Symantec™ SMS OTP Authentication Service 記述書

はじめに

Symantec™ SMS OTP Authentication Service は、オンラインサービスプロバイダおよび企業が、ワンタイムパスワードクレデンシャルを SMS テキストメッセージとして携帯電話に安全に発行できるようにします。Symantec SMS OTP Authentication Service では、VIP Authentication Service または Unified Authentication OTP Service のいずれかを使用する必要があります。

本サービスの主要なコンポーネントは次のとおりです。

- SMS ワンタイムパスワードクレデンシャル（SMS OTP クレデンシャル）
- クレデンシャルのプロビジョニングおよび検証用の Web サービス API

本サービス記述書では、以下に記載されたソフトウェアおよびサービスコンポーネントを含む、SMS OTP Authentication Service の主要な要素の概要を示します。本サービス記述書には、VIP Authentication Service または UA OTP Service の詳細は記載されていません。詳しくは、それぞれのサービス記述書を参照してください。

1. SMS OTP Authentication Service のコンポーネント

a. SMS OTP クレデンシャル

SMS OTP クレデンシャルは、共有鍵と一意の携帯電話番号の両方から構成されます。共有鍵は、企業またはシマンテックのデータセンターにホスティングされている認証インフラストラクチャで保存および保護されます。SMS OTP クレデンシャルは、既知の暗号アルゴリズムを使用して OTP 値を生成する際にシマンテックによって使用されます。生成された OTP は、SMS ネットワーク経由でエンドユーザーの携帯電話機に配信されます。受信された OTP は生成された OTP 値と比較されます。値が一致すると、クレデンシャルが検証／認証を実施します。SMS OTP クレデンシャルは匿名であり、ローカルユーザー識別子と結合して 2 番目の認証要素となります。

b. SMS OTP クレデンシャルのプロビジョニング

SMS OTP クレデンシャルは、新しい携帯電話番号を登録する企業からの要求に応じて、シマンテックにより動的に生成されます。その際、シマンテックは、クレデンシャルを生成して OTP をエンドユーザーの携帯電話に送信し、該当するエンドユーザーがその携帯電話を所有していることを確認します。企業によって行われる追加の API 呼び出しによって所有が確認されると、それ以降の認証に SMS OTP クレデンシャルを使用できるようになります。本サービスでは、クレデンシャルのコピーを暗号化形式で企業またはシマンテックのデータセンターに安全に保管します。クレデンシャルは、TripleDES 暗号アルゴリズムを使用して暗号化されます。

c. SMS OTP クレデンシャルの発行と配布

お客様は、エンドユーザーへのクレデンシャルの発行に関する責任を負います。このクレデンシャルの配布に伴う配送業務は、各企業によって管理および実施されます。

エンドユーザーへのクレデンシャルの発行に際して、企業は以下の作業を行うものとします。

- 必要なすべてのエンドユーザー識別情報を入手します。
- 必要なすべてのクレデンシャル識別情報を入手します。
- エンドユーザーがクレデンシャルの使用条件を順守するように義務付けます。

d. SMS OTP クレデンシャルの検証

エンドユーザーが自分の SMS OTP クレデンシャルに関するアクティブ化プロセスを完了し、それを当該企業の Web サイトでの ID に結合すると、企業はそのエンドユーザーに対して、その SMS OTP クレデンシャルから OTP を送信して 2 番目の要素による認証を行うように要求します。企業は、そのエンドユーザーの最初の要素のクレデンシャルを検証し、ローカルユーザーストアから携帯電話番号を取得して、検証のために当該携帯電話番号と OTP の両方をシマンテックに転送します。それを受けてシマンテックは、有効または無効のメッセージを企業に返します。

e. 構成および管理コンソール

UA OTP ソフトウェアの一部としてインストールされる構成および管理コンソールには、SMS OTP クレデンシャルに固有の以下の機能が含まれています。

- SMS OTP クレデンシャルの無効化/有効化
- SMS OTP クレデンシャルのテスト

2. 監査証跡

SMS OTP クレデンシャルの監査証跡は、ハードウェアベースのクレデンシャルに対して発行されるものとまったく同様に処理されます。

3. SMS 配信のサービスレベル契約書

適用可能な VIP Authentication Service のサービスレベル契約書内に、これと矛盾するいかなる文言がある場合でも、SMS OTP クレデンシャルの配信は以下の条件に従うものとします(「」で囲まれた語は、サービスレベル契約書内に定義された意味を持つものとします)。

