Unified Authentication One-Time Password Service Description

Introduction

Symantec™ Unified Authentication One-Time Password Service ("UA Service") enables enterprises with increased security for their applications in the form of two-factor authentication. The UA Service includes a broad set of features, such as:

- Support of Open AuTHentication (OATH)-based One-Time Password (OTP) hardware and software credentials, such as tokens, display cards, mobile phones, etc.
- Enables use of SMS OTP credentials for authentication
- Integration with existing enterprise directory technologies, such as LDAP, ODBC, etc.
- Availability of localization features to adapt to different regions and languages
- Use of a centralized, Symantec-hosted, off-site authentication service, leveraging Symantec's trusted infrastructure
- Integration with the Symantec™ Validation and ID Protection (VIP) Service to enable the enterprise to leverage internal distribution of credentials for use across the VIP Network and accept credentials that are already active with other enterprises in the VIP Network

Key components of the UA Service include:

- OTP credentials embedded in devices, such as traditional hardware tokens, innovative cards or software-based solutions for mobile phones or for out of band delivery
- Lightweight enterprise software that enable credential provisioning, validation, activation and management services and include web-based applications for end-user self service and administrative functions
- Application integration toolkit
- Logging components that enable enterprise audits
- Optional tools and documentation to allow enterprises to a create a UA Service "Language Pack" with localized resources
- Optional integration components to support OTP authentication for desktop log-on, web access to e-mail, and single sign-on for web applications

This Service Description outlines the primary elements of the UA Service including the software and service components described below. This Service Description does not provide details of the VIP Authentication Service, Symantec™ Mobile Fulfillment Service or Symantec™ SMS OTP Authentication Service, which are described in their respective service descriptions.

UA Service Components

Credentials

A credential consists of both a shared key and a unique credential ID ("Credential"). The shared key is protected by and/or embedded in a token or a software or hardware device ("Device") in the physical possession of an end-user. Using a known cryptographic algorithm, the Credential is used by the Device and the UA Service to generate an OTP value. The OTP is also referred to as a "Security Code" throughout the product documentation. The OTP generated by the Device can then be compared to the OTP value generated for such Device by the UA Service, and if the values match, the Credential will be validated. Symantec™ UA Credential complies with the OATH standard and can be embedded in a multitude of form factors:

- Symantec™ Security Token is the traditional enterprise authentication token, capable of generating an OTP and showing it to the end-user through a dedicated display. No client software needs to be deployed on the end-user desktop.
- Symantec™ Hybrid Security Token is an all-in-one security token capable of both OTP and PKI authentication (*client certificates sold separately*). For certificate operations, the token has a USB connector and embeds a smart card. Drivers must be installed on the client desktop to enable

communication between the end-user and the token cryptographic processor via the USB connector. The Hybrid Security Token also has a dedicated display for end-users to get the OTP, identical in functionality to the Security Token

- Symantec™ Security Card is a security credential that can offer the same capability as the Security Token in a card that fits in a wallet. It can be customized with your corporate logo, branding, and custom colors to suit your business.
- Symantec™ *Access for Mobile* is a security credential embedded on an application designed to run on a mobile device possessed by an end-user. It can be customized with your corporate logo, branding, and custom colors to suit your business.

Credential Provisioning

A Device contains a Credential (defined above) that is provisioned and known only to the Symantec-hosted authentication service. Credential provisioning can be achieved using one of the two available methods:

- Bulk credential provisioning is accomplished by loading a list of Credentials and their corresponding shared keys from an encrypted file.
- Dynamic credential provisioning relies on an SSL protected web-services based API that allows Devices to request a Credential and a shared secret whenever needed. The UA Service generates Credentials on-demand and provisions such Credentials securely to the end-user.

Credentials are not accessible from outside the Device. Within a dedicated hardware Device, there is space to store the Credential and only the application found inside can access it. Accessing the Credential would necessitate physically breaking into the Device, which would render the Credential unusable. In the case of a Credential stored in a software Device, the Credential is stored encrypted using an encryption key only accessible to the software Device.

As part of the Credential Provisioning processes described above, the UA Service securely stores a copy of the Credential in encrypted form. The Credential is encrypted using a TripleDES encryption algorithm.

Validation Service

The UA Service supports two-factor authentication by utilizing a first and second factor authentication. The first factor, "what you know," can be a personal identification number ("PIN") or a password associated with each end-user. This is stored in the enterprise directory. The second factor, "what you have," is a One Time Password (OTP aka Security Code) generated by the Credential. OTP validation is performed by the Symantec-hosted validation service. For each validation request sent to the UA server, the first-factor validation is performed locally at the enterprise directory. The UA server then forwards the credential ID and OTP value to the Symantec-hosted validation service. The Symantec-hosted validation service authenticates the OTP value, or second factor.

