JCCH・セキュリティ・ソリューション・システムズ

プライベートCA Gléas ホワイトペーパー

PingFederateのクライアント証明書認証設定
（Office365 先進認証）

Ver. 1.0
2017 年 3 月

目次

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベートCA Gléas」で発行したクライアント証明書を利用して、Ping Identity社のSSOサーバ「PingFederate」経由でMicrosoft Corporationのクラウドサービス「Office 365」の認証をおこなう環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- SAML IDP：Windows Server 2012 R2 Standard / PingFederate 8.2.2
  ※以後、「PingFederate」と記載します
  ※以下のコネクタを追加インストールしています
  - Office365 Connector 2.0.2
  - X.509 Integration Kit 1.2
- SaaSサービス：Office 365 Enterprise E3
  ※以後、「Office365」と記載します
  ※Office365をサービスプロバイダとして利用するには、ビジネスプランのサブスクリプションが必要になります
- ドメインコントローラ： Microsoft Windows Server 2012 R2 Standard
  ※以後、「AD」と記載します
  ※以下のツールをインストールしています
  - Microsoft Online Services サインイン アシスタント
  - Windows PowerShell用 Microsoft Azure Active Directory モジュール
  - Azure AD Connect
- JS3 プライベートCA Gléas （バージョン1.14.6）
  ※以後、「Gléas」と記載します
- クライアント：Windows 10 Pro / Internet Explorer 11 / Excel 2016

※以後、「PC」と記載します

- クライアント：iPhone 5c（iOS 10.2）/
  Outlook 2.12.0 / Microsoft Authenticator 5.1.2

※以後、「iPhone」と記載します

※iOSでは、Microsoft Authenticatorが必要になるので事前にインストールしておきます

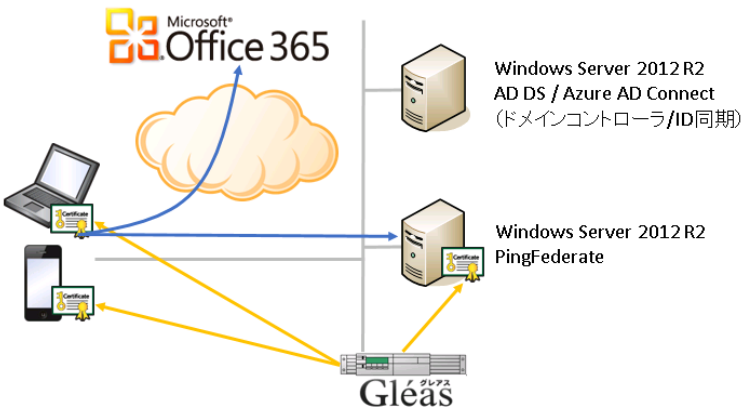
以下については、本書では説明を割愛します。

- Pingの基本的な設定（データストア（Active Directory）の設定含む）、ConnectorやIntegration Kitのインストール
  なお本書では、PingFederateのhttpsのポート設定は以下の通りになっていることを前提としています（<pf_install_directory>¥pingfederate¥bin¥run.properties で確認可能です）
  httpsプライマリポート（pf.https.port）：9031
  httpsセカンダリポート（pf.secondary.https.port）：9032
- Gléasでのアカウント登録や各種証明書発行
  今回は以下の証明書を発行する前提です
  - SSLサーバ証明書
  - SAMLアサーションの署名用証明書
  - クライアント証明書
- Windows ServerやWindowsドメインのセットアップ
- Azure AD Connectを用いたOffice365のユーザプロビジョニング
- PC、iPhoneでのネットワーク設定等の基本設定

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



1. Gléasでは、PingFederate用にSSLサーバ証明書・アサーションの署名用証明書を、PC・iPadの利用者にクライアント証明書を発行する
2. PC：クライアントはブラウザやOfficeアプリケーション（本書ではExcel 2016を利用）でOffice365にアクセスすると、認証先としてPingFederateにリダイレクトされる
3. iOS：Officeモバイルアプリ（本書ではOutlookを利用）でOffice365にアクセスすると、認証先としてPingFederateにリダイレクトされる
4. PingFederateではクライアント証明書認証をおこなう。証明書に記載されているユーザアカウント情報に基づきADより必要な情報を取得し、Office365に送信しログインする。

1.4. 電子証明書の発行時における留意事項

本書の設定内容において、Gléasで電子証明書の発行操作をする際には以下の点に留意する必要があります。

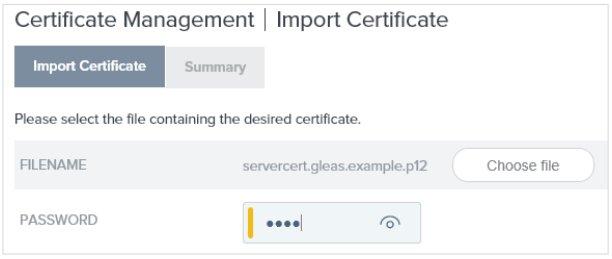
- クライアント証明書
  サブジェクトの代替名（Subject Alt Name）に、ADのユーザ名（userPrincipalName属性）と、有効なCRL配布ポイントが含まれるようにしておきます。

