DigiCert® KeyLocker
クラウド秘密鍵ストレージサービス
～ご利用手順～

最終更新日：2024/04/05

DigiCert KeyLocker の利用手順（概要）

1. CertCentralでコードサイニング証明書製品を新規申請、更新申請します。

2. 申請フォームのプロビジョニングオプションで「DigiCert KeyLocker cloud HSM」を選択し申請を完了させます。
   - DigiCert KeyLockerでは、FIPS 140-2レベル3に準拠したHSMに秘密鍵を自動的に生成の上、安全に保管します。この秘密鍵でCSRを自動的に生成し申請したオーダーへ自動的にアップロードします。
   - コードサイニング証明書が発行されると、生成された鍵に関連付けられ、DigiCert KeyLockerに自動的に保存されます。

3. 組織の承認者（DigiCert KeyLockerの管理者）宛に送信されたメールから"DigiCert ONE"のDigiCert KeyLockerへサインインしてください。
   ◆「DigiCert KeyLocker」を利用するために、“DigiCert ONE（デジサートの別のソリューション）”のアカウント作成を承認者にメールが送信されます。
   - 申請者が組織の承認権限がある場合：申請者がDigiCert KeyLockerの管理者となります。
   - 申請者が組織の承認権限をない場合：承認者がDigiCert KeyLockerの管理者となります。

   ※ DigiCert KeyLockerの管理者は署名者となるユーザーの登録/設定をすることができます。

   ◆件名「Welcome to DigiCert ONE」もしくは「DigiCert ONEへようこそ」
   このメールには、DigiCert KeyLocker管理者となるユーザー名が含まれています。このメールで提供されたユーザー名のパスワード設定が必要です。
   本文内のリンクからお客様自身でパスワードとOTP（二要素認証）を設定してサインインしてください。

4. DigiCert KeyLockerへサインインした後、 DigiCert KeyLockerの管理者は署名者の登録を行います。
   - DigiCert KeyLockerの管理者もしくは、追加ユーザーを登録してオーダーの署名者を設定します。署名者として登録できるユーザーは1名（変更可）です。
   - 証明書が発行された後、割り当てられた署名担当者がDigiCert KeyLockerを利用して署名を行うことができます。
   - DigiCert KeyLocker は、証明書の有効期間に関わらず1オーダー毎に 1,000回まで署名することができます。署名可能回数の追加は申請後、CertCentralのオーダー詳細画面から追加購入が可能です。

5. DigiCert KeyLockerで署名環境を設定します。
   - 必要なツールのダウンロード、KeyLockerと連携するためのAPIトークン取得、署名時に提示するクライアント証明書を取得して設定します。

1.【CertCentral】新規 / 更新申請：OV/EVコードサイニング証明書

◆ 新規申請はCertCentral左メニュー[証明書の申請]から製品をご選択の上ご申請ください

日本語製品名称	英語製品名称
コードサイニング証明書	Code Signing
EVコードサイニング証明書	EV CodeSigning

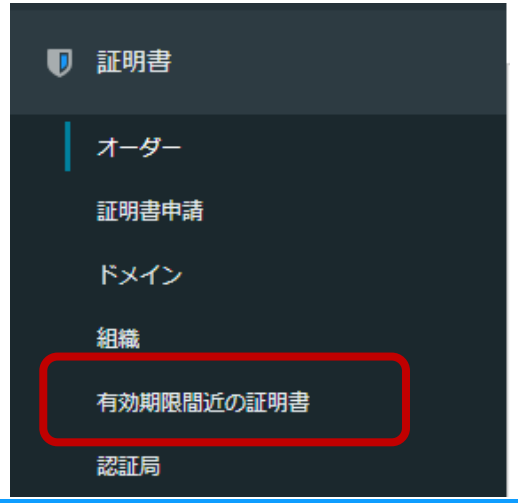
※ご注意ください※

- 新規申請/更新申請共に初回のご申請時でのみプロビジョニングオプション「DigiCert KeyLocker」を選択することが可能です。再発行申請で他のプロビジョニングから「DigiCert KeyLocker」へ変更することはできません。
- バウチャーをご利用の場合は、バウチャー券面にコードサイニング証明書の製品名と[KeyLocker]の表記があることを確認の上、バウチャー内のURLからご申請ください。

製品タイプ	有効期限	バウチャーの有効期限	トークン
コードサイニング証明書	1 年	2025-03-19	KeyLocker

[CertCentral]バウチャー(クーポン) を利用するうえでの注意点について
https://knowledge.digicert.com/ja/jp/solution/SO23021.html

◆ 更新申請はCertCentral左メニュー[証明書]＞[有効期限間近の証明書]からご申請ください

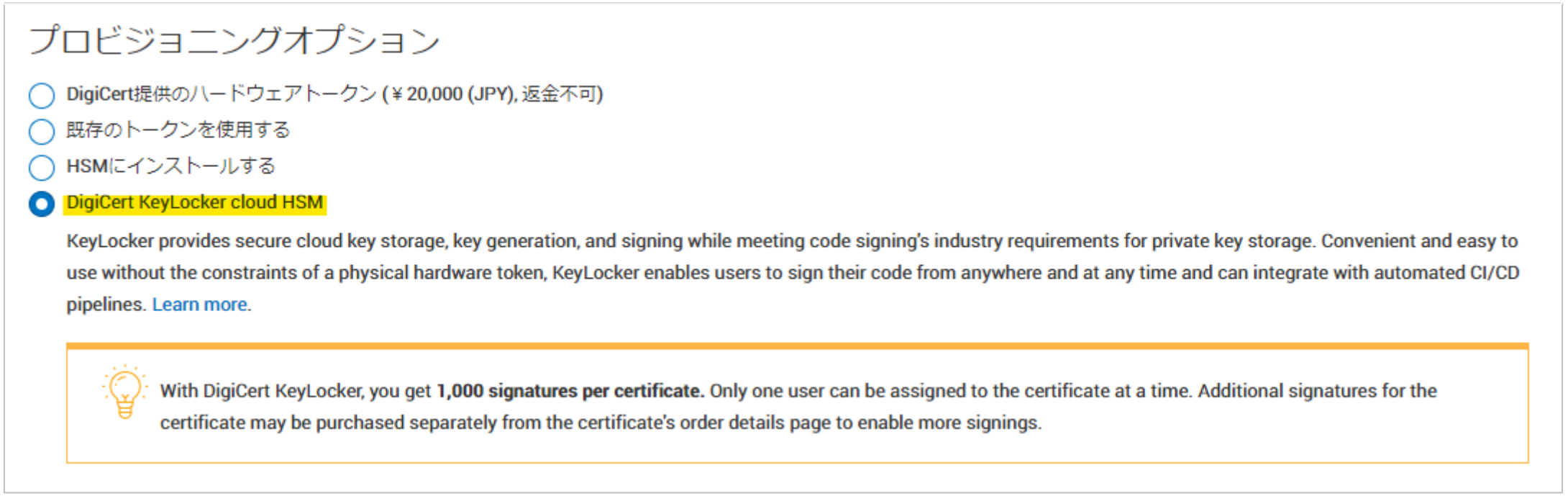


2.【CertCentral】証明書の申請 :プロビジョニングオプション

プロビジョニングオプションでは、OV/EVコードサイニング証明書の秘密鍵を格納する方法の選択をします。
DigiCert KeyLocker クラウド秘密鍵ストレージサービスは「DigiCert KeyLocker cloud HSM」をご選択ください。

企業認証コードサイニング証明書における秘密鍵の格納に関する要件
https://knowledge.digicert.com/ja/jp/generalinformation/INFO2526.html

- DigiCert KeyLocker は、証明書の有効期間に関わらず1オーダー毎に 1,000回まで署名することができます。署名可能回数の追加は申請後、CertCentralのオーダー詳細画面から追加購入が可能です。
- 署名者として登録できるユーザーは1名（変更可）です。