Provisioning Service

Token activation is the operation that activates the Credential for two-factor authentication. The service uses a secured SSL channel as the primary transport between the enterprise and the Symantec-hosted service. The credential ID is bound to the end-user in the enterprise directory, and an activation notification is sent to Symantec (along with proof of token possession) so that the token may be used for two-factor authentication.

Management Service

Each Credential can be tested using a supplied OTP to ensure that it functions correctly. If the Credential cannot be validated, it may need to be synchronized. This is accomplished by supplying two consecutive OTPs. If the Credential becomes locked due to multiple attempts to validate incorrect OTPs, it can be re-activated through an administrative enable operation. If access needs to be blocked on a temporary basis, an administrative function to disable the PIN (if used) or the Credential itself is available. The Credential can be unbound from the current end-user and bound to a different end-user for self or administrative re-activation, if permitted by an enterprise's internal IT policy.

For accounts enabled for VIP Authentication Service, the Credentials can be shared across the VIP Network and other enterprises' VIP credentials can be activated and used with the UA Service, as described in the VIP Authentication Service Description.

Self-Service Web Application

A self-service website is provided to allow end-users to activate, synchronize, and test their Credentials. Additional functionality exists for end-users to be able to reset their PIN. APIs are provided so that custom Self Service Applications can also be developed. This includes functionality for Credential activation, recovery of forgotten password, and synchronization of out-of-sync or locked token.

Administrative Web Application

An administration console provides for easy management of Credentials. From this interface, administrators can manage individual Credentials and end-user binding, lock/unlock Credentials, reset PINs, and assign Credentials in bulk to end-users. Role-based administration allows for designation of specific administrators to assigned management roles within UA.

Application Integration Toolkit

APIs are provided for development of custom applications for end-user and Credential management as well as integration into third-party applications. It includes management tools for the issuance, revocation, tracking and auditing of Credentials and more generally, to support Credential life-cycle management functions as well as administrative capabilities for end-user management, such as:

Self Service

Internal portals used for end-user functions can be enhanced with strong authentication Credential self management functionality such as activation, synchronization, password reset.

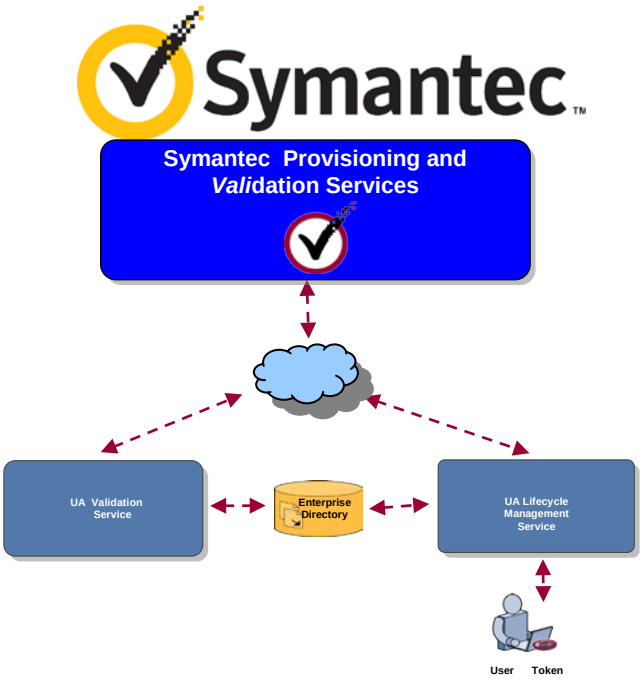
Help Desk Services

Supported Help Desk functions include all self-service applications: password reset, Credential resynchronization as well as lost/broken Credential. Where an end-user misplaces or breaks a Credential, the administrator can generate a temporary password that can be used instead of the OTP for a defined period of time.

Administration Services

One of the most important administration functions is Credential enablement/disablement. By disabling an end-user Credential, the administrator can also trigger the fall-back to single factor authentication.

Other important administration functions include manual Credential assignment (Credential-end-user binding) and Credential activation. These functions allow the administrator to manually bind a Credential to an end-user within the user store. Although the proposed Credential distribution model assumes no pre-binding until the end-user actually activates the Credential in a self-service mode, this function enables the administrator to manually assign a Credential to a specific end-user and possibly activating the Credential too.