2. PingFederateの設定

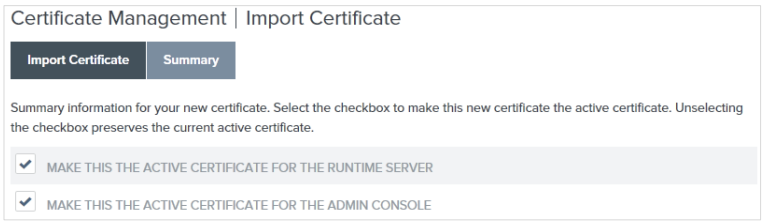
PingFederate の管理 Web 画面にログインし、以下の設定をおこないます。

2.1. サーバ証明書の設定

事前にGléasでサーバ証明書を発行し、ダウンロードしておきます。
Server Configuration > CERTIFICATE MANAGEMENT > SSL Server Certificateと進みます。
[Import]をクリックし、Gléasよりダウンロードしたサーバ証明書ファイルをアップロードします。PASSWORD欄にはGléasから証明書ファイルをダウンロードした際に設定したパスワードを入力します。

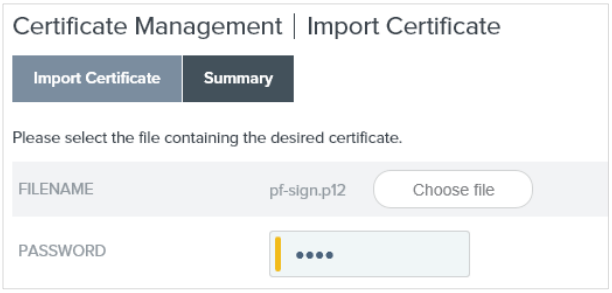


[Next]をクリックするとサマリ画面が表示されます。
“MAKE THIS THE ACTIVE CERTIFICATE FOR THE RUNTIME SERVER”がチェックされていることを確認し、[Save]をクリックして保存します。



2.2. 署名用証明書の設定

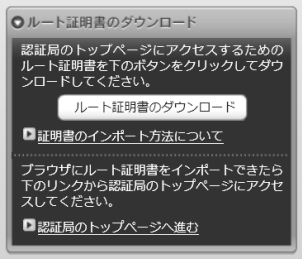
事前にGléasで署名用の証明書を発行し、ダウンロードしておきます。
Server Configuration > CERTIFICATE MANAGEMENT > Signing & Decryption Keys & Certificatesと進みます。
[Import]をクリックし、Gléasよりダウンロードしたサーバ証明書ファイルをアップロードします。PASSWORD欄にはGléasから証明書ファイルをダウンロードした際に設定したパスワードを入力します。



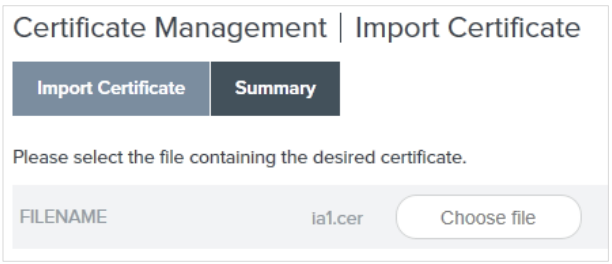
[Next]をクリックするとサマリ画面が表示されるので、内容を確認して[Save]をクリックして保存します。

2.3. ルート証明書の設定

事前に Gléas よりルート証明書をダウンロードしておきます。
※Gléas に http://hostname/（http であることに注意）でアクセスすると、ダウンロードが可能です



Server Configuration > CERTIFICATE MANAGEMENT > Trusted CAsと進みます。
[Import]をクリックし、Gléasよりダウンロードしたルート証明書ファイルをアップロードします

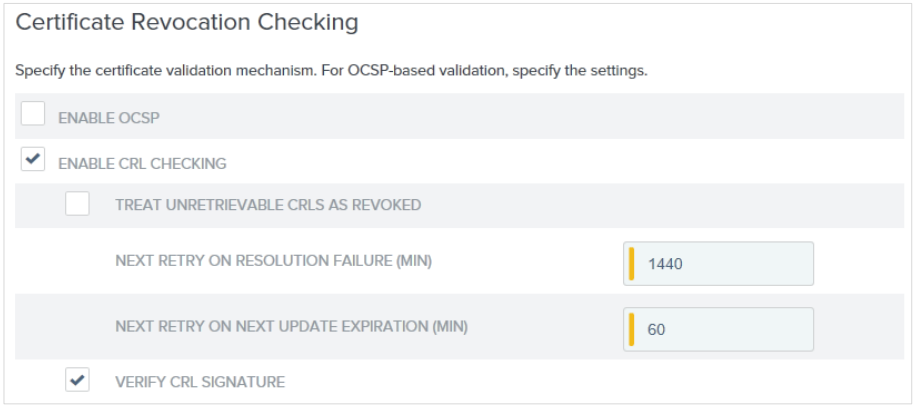


[Next]をクリックするとサマリ画面が表示されるので、内容を確認して[Save]をクリックして保存します。

2.4. 証明書の失効確認設定

Server Configuration > CERTIFICATE MANAGEMENT > Certificate Revocation Checkingと進み、以下の設定をおこないます。

