

【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 1 年 9 月 5 日 (2019.9.5)

【公開番号】特開 2019-118130 (P2019-118130A)
 【公開日】令和 1 年 7 月 18 日 (2019.7.18)
 【年通号数】公開・登録公報 2019-028
 【出願番号】特願 2019-39047 (P2019-39047)
 【国際特許分類】

H 0 4 M 3/42 (2006.01)

H 0 4 L 9/32 (2006.01)

【F I】

H 0 4 M 3/42 E

H 0 4 L 9/00 6 7 3 A

H 0 4 L 9/00 6 7 5 B

【手続補正書】

【提出日】令和 1 年 7 月 29 日 (2019.7.29)

【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】

特定のサービスを提供する機器であるサービス用機器と、当該特定のサービスを利用する際の認証を行う機器であって情報通信手段を介して前記サービス用機器と通信可能な機器である認証用機器と、を備えた情報通信システムにおいて、

前記サービス用機器と前記認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行うシステムであって、

前記認証用機器は、当該認証用機器側の秘密鍵である認証側秘密鍵と当該認証側秘密鍵に対応する公開鍵である認証側公開鍵とを生成して、当該認証側秘密鍵を記憶するとともに、当該認証側公開鍵を前記サービス用機器に送信する認証側登録部、を備えた認証側制御部を備え、

前記サービス用機器は、前記認証用機器から前記認証側公開鍵を受信すると、前記認証側公開鍵を前記特定のサービスに係る前記認証用機器の識別標識である内部ユーザ ID に対応付けて記憶するとともに、当該内部ユーザ ID を前記認証用機器に送信するサービス側登録部、を備えたサービス側制御部を備え、

前記サービス側制御部は、前記認証用機器から内部ユーザ ID を指定した認証を求める情報を受信すると、当該サービス用機器において用意した任意のデータであるサービス側元データを前記サービス側登録部に記憶されている前記内部ユーザ ID に対応する認証側公開鍵を用いて暗号化したデータであるサービス側暗号化データを前記認証用機器に送信するサービス側暗号部、を備え、

前記認証側制御部は、前記サービス用機器から受信したサービス側暗号化データを当該認証側登録部に記憶されている前記認証側秘密鍵を用いて復号化したデータであるサービス側復号化データに所定の演算を施して得られるサービス側演算化データを前記サービス用機器に送信する認証側復号部、を備え、

前記サービス側制御部は、前記認証用機器から受信したサービス側演算化データが、前記サービス側元データに当該所定の演算を施して得られるデータと一致する場合は、前記内部ユーザ ID が真正であると判定する内部ユーザ ID 真正判定部、を備えたこと、

を特徴とする、情報通信システム。

【請求項 2】

請求項 1 の情報通信システムにおいて、

前記サービス側登録部は、さらに、当該サービス用機器側の秘密鍵であるサービス側秘密鍵と当該サービス側秘密鍵に対応する公開鍵であるサービス側公開鍵とを生成して、当該サービス側秘密鍵を記憶するとともに、当該サービス側公開鍵を、当該サービス用機器に係る特定のサービスの識別標識であるサービス ID とともに、前記認証用機器に送信し、

前記認証側登録部は、さらに、前記サービス用機器から前記サービス側公開鍵を受信すると、当該サービス側公開鍵を当該サービス ID と関連付けて記憶し、

前記認証側制御部は、前記サービス用機器からサービス ID を指定した認証を求める情報を受信すると、当該認証用機器において用意した任意のデータである認証側元データを前記認証側登録部に記憶されている前記サービス ID に対応する前記サービス側公開鍵を用いて暗号化したデータである認証側暗号化データを前記サービス用機器に送信する認証側暗号部、を備え、

前記サービス側制御部は、前記認証用機器から受信した認証側暗号化データを当該サービス側登録部に記憶されているサービス側秘密鍵を用いて復号化したデータである認証側復号化データに所定の演算を施して得られる認証側演算化データを前記認証用機器に送信するサービス側復号部、を備え、

前記認証側制御部は、前記サービス用機器から受信した認証側演算化データが、前記認証側元データに当該所定の演算を施して得られるデータと一致する場合は、前記サービス ID が真正であると判定するサービス ID 真正判定部、を備えたこと、

を特徴とする、情報通信システム。

【請求項 3】

特定のサービスを提供する機器であるサービス用機器と、当該特定のサービスを利用する際の認証を行う機器であって情報通信手段を介して前記サービス用機器と通信可能な機器である認証用機器と、を備えた情報通信システムにおいて、

前記サービス用機器と前記認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行うシステムであって、

前記サービス用機器は、当該サービス用機器側の秘密鍵であるサービス側秘密鍵と当該サービス側秘密鍵に対応する公開鍵であるサービス側公開鍵とを生成して、当該サービス側秘密鍵を記憶するとともに、当該サービス側公開鍵を、当該サービス用機器に係る特定のサービスの識別標識であるサービス ID とともに、前記認証用機器に送信するサービス側登録部、を備えたサービス側制御部を備え、

前記認証用機器は、前記サービス用機器から前記サービス側公開鍵を受信すると、当該サービス側公開鍵を当該サービス ID と関連付けて記憶する認証側登録部、を備えた認証側制御部を備え、

