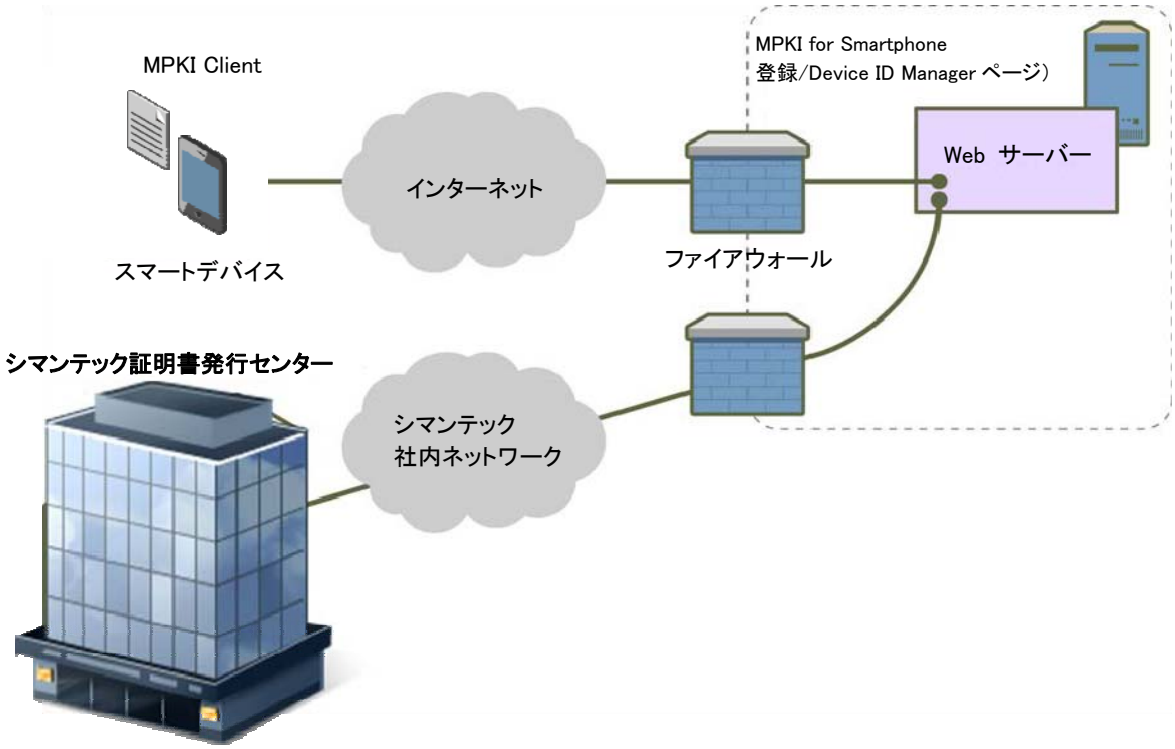
Symantec Managed PKI for Smartphone サービス記述書

はじめに

Symantec Managed PKI for Smartphone サービスは、Symantec Managed PKI 7.x バージョンにおいて、iOS デバイスおよび Android デバイスなどのスマートデバイス(タブレットを含む)に対して、証明書の新規申請や更新を受け付けるためのオンライン受付サイトの RA コンテンツおよびサーバーを提供します。また、スマートデバイスにはヘルパーソフトウェアとして、シマンテック製 MPKI Client(iOS、および Android 向けアプリケーション)を提供し、証明書の透過的な取得を実現します。本サービスでは、Symantec Trust Network のパブリック証明書は利用できません。

図 1 Symantec Managed PKI for Smartphone サービス構成

注: 点線内のシステムが MPKI for Smartphone サービスに該当します。



主要機能

- Managed PKI Device ID Manager
  Managed PKI Device ID Manager ページは、管理者がスマートデバイス向けの証明書を登録から承認、失効、更新までのライフサイクルプロセスを管理することができます。本機能は Symantec Managed PKI 7.x おける Managed PKI コントロールセンターに準じたものでスマートデバイス専用に操作を行うことができます。スマートデバイス向けには、事前に対象デバイスの情報を登録し、認証することによるデバイス認証になり、他の手段による認証を行うことはできません。

- MPKI Client
  MPKI Client は、本サービスで証明書を発行する際にスマートデバイスにインストールし、動作するソフトウェアで、iOS ならびにアンドロイド向けの各マーケットから最新のバージョンをダウンロードできます。本サービスでは、証明書発行に MPKI Client が必要です。

- 上記以外の Managed PKI の機能について

  Symantec Managed PKI サービス記述書(バージョン 7. xおよびそれ以前)に準じます。

付録 B – MPKI for Smartphone サービス利用規約

1. 定義

「管理者証明書」とは、Managed PKI 管理者として任命されたお客様側の従業員またはその他の信頼される者に対し、Managed PKI コントロールセンターにアクセスして管理業務を行うことのみを目的としてシマンテックが発行する証明書を指します。

「契約」とは、シマンテックとお客様の間で結ばれ、本サービス記述書に適用されるサービス注文書が発行された、プロフェッショナルサービス契約またはその他のマスター契約や規約を指します。

「証明書」または**「デジタル証明書」**とは、少なくとも発行元 CA の名前または識別情報、利用者の識別情報、利用者の公開鍵、証明書有効期間、証明書のシリアル番号、発行元 CA のデジタル署名を含むメッセージを指します。

