Alibaba Cloud Certificates Service

クイックスタート

Document Version20190705

目次

1 制限

Alibaba Cloud 証明書サービスには、次の制限があります。

- 2 種類のサーバー証明書 (Professional と Advanced) のみ利用可能です。 CA (認証局) が異なると、選択するプロダクトが異なります (または特定の種類の証明書が利用できません)。
- CA の要求に応じて、組織の正当かつ正規の資料を提出する必要があります。 Alibaba Cloud は、提供された資料をレビュー用に CA に送信します。 確認のために CA が連絡することがあります。
- CSR ファイルを生成する際、暗号化鍵の最小ビット長はハッシュアルゴリズムで RSA 2048 と SHA 256 です。
- Alibaba Cloud 証明書サービスが提供する証明書は PEM 形式です。

2 概要

本ページでは、デジタル証明書の購入方法、レビュー用情報の入力方法、証明書を Alibaba Cloud プロダクトにデプロイする方法を説明します。

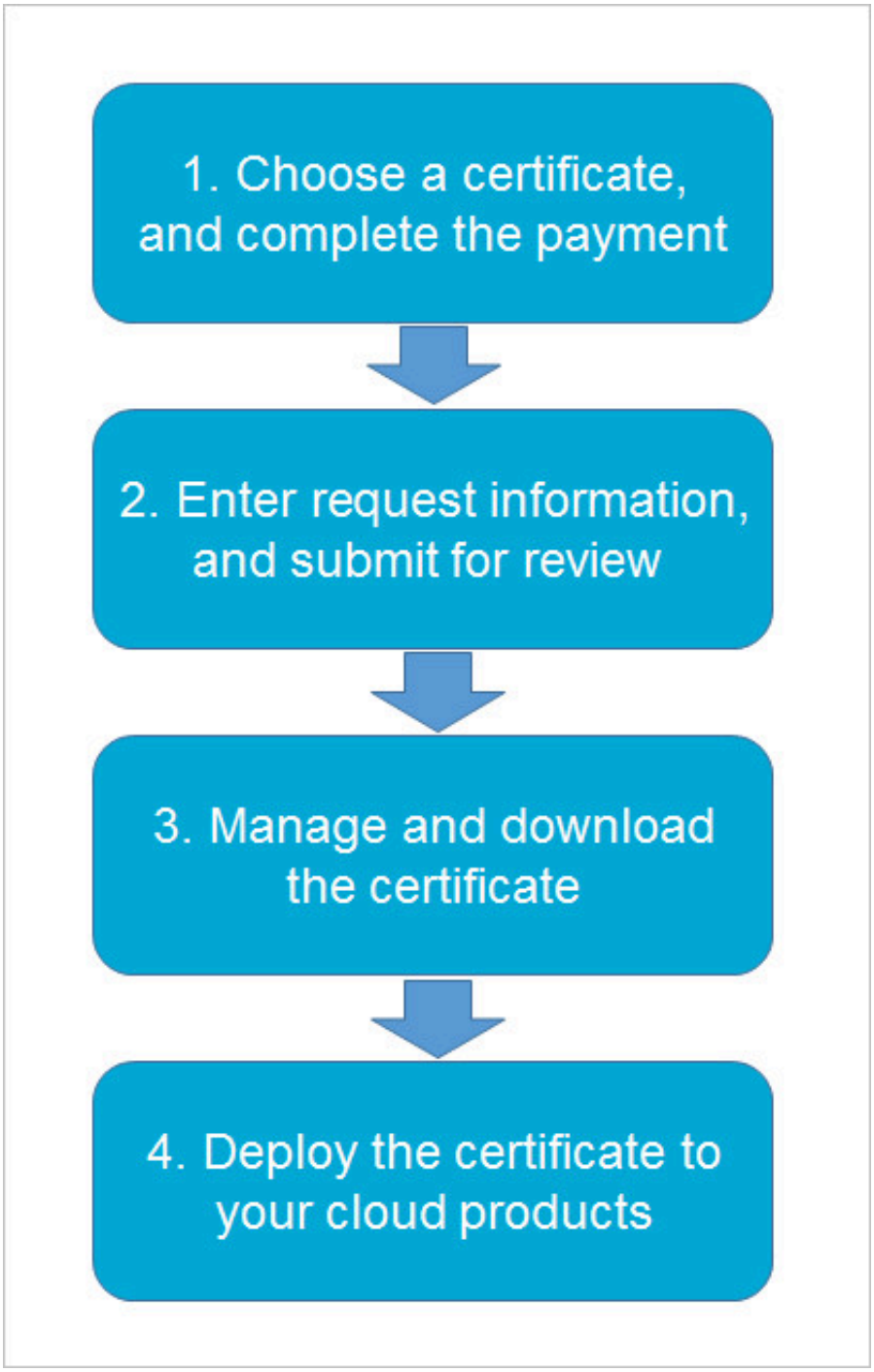
対象ユーザー

本ページは、以下のユーザーを対象にしています。

- デジタル証明書を購入する方法の習得、各種デジタル証明書の比較をしたいユーザー。
- デジタル証明書の購入、レビュー資料の申請をしたいユーザー。
- クラウドプロダクトへのデジタル証明書のデプロイをしたいユーザー。