a. サービス可用性

SMS OTP Authentication Service は、24 時間年中無休で 99.5% の可用性を維持します。「サービス可用性」とは、「計画的な停止時間」およびシマンテックの制御範囲外で発生するイベントを除いた「サービス」の「稼働時間」のことです。「サービス可用性」は、「サービス」が商業的に利用されるとき、すなわちシマンテックが当該「サービス」をすべての「お客様」に一般的に利用可能にした後に測定するものとします。商業的な利用には、「お客様」固有のテストおよび非本番環境は含まれません。

b. 計画的な停止時間/メンテナンス

シマンテックは、「サービス」のためのいかなる「計画的な停止時間」(シマンテックがプラットフォームのアップグレード、パッチ、修正プログラムを実装するための停止時間を含む)についても「お客様」に通知します。「計画的な停止時間」には次の種類があります。

i. 「計画的な停止時間」は、計画されたすべての「サービス」のメンテナンスを指し、米国東部時間の 01:00 AM ～ 08:00 AM に実施されます。シマンテックはこのような「計画的な停止時間」を必ず「定期メンテナンス」の 72 時間前に「お客様」に通知します。

ii. 「緊急メンテナンス」は、「サービス」に対して直ちに実施する必要があるメンテナンスを指し、時間帯/営業時間にかかわらず、また通知できる場合を除き、通知することなく行われます。

SYMANTEC SMS OTP AUTHENTICATION SERVICE 利用規約

1. 定義

「」で囲まれた語は、マスターサービス契約書、または本サービスが関連する適用可能なサービス記述書に規定された意味を持つものとします。

2. お客様の義務

「お客様」はクレデンシャルの発行者として、シマンテックに対し以下の点を表明および保証します。(i)「お客様」が、個人のものかどうかを問わず、本「サービス記述書」で意図されているとおりに(「お客様」が提供するデータを米国へ、およびシマンテックがかかる処理を公に実施している他の管轄地域において転送することを含み、それに限定されません)「お客様」が合法的にシマンテックに提供し、かつシマンテックが受信および処理することを許可するのに必要な、「エンドユーザー」に要求されるすべてのデータに関する必要な同意、権利、ライセンス、および権限を取得済みであること、(ii)シマンテックに提供されるデータが、いかなる第三者の特許、著作権、企業秘密、商標、サービスマーク、プライバシーの権利、広報、その他のいかなる「知的財産権」も侵害、悪用、妨害しておらず、これからもそうしないこと、(iii)本「サービス」を適用されるすべての法律に従ってのみ利用すること、(iv)本「サービス」をいかなる非合法、不正、不適切な目的をも支持してまたはそのために利用しないこと、また「お客様」が本「サービス」の承認されていない利用について知った場合は直ちにシマンテックに通知すること。

3. 免責

(a)第三者の要素 「お客様」は、ここに意図されている「サービス」を提供するにあたって、シマンテックが、シマンテックの制御下にない第三者(無線通信事業者、政府機関、およびそれと同様の主体(「SMS ネットワーク」)を含む)の施設、ネットワーク、接続、その他の行為に依存していることを認めます。シマンテックは、シマンテックの制御範囲にない、かかる第三者によるいかなる中断、遅延、停止、その他行為、または不作為に対しても責任を負わないものとします。

(b)第三者からの請求 「お客様」は、「エンドユーザー」に対し、無線通信事業者からの追加料金が発生する可能性があることについて注意を促すものとし、本「サービス」の一環として発行される SMS OTP クレデンシャルを含む SMS テキストメッセージの送受信に対する、かかる料金について単独で全責任を負うものとします。シマンテックは、かかる料金を「お客様」または「エンドユーザー」に対して払い戻す責任を負わないものとします。当該請求には、相互接続、アクセス、解約、ページャ、ワイヤレス、固定電話、その他、本「サービス」の提供における電話料金の請求が含まれ、それらに限定されません。

(c)SMS ネットワークの制限 「お客様」は本「サービス」を以下の行為に利用しないものとします。(i)ジャンクメール、スパム、迷惑メールをかかる内容の受信に同意していない個人または主体宛てに、またはそうでない場合でも、「お客様」がかかる内容を送信する法的な権利を有していない宛先に送信すること、(ii)違法、いやがらせ、強制的、名誉毀損、中傷、虐待的、脅迫、わいせつ、未成年者に有害、過剰な量の内容またはデータ、あるいはシマンテックまたは本「サービス」の提供に関係するいずれかの無線通信事業者の評判を傷つけるまたは損なう可能性のあるものを送信すること、そのような送信内容には、アルコール飲料、タバコ、銃火器、違法ドラッグ、ポルノ、犯罪、暴力、死、その他あらゆる疑わしい主題に関連する内容が含まれ、それらに限定されません。