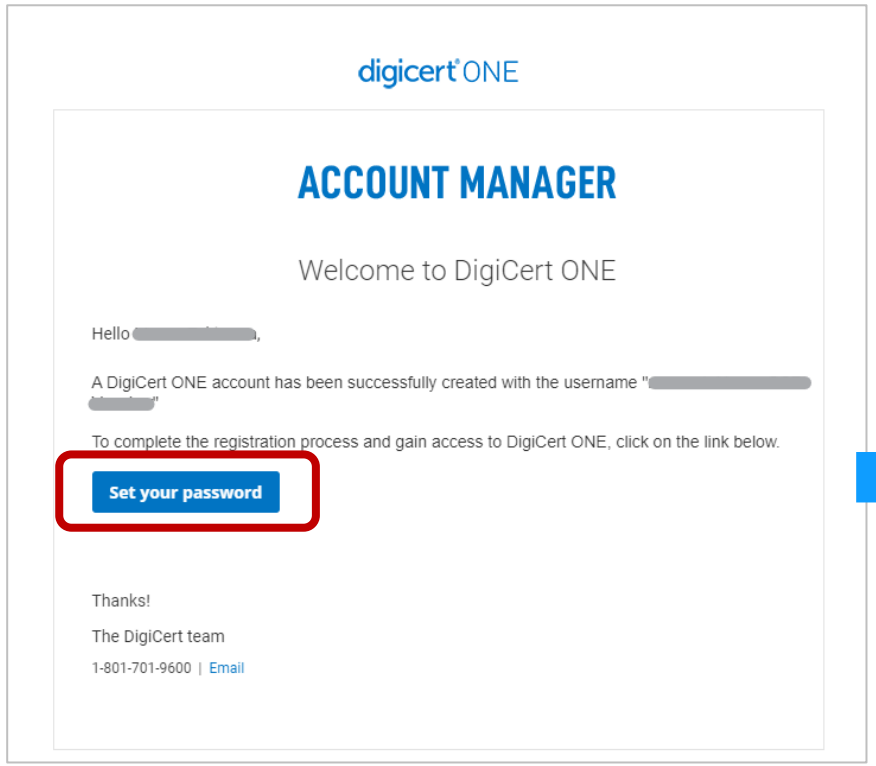


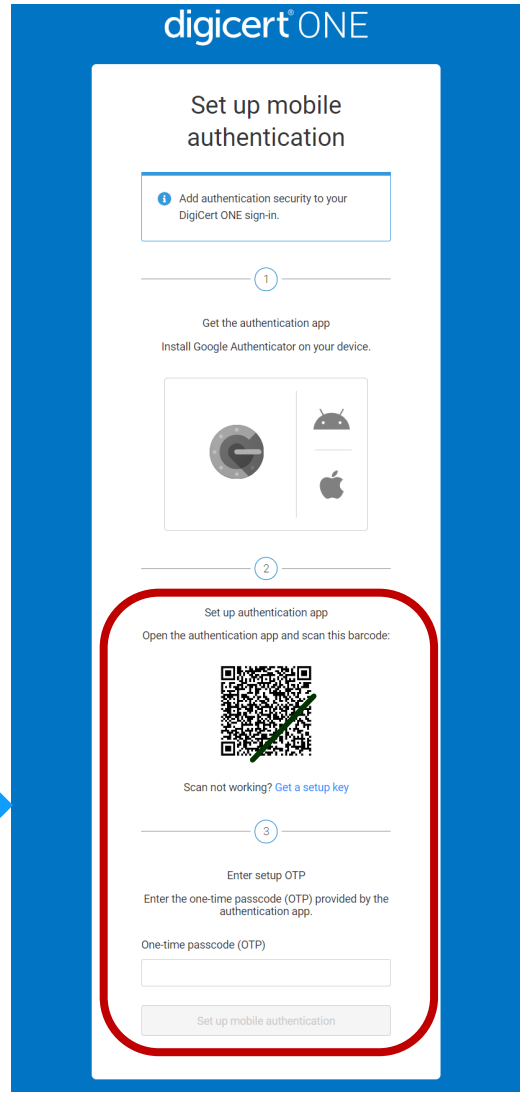
3-1.【DigiCert ONE】DigiCert KeyLockerにサインインする

1. 「DigiCert KeyLocker」を利用するために、“DigiCert ONE（デジサートの別のソリューション）”のアカウント作成のメールが届きます。
   メール本文内にある「Set your password」リンクからパスワードとOTP（二要素認証）を設定してサインインしてください。
   件名：「Welcome to DigiCert ONE」もしくは「DigiCert ONEへようこそ」
   From： no-reply@digicert.com

2. パスワードを８文字以上（小文字/大文字/記号/数字を含む）で設定します。

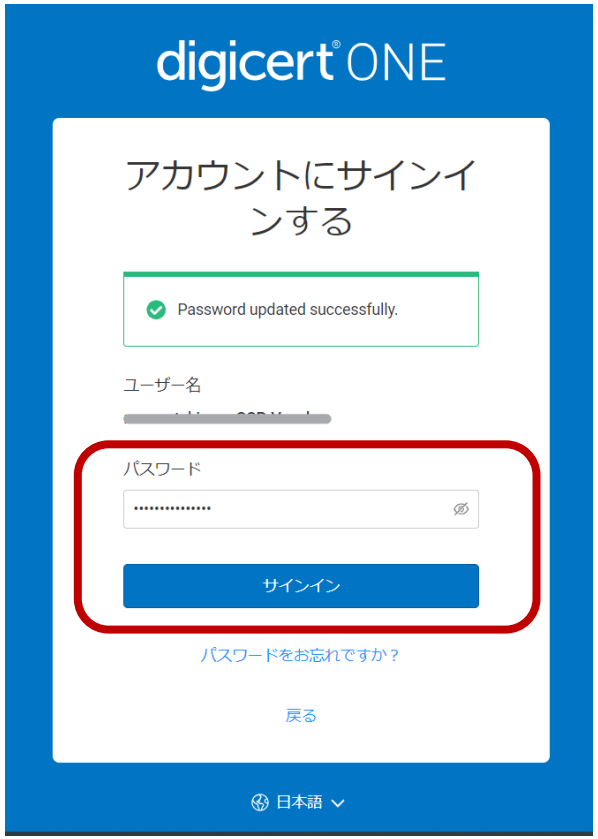
3. 二要素認証設定のためワンタイムパスワード（OTP）の設定画面が表示されます。
   Google Authenticator,Microsoft Authenticator等のOTPアプリケーションをインストールしたスマートフォン等のデバイスやブラウザ拡張機能のAuthenticator等でQRコードのスキャンまたはコードを入力し登録します。

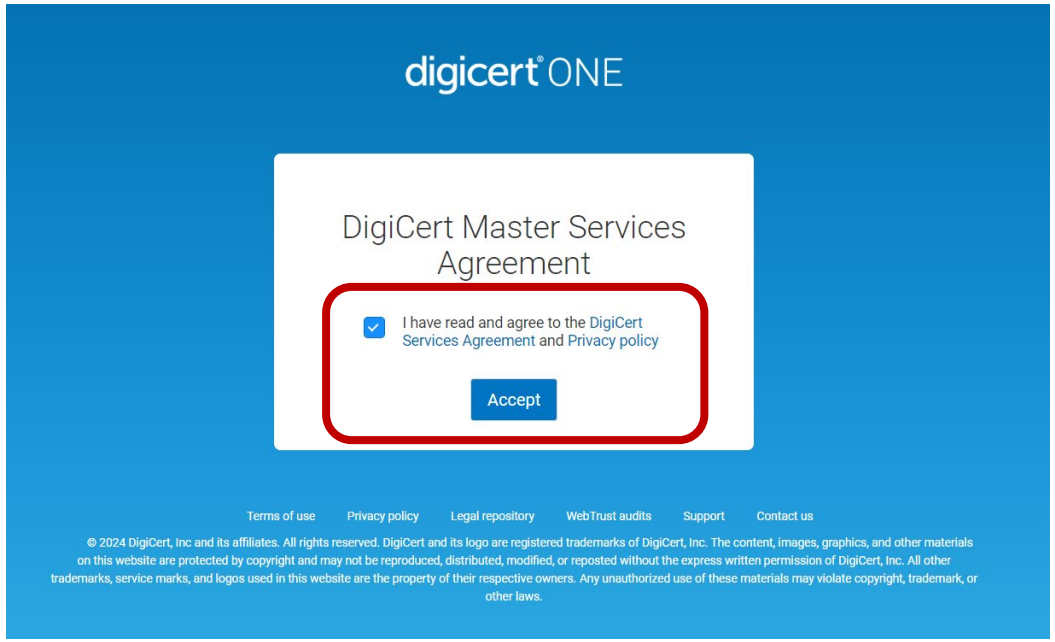




3-2.【DigiCert ONE】DigiCert KeyLockerにサインインする

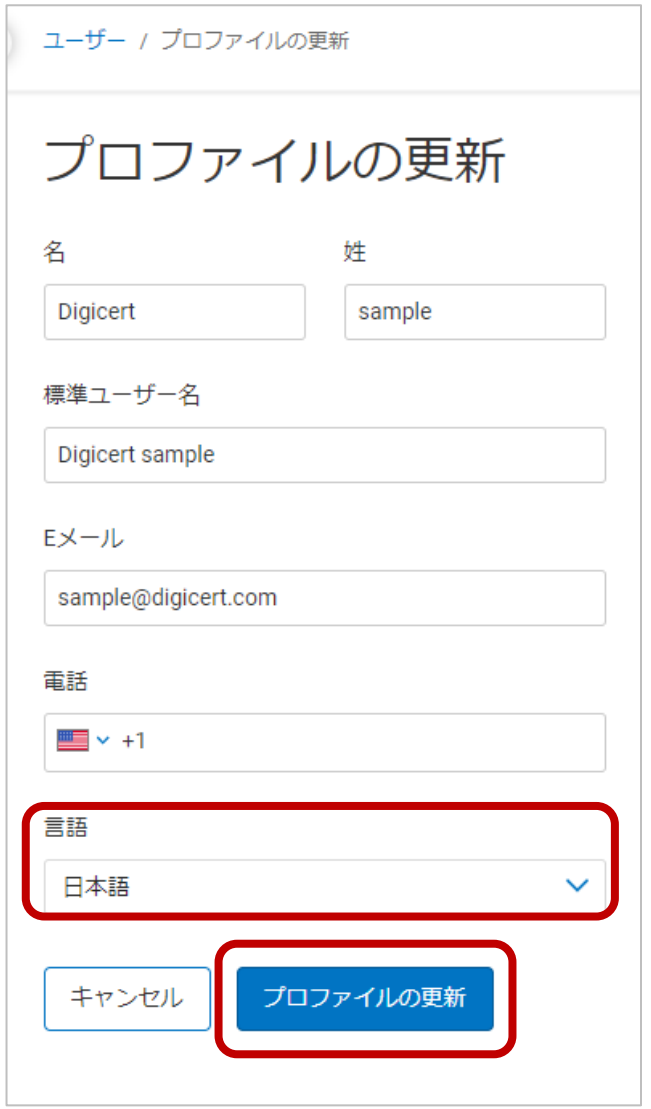
4. サインイン画面で設定したパスワードを入力し「サインイン」ボタンを押下します。
5. 「DigiCert Master Services Agreement」に同意のチェックを入れ「Accept」を押下します。
6. “DigiCert ONE”のDigiCert KeyLockerへサインインが完了しました。