- [Enable CRL Checking]をチェック
- [Verify CRL Signature]をチェック



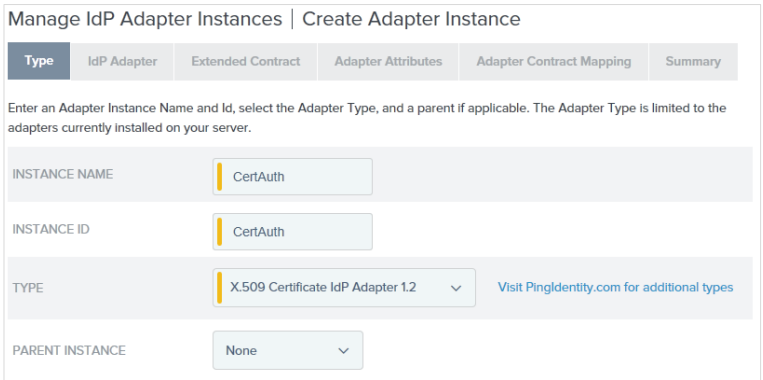
またこの状態で[Enable OCSP]をチェックし設定をおこなうことで、失効確認にOCSPとCRLを併用することも可能です（弊社未検証）。

2.5. X.509 Connector の設定

IDP Configuration ＞ APPLICATION INTEGRATION ＞ Adaptorsを選択します。
Manage IdP Adaptor Instancesで [Create New Instance]をクリックします。
その後、以下を設定します。

Typeタブで以下を設定します。

- INSTANCE NAME：　任意の名称
- INSTANCE ID：　任意の識別ID
- Type：　[X.509 Certificate IdP Adaptor]を選択

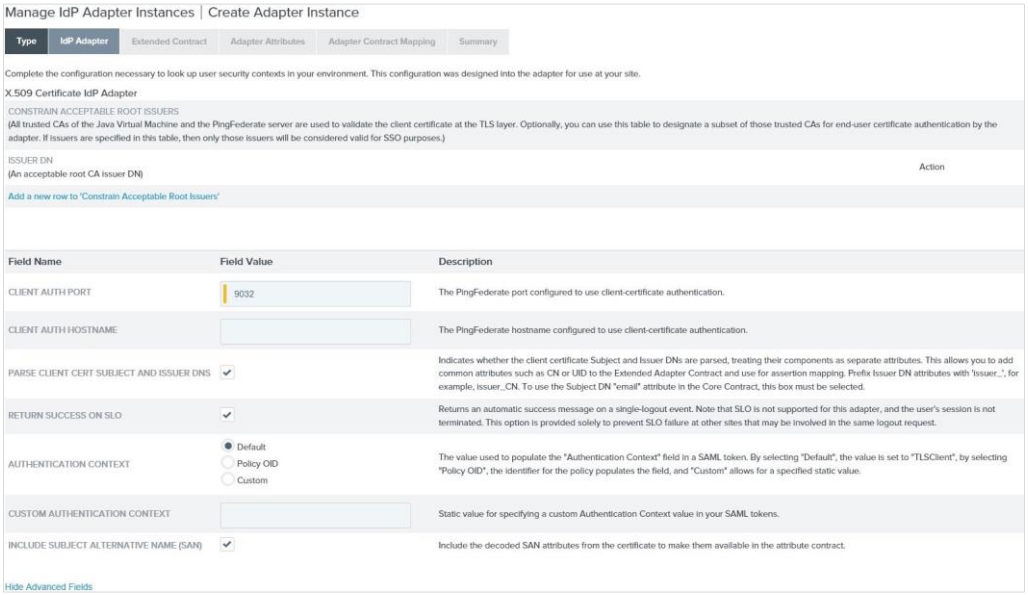


IdP Adaptorタブで以下を設定します。

- CLIENT AUTH PORT：9032（セカンダリのポート番号） を入力

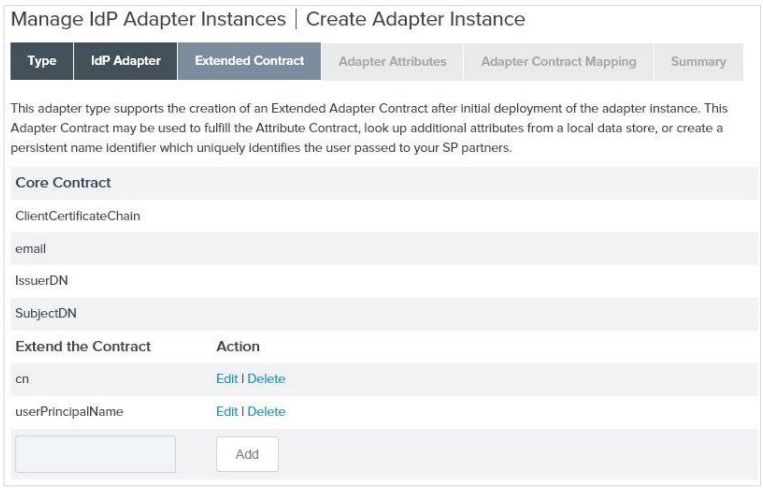
Show Advance Fieldsを展開し、

- INCLUDE SUBJECT ALTERNATIVE NAME (SAN)をチェック



Extend Contractタブで以下を設定します。

- Extend the Contractに、”cn”と”userPrincipalName”を追加



Adaptor Attributesタブで、以下を設定します。

- userPrincipalNameのPseudonymをチェック

Summaryタブで設定を確認し[Done] > [Save]とクリックして設定を保存します。

Manage IdP Adapter Instances | Create Adapter Instance

Type | IdP Adapter | Extended Contract | Adapter Attributes | Adapter Contract Mapping | Summary

IdP adapter instance summary information.