手順

デジタル証明書の購入および管理方法のフローチャートは次のとおりです。

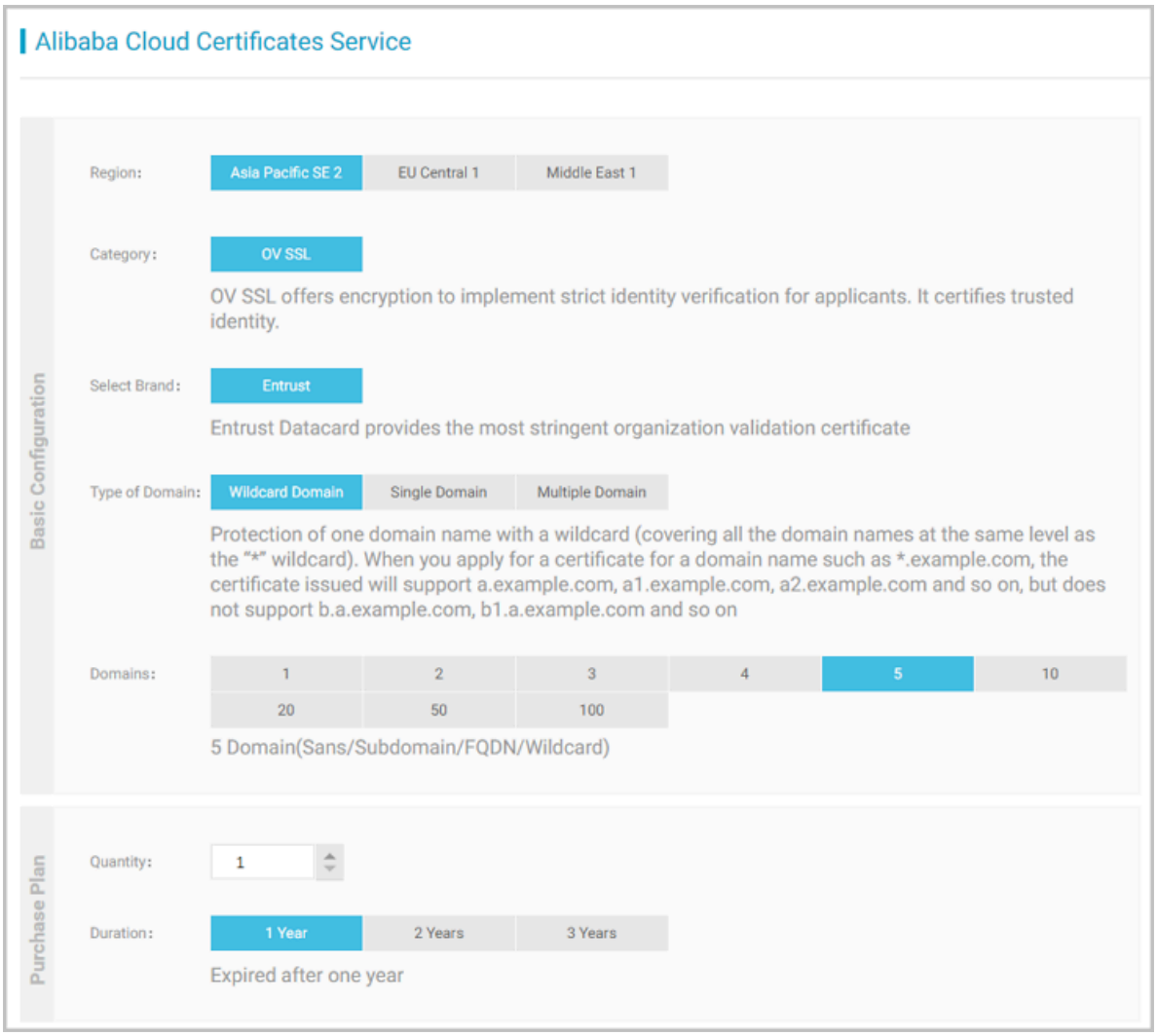


一般的に、以下の手順に従って Alibaba Cloud 証明書サービスを使用します。

1. 証明書の選択。
2. リクエスト情報の入力、レビュー用に申請。
3. 証明書の管理。
4. 他の Alibaba Cloud プロダクトへの証明書のデプロイ。

3 手順 1: 証明書の選択

1. にログインして SSL 証明書を購入します。



2. デジタル証明書を選択し、支払いをして証明書設定プロセスに入ります。

リージョンの選択。

証明書をインストールする Web サイトサーバーの場所に応じてリージョンを選択することを推奨します。

証明書ブランド (CA プロバイダー)

Alibaba Cloud は、以下の CA と連携してデジタル証明書を発行します。

Entrust: Entrust は、世界をリードする公開鍵インフラストラクチャプロバイダーです。 世界中でコミュニケーションが容易になる信頼できる仮想環境を構築しています。 Entrust は、Web サイト、ソフトウェア開発者、個人に信頼サービスを提供します。これには、Web サイト認証と

暗号化に特に対応する SSL サーバー証明書の発行が含まれ、世界の上位 500 の企業のうち 83% 超が Entrust SSL サーバー証明書を利用しています。

証明書タイプ

正規の認証局 (CA) と連携して、Alibaba Cloud はデジタル証明書を設定するための次のオプションを用意しています。

- OV SSL: OV SSL (Organization Validation SSL) 証明書の一種。 SSL Professional 証明書の詳細は次のとおりです。
  - CA がドメイン所有権と組織アイデンティティを検証します。
