

【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)

【公表番号】特表 2019-526868 (P2019-526868A)
【公表日】令和 1 年 9 月 19 日 (2019.9.19)
【年通号数】公開・登録公報 2019-038
【出願番号】特願 2019-514027 (P2019-514027)
【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シングルサインオン機能を提供するように構成されており、

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する、方法。

【請求項 2】

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いる、請求項 1 に記載の方法。

【請求項 3】

前記プロトコルは、OAuth またはセキュリティ・アサーション・マークアップ言語 (SAML) であり、前記 SSO マイクロサービスは、OAuth および SAML 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 2 に記載の方法。

【請求項 4】

前記 SSO 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 3 に記載の方法。

【請求項 5】

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 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、前記第 2 の要求の要求パラメータを正規化する、請求項 1 ~ 5 のいずれか 1 項に記載の方法。

【請求項 7】

前記アプリケーションは、複数のテナントによって使用され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 8】

前記第 1 のマイクロサービスは、ステートレスであり、データベースからデータを取り出して前記アイデンティティ管理サービスを実行する、請求項 1 ~ 7 のいずれか 1 項に記載の方法。

【請求項 9】

前記データベースおよび前記第 1 のマイクロサービスは、互いに独立してスケーリングするように構成されている、請求項 8 に記載の方法。

【請求項 10】

前記データベースは分散型データグリッドを含む、請求項 8 に記載の方法。

【請求項 11】

前記 S S O のシングルログアウト (S L O) を受信するステップと、
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 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、請求項 1 ~ 10 のいずれか 1 項に記載の方法。

【請求項 12】

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 の要求を前記複数のマイクロサービスのうちの第 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、前記複数のマイクロサービスのうちの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シングルサインオン機能を提供するように構成されており、前記 1 つ以上のプロセッサはさらに、

前記トークンを前記第 1 のマイクロサービスから受信し、

前記トークンを前記アプリケーションに与え、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、システム。

【請求項 13】

請求項 1 ~ 11 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。