Create Adapter Instance

Type	
Instance Name	CertAuth
Instance Id	CertAuth
Type	X.509 Certificate IdP Adapter 1.2
Class Name	com.pingidentity.adapters.idp.clientcert.ClientCertIdpAuthnAdapter
Parent Instance Name	None
IdP Adapter	
Client Auth Port	9032
Client Auth Hostname	
Parse Client Cert Subject and Issuer DNs	true
Return Success On SLO	true
Authentication Context	Default
Custom Authentication Context	
Include Subject Alternative Name (SAN)	false
Extended Contract	
Attribute	IssuerDN
Attribute	SubjectDN
Attribute	email
Attribute	ClientCertificateChain
Attribute	cn
Attribute	userPrincipalName
Adapter Attributes	
Mask all OGNL expression log values	false
Pseudonym	userPrincipalName

Adapter Contract Mapping

Attribute Sources & User Lookup	
Data Sources	(None)
Adapter Contract Fulfillment	
IssuerDN	IssuerDN (Adapter)
cn	cn (Adapter)
SubjectDN	SubjectDN (Adapter)
email	email (Adapter)
userPrincipalName	userPrincipalName (Adapter)
ClientCertificateChain	ClientCertificateChain (Adapter)
Issuance Criteria	
Criterion	(None)

2.6. サービスプロバイダの設定

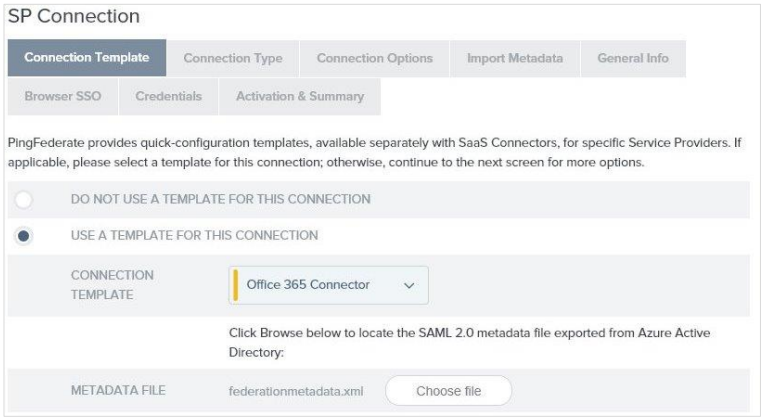
IDP Configuration > SP CONNECTIONSと進み、[Create New]ボタンをクリックし以下の設定をおこないます。

SP Connections > Connection Templateタブ

- USE A TEMPLATE FOR THIS CONNECTIONを選択
- CONNECTION TEMPLATEは、Office 365 Connector を選択
- METADATA FILEは、Office 365のメタデータをアップロード

※Office365のメタデータは、2017年2月現在以下のURLで公開されています

https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml

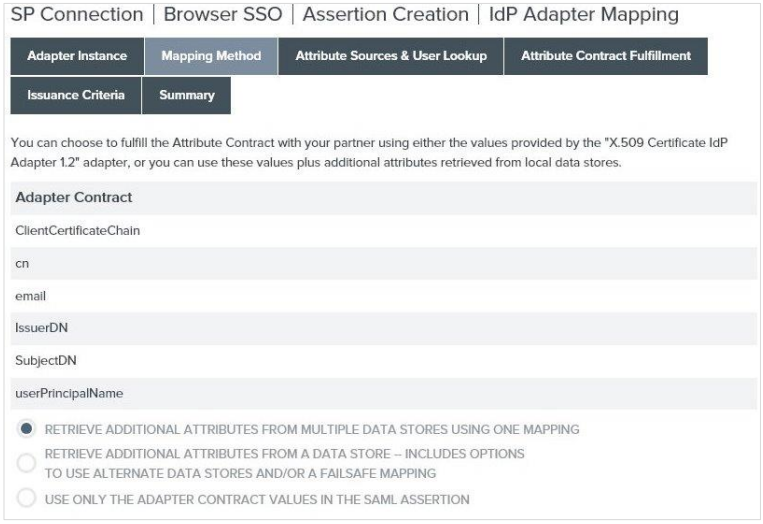


Browser SSOタブで、[Configure Browser SSO]ボタンをクリックします。
SP Connection | Browser SSO > Assertion Creationタブで、[Configure Assertion Creation]ボタンをクリックします。
SP Connection | Browser SSO | Assertion Creation > Authentication Source Mappingタブで[Map New Adaptor Instance]ボタンをクリックします。
SP Connection | Browser SSO | Assertion Creation | IdP Adaptor Mapping > Adaptor Instanceタブで以下を設定します。