  - 要求者の業務名が証明書に表示されます。
  - 証明書により、通信リンクに強力な暗号化が提供されます。
  - 証明書は最大 100 ドメインをサポートし、ワイルドカードドメインをサポートしています。
- EV SSL: EV SSL Extended Validation SSL) 証明書の一種。 SSL Advanced 証明書の詳細は次のとおりです。
  - CA が厳密にドメイン所有権と組織アイデンティティを検証します。
  - ほとんどのブラウザーでは、この証明書に緑色のアドレスバーが表示されます (Safari ブラウザーでは例外がいくつかあります)。
  - 要求者の組織アイデンティティの詳細が証明書に表示されます。
  - 証明書により、通信リンクに強力な暗号化が提供されます。
  - 証明書は最大 100 ドメインをサポートしています。

ドメイン保護

デジタル証明書を購入する前に、証明書で保護するドメインのタイプと数を決定する必要があります。 単一または複数のドメインまたはワイルドカードドメインを保護します。

- 単一ドメイン: デジタル証明書は 1 つのドメイン (buy.example.com など) のみを保護し、ワイルドカードはサポートしません。
- 複数ドメイン: デジタル証明書は複数のドメイン (buy1.example.com や buy2.example.com など) を保護しますが、ドメインの最大数は証明書タイプによって異なります。 通常、最大 100 ドメインを保護します。 ドメインオプション数に基づいて選択します。 ただし、ワイルドカードドメインはサポートされていません。
- ワイルドカードドメイン: デジタル証明書は、ワイルドカードで広範なドメインを保護します。 複数のワイルドカードサブドメインを保護する証明書は、現在利用できません。 たとえば、ワイルドカードドメイン * .example.com を使用して、a1.example.com

