MOBILE SECURITY SUITE (MSS) INTEGRATION VERIFICATION SERVICE PACKAGE DETAILS

1) Project Parameters

Maximum Service Hours included in this Package	Seventy-Eight (78) Hours
Expected Project Duration	Two (2) 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 Verification Service Package (the "Package") governs Supplier's provision of Professional Services to Customer to support the verification of Customer's OneSpan Mobile Security Suite implementation.
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 OneSpan Mobile Security Suite.
f) Customer must ensure that their implementation environment meets the minimum server requirements identified in the Product Documentation.
g) Supplier performs the integration verification on one (1) mobile application developed for both iOS and Android.
h) Customer personnel have experience with the programming languages relevant to the integration.
i) Customer commits to dedicated project availability of the following profiles:
    i) Mobile developer(s): to guide and explain the implemented solution to the degree requested by Supplier consultant
j) Customer to provide the completed MSS integration verification checklist prior to project kick-off.
k) Customer to grant read access to the application and plugin(s) source code where the MSS related functionality is implemented:
    i) Every flow related to any use-case involving any of the MSS SDKs
    ii) Every piece of code using any of the MSS SDKs
    iii) Every parameter being used or returned by any MSS SDK APIs
l) Customer will establish sufficient access to use Supplier's current remote services capability.
m) For the verification of the critical issues after reception of the Integration Verification Report (as defined below) report, Customer will make the necessary changes within one (1) month after the report for critical and high priority recommendations.

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 Professional Services, are fulfilled.
b) MSS security solution application workflow review
    i) Supplier will review the Customer's business requirements.
    ii) Supplier will perform a detailed review of the Customer's functional process flow where MSS modules are used.
    iii) Supplier will work with the Customer to complete the Application Functionality Worksheets.
c) MSS integration verification workshop
    i) Supplier will validate Customer's mobile application and provide feedback and recommendations based on the application workflow review including:
        (1) Customer's use of MSS SDK calls for iOS and Android.
        (2) Customer's use of MSS security features.
        (3) Customer's use of MSS integration rules, requirements and best practices.
d) Integration verification report
    i) Supplier will create a solution verification and MSS integration verification report documenting the

feedback and recommendations from the integration verification review (the "Integration Verification Report").

e) Verification of critical issues
   i) At latest within one (1) month after the report, Supplier will validate the Customer's corrections of all remarks that were flagged in the report as being 'Critical'.

5) Project Deliverables

Deliverable #	Deliverable Description
0001	Integration Verification Report, delivered two (2) calendar weeks after the review workshop.
0002	Post-review verification of report remarks flagged 'Critical'.

6) Exclusions

a) Build or modification of Customer's mobile application(s).
b) Integration support or training on MSS, outside of basic questions and answers related to the verification recommendations.
c) Custom development by Supplier.
d) The code review will not cover
e) The User Interface and User Experience
f) The coding style – unless it weakens the application or breaks a functionality
g) Parts of the code not related to MSS SDKs
h) More than one (1) mobile application
i) Penetration testing
j) Windows and Blackberry Mobile operating system integration verification.
k) Verification of critical issues later than one (1) month after the Integration Verification Report has been delivered.
l) Integration verification of Customer's OneSpan Authentication Server Framework (OASF)
m) Installation, configuration, backup or management of any third-party software or hardware (such as operating systems, databases, network settings, backup systems, monitoring solution, Active Directory or other Windows Services, load balancers, server hardware, firewall).
n) Any Professional Services not expressly addressed in this Package.
o) Professional Services within this Package scope, beyond the 12-month timespan.