＩサービスプロセッサに、デジタル証明書に対する前記要求を送信することと、
デジタル証明書に対する前記要求内の情報が正しい場合に、
前記デジタル証明書を作成すること、および前記デジタル証明書を前記ＰＫＩサービスプロセッサから受信することと、
前記デジタル証明書をセキュアメモリに格納することであって、前記セキュアメモリが、前記ユーザー装置によってアクセス可能でなく、前記ＳＤＰプロセッサが、前記デジタル証明書の使用により検証を要求するように構成されることと、および
前記ＳＤＰによって、前記セキュアメモリから機密データを読み取り、かつ前記機密データを前記ユーザー装置に送信して、前記機密データを使用するアプリケーションを開発することと
を含む、機密情報を提供する方法。
【請求項２】
前記ユーザー装置から、デジタル的に署名する文書を受信することと、

前記ＰＫＩサービスプロセッサに、前記ユーザー装置に関連したデジタル証明書を検証する要求を送信することと、
前記ＰＫＩサービスプロセッサから、前記デジタル証明書の有効性の指標を受信することと、
前記指標が有効なデジタル証明書を示している場合に、
ユーザーごとにＳＤＰによって生成された前記デジタル証明書秘密鍵に基づき前記文書にデジタル的に署名することと、および
前記署名された文書をエンドユーザーに提供することと

をさらに含む、請求項１に記載の方法。
【請求項３】
前記ユーザー装置から、署名する文書および前記デジタル証明書を受信することと、
前記ＰＫＩサービスプロセッサに、前記デジタル証明書を提供することと、
前記ＰＫＩサービスプロセッサから、前記デジタル証明書の有効性の指標を受信することと、
前記指標が有効なデジタル証明書を示している場合に、前記文書の有効性の指標を前記ユーザー装置に提供することと
をさらに含む、請求項１に記載の方法。
【請求項４】
前記検証が、セッションごとに変更される、データ転送に対して使用される対称鍵の使用を含む、請求項１に記載の方法。
【請求項５】
前記デジタル証明書が、エンドユーザーによって管理されない、請求項１に記載の方法。
【請求項６】
前記ＳＤＰが、エンドユーザーのためにＰＫＩ認証情報およびサービスを管理するように構成されている、請求項１に記載の方法。
【請求項７】
前記検証が、二重認証プロセスの使用を含む、請求項１に記載の方法。
【請求項８】
前記ＳＤＰが、２つ以上の供給源から導出されるマルチパス対称鍵を使用するように構成されている、請求項１に記載の方法。
【請求項９】
前記セキュリティトークンを前記ユーザー装置に対して復元することをさらに含む、請求項１に記載の方法。
【請求項１０】
前記ＳＤＰが、両方向性が認証されて暗号化されたチャネルを提供するように構成されている、請求項１に記載の方法。
【請求項１１】
セキュアアプリケーションの開発に使用するための機密情報を提供するシステムであって、
セキュア開発プラットフォーム（ＳＤＰ）であって、前記ＳＤＰが、受信器に結合されたＳＤＰプロセッサを含み、前記受信器が、セキュリティ情報をエンドユーザーから受信するように構成されている、セキュア開発プラットフォーム（ＳＤＰ）と、
セキュリティトークンを、前記セキュリティ情報に基づきユーザー装置と交換し、かつ、前記ユーザー装置から、デジタル証明書に対する要求を受信するように構成された、通信インタフェースと、
ＰＫＩサービスプロセッサに、デジタル証明書に対する前記要求を送信するように構成された送信器と、
デジタル証明書に対する前記要求内の情報が、前記デジタル証明書要求内の情報と一致

する場合に、前記デジタル証明書を前記ＰＫＩサービスプロセッサから受信するように構成された受信器と
を含み、
前記デジタル証明書が、前記ユーザー装置よってアクセス可能でないセキュアメモリ内に格納され、かつ前記ＳＤＰが、前記セキュアメモリから機密データを更に読み取り且つ前記機密データを前記ユーザー装置に送信して、前記機密データを使用するアプリケーションを開発する、
機密情報を提供するシステム。
【請求項１２】
前記ＰＫＩサービスプロセッサに、検証するデジタル証明書を送信するように構成された送信器と、
前記ＰＫＩサービスプロセッサから、前記デジタル証明書の有効性の指標を受信するように構成された受信器と
をさらに含み、
前記ＳＤＰが、有効性の前記指標ならびにＳＤＰによって生成および格納されたＰＫＩ鍵ペアに基づき、前記文書にデジタル的に署名する、
請求項１１に記載のシステム。
【請求項１３】
デジタル証明書および検証する文書を送信するように構成された送信器であって、前記デジタル証明書が前記ＰＫＩサービスプロセッサによって検証される、送信器と、
前記ＰＫＩサービスプロセッサから前記デジタル証明書の有効性の指標を受信するように構成された受信器と
をさらに含み、
前記ＳＤＰが、前記文書を検証して、有効性の前記指標を前記ユーザー装置に提供する、
請求項１１に記載のシステム。
【請求項１４】
前記検証が、セッションごとに変更される、データ転送に対して使用される対称鍵の使用を含む、請求項１１に記載のシステム。
【請求項１５】
前記デジタル証明書が、エンドユーザーによって管理されない、請求項１１に記載のシステム。
【請求項１６】
前記ＳＤＰが、エンドユーザーのためにＰＫＩ認証情報およびサービスを管理するように構成されている、請求項１１に記載のシステム。
【請求項１７】
前記検証が、二重認証プロセスの使用を含む、請求項１１に記載のシステム。
【請求項１８】
前記ＳＤＰが、２つ以上の供給源から導出されるマルチパス対称鍵を使用するように構成されている、請求項１１に記載のシステム。
【請求項１９】
前記セキュリティトークンを前記ユーザー装置に対して復元するように構成された通信インタフェースをさらに含む、請求項１１に記載のシステム。
【請求項２０】
前記ＳＤＰが、両方向性が認証されて暗号化されたチャネルを提供するように構成されている、請求項１１に記載のシステム。