ID パスワード発行申請マニュアル

認定タイムスタンプ byGMO

GlobalSign by GMO

Ver 1.0.0 2024/06/11

目次

初回のお客さまの ID パスワード発行や変更時など、お客様と弊社で ID パスワード情報をやり取りする際、セキュリティのためファイル暗号化をしてメールにてお渡しします。
以下の手順に沿ってパスワードを暗号化する秘密鍵、公開鍵の生成、ID パスワード情報の復号を行ってください。

本マニュアルは、その手順をご案内するものです。コマンドの意味等につきましては、各情報サイトや参考書籍等でご確認ください。

1 事前準備

Openssl のコマンド操作が必要です。
Openssl を使用できる環境をご準備ください。

Openssl 公式ウェブサイト ダウンロードページ:
https://www.openssl.org/source/

Windows をお使いのお客様はこちらのページをご参照ください。
https://jp.globalsign.com/support/ssl/confinfo/opnssl-command.html

2 鍵ペアを生成する

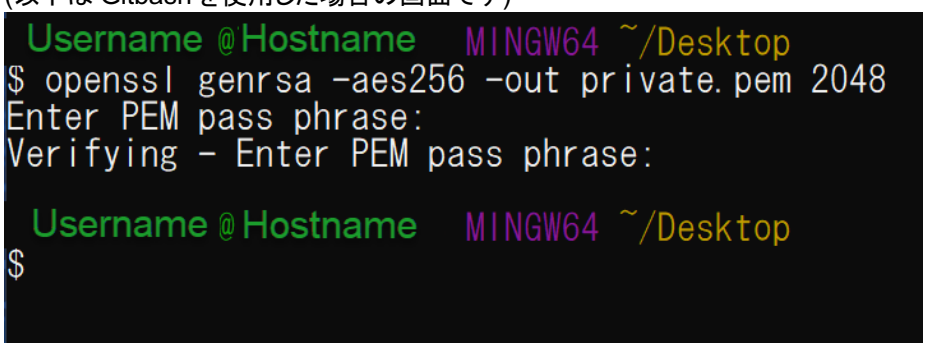
次の手順に沿って、ID パスワード情報の弊社による暗号化、お客さまによる復号のための鍵ペアを生成してください。

2.1 操作画面を開き、生成した鍵ファイルを保存するディレクトリに移動します。
コマンド例:
```
cd Desktop/
```

2.2 次のコマンドを実行し、鍵を生成します。
```
openssl genrsa -aes256 -out private.pem 2048
```

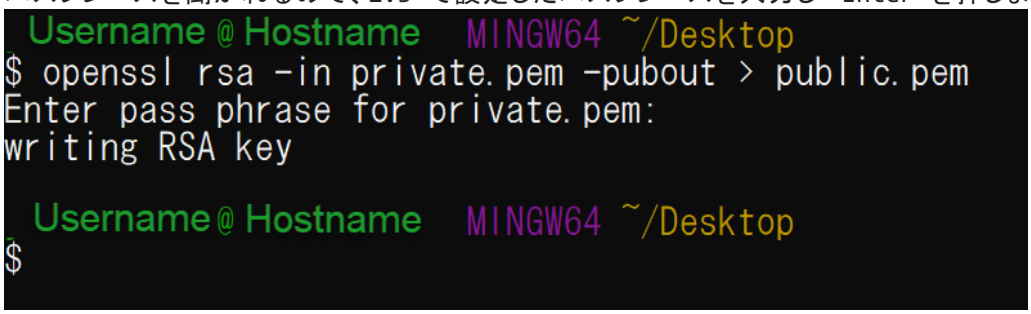
2.3 PEM pass phrase を聞かれるので、今回生成する鍵専用のパスフレーズを 2 回入力し Enter を押します。
※パスフレーズを 16 桁以上で作成することをお勧めします。

成功すると、画面表示はこのようになります。
(以下は Gitbash を使用した場合の画面です)

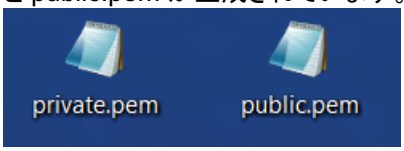


2.4 次のコマンドを実行し、公開鍵を取り出します。
```
openssl rsa -in private.pem -pubout > public.pem
```

2.5　パスフレーズを聞かれるので、2.3 で設定したパスフレーズを入力し Enter を押します。



2.6　本マニュアルではデスクトップに移動してコマンドを実行したので、デスクトップ上に private.pem と public.pem が生成されています。



【重要】
private.pem はパスワードの復号に必要です。外部に公開せず大事に保管してください。
public.pem は弊社営業担当へメールにてお送りください。

3 ID パスワード復号

ID パスワードは弊社より営業担当者を通じて暗号化した状態でお送りいたします。
次の手順で送られてきたファイルを復号し、ID パスワードをご確認ください。

2.7　弊社から送られてきた暗号化された ID パスワードファイルを 2.6 で生成した private.pem と同じディレクトリに置きます。

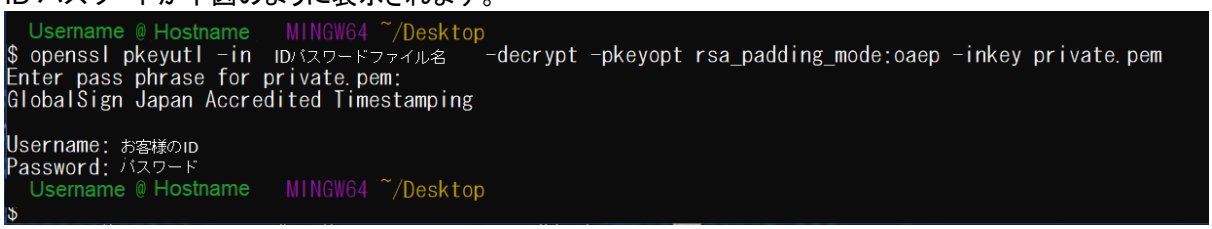
2.8　Openssl を開いてください。

2.9　private.pem と ID パスワードファイルが置かれているディレクトリに移動します。
コマンド例:
`cd Desktop/`

2.10　次のコマンドを実行し、復号します。
`openssl pkeyutl -in 暗号化された ID パスワードファイル名 -decrypt -pkeyopt rsa_padding_mode:oaep -inkey private.pem`

2.11　パスフレーズを聞かれるので、本マニュアルの 2.3 で設定したパスフレーズを入力します。

2.12　ID パスワードが下図のように表示されます。



以上です。

GMO グローバルサイン株式会社
〒150-0043 東京都渋谷区道玄坂 1-2-3　渋谷フクラス
TEL：03-6370-6500　https://jp.globalsign.com