Audit Trails

Significant events are recorded on a transaction-by-transaction basis. Audit records are maintained independently in multiple media depending upon the sensitivity of the event. Audit trails are created for all OTP transactions, including passed and failed validations, passed and failed activations, and passed and failed PIN resets. In addition, end-user administration contains audit logs that record functions executed by individual administrators.

Localization

Localization tools enable the UA Service to be altered such that various interface screens, menus, and other graphical components display in a specified local language. It also allows enterprises to co-brand certain UA Service components, as described in the product documentation. This optional component is comprised of:

- Localization Documentation – Instructions to assist enterprises in the localization process and provides detailed steps required to create a UA Service Language Pack. This document describes the applicable resources, such as the Self-Service web application, that need to be translated and their respective locations. It also includes co-branding principles and guidelines.
- Language Pack Builder – Software that processes the localized input files generated locally and create a UA Service Language Pack.

The UA Service Language Pack, once developed, is installed on top of a standard UA Service installation. This operation will effectively apply the localized resources, overwriting the standard values. Once installed, UA Service Language Pack modifies the behavior of the UA Service such that only the localized resources will be displayed.

Third Party Integrations

The UA Service includes documents and custom plug-ins where necessary, that layer two factor authentication on top of many popular enterprise applications that require end-user based access. The respective documents and software are distributed on-line. The website is updated on a regular basis with new integrations.

UNIFIED AUTHENTICATION OTP SERVICE TERMS AND CONDITIONS

1. DEFINITIONS

"Agreement" means the Master Services Agreement or such other agreement entered into between Symantec and Customer under which the Service Order applicable to this Service Description is issued.

"Credential" consists of both a shared secret and a Credential ID. The shared secret is protected by, and/or embedded in a device in the physical possession of an end user.

"Credential ID" is an alphanumeric string that can vary in length from 12 to 16 characters that identifies the Credential.

"Service Administrator" or "SA" is a duly authorized employee of Customer that is responsible for carrying out the functions of an SA specified below.

"User" means a person issued a Credential provisioned for authentication through the UA Service.

2. CUSTOMER'S OBLIGATION

(a) Appointment. Customer shall appoint one or more authorized Customer employees as Service Administrators (SA(s)). Such SA(s) shall be entitled to appoint additional SAs on Customer's behalf. Customer shall cause SAs appointed hereunder to abide by the terms of this Agreement and the OTP Authentication Service Administrator's Handbook.

(b) Administrator Functions. Customer is responsible for all Credential issuance, activation, and revocation activities, which shall be performed by Customer's SA(s). If a User who had been issued a Credential by Customer ceases to be affiliated with Customer, then Customer shall deprovision such User by disabling such User at the Customer directory level, and deactivating the Credential issued to such User. Such Credential may thereafter be reassigned to another licensed User through the standard provisioning process. If an active Credential is lost or stolen, Customer shall promptly deactivate such Credential. If an SA ceases to have the authority to act as SA on behalf of Customer, then Customer shall promptly prevent such SA from performing the administrator functions set forth above.

(c) Customer's Warranties. In addition to the express limited warranties set forth in the Agreement, Customer warrants to Symantec that: (i) Customer's SA(s) has been (since the time of the PIN creation) and will remain the only person (other than the applicable User) possessing or having access to Users' PIN and other activation information, and no unauthorized person has had or will have access to such information; and (ii) Customer will not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any Symantec system, software or Service.

3. SYMANTEC'S OBLIGATIONS

(a) Installation. Symantec recommends that Customer utilize Symantec Professional Services consultants to install the UA Service.

(b) UA Service. Following completion of the requisite installation, Symantec shall deliver the UA Service for the duration of the term of service. Upon receipt of a valid Credential ID and activation request from Customer's SA, Symantec will verify such Credential ID to a Credential issued by Symantec to Customer, and activate the UA Service for such Credential. Following such activation, Symantec will perform the UA Service for such Credential, and return pass/fail authentication responses to Customer authentication requests, based on the correspondence of the OTP password information submitted to Symantec for such Credential. Symantec shall be subject to its standard Service Level Agreement for PKI and Authentication services.

4. LOCALIZATION

Symantec makes reasonable efforts to ensure the accuracy and completeness of the information found in the Language Pack in their original English version, but bears no responsibility whatsoever for translated information or text when translated into a language outside of English. Symantec makes no warranties of any kind (whether express, implied or statutory) with respect to the translated textual information contained in and arising out of Customer's use of the Language Pack and assumes no liability to Customer or any third party for any loss or damage (whether direct or indirect) caused by any errors, omissions, or statements of any kind contained therein for any reason relating to such translation.