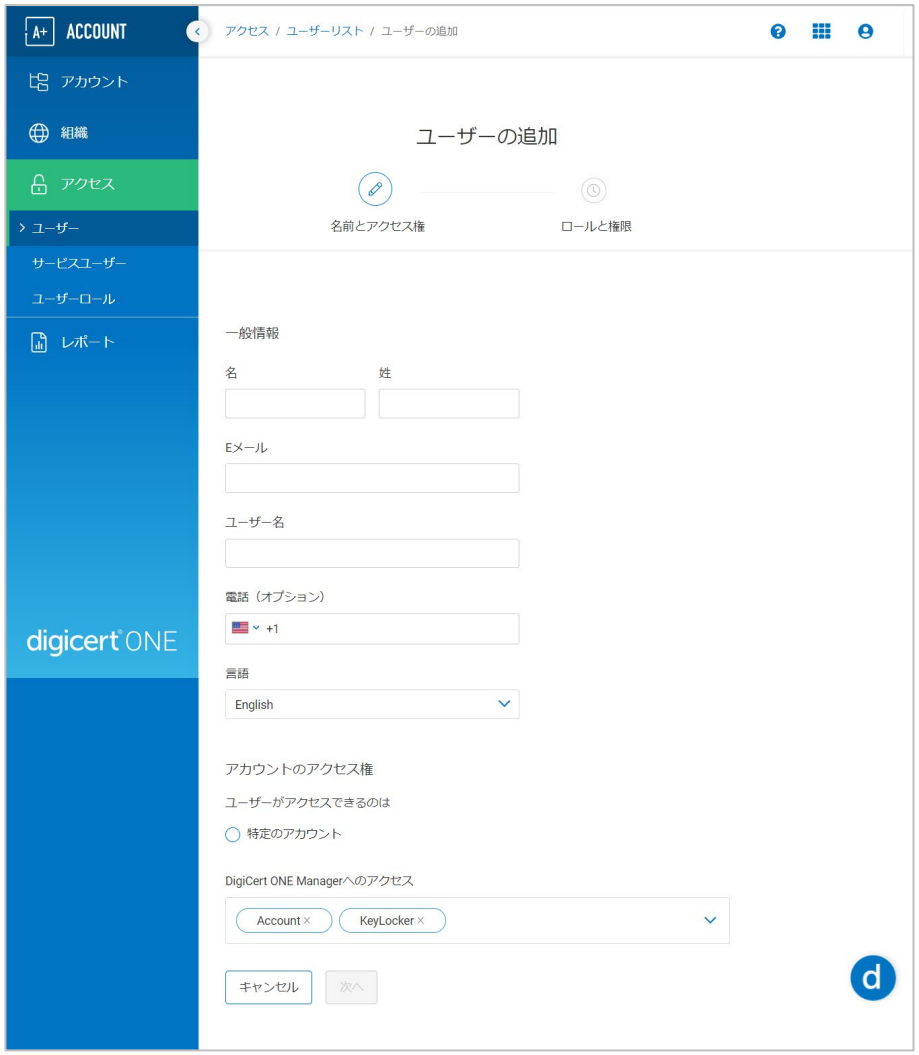


3-3. 補足【DigiCert ONE】言語設定方法（日本語へ切り替える）

1. DigiCert ONEの画面右上にある人型のアイコンをクリックします。
2. 「管理者プロファイル」を選択します。
3. 画面右側にある鉛筆マークをクリックします。
4. 「Language（言語）」で「Japanese（日本語）」を選択し「プロファイルの更新」を押下して設定完了です。



4-1.【DigiCert ONE】DigiCert KeyLockerで署名者のユーザーを追加する



1. DigiCert ONEにサインインした後、Account左メニュー[アクセス]>[ユーザー]へアクセスします。
2. 「ユーザーの追加」を選択します。
3. ユーザー登録画面で必要事項を記入して「次へ」進めます。

項目	入力内容
名/姓	名/姓を入力します
Eメール	ご担当者様のEメールアドレスを入力します
ユーザ名	サインイン時のユーザー名を入力します。 ※Eメールアドレスである必要はありません
電話（オプション）	ブランク（未記入）で構いません
言語	日本語を選択
アカウントのアクセス権	「特定のアカウント」を選択しアカウントを選択します
DigiCert ONE Managerへのアクセス	KeyLockerを選択します ※ユーザーアカウントの管理権限が必要である場合は「Account」も選択してください

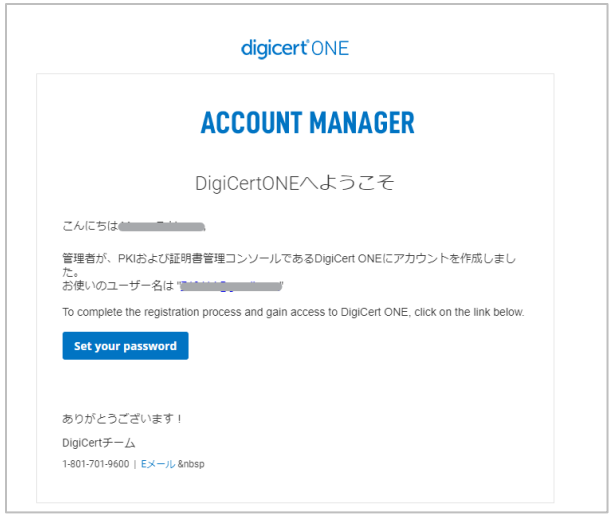
4-2.【DigiCert ONE】DigiCert KeyLockerで署名者のユーザーを追加する

4. ロールと権限の選択をして署名するユーザーの追加を完了させます。

- DigiCert KeyLockerでアカウント設定とユーザアクセスを管理する管理者権限を含める場合
  - AccountManager：アカウント管理者（Account admin）を選択
  - Keylocker ：STMキーロッカー管理者（STM Keylocker admin）を選択

- 署名担当者としてのみ登録し管理者権限によるアカウントの編集権利を持たせない場合
  - AccountManager：デフォルトのユーザー（Default user）
  - Keylocker ： STMキーロッカーユーザー（STM Keylocker user）

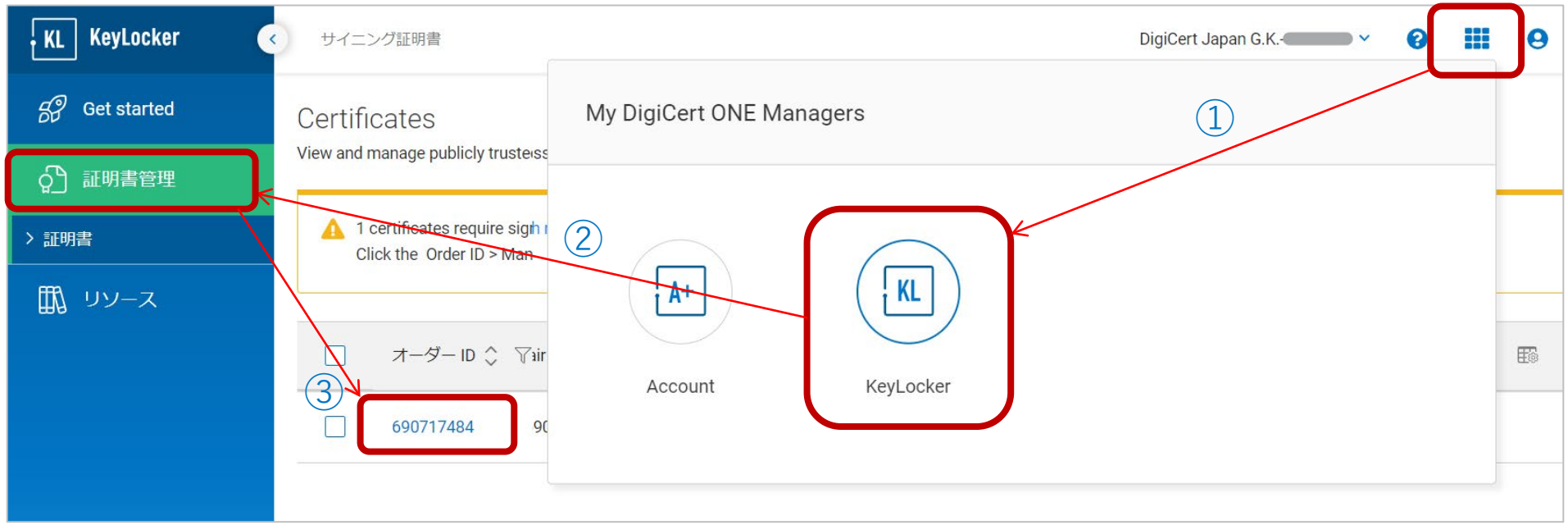
参考サイト：サービスユーザーアカウント（英語）
https://docs.digicert.com/ja/digicert-keylocker/general/users/types-of-users/user.html



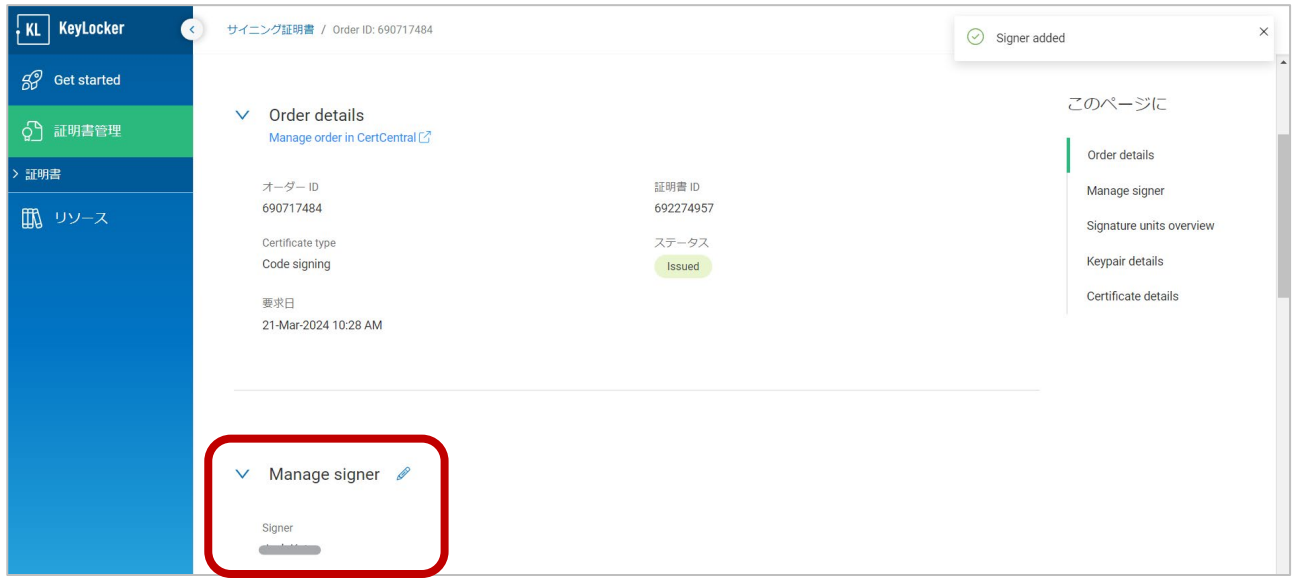
5. ユーザーの追加が完了した後、追加したEメールアドレス宛に「DigiCert KeyLocker」を利用するための、“DigiCert ONE（デジサートの別のソリューション）”のWelcomeメールが届きます。3-1、3-2の手順を参考にして設定してください。

