【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】令和4年6月8日(2022.6.8)

【国際公開番号】WO2020/072342
【公表番号】特表2022-501872(P2022-501872A)
【公表日】令和4年1月6日(2022.1.6)
【出願番号】特願2021-509157(P2021-509157)
【国際特許分類】
H04L 9/32(2006.01)
H04L 9/14(2006.01)
G06F 21/34(2013.01)
G06F 21/60(2013.01)
G06F 21/64(2013.01)
G06Q 20/34(2012.01)
【ＦＩ】
H04L 9/00 675A
H04L 9/00 641
G06F 21/34
G06F 21/60 320
G06F 21/60 360
G06F 21/64
G06Q 20/34

【手続補正書】
【提出日】令和4年5月31日(2022.5.31)
【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】
プロセッサと、
メモリと、を備えるサーバであって、
前記プロセッサは、
認証多様化された鍵に基づいてセッション鍵を生成し、
１つまたは複数の暗号化アルゴリズムおよび前記セッション鍵を使用して暗号化結果を検証し、
１つまたは複数のログイン資格情報を認証し、
前記認証に基づいて、情報の共有を承認するように構成される、サーバ。
【請求項２】
前記プロセッサは、要求を送信するようにさらに構成され、
前記情報は、前記要求に関連付けられている、請求項１に記載のサーバ。
【請求項３】
前記要求は、所定のタイムアウト期間に関連付けられている、請求項２に記載のサーバ。
【請求項４】
前記プロセッサは、１つまたは複数のチャレンジを介して前記１つまたは複数のログイン資格情報を認証することに基づいて、前記要求に関連付けられた前記情報の１つまたは複数の部分の共有を承認するようにさらに構成される、請求項２に記載のサーバ。

【請求項５】
前記１つまたは複数の部分は、年齢の証明に対応している、請求項４に記載のサーバ。
【請求項６】
前記メモリは、マスター鍵および一意の識別子を含み、
前記プロセッサは、前記マスター鍵および一意の識別子に基づいて前記認証多様化された鍵を生成するようにさらに構成される、請求項１に記載のサーバ。
【請求項７】
前記暗号化結果は、前記１つまたは複数の暗号化アルゴリズムを使用したカウンタ値に基づいて非接触カードによって生成される、請求項１に記載のサーバ。
【請求項８】
前記プロセッサは、前記要求に関連付けられた前記情報の１つまたは複数の部分の共有を承認するようにさらに構成される、請求項１に記載のサーバ。
【請求項９】
前記情報は、機密情報を含み、
前記情報は、安全な要素から取得される、請求項１に記載のサーバ。
【請求項１０】
プロセッサが、マスター鍵および一意の識別子に基づいて、認証多様化された鍵を生成することと、
前記プロセッサが、前記認証多様化された鍵に基づいて、セッション鍵を生成することと、
前記プロセッサが、１つまたは複数の暗号化アルゴリズムおよび前記セッション鍵を使用して暗号化結果を検証することと、
前記プロセッサが、１つまたは複数のログイン資格情報を認証することと、
前記プロセッサが、情報の共有を承認することと、
のステップを含む、方法。
【請求項１１】
前記方法は、
前記プロセッサが、要求を送信することをさらに含み、
前記情報は、前記要求に関連付けられており、
前記要求は、所定のタイムアウト期間に関連付けられている、請求項１０に記載の方法。
【請求項１２】
前記方法は、
前記プロセッサが、１つまたは複数のチャレンジを介して前記１つまたは複数のログイン資格情報を認証することに基づいて、前記要求に関連付けられた前記情報の１つまたは複数の部分の共有を承認することをさらに含む、請求項１１に記載の方法。
【請求項１３】
前記情報は、機密情報を含む、請求項１０に記載の方法。
【請求項１４】
前記暗号化結果は、前記１つまたは複数の暗号化アルゴリズムを使用してカウンタ値に基づいて生成される、請求項１０に記載の方法。
【請求項１５】
前記方法は、
前記プロセッサが、安全な要素から前記情報を取得することをさらに含む、請求項１０に記載の方法。
【請求項１６】
プロセッサと、
メモリであって、前記メモリは、カウンタ値および１つまたは複数の鍵を含む、メモリと、
通信インターフェースと、を備える非接触カードであって、
前記プロセッサは、

前記通信インターフェースが第１の通信範囲の範囲内にあるときに、前記カウンタ値を更新し、
前記１つまたは複数の鍵および前記カウンタ値に基づいて、第１の暗号化結果を作成し、
前記第１の通信範囲を介して、前記第１の暗号化結果を送信し、
前記通信インターフェースが第２の通信範囲の範囲内にあるときに、前記カウンタ値を更新し、
前記１つまたは複数の鍵および前記カウンタ値に基づいて、第２の暗号化結果を作成し、
前記第２の通信範囲を介して、前記第２の暗号化結果を送信することであって、前記第２の暗号化結果は、データへのアクセスを承認する、ように構成される、非接触カード。
【請求項１７】
前記通信インターフェースが前記第２の通信範囲の範囲内にあるときに、前記カウンタ値を更新する前に、
前記プロセッサは、
前記通信インターフェースを介して、前記第１の通信範囲を介してデータの要求を受信するようにさらに構成され、
前記第２の通信範囲を介した前記第２の暗号化結果の前記送信は、前記要求に応答し、
前記データは、前記要求に関連付けられている、請求項１６に記載の非接触カード。
【請求項１８】
前記要求は、前記データへのアクセスが承認された後に、期限切れになる、請求項１７に記載の非接触カード。
【請求項１９】
前記プロセッサは、前記第２の通信範囲を介して１つまたは複数のログイン資格情報を送信するようにさらに構成される、請求項１６に記載の非接触カード。
【請求項２０】
前記データは、個人を特定できる情報を備え、
前記データは、クラウドストレージ、安全な要素、およびブロックチェーンのグループから選択された少なくとも１つに格納される、請求項１６に記載の非接触カード。