前記認証側制御部は、前記サービス用機器からサービス ID を指定した認証を求める情報を受信すると、当該認証用機器において用意した任意のデータである認証側元データを前記認証側登録部に記憶されている前記サービス ID に対応する前記サービス側公開鍵を用いて暗号化したデータである認証側暗号化データを前記サービス用機器に送信する認証側暗号部、を備え、

前記サービス側制御部は、前記認証用機器から受信した認証側暗号化データを当該サービス側登録部に記憶されているサービス側秘密鍵を用いて復号化したデータである認証側復号化データに所定の演算を施して得られる認証側演算化データを前記認証用機器に送信するサービス側復号部、を備え、

前記認証側制御部は、前記サービス用機器から受信した認証側演算化データが、前記認証側元データに当該所定の演算を施して得られるデータと一致する場合は、前記サービス ID が真正であると判定するサービス ID 真正判定部、を備えたこと、

を特徴とする、情報通信システム。

【請求項 4】

請求項 1 ないし 3 のいずれかの情報通信システムに用いられる前記サービス用機器。

【請求項 5】

請求項 1 ないし 3 のいずれかの情報通信システムに用いられる前記認証用機器。

【請求項 6】

コンピュータを、請求項 4 のサービス用機器のサービス側制御部、または、請求項 5 の認証用機器の認証側制御部として機能させるためのプログラム。

【請求項 7】

請求項 6 のプログラムを記憶した記録媒体。

【請求項 8】

特定のサービスを提供する機器であるサービス用機器と、当該特定のサービスを利用する際の認証を行う機器であって情報通信手段を介して前記サービス用機器と通信可能な機器である認証用機器と、を備えた情報通信システムであって、前記サービス用機器と前記認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行う情報通信システム、を用いて行う情報通信方法であって、

前記認証用機器が、当該認証用機器側の秘密鍵である認証側秘密鍵と当該認証側秘密鍵に対応する公開鍵である認証側公開鍵とを生成して、当該認証側秘密鍵を記憶するとともに、当該認証側公開鍵を前記サービス用機器に送信する認証側登録ステップと、

前記サービス用機器が、前記認証用機器から前記認証側公開鍵を受信すると、前記認証側公開鍵を前記特定のサービスに係る前記認証用機器の識別標識である内部ユーザ ID に対応付けて記憶するとともに、当該内部ユーザ ID を前記認証用機器に送信するサービス側登録ステップと、

前記サービス用機器が、前記認証用機器から内部ユーザ ID を指定した認証を求める情報を受信すると、当該サービス用機器において用意した任意のデータであるサービス側元データを前記サービス側登録部に記憶されている前記内部ユーザ ID に対応する認証側公開鍵を用いて暗号化したデータであるサービス側暗号化データを前記認証用機器に送信するサービス側暗号ステップと、

前記認証用機器が、前記サービス用機器から受信したサービス側暗号化データを当該認証側登録部に記憶されている前記認証側秘密鍵を用いて復号化したデータであるサービス側復号化データに所定の演算を施して得られるサービス側演算化データを前記サービス用機器に送信する認証側復号ステップと、

前記サービス用機器が、前記認証用機器から受信したサービス側演算化データが、前記サービス側元データに当該所定の演算を施して得られるデータと一致する場合は、前記内部ユーザ ID が真正であると判定する内部ユーザ ID 真正判定ステップと、

を備えたこと、

を特徴とする、情報通信方法。

【請求項 9】

特定のサービスを提供する機器であるサービス用機器と、当該特定のサービスを利用する際の認証を行う機器であって情報通信手段を介して前記サービス用機器と通信可能な機器である認証用機器と、を備えた情報通信システムであって、前記サービス用機器と前記認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行う情報通信システム、を用いて行う情報通信方法であって、

前記サービス用機器が、当該サービス用機器側の秘密鍵であるサービス側秘密鍵と当該サービス側秘密鍵に対応する公開鍵であるサービス側公開鍵とを生成して、当該サービス側秘密鍵を記憶するとともに、当該サービス側公開鍵を、当該サービス用機器に係る特定のサービスの識別標識であるサービス ID とともに、前記認証用機器に送信するサービス側登録ステップと、

前記認証用機器が、前記サービス用機器から前記サービス側公開鍵を受信すると、当該サービス側公開鍵を当該サービス ID と関連付けて記憶する認証側登録ステップと、

前記認証用機器が、前記サービス用機器からサービス ID を指定した認証を求める情報

を受信すると、当該認証用機器において用意した任意のデータである認証側元データを前記認証側登録部に記憶されている前記サービスIDに対応する前記サービス側公開鍵を用いて暗号化したデータである認証側暗号化データを前記サービス用機器に送信する認証側暗号ステップと、

前記サービス用機器が、前記認証用機器から受信した認証側暗号化データを当該サービス側登録部に記憶されているサービス側秘密鍵を用いて復号化したデータである認証側復号化データに所定の演算を施して得られる認証側演算化データを前記認証用機器に送信するサービス側復号ステップと、

前記認証用機器が、前記サービス用機器から受信した認証側演算化データが、前記認証側元データに当該所定の演算を施して得られるデータと一致する場合は、前記サービスIDが真正であると判定するサービスID真正判定ステップと、

を備えたこと、

を特徴とする、情報通信方法。