4-3.【DigiCert ONE】DigiCert KeyLockerで署名者を登録/変更する

1. DigiCert ONEの画面右上にあるマークをクリックし表示されたメニューアイコンの「KeyLocker」をクリックします。
2. 左メニュー「証明書管理」を選択します。
3. 「Certificates」の一覧にCertCentralで申請したオーダー番号と同じオーダーIDの数字をクリックします。



4-4.【DigiCert ONE】DigiCert KeyLockerで署名者を登録/変更する

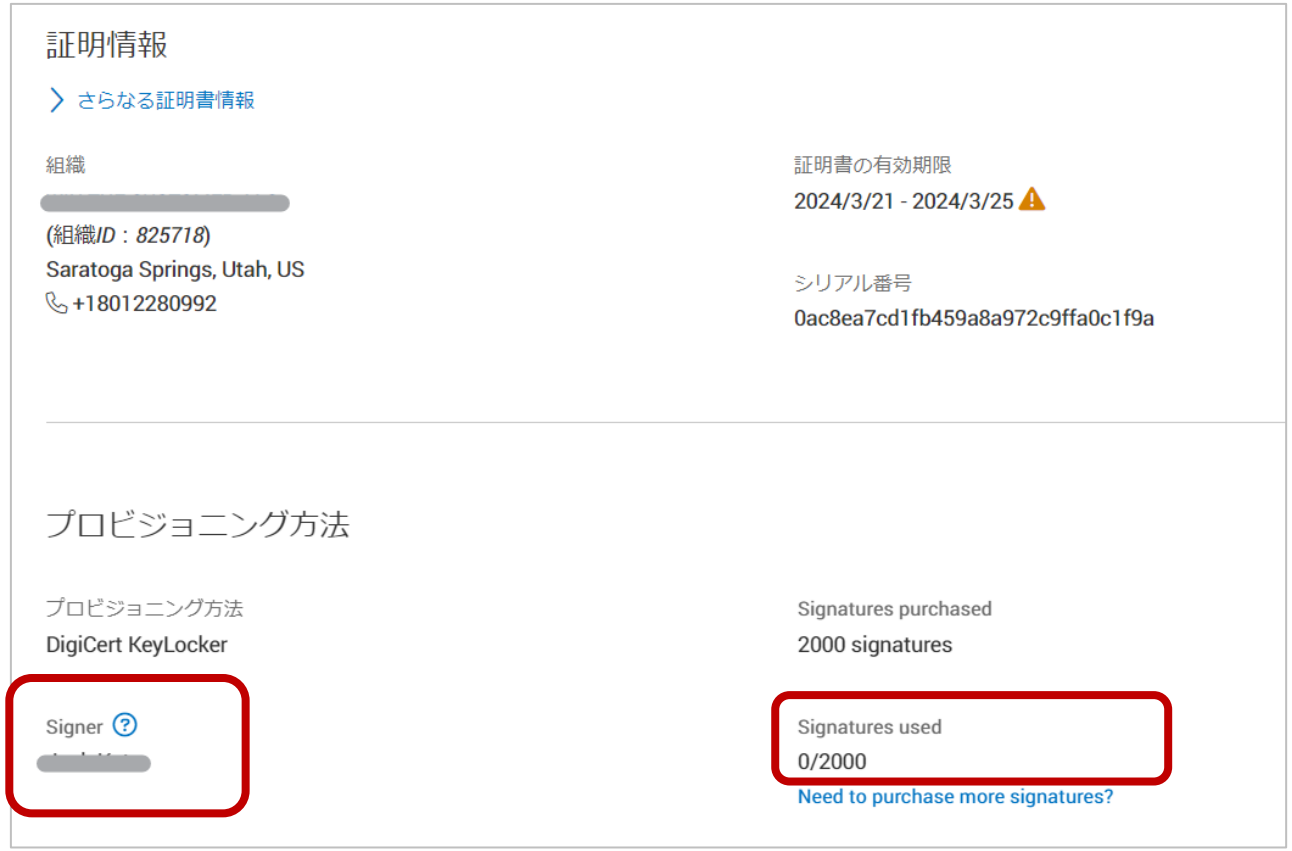


4. オーダー詳細画面内にある「Manage signer」で署名者を追加するために「Add a signer」をクリックします。

5. 右側に表示されるメニュー「Add a signer」の「User」から署名者をプルダウンから選択しチェックボックスにチェックします。署名者として登録できるユーザーは1名までです。署名者を変更をする際は鉛筆マークから編集が可能です。

6. オーダー詳細画面内にある「Manage signer」に署名者が登録されたことを確認します。

4-5.【CertCentral】DigiCert KeyLockerで登録した署名者を確認する

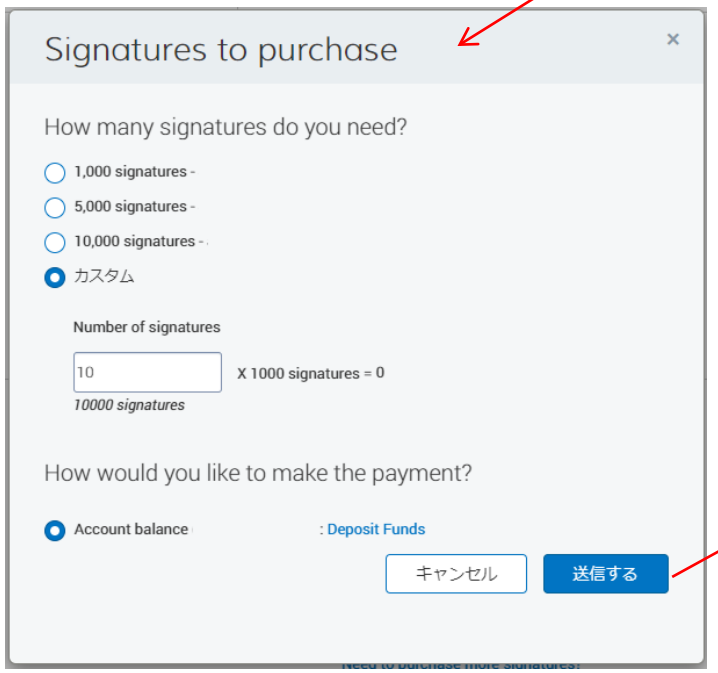


7. CertCentralへサインインし、CertCentral左メニュー[証明書]>[オーダー]から対象のオーダー番号の数字をクリックし、オーダー詳細画面を開きます。

8. 「プロビジョニングオプション」の箇所にある「Signer」で現在の署名者を確認することができます。署名者を変更する場合は、4-4.の手順を参照しDigiCert KeyLockerの「Manage signer」で署名者を変更してください。CertCentral上では変更はできません。

9. 「Signatures used」箇所ではこれまでの署名回数を確認することが可能です。

4-6. 補足【CertCentral】署名可能回数を追加する



DigiCert KeyLocker は、証明書の有効期間に関わらず1オーダー毎に 1,000回まで署名することができます。署名可能回数の追加は申請後、CertCentralオーダー詳細画面から追加購入が可能です。

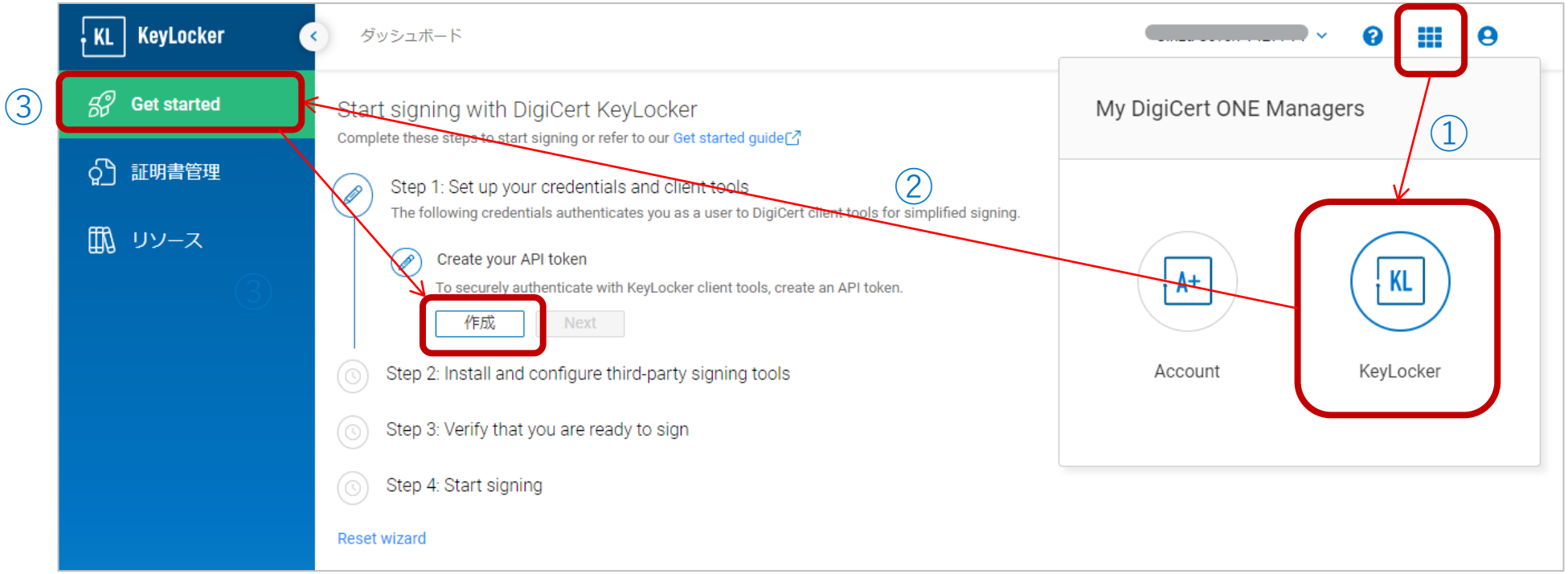
1. CertCentralへサインインします。
2. CertCentral左メニュー[証明書]>[オーダー]から対象のオーダー番号をクリックします。
3. オーダー詳細画面内「プロビジョニングオプション」の「Signatures used」 から「Need to purchase more signatures?」をクリックします。
4. 1000回、5000回、10000回、カスタム（1000回単位の必要数）と支払方法を選択し「送信する」を押下します。
5. 署名可能回数の追加完了の通知メールとご請求が確定します。期日までにお支払いください。
6. 「Signatures purchased（購入した署名回数）」と「Signatures used（使用した署名回数）」の分母の回数が増えていることを確認してください。