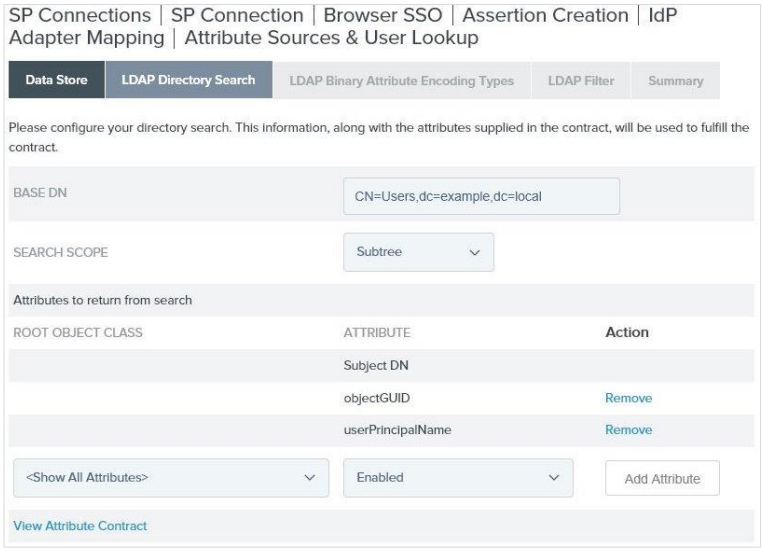
- ADAPTOR INSTANCEで、2.5項で設定したインスタンスを選択

Mapping Methodタブで以下を設定します。

- “RETRIVE ADDITIONAL ATTRIBUTES FROM MULTIPLE DATA STORES USING ONE MAPPING”を選択

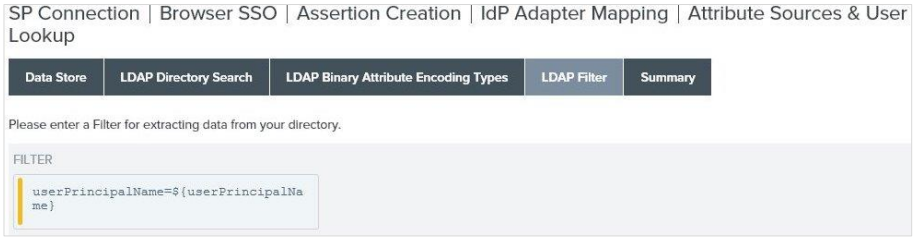


Attribute Sources & User Lookupタブでは、[Add Attribute Source]ボタンをクリックします。
SP Connection | Browser SSO | Assertion Creation | IdP Adaptor Mapping | Attribute Sources & User Lookup > Data Storeタブでは、設定済みのデータストア（Active Directory）を指定します。
LDAP Directory Searchタブでは、LDAPの検索条件を設定します。ここでAttribute to return from searchに、”ObjectGUID”と”userPrincipalName”を追加します。



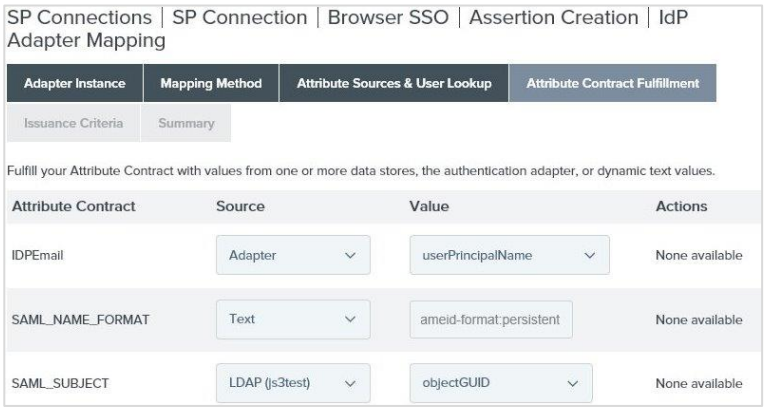
LDAP Binary Attribute Encoding Typeタブにて、objectGUIDのエンコーディングタイプを、”Base64”に設定します。
※LDAP Binary Attribute Encoding Typeタブが出現しない場合は、データストアのADの詳細設定でobjectGUIDをバイナリ属性として設定する必要があります

LDAP Filterタブで、Filter欄に“userPrincipalName=${userPrincipalName}”を入力します。



Summaryタブで設定内容を確認し[Done]をクリックします。
SP Connection | Browser SSO | Assertion Creation | IdP Adaptor Mapping > Attribute Contract Fulfillmentタブで以下を設定

- IDPEmail
  Source:　Adaptor
  Value:　userPrincipalName
- SAML_NAME_FORMAT
  Source:　Text
  Value:　urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- SAML_SUBJECT
  Source:　LDAP(データストア名)
  Value:　objectGUID



Summaryタブで設定内容を確認し[Done]をクリックします。

SP Connection | Browser SSO | Assertion Creation > Summaryタブで設定内容を確認し、[Done]をクリックします。

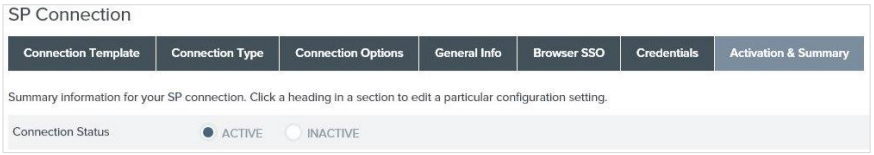
SP Connection | Browser SSO > Protocol Settingタブ・SAML Profilesタブの設定等は環境にあわせておこない、Summaryタブで設定内容を確認し、[Done]をクリックします。

SP Connection > Credentialsタブで[Configure Credentials]をクリックし、SP Connection | Credentials > Digital Signature Settingsタブで以下の設定をおこないます。

