MOBILE SECURITY SUITE (MSS) INTEGRATION STARTER PACKAGE DETAILS

1) Project Parameters

Maximum Service Hours included in this Package	One Hundred Sixty-Two (162) Hours
Expected Project Duration	Five (5) 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 Mobile Security Suite (MSS) Integration Starter Package (the "Package") governs Supplier's provision of Professional Services to Customer to support the Customer's MSS integration.
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) Services can be provided on-site at Customer's location subject to an additional travel and lodging expense billed separately.
e) Customer must have valid licenses for:
   i) OneSpan Mobile Security Suite
   ii) OneSpan Authentication Server Framework, OneSpan Authentication Server, or OneSpan Cloud Authentication
f) Customer must ensure that their implementation environment meets the minimum server requirements identified in the product documentation.
g) Customer will establish sufficient access to use Supplier's current remote services capability.
h) Customer personnel must be able to provide input regarding the current processes for authentication, transaction approval, Customer registration and the planned application architecture.
i) All development performed by the Customer.
j) Customer has a previously installed OneSpan Authentication Server / OneSpan Authentication Server Appliance version 3.x or above, OneSpan Authentication Server Framework, or OneSpan Cloud Authentication, and the previous installed application is currently operational with no outstanding Support issues.

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.
b) MSS workshop
   i) Supplier will provide a product update for MSS specific to the current OneSpan Authentication Server, OneSpan Authentication Server Framework, or OneSpan Cloud Authentication solution currently in use by the Customer.
   ii) Supplier will provide MSS SDK competency development instruction.
   iii) Supplier will work with the Customer to define their MSS functionality requirements and complete an MSS parameter sheet.
c) MSS integration support
   i) Supplier will provide engineering guidance to the Customer in support of their efforts to implement the MSS SDK.
d) Integration validation service
   i) MSS security solution application workflow review
      (1) Supplier will review the Customer's business requirements.
      (2) Supplier will perform a detailed review of the Customer's functional process flow where MSS modules are used.
      (3) Supplier will work with the Customer to complete application functionality worksheets.
   ii) MSS solution validation review
      (1) Supplier will validate the Customer's use of MSS SDK calls for iOS and Android.
      (2) Supplier will validate the Customer's use of MSS security features.

(3) Supplier will validate the Customer's use of MSS integration rules.
iii) Validation review workshop
(1) Supplier will conduct a workshop with the Customer to provide feedback and recommendations resulting from the integration validation review.
iv) Integration validation report
(1) Supplier will create a solution validation and MSS integration validation report documenting the feedback and recommendations from the integration Validation review (the "Integration Validation Report").
v) Validation of Critical issues
(1) Supplier will validate the Customer's corrections of all remarks that were flagged in the Integration Validation Report as being 'Critical'.

5) Project Deliverables

Deliverable #	Deliverable Description
0001	Materials used during the MSS SDK competency development.
0002	Completed MSS parameter sheet.
0003	Integration Validation Report, delivered two (2) calendar weeks after the review workshop.
0004	Post-review validation of report remarks flagged 'Critical'

6) Exclusions

a) Custom development by Supplier.
b) Future updates to MSS application on target App Stores.
c) Application publishing or publishing support
d) Configuration or programming of third-party or other applications/hardware.
e) Custom Documentation.
f) OneSpan Authentication Server Framework Upgrade
g) OneSpan Authentication Server Upgrade
h) The following SDKs:
    a. Client device data collector SDK
    b. Application Shielding SDK (RASP)
    c. OneSpan Sign SDK
    d. Bluetooth SDK
i) Windows and Blackberry Mobile operating system integration validation.
j) Validation of 'Critical' issues later than one (1) month after the Integration Validation Report has been delivered.
k) Any Professional Services not expressly addressed in this Package.
l) Professional Services within this Package scope, beyond the 12-month timespan.