※ご注意ください※

- 署名回数追加専用バウチャーはご提供がございません。バウチャーでご申請いただいた場合も署名回数ご追加時のご請求はCertCentral上でご設定されているお支払い方法（請求書払いもしくはクレジットカード等）となります。

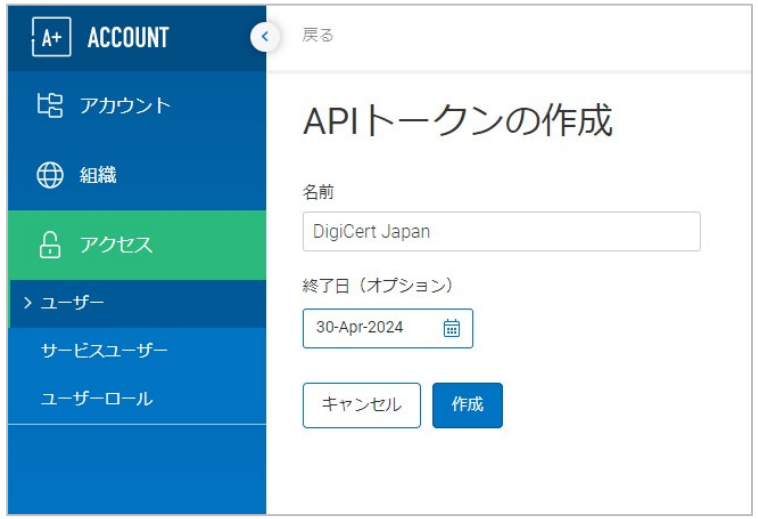
5-1. 【DigiCert ONE】DigiCert KeyLockerで署名環境を設定する

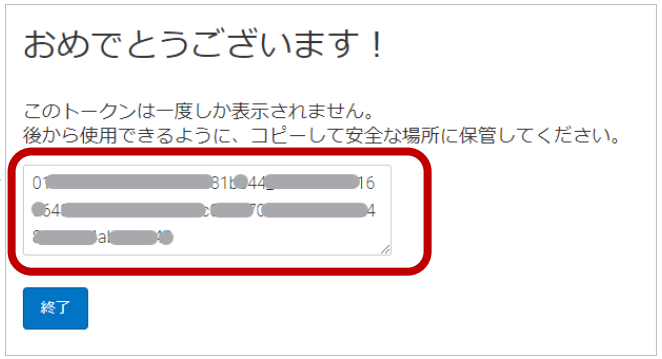
1. DigiCert ONEの画面右上にあるマークをクリックし表示されたメニューアイコンの「KeyLocker」をクリックします。
2. 左メニュー「Get started」を選択します。
3. 「Start signing with DigiCert keyLocker」のStep1～4までを設定します。
4. 「Create your API token」の「作成」をクリックします。

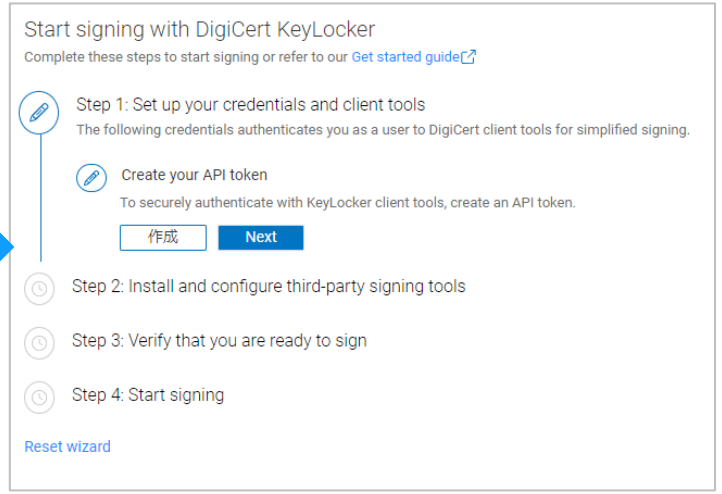


5-2. 【DigiCert ONE】 「Start signing with DigiCert keyLocker」 Step 1-1

5. 「Create your API token」の「作成」をクリックするとブラウザの別タブが展開され、APIトークンの作成画面となります。
6. APIトークンの「名前」を任意の文字列で入力します。
7. 「終了日（オプション）」は必要に応じてAPIトークンの利用期間（終了日）を設定します。未設定でも構いません。
8. 「作成」ボタンをクリックすると署名で利用する証明書を連携させるためのAPIトークンが表示されます。**あとで設定の際に必要となりますので、このトークンを必ずテキストなどへコピー＆ペーストして大切に保存してください。**
9. 「終了」をクリックしてブラウザのタブを閉じます。
10. 「Start signing with DigiCert keyLocker」のブラウザタブへ戻り、「Next」ボタンをクリックします。







5-3. 【DigiCert ONE】 「Start signing with DigiCert keyLocker」 Step 1-2

11. 「Create your client authentication certificate」の「作成」をクリックするとブラウザの別タブが展開され、署名時に必要なクライアント証明書の設定と生成画面となります。

12. 「ニックネーム」には証明書を管理するための名称を入力してください。利用可能な文字はすべて半角の英字/数字/スペース/ダッシュ/アンダースコアのみです。

13. 「終了日」はクライアント証明書の利用期間（終了日）を設定します。オーダーの期間や運用上必要とされる期間でご設定ください。

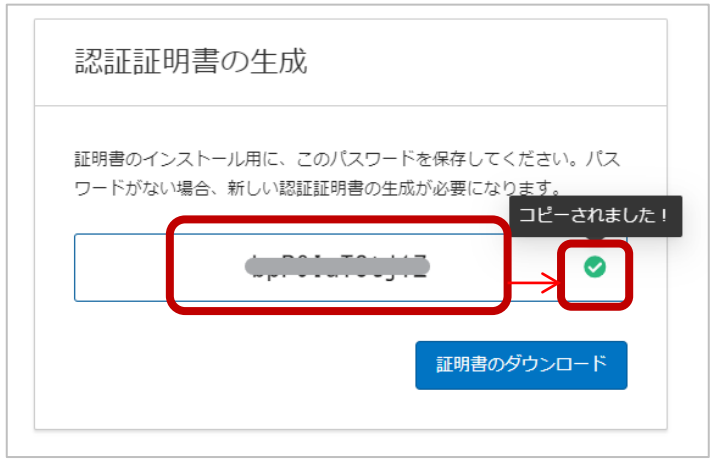
14. 「暗号化」と署名ハッシュアルゴリズム」は推奨とされる値が選択されていることを確認し「証明書の生成」ボタンをクリックします。

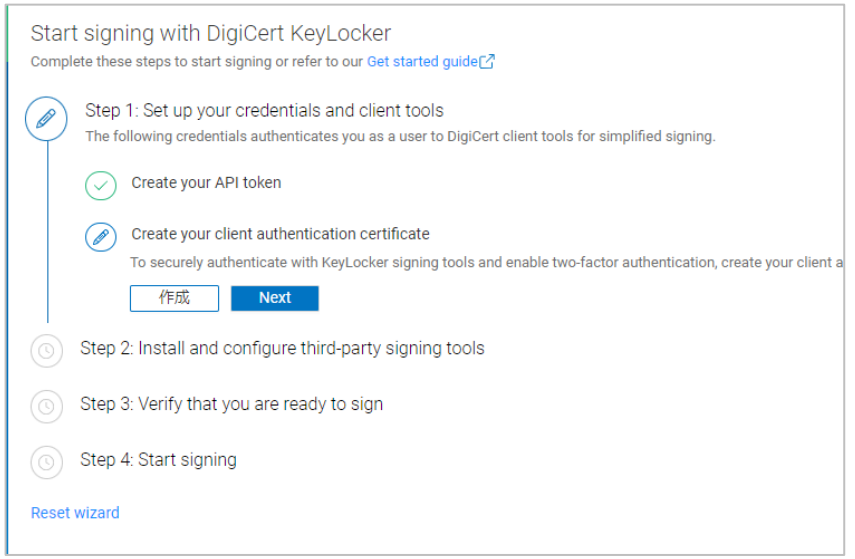
5-4. 【DigiCert ONE】 「Start signing with DigiCert keyLocker」 Step 1-2

15. クライアント証明書の生成画面に遷移し、署名時に提示するクライアント証明書のパスワードが表示されます。**あとで設定の際に必要となりますので、このパスワードが表示されているマークをクリックしてコピーし必ずテキストなどへペーストして大切に保存してください。**マークをクリックすることで「証明書のダウンロード」ボタンが表示されます。

16. クライアント証明書「Certificate_pkcs12.p12」ファイルのダウンロードを開始します。任意のフォルダ等へダウンロードの上、保存してください。

17. 「閉じる」をクリックすると「Start signing with DigiCert keyLocker」のブラウザタブへ戻り、「Next」ボタンをクリックします。

