【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21年5月28日(2009.5.28)

【公表番号】特表2008-538482(P2008-538482A)
【公表日】平成20年10月23日(2008.10.23)
【年通号数】公開・登録公報2008-042
【出願番号】特願2008-507705(P2008-507705)
【国際特許分類】
Ｈ０４Ｗ　12/04　(2009.01)
Ｈ０４Ｗ　12/06　(2009.01)
Ｈ０４Ｗ　88/02　(2009.01)
Ｈ０４Ｗ　88/18　(2009.01)
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｑ　7/00　１８２
Ｈ０４Ｑ　7/00　１８３
Ｈ０４Ｑ　7/00　６４１
Ｈ０４Ｑ　7/00　６７０
Ｈ０４Ｌ　9/00　６０１Ａ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成21年4月10日(2009.4.10)
【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】
ユーザ機器で遂行され、そして、前記ユーザ機器と複数のネットワーク・アプリケーション機能との間の通信を認証するのに用いる鍵素材の生成方法であって、
前記ユーザ機器がブートストラッピング鍵要求をサーバに提供したことに応答して、前記ユーザ機器で第１の鍵素材を決定し、そして、
前記第１の鍵素材を用いて複数の第２の鍵を前記ユーザ機器で決定することを含み、前記第２の鍵の各々は、各ネットワーク・アプリケーション機能に対して前記サーバが生成し、そして、前記ブートストラッピング鍵要求の受信に応答して各ネットワーク・アプリケーション機能に提供される、第３の鍵に一致する、
方法。
【請求項２】
前記ユーザ機器が、ブートストラッピング鍵プロビジョニングの要求を前記サーバに提供し、
ホーム加入者サーバ、ホーム・ロケーション・レジスタ、および認証、認可およびアカウンティング・サーバのうちの少なくとも１つに格納されているブートストラッピング情報にアクセスすること含み、前記ブートストラッピング情報へのアクセスは、ユーザ・プロファイル、認証ベクトル、鍵値、ユーザ・セキュリティ設定、前記複数のネットワーク・アプリケーション機能のうちの少なくとも１つのネットワーク・アプリケーション機能の指示、および前記少なくとも１つのネットワーク・アプリケーション機能のアドレスのうちの少なくとも１つへのアクセスを含み、そして、

前記第１の鍵素材を決定することは、前記ブートストラッピング情報に基づいて第１の鍵素材を決定することを含む、請求項１に記載の方法。
【請求項３】
前記複数の第２の鍵を決定する前に、ブートストラッピング鍵生成プロセスを使用して、ブートストラッピング・サーバ機能を認証することを含む請求項２に記載の方法。
【請求項４】
前記複数の第２の鍵を決定することが、前記複数のネットワーク・アプリケーション機能に関連する複数のルート鍵を決定することを含み、前記ユーザ機器は、対応するルート鍵を用いて前記複数のネットワーク・アプリケーション機能の各々への安全な通信を確立することができる、請求項１に記載の方法。
【請求項５】
サーバで遂行され、そして、ユーザ機器と複数のネットワーク・アプリケーション機能との間の通信を認証するのに用いる鍵素材の生成方法であって、
前記サーバで受信した前記ユーザ機器からのブートストラッピング鍵要求に応答して、前記サーバで第１の鍵素材を決定し、
前記第１の鍵素材を用いて複数の第２の鍵を決定することを含み、前記複数の第２の鍵は、前記ブートストラッピング鍵要求を提供したことに応答して前記ユーザ機器が生成した複数の第３の鍵と一致するものであり、前記複数の第３の鍵は、前記第１の鍵素材を用いて前記ユーザ装置が生成したものであり、そして、
前記複数の第２の鍵の各々を、前記サーバから、前記複数のネットワーク・アプリケーション機能のうちの１つに提供する、
ことを含む方法。
【請求項６】
前記ユーザ機器からブートストラッピング鍵プロビジョニングの要求を受信し、
ホーム加入者サーバ、ホーム・ロケーション・レジスタ、および認証、認可およびアカウンティング・サーバのうちの少なくとも１つに格納されているブートストラッピング情報にアクセスすることを含み、前記ブートストラッピング情報へのアクセスは、ユーザ・プロファイル、認証ベクトル、鍵値、ユーザ・セキュリティ設定、前記複数のネットワーク・アプリケーション機能のうちの少なくとも１つのネットワーク・アプリケーション機能の指示、および前記少なくとも１つのネットワーク・アプリケーション機能のアドレスのうちの少なくとも１つへのアクセスを含み、そして、
前記第１の鍵素材を決定することは、前記ブートストラッピング情報に基づいて第１の鍵素材を決定することを含む、請求項５に記載の方法。
【請求項７】
前記第１の鍵素材を決定する前に、ブートストラッピング鍵生成プロセスを使用して前記ユーザ機器を認証することを含む請求項５に記載の方法。
【請求項８】
前記複数の第２の鍵を決定することが、鍵導出関数を前記第１の鍵素材に適用することによって複数のルート鍵を決定することを含む請求項６に記載の方法。
【請求項９】
前記複数の第２の鍵を前記複数のネットワーク・アプリケーション機能に提供することが、実質的に、前記複数の第２の鍵のうちの１つを使用して前記ユーザ機器と前記少なくとも１つのネットワーク・アプリケーション機能との間に少なくとも１つの安全な接続が形成される前に、前記複数のネットワーク・アプリケーション機能へ前記複数の第２の鍵を提供することを含む請求項６に記載の方法。