【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】平成24年3月22日(2012.3.22)

【公表番号】特表2011-525028(P2011-525028A)
【公表日】平成23年9月8日(2011.9.8)
【年通号数】公開・登録公報2011-036
【出願番号】特願2011-514676(P2011-514676)
【国際特許分類】
Ｇ０６Ｆ　21/20　　(2006.01)
Ｈ０４Ｌ　 9/32　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　15/00　　３３０Ｂ
Ｈ０４Ｌ　 9/00　　６７３Ａ

【手続補正書】
【提出日】平成24年2月2日(2012.2.2)
【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】
クライアント、１つ又は複数のアイデンティティプロバイダ、および１つ又は複数の信頼当事者を有するフェデレートされたコンピュータシステムのクライアントコンピュータにおいて、前記信頼当事者の１つ又は複数のサービスにアクセスするために、前記クライアントが用いることができるセキュリティトークンを取得することに関して、前記クライアントが独立して前記アイデンティティプロバイダのロケーションを解決する方法であって、
前記クライアントコンピュータが、前記信頼当事者に接触して、前記信頼当事者の１つ又は複数のサービスにアクセスするステップと、
前記クライアントコンピュータが、１つ又は複数のポリシーファイルを前記信頼当事者から受信するステップと、
ここで、前記１つ又は複数のポリシーファイルは、１つ又は複数の信頼されているアイデンティティプロバイダのセットに対応する汎用名を識別する情報を含み、
前記クライアントコンピュータが、前記識別された汎用名を自動的に解決して、前記信頼されているアイデンティティプロバイダの１つの、１つ又は複数のネットワークエンドポイントを取得するステップと、
前記１つ又は複数のネットワークエンドポイントを認証すると、前記クライアントコンピュータが、前記１つの解決したアイデンティティプロバイダに接触して、１つ又は複数のセキュリティトークンを取得するために用いる１つ又は複数のデジタルアイデンティティ表示を取得し、またこれに応答して前記クライアントコンピュータが、少なくとも、１つ又は複数の要求を前記解決したアイデンティティプロバイダに送信して、任意の利用可能なデジタルアイデンティティ表示プロビジョニングサービスに関する情報を取得し、さらに前記クライアントコンピュータが、前記解決したアイデンティティプロバイダに用いられるデジタルアイデンティティ表示プロビジョニングサービスに関する情報を含む１つ又は複数のメッセージを受信するステップと
を具えたことを特徴とする方法。
【請求項２】

前記汎用名は、前記１つの信頼されているアイデンティティプロバイダのネットワークエンドポイントを具えたことを特徴とする請求項１記載の方法。
【請求項３】
前記汎用名は、前記１つの信頼されているアイデンティティプロバイダに対応するドメイン名を具えたことを特徴とする請求項１記載の方法。
【請求項４】
前記識別された汎用名を自動的に解決するステップは、１つ又は複数の要求を解決サービスに送信するステップをさらに具えたことを特徴とする請求項３記載の方法。
【請求項５】
前記１つ又は複数のポリシーファイルの前記情報、および前記アイデンティティプロバイダからの前記１つ又は複数のメッセージで受信した前記情報の１つ又は両方が、１つ又は複数のメタデータ要素をさらに具えたことを特徴とする請求項１記載の方法。
【請求項６】
１つ又は複数の追加のメッセージを前記解決サービスに送信するステップをさらに具え、前記１つ又は複数の追加のメッセージは、前記解決したアイデンティティプロバイダからの前記１つ又は複数のメッセージで受信した前記情報の解決を要求することを特徴とする請求項１記載の方法。
【請求項７】
前記デジタルアイデンティティ表示プロビジョニングサービスに対応するネットワークエンドポイントを識別するステップと、
前記クライアントが、１つ又は複数のメッセージを前記デジタルアイデンティティ表示プロビジョニングサービスに送信して、デジタルアイデンティティ表示を取得するステップと
をさらに具えたことを特徴とする請求項１記載の方法。
【請求項８】
前記解決したアイデンティティプロバイダに使用する１つ又は複数のデジタルアイデンティティ表示を、前記プロビジョニングサービスから受信するステップをさらに具えたことを特徴とする請求項７記載の方法。
【請求項９】
前記クライアントが、前記受信したデジタルアイデンティティ表示に対応する情報を含む１つ又は複数の追加のメッセージを前記解決したアイデンティティプロバイダに送信するステップと、
前記解決したアイデンティティプロバイダから、１つ又は複数のセキュリティトークンを含む１つ又は複数のメッセージを受信するステップと
をさらに具えたことを特徴とする請求項８記載の方法。
【請求項１０】
前記クライアントが、前記アイデンティティプロバイダから受信した前記１つ又は複数のトークンを含む１つ又は複数のメッセージを前記信頼当事者に送信するステップと、
前記１つ又は複数のサービスへのアクセスを許可したことを示す前記信頼当事者からの１つ又は複数の応答を受信するステップと
をさらに具えたことを特徴とする請求項９記載の方法。
【請求項１１】
アイデンティティプロバイダ、１つ又は複数のクライアント、および１つ又は複数の信頼当事者を有するフェデレートされたコンピュータシステムの前記アイデンティティプロバイダにおいて、前記信頼当事者が与えた情報を解決する前記クライアントに、１つ又は複数のデジタルアイデンティティ表示、および１つ又は複数のセキュリティトークンを提供する方法であって、
前記クライアントのユーザを前記信頼当事者に検証するために前記クライアントによって用いられる１つ又は複数のセキュリティトークンを取得するために後に使うことができる１つ又は複数のＤＩＲを確立するための、１つ又は複数のデジタルアイデンティティ表