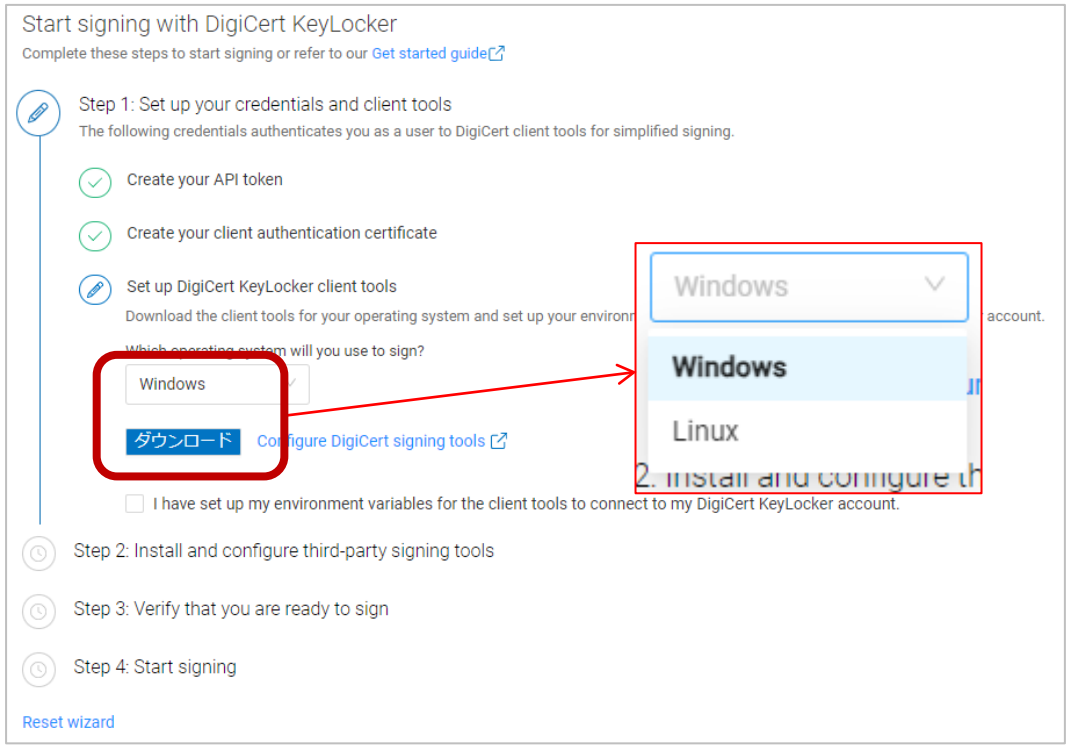


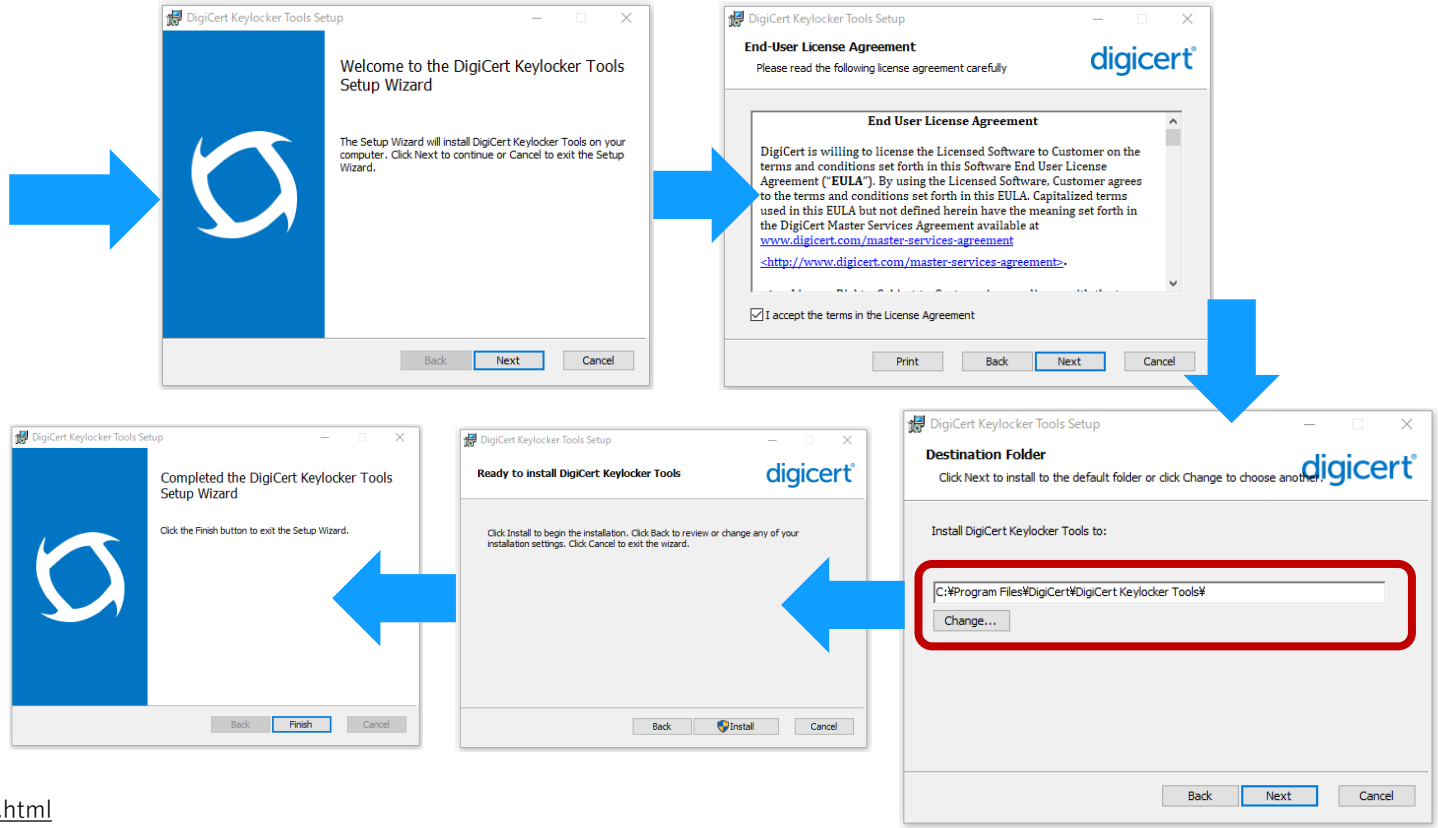


5-5. 【DigiCert ONE】 「Start signing with DigiCert keyLocker」 Step 1-3

18. 「Set up DigiCert KeyLocker client tools」では、DigiCert KeyLockerクライアントツールをダウンロードし、DigiCert KeyLockerアカウントに接続するための環境変数を設定します。 署名に使用するオペレーティングシステムをプルダウンメニューから選択しダウンロードしてください。Mac OSでご利用いただく際はDigiCert KeyLocker左メニューの[リソース]>[クライアントツール]から「Keylocker Mac Clients」をダウンロードしてください。ダウンロードをするとチェックボックスが表示されるのでチェックを入れます。

19. ダウンロードしたファイル(例)「Keylockertools-windows-x64.msi」を実行しウィザードに従ってシステムにツールをインストールします。インストールで指定した先（フォルダ名）を忘れないようにしてください。

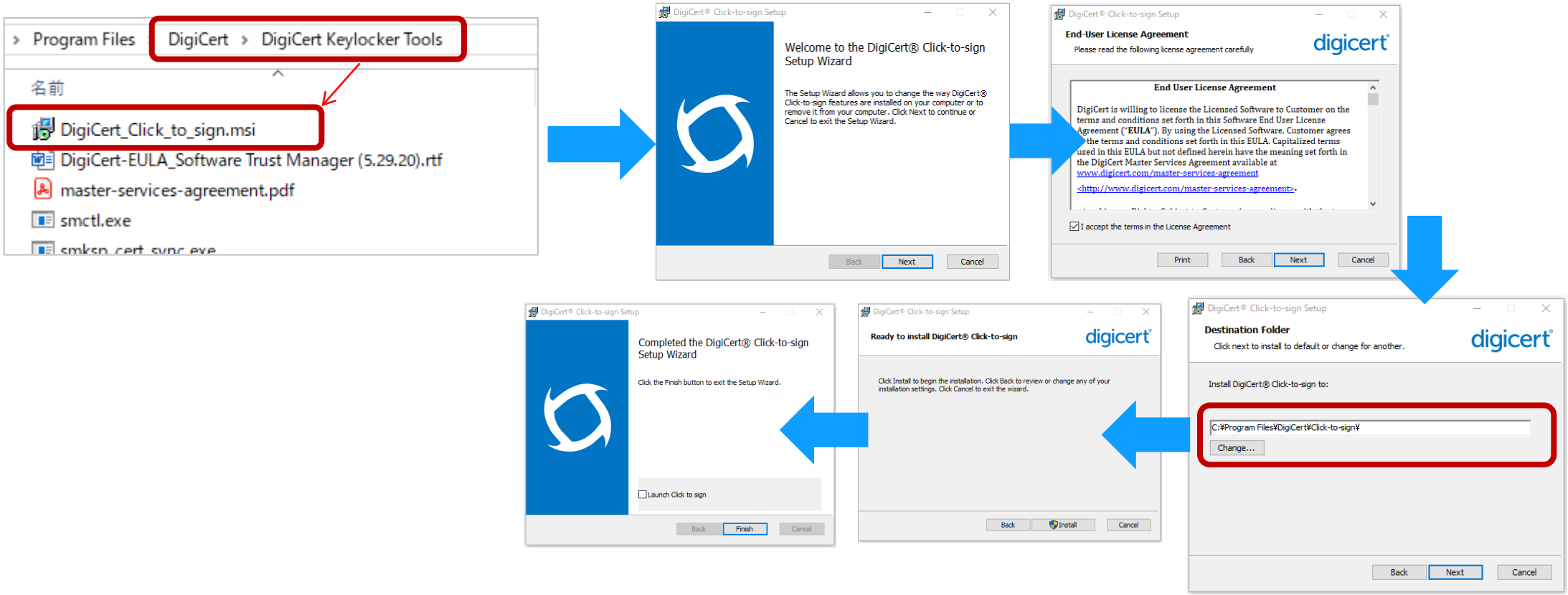




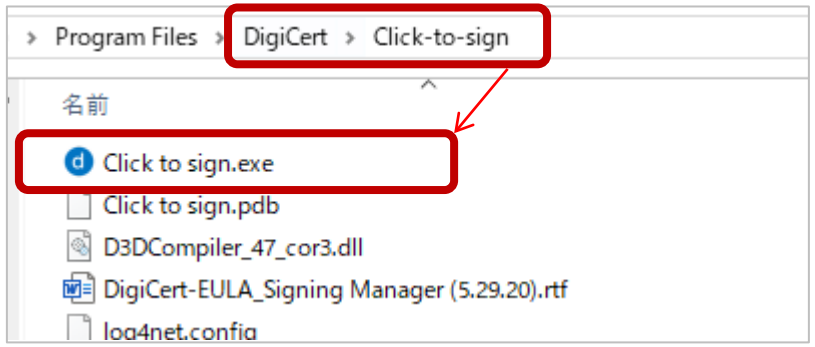
参考サイト：Windows clients installer (recommended) - DigiCert署名ツールの設定 （英語）
https://docs.digicert.com/en/digicert-keylocker/tools/tool-packages/windows-clients-installer.html