- SIGNING CERTIFICATEは、2.2項で設定した署名用証明書を選択
- SIGNING ALGORITHMは、”RSA SHA256”を選択

Summaryタブで設定内容を確認し、[Done]をクリックします。

SP Connection > Activation & Summaryタブで、ACTIVEを選択し[Save]をクリックし設定を保存します。



PingFederateの設定は以上です。

3. Office365（Azure AD）の設定

Office365 の認証をおこなう Azure Active Directory の設定変更のため、「Windows PowerShell 用 Windows Azure Active Directory モジュール」を起動します。

以下のコマンド入力し、Office365 の管理者権限を持つアカウントでログインします。

```
Connect-MsolService
```

ログイン後に以下を入力し、対象ドメインをフェデレーションドメインに変更します。

```
$domainName = "<Federated Domain_Name>"
$pingfederate = "https://<Hostname>:9031"
$brandName = "PingFederate"
$issuer = "<PingFederate_SAML_2_entity_id>"
$spId = "urn:federation:MicrosoftOnline"
$activeLogOn = "$pingfederate/idp/sts.wst"
$logOff="$pingfederate/idp/SLO.saml2"
$metaData="$pingfederate/pf/sts_mex.ping?PartnerSpId=$spId"
$passiveLogOnPF="$pingfederate/idp/SSO.saml2"
$certData="<2.2 項で設定した署名用証明書（テキスト形式）>
Set-MsolDomainAuthentication -DomainName "$domainName" `
-FederationBrandName "$brandName" -Authentication Federated `
-PassiveLogOnUri "$passiveLogOnPF" -SigningCertificate "$certData" `
-IssuerUri "$issuer" -ActiveLogOnUri "$activeLogOn" `
-LogOffUri "$logOff" -MetadataExchangeUri "$metaData" `
-PreferredAuthenticationProtocol SAMLP
```

※<PingFederate_SAML_2_entity_id>は、PingFederate の設定画面の以下項目に設定されているものとなります
Server Configuration > System Settings > Server Settings > Federation Info > SAML 2.0 Entity ID

以下のコマンドを実行することで設定内容の確認が可能です。

```
Get-MsolDomainFederationSettings -DomainName <DomainName>
```

※Exchange Online で先進認証を有効にするためには、以下の操作が必要です。
https://support.office.com/en-us/article/Enable-Exchange-Online-for-modern-authentication-58018196-f918-49cd-8238-56f57f38d662

4. Gléasの管理者設定（PC）

GléasのUA（申込局）より発行済み証明書をPCにインポートできるよう設定します。
※下記設定は、Gléas納品時等に弊社で設定を既に行っている場合があります

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA（申込局）をクリックします。

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

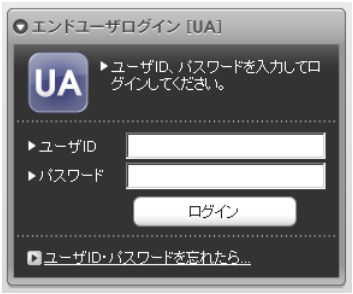
- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

設定終了後、[保存]をクリックし設定を保存します。
各項目の入力が終わったら、 [保存]をクリックします。

5. クライアント操作（PC）

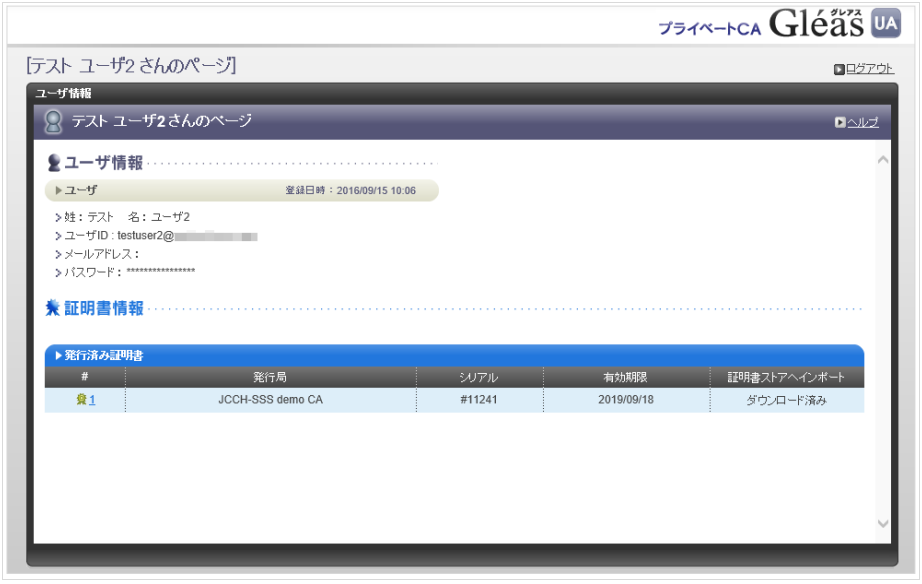
5.1. クライアント証明書のインポート

Internet ExplorerでGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、Gléasでのユーザ IDとパスワードを入力しログインします。



ログインすると、ユーザ専用ページが表示されます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。
※初回ログインの際は、ActiveXコントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。

