

【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6部門第3区分  
【発行日】令和2年11月12日(2020.11.12)

【公開番号】特開2019-164794(P2019-164794A)  
【公開日】令和1年9月26日(2019.9.26)  
【年通号数】公開・登録公報2019-039  
【出願番号】特願2019-55074(P2019-55074)  
【国際特許分類】  
    G 0 6 F 21/41 (2013.01)  
【F I】  
    G 0 6 F 21/41

【手続補正書】

【提出日】令和2年9月30日(2020.9.30)

【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】

クラウドベースのアイデンティティおよびアクセス管理を提供する方法であって、前記方法は、

アプリケーションにアクセスすることを可能にするように構成されたアイデンティティ管理サービスを求める第1の要求を受信するステップと、

前記第1の要求を第1のマイクロサービスに送信するステップとを含み、前記第1のマイクロサービスは、トークンを生成することによって前記アイデンティティ管理サービスを実行し、前記第1のマイクロサービスは、シングルサインオン(SSO)マイクロサービスに第2の要求を送信することによって少なくとも部分的に前記トークンを生成し、前記SSOマイクロサービスは、異なるプロトコルに基づく異なるマイクロサービスにまたがるSSO機能を提供するように構成されており、

前記SSOマイクロサービスは、SSOを実現し、クッキーを生成し、前記クッキーは、グローバルステートを含み、異なるマイクロサービスとの通信に使用され、前記方法はさらに、

前記SSOのシングルログアウト(SLO)を受信するステップと、

前記クッキーを利用して前記アプリケーションから繰り返しログアウトするステップとを含み、第1のプロトコルのアプリケーションからの各ログアウト後に、前記SSOマイクロサービスへのリダイレクトを実行することにより、異なるプロトコルのアプリケーションからのログアウトをトリガする、方法。

【請求項2】

前記クッキーは、前記SSOにサインインされたアプリケーションを示す、請求項1に記載の方法。

【請求項3】

前記トークンを前記第1のマイクロサービスから受信するステップと、

前記トークンをアプリケーションに与えるステップとをさらに含み、前記トークンは前記アプリケーションにアクセスすることを可能にする、請求項1または2に記載の方法。

【請求項4】

前記第1のマイクロサービスは、前記プロトコルに基づいて認証機能を提供するように構成されている、請求項1～3のいずれか1項に記載の方法。

**【請求項 5】**

前記プロトコルは、O A u t h またはセキュリティ・アサーション・マークアップ言語 ( S A M L ) であり、前記 S S O マイクロサービスは、O A u t h および S A M L 双方にまたがる S S O 機能を提供するように構成されている、請求項 4 に記載の方法。

**【請求項 6】**

前記 S S O マイクロサービスは、セッションクッキーとして構成されたグローバルセッションを生成し、前記グローバルセッションを前記第 1 のマイクロサービスに与える、請求項 5 に記載の方法。

**【請求項 7】**

前記第 1 のマイクロサービスは、前記グローバルセッションを前記トークンに変換する、請求項 6 に記載の方法。

**【請求項 8】**

前記トークンを前記第 1 のマイクロサービスから受信するステップと、  
前記トークンを前記アプリケーションに与えるステップとを含み、前記トークンは前記アプリケーションにアクセスすることを可能にし、  
前記第 1 のマイクロサービスは、プロトコルに基づいて認証機能を提供するように構成されており、  
前記プロトコルは、O A u t h またはセキュリティ・アサーション・マークアップ言語 ( S A M L ) であり、前記 S S O マイクロサービスは、O A u t h および S A M L 双方にまたがるシングルサインオン機能を提供するように構成されている、請求項 1 ~ 6 のいずれか 1 項に記載の方法。

**【請求項 9】**

クラウドベースのアイデンティティおよびアクセス管理を提供するためのシステムであって、前記システムは、

複数のテナントと、

複数のマイクロサービスと、

1 つ以上のプロセッサとを備え、前記 1 つ以上のプロセッサは、

アプリケーションにアクセスすることを可能にするように構成されたアイデンティティ管理サービスを求める第 1 の要求を受信し、

前記第 1 の要求を第 1 のマイクロサービスに送信し、前記第 1 のマイクロサービスは、トークンを生成することによって前記アイデンティティ管理サービスを実行し、前記第 1 のマイクロサービスは、シングルサインオン ( S S O ) マイクロサービスに第 2 の要求を送信することによって少なくとも部分的に前記トークンを生成し、前記 S S O マイクロサービスは、異なるプロトコルに基づく異なるマイクロサービスにまたがる S S O 機能を提供するように構成されており、

前記 S S O マイクロサービスは、S S O を実現し、クッキーを生成し、前記クッキーは、グローバルステートを含み、異なるマイクロサービスとの通信に使用され、前記 1 つ以上のプロセッサはさらに、

前記 S S O のシングルログアウト ( S L O ) を受信し、

前記クッキーを利用して前記アプリケーションから繰り返しログアウトし、第 1 のプロトコルのアプリケーションからの各ログアウト後に、前記 S S O マイクロサービスへのリダイレクトを実行することにより、異なるプロトコルのアプリケーションからのログアウトをトリガする、システム。

**【請求項 10】**

請求項 1 ~ 8 のいずれか 1 項に記載の方法をプロセッサに実行させるためのコンピュータ読取可能プログラム。