や a2.example.com などのドメインは保護しますが、a1.sport.example.com や a2.thanks.example.com は保護できません。

 注 :

Alibaba Cloud は、ドメイン情報の入力時に選択したドメインの数とタイプを検証します。 複数ドメインの保護を選択する場合、選択したすべてのドメインを同時に提出する必要があります。

証明書の有効期間

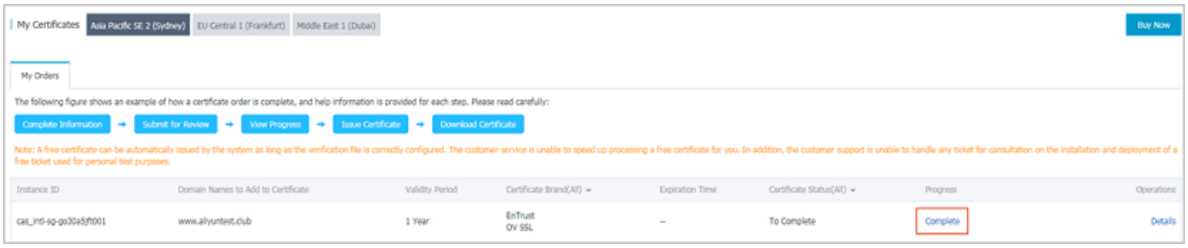
デジタル証明書にはすべて有効期間があります。 デジタル証明書の有効期間は、証明書の発行後に計算されます。 証明書の有効期間は 1 年または 2 年を選択します。

4 手順 2: 情報の入力

デジタル証明書を購入したら、証明書申請リクエストを完了するために証明書の詳細を入力してレビュー用に送信する必要があります。

以下の手順に従って情報を入力します。

1. 証明書サービス管理コンソールにログインします。
2. 購入した証明書があるリージョンを選択します。
3. [マイ注文] リストで、証明書インスタンスを選択し、[入力] をクリックして、[情報入力] ページに移動して証明書の詳細を入力します。



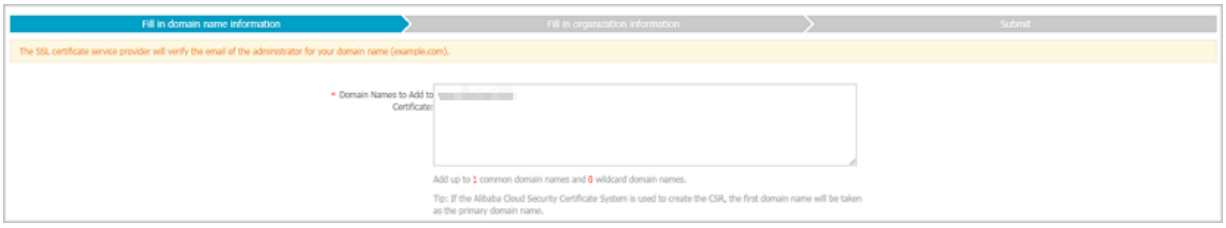
4. [レビューに送信] をクリックして証明書申請リクエストを申請します。

ドメイン情報の入力

証明書の購入時に選択したドメインのタイプと数に基づいて、ドメイン情報を入力します。 たとえば、複数ドメインを保護し、保護するドメインの数を 5 と指定する場合、この手順で 5 つのドメイン (1 行に 1 つ) をすべて入力します。