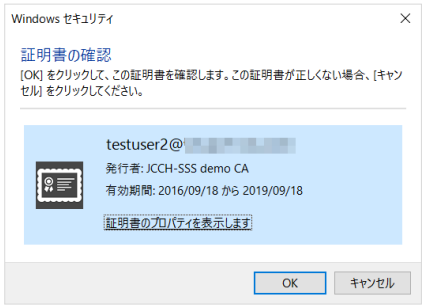
「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。



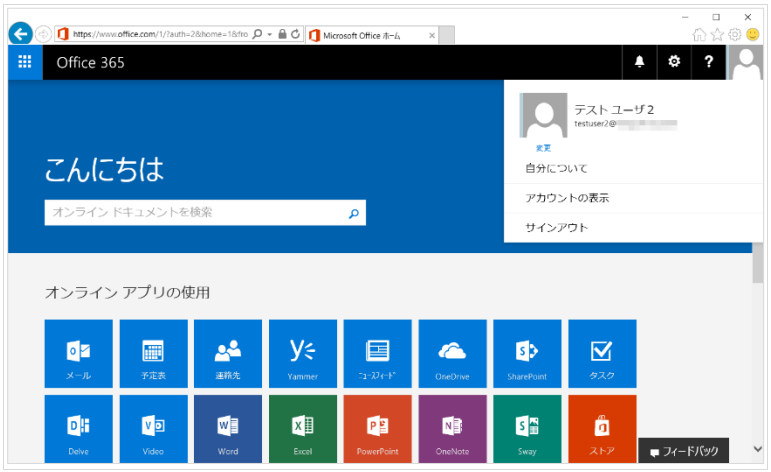
5.2. Office365 へのアクセス（ブラウザ）

Internet ExplorerでOffice365へアクセスし、ドメイン名を含むユーザIDを入力します。その後、PingFederateに転送されクライアント証明書を求められます。

※PingFederateのURLがローカルイントラネットゾーンに設定されている場合など、IEの設定によっては以下の「Windows セキュリティ」画面は表示されない場合もあります



認証が完了すると、Office365のポータル画面が表示されます。

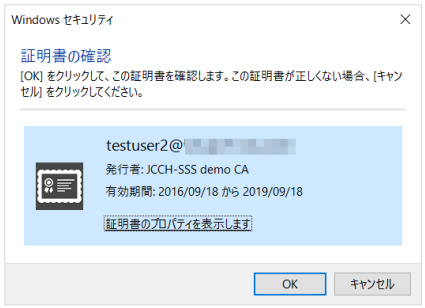


5.3. Office365 へのアクセス（Office アプリ）

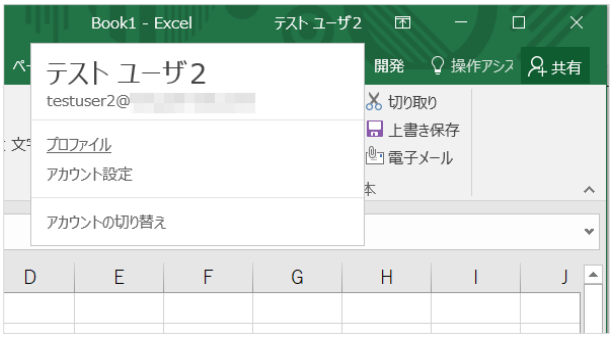
Excel 2016をひらきタイトルバーにある[サインイン]をクリックします。

Office365ログイン用のユーザIDを入力します。

その後、ブラウザでのアクセスと同様にクライアント証明書を提示するよう求められます。



認証に成功するとログインユーザが表示されるようになります。



同時にOneDriveやSharePoint Onlineにもログインするので、オンラインストレージを透過的に利用することが可能です。

また一度ログインした情報はキャッシュされるので、他のOfficeアプリケーションを開いてもログインした状態になります。

証明書を提示しない場合は以下のメッセージが表示されます。

失効された証明書でアクセスすると、ログインに失敗します。
この時にPingFederateのserver.logには、以下のログが書き込まれます。

```
[com.pingidentity.crypto.RevocationCheckerImpl] Certificate issued to <証明書サブジェクト> has been revoked as indicated by CRL found at <証明書CRL配布ポイント>
```

※server.logファイルは <pf_install_directory>¥pingfederate¥log にあります

6. Gléas の管理者設定（iPhone）

Gléas で、発行済みのクライアント証明書を iPhone にインポートするための設定を記載します。

※　下記設定は、Gléas の納品時に弊社で設定を既にしている場合があります

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA（申込局）をクリックします。
[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック
  この設定を行うと、GléasのUAからインポートから指定した時間（分）を経過した後は、構成プロファイルのダウンロードが不可能になります（インポートロック機能）。これにより複数台のデバイスへの構成プロファイルのインストールを

制限することができます。

設定終了後、[保存]をクリックし設定を保存します。

[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利用する]をチェックします。

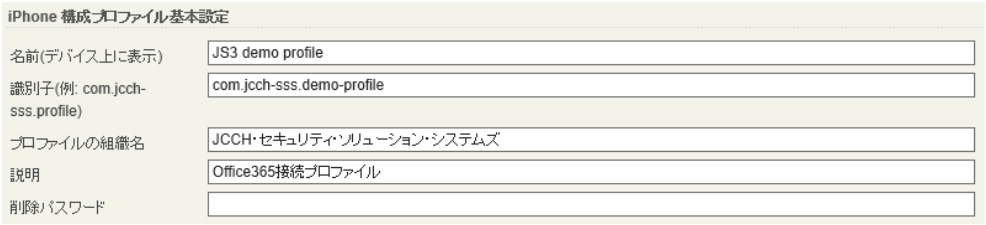
構成プロファイル生成に必要となる情報を入力する画面が展開されるので、以下設定を行います。