5-6. 【DigiCert ONE】 「Start signing with DigiCert keyLocker」 Step 1-3

20. ファイル(例)「Keylockertools-windows-x64.msi」をインストールで指定した先（フォルダ名）を開き、「DigiCert_Click_to_sign.msi」アプリケーションを実行しウィザードに従ってシステムにツールをインストールします。インストールで指定した先（フォルダ名）を忘れないようにしてください。



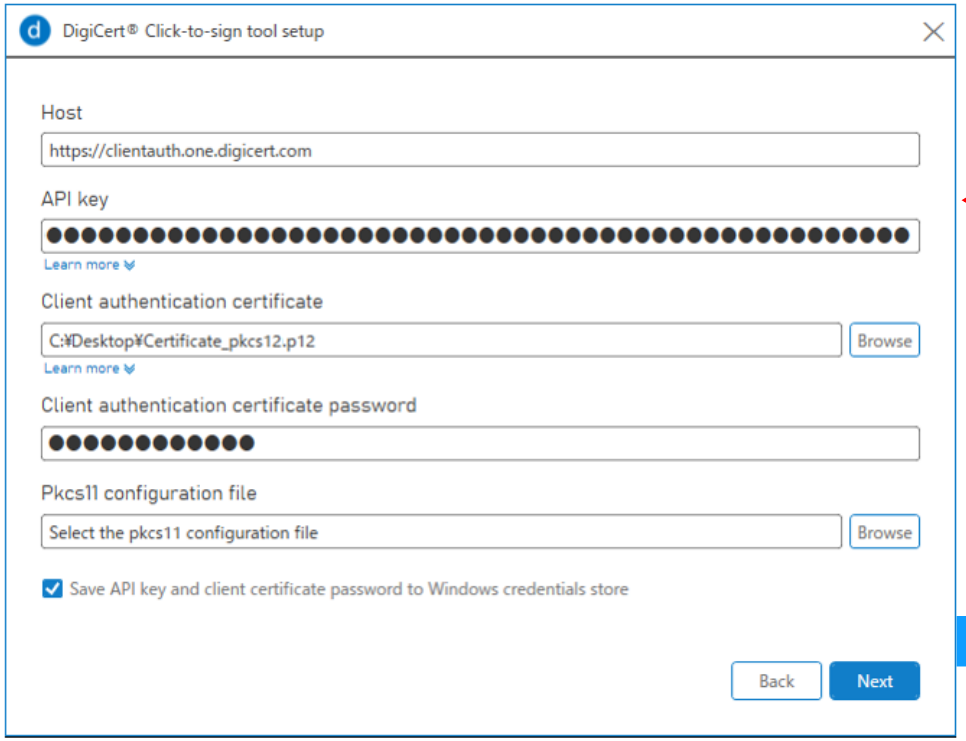
5-7. 【DigiCert ONE】 「Start signing with DigiCert keyLocker」 Step 1-3

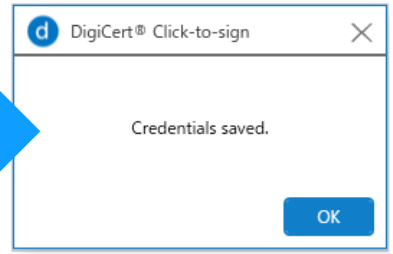


21. 「DigiCert_Click_to_sign.msi」アプリケーションをインストールで指定した先（フォルダ名）を開き、「Click to sign.exe」アプリケーションを実行します。

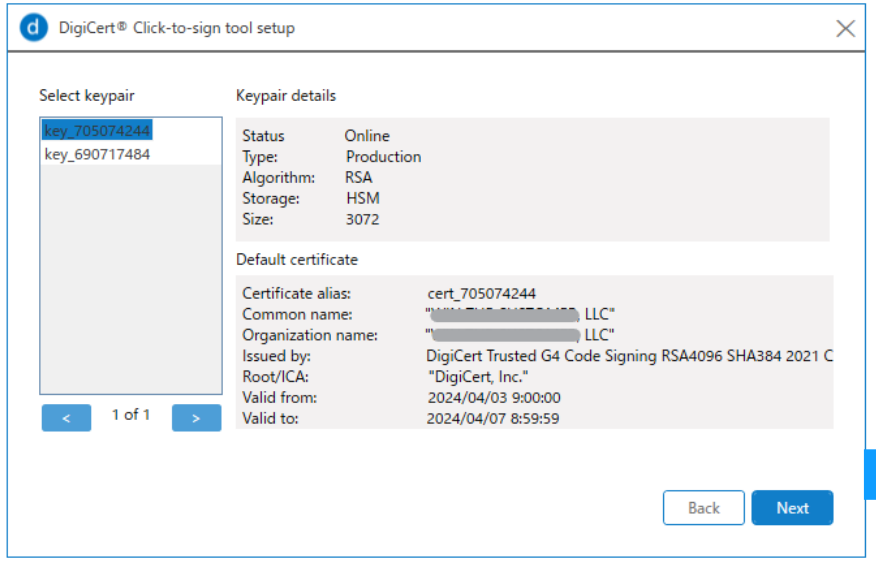
22. DigiCertの「Click to sign.exe」アプリケーションは、DigiCert KeyLockerのAPIと統合、署名をするために必要なユーザー資格情報をセットアップして保存します。セットアップ画面で必要情報を入力し、「Next」をクリックします。

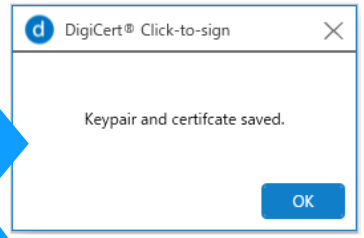
- Host：https://clientauth.one.digicert.com
- API Key：5-2. で保存したAPIトークン
- Client authentication certificate： 5-4.で取得したクライアント証明書へのパスを指定します。
- Client authentication certificate password：5-4.で保存したクライアント証明書のパスワードを入力します。
- Pkcs11 configuration file：デフォルト値のままにしてください。
- Save API key and client certificate password to Windows credential store：チェックボックスをオンにします。

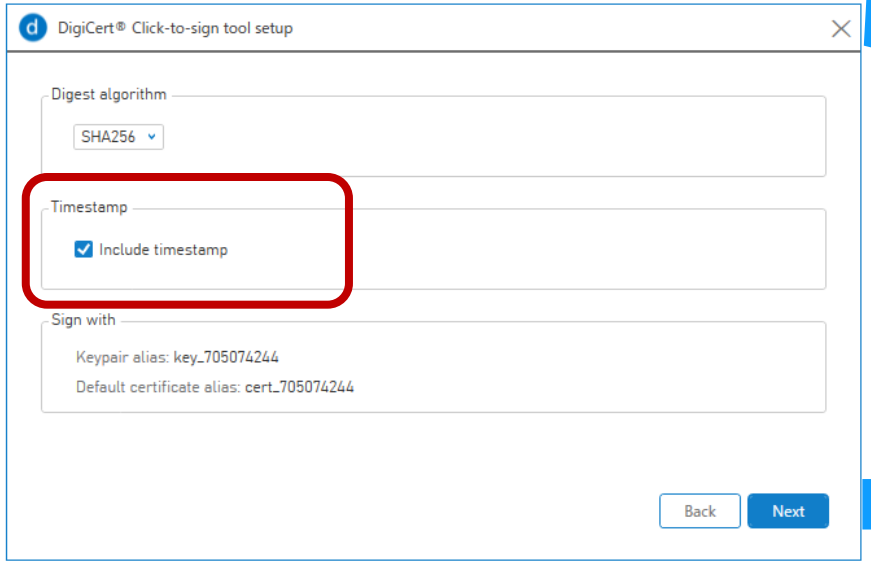


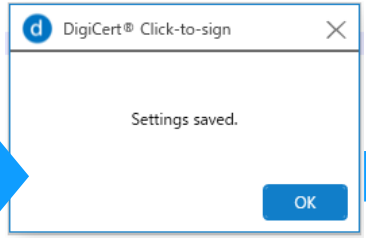


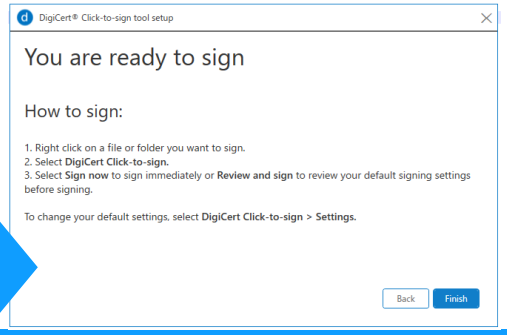
5-8. 【DigiCert ONE】 「Start signing with DigiCert keyLocker」 Step 1-3











23. 「Select keypair」枠内で署名時に利用する証明書のオーダー番号を選択し、右側に表示されている証明書情報が正しいことを確認の上、「Next」をクリックします。
例：key_<オーダー番号>

24. 署名する「digest algorithm（アルゴリズム）」を選択、署名にタイムスタンプを含める場合は「Timestamp」のチェックボックスにチェックの上、「Next」をクリックします。

25. セットアップが完了しました。

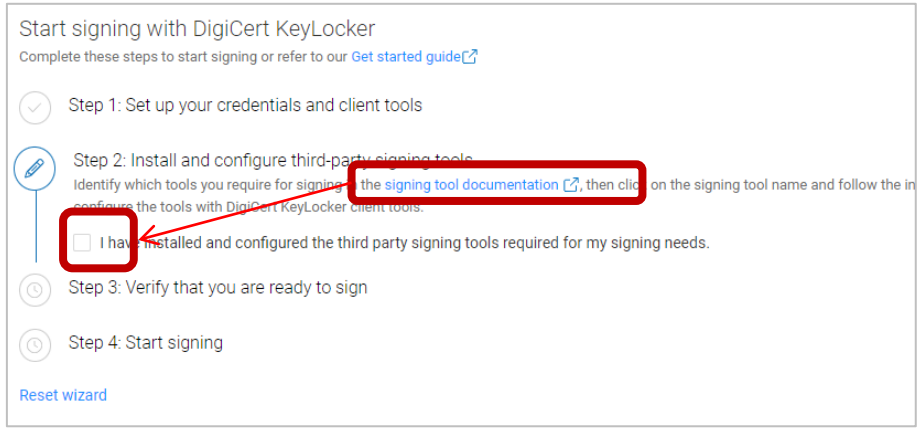
5-9. 【DigiCert ONE】 「Start signing with DigiCert keyLocker」 Step 2/3/4

