

MOBILE AUTHENTICATOR STUDIO (MAS) RECURRING UPGRADE AND APP STORE PUBLISHING PACKAGE DETAILS

1) Project Parameters

Maximum Service Hours included in this Package	Forty-Eight (48) hours
Expected Project Duration	Twelve (12) Months
Location of Professional Services	Remote

2) Governing Terms

The Professional Services are delivered pursuant to the Master Terms available for review at www.onespan.com/master-terms, including the Professional Services Schedule at <https://www.onespan.com/professional-services> (the "PS Schedule"), unless Customer has previously executed a written agreement for the sale of the Services, in which case such agreement shall control (the "Contract"). Terms not defined herein shall have the meaning given them in the Contract.

3) Assumptions and Pre-requisites

- a) This OneSpan MAS Recurring Upgrade and App Store Publishing Package (the "Packaged Services") describe Supplier's provision of Professional Services to Customer to upgrade Customer's MAS application and assist with its publication during a period of one (1) year.
- b) Packaged Services are performed remotely and during standard business hours of the Supplier office providing the Service ("Service Hours"), unless otherwise agreed in writing.
- c) Supplier can perform services outside of "Service Hours" at an additional expense through a separate agreement.
- d) Customer must have valid licenses for:
 - i) OneSpan Mobile Authenticator Studio ("MAS")
 - ii) Application Shielding (When applicable)
- e) Customer must ensure that their implementation environment meets the minimum server requirements identified in the Product Documentation.
- f) Customer will establish sufficient access to use Supplier's current remote services capability.
- g) Prior publishing of the MAS application on at least one (1) app store by the Customer or with OneSpan's support where Customer has purchased MAS Base Implementation Package
- h) Customer has maintained in their possession the customization tool used to publish their existing MAS application.
- i) Customer must have the required accounts for publishing the updated MAS application on the Apple and/or Google App Store (the "Target App Stores"). When OneSpan provides the publishing service, the Customer will share credentials or delegate access to Supplier to enable OneSpan to access the Target App Store and to deliver the Service.
- j) Only one (1) MAS application is in scope.
- k) Customer will prepare and provide any content for Target App Stores (i.e.. Images and text). This package will automatically renew and be invoiced every twelve (12) months unless cancelled in writing at least sixty (60) days prior to renewal.
- l) If multiple languages are required, the customer is responsible for providing the equivalent text in the desired language.
- m) Customer must provide the required information during the application creation process in the relevant stores, (screenshots in different dimensions, Application description, help links..etc.)

4) Services

- a) Project kickoff conference call
 - i) Supplier will conduct a project kickoff call to set objectives and explain project phases and scope.
 - ii) Supplier will work with the Customer to see that all prerequisites and requirements conditional for the provisioning of the Services, are fulfilled.
 - iii) Review current server architecture and define OneSpan Authentication Server upgrade path.
- b) Version upgrade MAS binary and/or Application Shielding/RASP version and testing.
 - i) Supplier will obtain Customer's latest GUI and functionality configuration, apply the MAS and/or Application Shielding version update and rebuild the MAS binary package(s).
 - ii) Supplier will test the updated MAS binary package(s).
- c) Integration support during Customer validation of the updated MAS binary
 - i) Supplier will provide the updated MAS binary package(s) and provide engineering guidance to the Customer during their efforts to validate the binary.
- d) MAS signing and publishing
 - i) Supplier will sign the updated MAS application(s) with Customer's private key(s).
 - ii) Supplier will submit MAS application(s) to Target App Store for validation by Apple and Google.

- iii) Supplier will provide best practices to get the MAS application(s) approved by Apple and Google.
- iv) Supplier will include "What's new" text on the Target App Store.
- e) Updated customization tool
 - i) Supplier will provide the Customer with the latest GUI and functionality configuration based on the update MAS binary package(s)..

5) Project Deliverables

Deliverable #	Deliverable Description
0001	Customer MAS application binary package(s) updated to the newest version of the MAS application and/or Application Shielding for both Customer's testing and production environments and signed with Customer's private key.
0002	Updated, signed and validated production Customer MAS application submitted for review and publication on the Target App Stores.

6) Exclusions

- a) Additional updates on top of the three (3) updates included in this Package within a twelve (12) month period.
- b) Migration to a new major version of Mobile Authenticator Studio (version 4 to 5). (Available through a separate offering).
- c) Configuration of, or for, third party applications or hardware.
- d) Any change in the configuration, parameters or functionalities included in the current MAS application.
- e) Updates to the content of the Target App Store(s) other than the updated application binary package(s).
- f) Creation of test users or test accounts to allow the validation of the MAS Application by the Target App Stores.
- g) Creation of a video demonstrating the flow of the MAS Application.
- h) Any unsupported mobile device as per the requirements of MAS. The MAS software depends on the new releases of Android and iOS. It follows the official directives of Android and iOS supported devices when needed. OneSpan cannot guarantee the support of hardware devices outside of the list of supported devices as published by Apple and/or Google.
- i) Application Shielding competency development or integration support. (Available through a separate offering).
- j) Support for mobile application penetration testing.
- k) Creation, update, and storage of application upload key and certificates for Target App stores.
- l) Supplier creation of custom documentation.
- m) Any Professional Services not expressly addressed in this Package.
- n) Professional Services within this Package scope, beyond the 12-month timespan.