【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19年4月19日(2007.4.19)

【公開番号】特開2006-180561(P2006-180561A)
【公開日】平成18年7月6日(2006.7.6)
【年通号数】公開・登録公報2006-026
【出願番号】特願2006-77107(P2006-77107)
【国際特許分類】
Ｈ０４Ｌ　9/14　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６４１

【手続補正書】
【提出日】平成19年3月1日(2007.3.1)
【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】
通信ネットワークでユーザ端末によりセキュアな通信セッションを提供するための方法であって：
セキュアな通信方法を用いてユーザ端末によりセキュア鍵及びセキュアシードを受信する段階であって、前記セキュア鍵及び前記セキュアシードは、前記のセキュアな通信セッション中に用いるために前記ユーザ端末における記憶について適切である、段階；
現セッション鍵を用いて前記ユーザ端末によりデータを暗号化し且つ送信し、前記現セッション鍵を用いて前記ユーザ端末により受信されたデータを復号化する段階であって、前記セキュア鍵は、最初は前記の現在のセッション鍵として用いられる、段階；並びに
後続セッション鍵を前記ユーザ端末により定期的に受信し、後続通信中に前記現セッション鍵として前記後続セッション鍵を用いる、段階；
を有することを特徴とする方法。
【請求項２】
請求項１に記載の方法であって、前記セキュアな通信セッションを終了するように前記ユーザ端末によりログオフメッセージを送信する段階であって、前記ログオフメッセージは暗号化フォームの形をとり且つ前記セキュア鍵を有する、段階を更に有する、ことを特徴とする方法。
【請求項３】
通信ネットワークでモバイル端末によりセキュアな通信セッションを提供するための方法であって：
セキュアな通信方法を用いて前記モバイル端末によりセキュア鍵を受信する段階であって、前記セキュア鍵は、前記のセキュアな通信セッション中に用いるために前記モバイル端末において記憶される、段階；
現セッション鍵を用いて前記モバイル端末によりデータを暗号化し且つ送信し、前記現セッション鍵を用いて前記モバイル端末により受信されたデータを復号化する段階；及び
前記のセキュアな通信セッションを終了するように前記モバイル端末によりログオフメッセージを送信する段階であって、前記ログオフメッセージは暗号化フォームの形をとり且つ前記セキュア鍵を有する、段階；
を有することを特徴とする方法。

【請求項４】
請求項３に記載の方法であって、前記モバイル端末によりセキュアシードを受信する段階であって、前記セキュアシードは、前記のセキュアな通信セッション中に用いるために前記モバイル端末に記憶される、段階を更に有する、ことを特徴とする方法。
【請求項５】
請求項４に記載の方法であって、前記セキュアシードを用いて後続セッション鍵を定期的に作成する段階を更に有する、ことを特徴とする方法。
【請求項６】
請求項４に記載の方法であって、新しい鍵と前記セキュアシードとの組み合わせを用いて後続セッション鍵を定期的に作成する段階であって、前記新しい鍵は前記セキュア鍵を用いて作成される、段階を更に有する、ことを特徴とする方法。
【請求項７】
請求項６に記載の方法であって、前記後続セッション鍵を定期的に作成する段階は、前記新しい鍵と前記セキュアシードとを結び付けることにより後続セッション鍵を作成する段階と、前記後続セッション鍵を作成するようにハッシュアルゴリズムを実行する段階とから構成される、ことを特徴とする方法。
【請求項８】
通信ネットワークでモバイル端末によりセキュアな通信セッションを提供するための方法であって：
セキュアな通信方法を用いて前記通信ネットワークによりセキュア鍵を受信する段階であって、前記セキュア鍵は、前記のセキュアな通信セッション中に用いるために前記通信ネットワークに記憶される、段階；
現セッション鍵を用いて前記通信ネットワークによりデータを暗号化し且つ送信し、前記現セッション鍵を用いて前記通信ネットワークにより受信されたデータを復号化する段階であって、前記セキュア鍵は、最初は前記現セッション鍵として用いられる、段階；並びに
前記通信ネットワークにより後続セッション鍵を定期的に受信し、後続通信中に前記現セッション鍵として前記後続セッション鍵を用いる、段階；
を有することを特徴とする方法。
【請求項９】
請求項８に記載の方法であって、前記通信ネットワークによりログオフメッセージを受信する段階であって、前記ログオフメッセージは暗号化フォームの形をとり且つ前記セキュア鍵を有する、段階を更に有する、ことを特徴とする方法。
【請求項１０】
通信ネットワークでモバイル端末によりセキュアな通信セッションを提供するための方法であって：
ユーザ認証フェーズ中に前記モバイル端末に少なくとも２つの共有秘密をインストールし、それにより、第１秘密は最初のセッション鍵であり、第２秘密は後続セッション鍵を作成するようにセキュアシードとして用いられる段階；
を有することを特徴とする方法。
【請求項１１】
請求項１０に記載の方法であって、新しい鍵を作成し、前記新しい鍵を現セッション鍵により暗号化する段階を更に有する、ことを特徴とする方法。
【請求項１２】
請求項１１に記載の方法であって、前記新しい鍵を作成する段階は、前記セキュアシードに前記現セッション鍵を結び付ける段階を有する、ことを特徴とする方法。
【請求項１３】
請求項１２に記載の方法であって、前記の結び付けられた結果にハッシュアルゴリズムを適用することにより新しいセッション鍵を作成する段階を更に有する、ことを特徴とする方法。