「証明書申請者」とは、CA に証明書の発行を要求する個人または委任代理人を指します。

「証明書申請」とは、証明書申請者(または委任代理人)から CA に提出される証明書発行要求を指します。

「証明書署名ユニット」または**「CSU」**とは、証明書への署名と鍵の保管用に設計されたハードウェア装置またはソフトウェアを指します。

「認証局」または**「CA」**とは、証明書を発行、停止、失効する権限を持つ個人を指します。

「誤発行」とは、(a)証明書の主体として指定されている人物とは異なる人物に証明書を発行すること、(b)証明書の主体として指定されている人物の認可なく証明書を発行することを指します。

「鍵生成」とは、シマンテックがお客様の公開鍵/秘密鍵を厳密な手順に従って適切に生成し、生成された秘密鍵と関連ドキュメントを保管する手続きを指します。

「Managed PKI 管理者」とは、登録局の従業員、または登録局の業務を行う権限を与えられたその他の信頼される者を指します。

「証明書有効期間」とは、証明書が発行された日時(または証明書に記載されている、それより後の特定の日時)から、有効期限が切れる日時またはそれ以前の失効が実行された日時までの期間を指します。

「プライベート階層」とは、お客様のルート CA から、1つ以上の認証局、そして利用者へとつながるチェーンの中で、お客様が定めた手順に従って証明書を発行する一連の CA によるドメインです。プライベート階層で発行される証明書は、組織が社内で発行を認可することを目的としており、公共のチャネルを介して組織や個人の間でやり取りすることは目的としていません。

「秘密鍵」とは、デジタル署名の作成に使用される数学的な鍵を指します。この鍵は他人に知られないように、所有者が秘密に保管する必要があります。アルゴリズムによっては、対になる公開鍵で暗号化された機密のメッセージやファイルを復号化するためにも使用されます。

「公開鍵」とは、対になる秘密鍵で作成された署名の検証に使用される数学的な鍵を指します。この鍵は一般に公開されます。アルゴリズムによっては、メッセージやファイルを暗号化するためにも使用されます。暗号化されたメッセージやファイルは、対になる秘密鍵で復号化できます。

「登録局」または**「RA」**とは、証明書申請者の身元確認と認証、証明書失効要求の手続き開始と伝達、証明書の更新または鍵更新の申請承認を行うエンティティを指します。RA は、証明書申請者の代理人とは異なります。RA は、RA の認可された Managed PKI 管理者以外に証明書申請の承認権限を委任することはできません。

「シート」とは、サービスの正規エンドユーザーである単一の利用者を指します。その利用者に実際に発行された証明書数は関係ありません。

「利用者」とは、証明書の主体であり、発行対象である、個人またはエンティティを指します。利用者は、発行時に証明書に含まれる公開鍵に対応した秘密鍵を使用でき、使用する権限を持ちます。

「信頼される者」とは、お客様およびお客様の製品、サービス、設備、手順の基盤をなす信頼性に対して責任を持つ、お客様の従業員、契約社員、コンサルタントを指します。

2. 提供内容

本サービスによる業務範囲を以下に記します。

(a) 管理者がデバイス認証用に利用する管理者コンソールである Device ID Manager の提供

(b) スマートデバイス側にインストールする MPKI Client の提供

(c) システム運用

本サービスは別途定める時間帯を除き、本サービス提供のために必要なシステムを、原則として 24 時間稼働します。また、その運用範囲は以下のとおりとします。

・サーバー運用

サーバー監視(死活監視、プロセス監視)

日次差分／週次フルバックアップ

バージョンアップ、脆弱性対策(パッチ適用等)

サポートサービス記述書にしたがったサポート

・不正侵入検知

24 時間の不正アクセス監視

バージョンアップ、脆弱性対策(パッチ適用等)

1 営業日以内の障害対応

・ファイアウォール

共用ファイアウォール

バージョンアップ、脆弱性対策(パッチ適用

等）
1 営業日以内の障害対応
セキュリティチェック
サービス導入時に稼働プロセスのセキュリティホールを診断

なお、以下についてはシマンテックにて決定、運用されます。
・障害時代替機
・ウェブサーバーのホスト名、ホストの SSL サーバー用 ID

本サービスにおいてシマンテックが指定するログについては、原則、お客様に提供しません。
バージョンアップ、脆弱性対策作業についてはメンテナンス実施時に行います。

3. サービス提供の中断

システム・メンテナンス、バックアップおよび機能のアップグレードを行うために、毎週 6 時間を上限として本サービスの提供を中断し、本サービスの中断時間は、MPKI 管理者宛てに通知します。
メンテナンス時間
毎週土曜日 0:00～4:00

1 週間に 6 時間を超えて本サービスを中断する必要がある場合、お客様に同様の方法で予め通知します。また、次のいずれかの場合に、シマンテックは本サービスを中断または提供中止をすることがあります。この場合、お客様に同様の方法で予め通知いたします。
(a)天災、地変、その他の非常事態が発生した場合
(b)シマンテックの管理する設備もしくはシステムの保守を緊急に行う必要がある場合
(c)SSL サーバーID の新規取得、更新、入れ替えに必要となる作業が必要である場合
(d)その他シマンテックが必要と認めた場合

4. ログの提供

お客様の目的にかかわらず、原則として提供いたしません。

5. その他事項

お客様が任命した Managed PKI の管理者は、同時に、本サービスにおける Device ID Manager の管理者として提供する CPS 条項を利用者に従わせる義務を持つものとします。
本項以外の事項はサービスの本体となる Managed PKI のサービス記述書に従うものとします。