示プロビジョニングサービスを求める前記クライアントからの１つ又は複数の要求を前記アイデンティティプロバイダで受信するステップと、
前記アイデンティティプロバイダによって信頼される少なくとも１つのデジタルアイデンティティプロビジョニングサービスを識別する情報を、前記クライアントに提供するステップと、
ここで、前記情報は、前記クライアントが前記デジタルアイデンティティプロビジョニングサービスにアクセス可能とする前に解決すべき１つ又は複数のネットワークエンドポイントに到達する必要がある、前記１つ又は複数のデジタルアイデンティティプロビジョニングサービスに対応する１つ又は複数の汎用名を有し、
前記クライアントから受信した１つ又は複数のデジタルアイデンティティ表示を認証するステップと、
ここで、前記アイデンティティプロバイダは、前記受信した１つ又は複数のデジタルアイデンティティ表示が有効であると判定し、
前記認証された１つ又は複数のデジタルアイデンティティ表示に対応する１つ又は複数のセキュリティトークンを提供するステップと
を具えたことを特徴とする方法。
【請求項１２】
前記クライアントに情報を提供するステップは、
前記１つ又は複数のデジタルアイデンティティプロビジョニングサービスを識別する前記情報を含む１つ又は複数のドキュメントを公開するステップと、
前記１つ又は複数のドキュメントにデジタル署名を行うステップと
をさらに具えたことを特徴とする請求項１１記載の方法。
【請求項１３】
前記公開された１つ又は複数のドキュメントの前記提供された情報は、１つ又は複数のメタデータ要素を具えたことを特徴とする請求項１１記載の方法。
【請求項１４】
前記クライアントに提供された前記情報は、前記信頼されている１つ又は複数のデジタルアイデンティティプロビジョニングサービスに対応する前記１つ又は複数のネットワークエンドポイントを具えたことを特徴とする請求項１１記載の方法。
【請求項１５】
前記１つ又は複数のデジタルアイデンティティ表示を認証するステップは、
前記信頼当事者と使用する前記１つ又は複数のセキュリティトークンを求める前記クライアントからの１つ又は複数の新しい要求を、前記アイデンティティプロバイダで受信するステップと、
前記１つ又は複数の新しい要求の前記１つ又は複数の有効なデジタルアイデンティティ表示を識別するステップと
をさらに具えたことを特徴とする請求項１１記載の方法。
【請求項１６】
前記１つ又は複数のデジタルアイデンティティ表示を認証するアクトは、前記受信した１つ又は複数のデジタルアイデンティティ表示が、前記信頼されているデジタルアイデンティティプロビジョニングサービスの１つから取得されたことを判定するステップをさらに具えたことを特徴とする請求項１５記載の方法。
【請求項１７】
クライアント、１つ又は複数のアイデンティティプロバイダ、および１つ又は複数の信頼当事者を有するフェデレートされたコンピュータシステムのクライアントコンピュータにおいて、コンピュータ実行可能命令をそのコンピュータプログラム上に記憶したコンピュータプログラムであって、前記コンピュータ実行可能命令を実行すると、前記クライアントコンピュータの１つ又は複数の処理装置は、
前記クライアントコンピュータが、前記信頼当事者に接触して、前記信頼当事者の１つ又は複数のサービスにアクセスするステップと、

前記クライアントコンピュータが、１つ又は複数のポリシーファイルを前記信頼当事者から受信するステップと、

ここで、前記１つ又は複数のポリシーファイルは、１つ又は複数の信頼されているアイデンティティプロバイダのセットに対応する汎用名を識別する情報を含み、

前記クライアントコンピュータが、前記識別された汎用名を自動的に解決して、前記信頼されているアイデンティティプロバイダの１つの、１つ又は複数のネットワークエンドポイントを取得するステップと、

前記１つ又は複数のネットワークエンドポイントを認証すると、前記クライアントコンピュータが、前記１つの解決したアイデンティティプロバイダに接触して、１つ又は複数のセキュリティトークンを取得するために用いる１つ又は複数のデジタルアイデンティティ表示を取得し、またこれに応答して前記クライアントコンピュータが、少なくとも、１つ又は複数の要求を前記解決したアイデンティティプロバイダに送信して、任意の利用可能なデジタルアイデンティティ表示プロビジョニングサービスに関する情報を取得し、さらに前記クライアントコンピュータが、前記解決したアイデンティティプロバイダに用いられるデジタルアイデンティティ表示プロビジョニングサービスに関する情報を含む１つ又は複数のメッセージを受信するステップと

を含む方法を実行するコンピュータプログラム。