その後、Alibaba Cloud は入力したドメイン情報を検証します。

> 注 :
> CA は、申請されたドメインの所有権を確認する必要があります。 ドメイン所有権を検証するように促す CA からのメールを受信する場合があります。 検証のために詳細を申請した後は、指定されたメールボックスを定期的に確認する必要があります。情報を申請した後、速やかに受信トレイ (申請者の受信トレイ) を確認して、検証します。 検証を行わないと、証明書レビューに失敗することがあります。ドメイン名の所有権の検証に失敗すると、証明書レビューに失敗します。

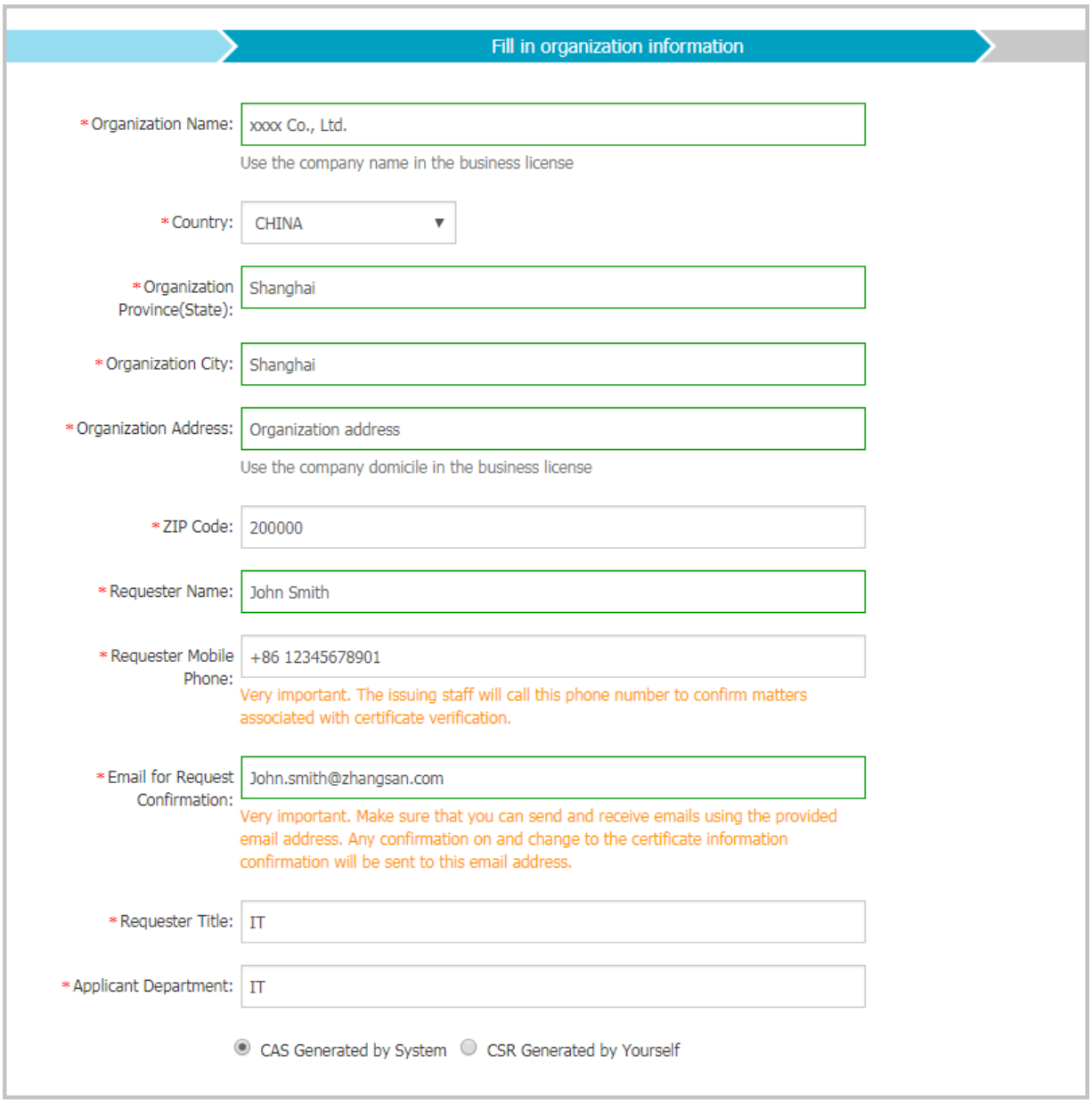


リクエスト情報の入力

SSL Professional または Advanced 証明書を購入するには、組織の詳細情報を入力する必要があります。

組織情報の入力

必要に応じて組織情報を入力します。 これらの詳細をさらに使用して、組織の信頼性を検証します。



関連情報のアップロード

システムで生成された CSR を使用して CSR ファイルを生成することを推奨します。

- その結果、システムで秘密鍵が自動的に生成されます。 証明書リクエストが完了したら、証明書と秘密鍵を証明書管理リストから直接ダウンロードします。

- CSR (証明書署名リクエスト) 証明書リクエストファイルを自身で生成して手動でアップロードすることも可能です。 CSR ファイルの生成方法については、「CSR ファイルの生成方法」をご参照ください。

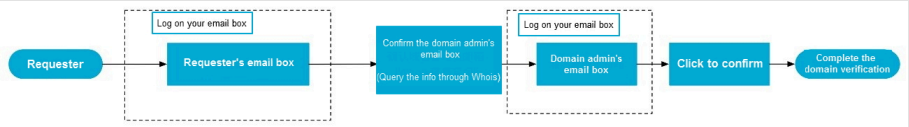
> 注:
>
> - 証明書申請を成功させるため、CSR ファイル形式が正確である必要があります。
> - CSR ファイルを生成するときに、秘密鍵を安全に保管する必要があります。 秘密鍵は、証明書と 1 対 1 対応しています。 秘密鍵を紛失すると、デジタル証明書は使用できなくなります。 Alibaba Cloud は、秘密鍵の管理や保管について責任を負いません。 秘密鍵を紛失したり、忘れた場合、新しいデジタル証明書を購入して、元の証明書と置き換える必要があります。

レビュー用に申請