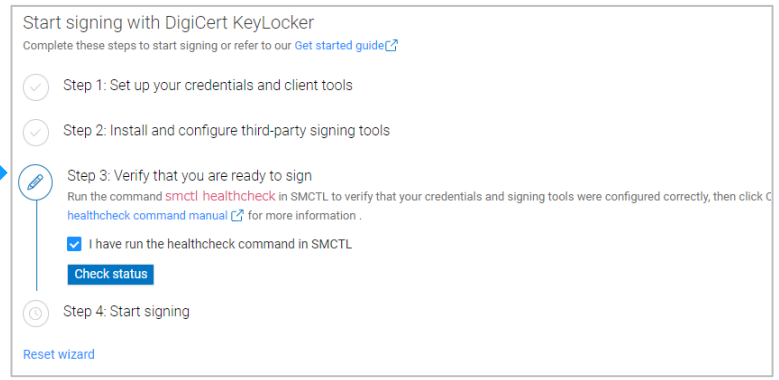
26. Step 2では、サードパーティ署名ツールのインストールと設定 署名ツールのドキュメントで署名に必要なツールを確認し、署名に必要な署名ツールのダウンロード等を行い環境を整えます。説明文章内にある「signing tool documentation 」の文字をクリックした後、チェックボックスが表示されますのでチェックを入れます。

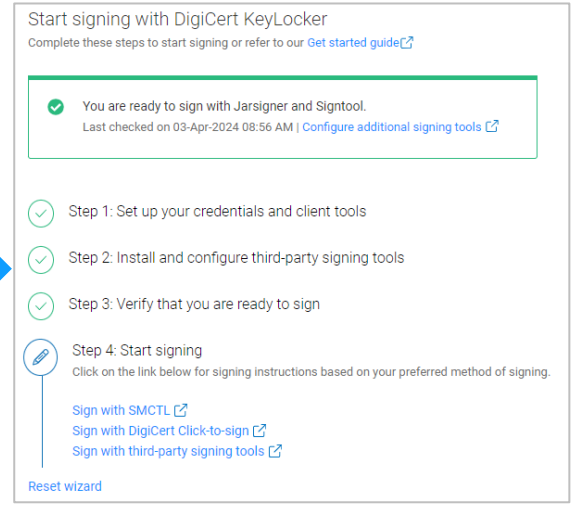
27. Step 3では、署名の準備が整っていることを確認します。 SMCTL で smctl healthcheck コマンドを実行し、認証情報と署名ツールが正しく設定され ていることを確認してから「Check status」をクリックします。詳細については、 healthcheck command manual のマニュアルを参照してください。

28. Step 4では、ご希望の署名方法に基づいて署名手順をご確認ください。すべての設定はこれで完了です。

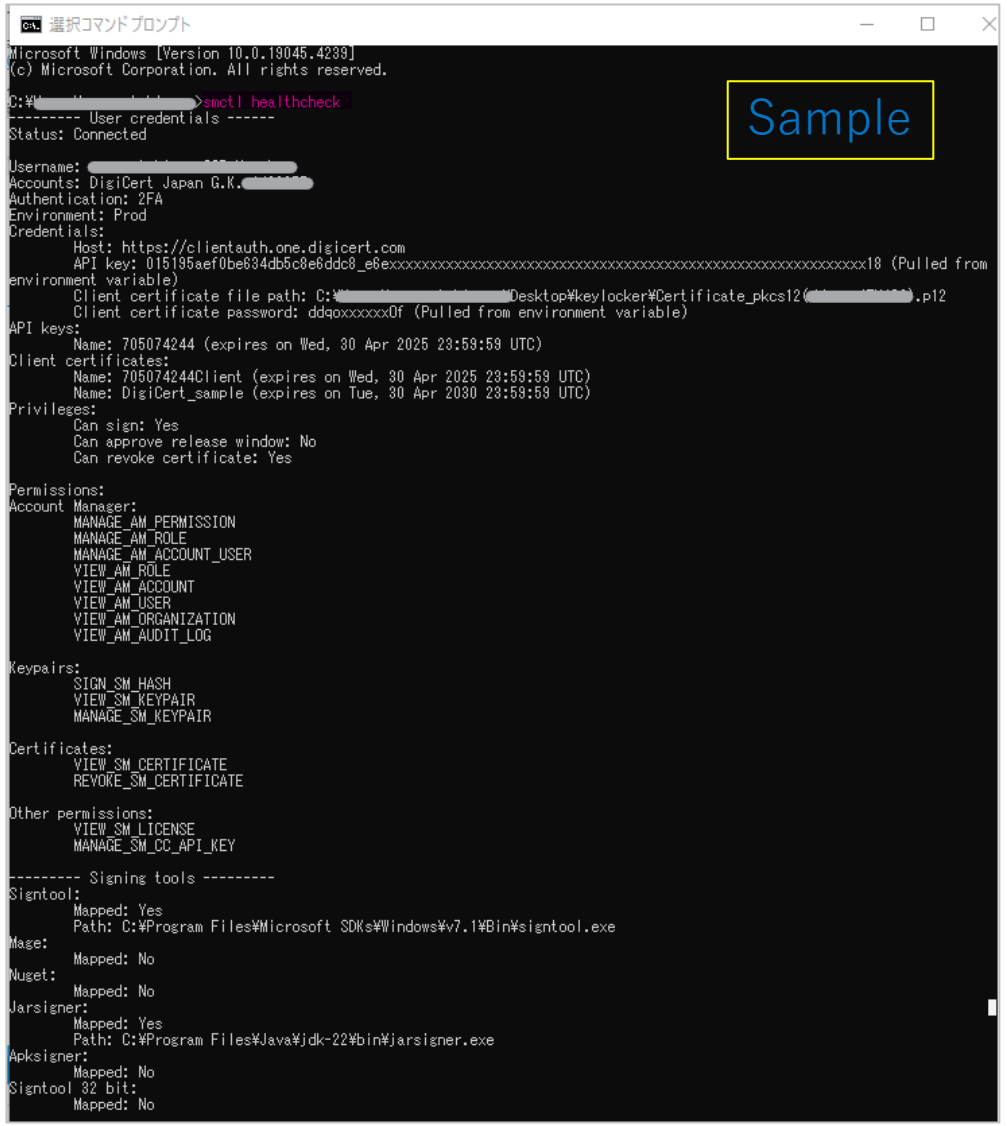
- Sign binaries with SMCTL - SMCTL を使用してバイナリに署名する
https://docs.digicert.com/en/digicert-keylocker/sign-with-digicert-signing-tools/sign-with-smctl.html
- Sign with DigiCert® Click-to-sign - DigiCert® Click-to-Signによる署名
https://docs.digicert.com/en/digicert-keylocker/sign-with-digicert-signing-tools/sign-with-digicert-click-to-sign.html
- Sign with third-party signing tools -サードパーティの署名ツールを使用して署名する
https://docs.digicert.com/en/digicert-keylocker/signing-tools.html







5-9. 補足【DigiCert ONE】 Step 3 トラブルシューティング



1. Windows画面左下にある虫眼鏡マークをクリックし「コマンドプロンプト」と検索して実行します。

2. 「smctl healthcheck」もしくは「smctl –help」、「smctl –h」のいづれかを入力しEnterキーを押します。

3. 「--------- User credentials ------・・・・」と情報が表示されたら、「 Credentials: 」以降に5-7.で設定した情報の表示、 「Privileges: 」箇所で「Can sign: Yes」と表示されていること、「--------- Signing tools ---------」箇所で署名ツールが連携されていることを確認してください。

4. 確認ができた後「Check status」をクリックしStep 3を完了させます。

➢ トラブルシューティング
コマンドプロンプトで情報が表示されない場合は、ディレクトリのpathが設定されていません。以下[cd]コマンドでチェックするディレクトリ（フォルダ）を変更してお試しください。

例：
C:¥Users¥XXXXXX>cd C:¥Program Files¥DigiCert¥DigiCert Keylocker Tools
C:¥Program Files¥DigiCert¥DigiCert Keylocker Tools>smctl -h

※Command sampleは以下Docsを参照してください。
Healthcheck Troubleshoot- SMCTL で正しく構成されているかどうかを確認する
https://docs.digicert.com/en/digicert-keylocker/tools/command-line-interface/smctl-command-manual/healthcheck.html#healthcheck-commands-488627

関連サイト（Docs）

※一部英語サイトとなりますのでご不便である場合にはブラウザの翻訳機能などをご活用ください。

DigiCert KeyLocker
https://docs.digicert.com/ja/digicert-keylocker.html

Windows clients installer (recommended) - DigiCert署名ツールの設定
https://docs.digicert.com/en/digicert-keylocker/tools/tool-packages/windows-clients-installer.html

Signing Manager Controller (SMCTL) command manual – SMCTL コマンドマニュアル
https://docs.digicert.com/en/digicert-keylocker/tools/command-line-interface/smctl-command-manual.html

Healthcheck Troubleshoot- SMCTL で正しく構成されているかどうかを確認する
https://docs.digicert.com/en/digicert-keylocker/tools/command-line-interface/smctl-command-manual/healthcheck.html#healthcheck-commands-488627

Signing Manager Controller (SMCTL) – SMCTL で統合できる署名ツール
https://docs.digicert.com/en/digicert-keylocker/tools/command-line-interface/smctl.html

Files supported for signing（署名できるファイルの種類）
https://docs.digicert.com/en/digicert-keylocker/sign-with-digicert-signing-tools/files-supported-for-signing.html

DigiCert® Click-to-sign
https://docs.digicert.com/ja/digicert-keylocker/tools/signing-tools/digicert-click-to-sign.html