画面レイアウト

- [iPhone用レイアウトを利用する]をチェック
- [ログインパスワードで証明書を保護]をチェック

iPhone構成プロファイル基本設定

- [名前]、[識別子]に任意の文字を入力（必須項目）
- [削除パスワード]を設定すると、iPhoneユーザが設定プロファイルを削除する際に管理者が定めたパスワードが必要となります（iPhoneユーザの誤操作等による構成プロファイルの削除を防止できます）



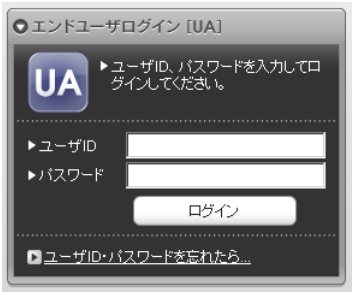
各項目の入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

7. クライアント操作（iPhone）

7.1. クライアント証明書のインポート

iPhoneのブラウザ（Safari）でGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。



ログインすると、そのユーザ専用ページが表示されるので、[ダウンロード]をタップし、構成プロファイルのダウンロードを開始します。
※インポートロックを有効にしている場合は、この時点からカウントが開始されます

自動的にプロファイル画面に遷移するので、[インストール]をタップします。
なお、[詳細]をタップすると、インストールされる証明書情報を見ることが可能ですので、必要に応じ確認してください。

以下のようなルート証明書のインストール確認画面が現れますので、内容を確認し[インストール]をクリックして続行してください。
※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります。

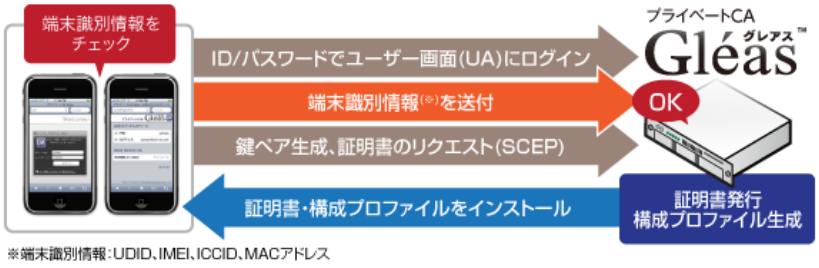
インストール完了画面になりますので、[完了]をタップしてください。

元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトします。

以上で、iPhoneでの構成プロファイルのインストールは終了です。
なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可となります。

7.2. OTAエンロールメントを利用した証明書発行について

Gléasでは、iOSデバイスに対するOver The Air（OTA）エンロールメントを利用した証明書の発行・構成プロファイルの配布も可能です。
OTAを利用すると事前に指定した端末識別番号を持つ端末だけに証明書の発行を限定することも可能になります。

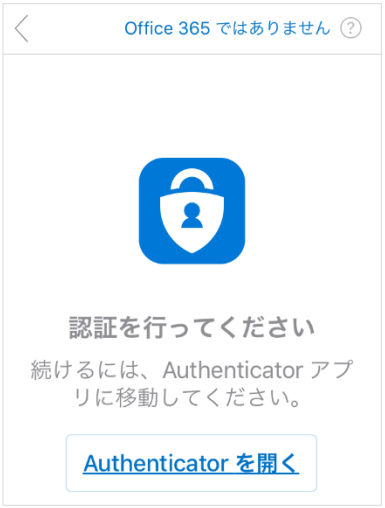


詳細は最終項のお問い合わせ先までお問い合わせください。

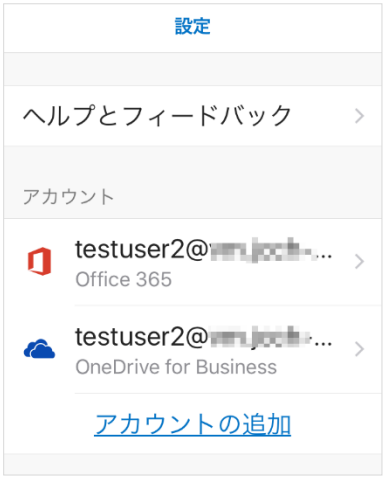
7.3. Office365へのアクセス

Outlook アプリを起動してアカウントの追加をおこないます。

画面の指示にしたがい、Microsoft Authenticator を開きます。



その後、証明書認証がバックグラウンドでおこなわれ、ログインが完了しメール閲覧が可能となります。
この状態で Outlook アプリの[設定]をタップすると、Office365 や OneDrive にログインしていることがわかります。



有効な証明書を提示できない場合は、以下のようになります。

また Microsoft Authenticator を見ると、Azure AD にログインできたことが記録されています。
（Microsoft Authenticator を認証に使う他 Office モバイルアプリもこの認証結果情報を参照します）

8. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■PingFederateに関するお問い合わせ先
マクニカネットワークス株式会社
Mail:　ping-sales@cs.macnica.net

■Gléasや検証用の証明書に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ
営業本部
Tel:　050-3821-2195
Mail:　sales@jcch-sss.com