【請求項１４】
請求項１３に記載の方法であって、後続通信において前記新しいセッション鍵を用いる段階を更に有する、ことを特徴とする方法。
【請求項１５】
通信ネットワークでモバイル端末によりセキュアな通信セッションを提供するための方法であって：
ユーザ認証フェーズ中にアクセスポイントにおいて少なくとも２つの共有秘密をインストールし、それにより、第１秘密は最初のセッション鍵であり、第２秘密は後続セッション鍵を作成するようにセキュアシードとして用いられる段階；
を有することを特徴とする方法。
【請求項１６】
請求項１５に記載の方法であって、新しい鍵を作成し、前記新しい鍵を現セッション鍵により暗号化する段階を更に有する、ことを特徴とする方法。
【請求項１７】
請求項１６に記載の方法であって、前記新しい鍵を作成する段階は、前記セキュアシードに前記現セッション鍵を結び付ける段階を有する、ことを特徴とする方法。
【請求項１８】
請求項１７に記載の方法であって、前記の結び付けられた結果にハッシュアルゴリズムを適用することにより新しいセッション鍵を作成する段階を更に有する、ことを特徴とする方法。
【請求項１９】
請求項１８に記載の方法であって、後続通信において前記新しいセッション鍵を用いる段階を更に有する、ことを特徴とする方法。
【請求項２０】
モバイル端末と通信ネットワークとの間にセキュアな通信セッションを提供するための方法であって：
前記セキュアシードは暗号化ログオフ要求において現れるようなセキュアシードを伴う前記暗号化ログオフ要求をセッションログオフ中に前記モバイル端末により送信する段階；
を有することを特徴とする方法。
【請求項２１】
モバイル端末と通信ネットワークとの間のセキュアな通信セッションを提供するためのアクセスポイントであって：
セキュアな通信方法を用いてセキュア鍵及びセキュアシードを送信するための手段；
前記セキュア鍵を用いてデータを暗号化するための手段；並びに
前記セキュアシードを用いて後続セッション鍵を定期的に作成するための手段；
を有することを特徴とするアクセスポイント。
【請求項２２】
請求項２１に記載のアクセスポイントであって、後続セッション鍵を定期的に作成するための手段は、新しい鍵と前記セキュアシードとの組み合わせを用いて後続セッション鍵を作成するための手段を有し、前記新しい鍵は前記セキュア鍵を用いて作成される、ことを特徴とするアクセスポイント。
【請求項２３】
請求項２１に記載のアクセスポイントであって、後続セッション鍵を定期的に作成するための手段は、新しい鍵と前記セキュアシードとを結び付けることにより続くセッション鍵を作成するための手段と、前記の続くセッション鍵を作成するようにハッシュアルゴリズムを実行するための手段とを有する、ことを特徴とするアクセスポイント。
【請求項２４】
通信ネットワークによりセキュアな通信セッションを提供するための端末装置であって：

セキュア鍵とセキュアシードとを受信するための手段、及び前記セキュアな通信セッション中に用いるために前記セキュア鍵と前記セキュアシードとを記憶するための手段；
データを受信するための手段、及び前記のセキュアな通信セッション中に現セッション鍵を用いて前記データを復号化するための手段であって、前記セキュア鍵は最初は前記現セッション鍵として用いられる、前記データを受信するための手段及び復号化するための手段；
前記の現セッション鍵を用いてデータを暗号化及び送信するための手段；並びに
前記現セッション鍵と前記セキュアシードとを用いて後続セッション鍵を作成するための手段であって、前記後続セッション鍵は、その後、後続通信のために前記現セッション鍵として用いられる、手段；
を有することを特徴とする端末装置。
【請求項２５】
請求項２４に記載の端末装置であって、前記端末装置はモバイル端末を有し、前記通信ネットワークは無線ローカルエリアネットワークを有する、ことを特徴とする端末装置。
【請求項２６】
モバイル端末と通信ネットワークとの間のセキュアな通信セッションを提供するためのアクセスポイントであって：
セキュア鍵とセキュアシードとを送信するための手段、及び前記セキュアな通信セッション中に用いるために前記セキュア鍵と前記セキュアシードとを記憶するための手段；
データを暗号化するための手段、前記モバイル端末にデータを送信するための手段、データを受信するための手段及び前記のセキュアな通信セッション中に現セッション鍵を用いて前記モバイル端末からデータを復号化するための手段であって、前記セキュア鍵は最初は前記現セッション鍵として用いられる、それらの手段；
前記現セッション鍵と前記セキュアシードとを用いて後続セッション鍵を作成するための手段であって、前記後続セッション鍵は、その後、後続通信のための前記現セッション鍵として用いられる、手段；
を有することを特徴とするアクセスポイント。