申請後、Alibaba Cloud は証明書の資格認定を検証します。 このプロセスに必要な時間は、各 CA の個々の要件によって異なります。 そのため、通知に関して電子メールと電話を定期的に確認する必要があります。

検証に失敗した場合、リクエスト情報 (特に、組織の資格認定レビュー) を修正および更新し、別のレビュー用に再申請します。

> 注:
> 申請受領後、CA はドメイン情報の検証を依頼する検証メールを送信します。 ドメイン検証が行われないと、証明書レビューに合格できず、検証が完了するまで証明書はUnder Reviewステータスのままとなります。



5 手順 3: 証明書の管理

証明書リクエストが承認されたら、Alibaba Cloud 証明書サービスコンソールで証明書を管理します。

1. Alibaba Cloud 証明書サービス管理コンソール にログインし、[マイ証明書] をクリックします。
2. [マイ証明書] リストでデジタル証明書を表示し、管理します。

6 手順 4: 他のクラウドプロダクトへのデプロイ

承認されたデジタル証明書を CDN、Anti-DDoS Pro、WAF、Server Load Balancer などの他の Alibaba Cloud プロダクトにプッシュします。

デジタル証明書をクラウドプロダクトにプッシュする前に、秘密鍵をアップロードする必要があります。 証明書リクエストを送信するときに ”システムで生成された CSR” を選択した場合、秘密鍵はシステムで保存され、再度アップロードする必要はありません。

 注 :

秘密鍵は証明書と 1 対 1 で対応しているため、必ず正しい秘密鍵をアップロードする必要があります。 秘密鍵の詳細については、「公開鍵と秘密鍵の概要」をご参照ください。

 注 :

秘密鍵を紛失すると、デジタル証明書は使用できなくなります。 Alibaba Cloud は、秘密鍵の管理や保管について責任を負いません。 また、秘密鍵を紛失したり、忘れた場合、新しいデジタル証明書を購入して、元の証明書と置き換える必要があります。 秘密鍵をアップロードした後は、再度ダウンロードすることはできません。 したがって、元の秘密鍵は安全に保存するようにしてください。