ONESPAN AUTHENTICATION SERVER FRAMEWORK (OASF) INTEGRATION VALIDATION PACKAGE DETAILS

1) Project Parameters

Maximum Service Hours included in this Package	Sixty-Six (66) 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 OneSpan Authentication Server Framework (OASF) Integration Validation Service Package (the "Packaged Services") describe Supplier's provision of Professional Services to Customer to support the validation of Customer's OneSpan Authentication Server Framework 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 additional travel and lodging expense billed separately.
e) Customer must have a valid license for OneSpan Authentication Server Framework.
f) Customer must ensure that their implementation environment meets the minimum server requirements identified in the product documentation.
g) Customer personnel have experience with the programming languages relevant to the integration.
h) Customer to provide the completed OneSpan Authentication Server Framework integration validation checklist prior to project kick-off.
i) Customer to grant access to the architecture and infrastructure information with the OneSpan Authentication Server Framework integration validation.
j) Customer to grant read access to the application source code where the OneSpan Authentication Server Framework related functionality is implemented.
k) Customer personnel must be able to provide input regarding the current processes for authentication, transaction approval, Customer registration and the planned application architecture.
l) Customer will establish sufficient access to use Supplier's current remote services capability.
m) For the validation of the critical issues after reception of the report, Customer commits to making the necessary changes within one (1) month after the report for critical, high and medium 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 Services, are fulfilled.
b) OneSpan Authentication Server Framework (OASF) security solution application workflow review
   i) Supplier will review the Customer's Business requirements and technical flows
   ii) Supplier will review the Customer's functional process flows where OneSpan Authentication Server Framework (OASF) modules are used
c) OneSpan Authentication Server Framework (OASF) integration validation workshop
   i) Supplier will validate Customer's application and provide feedback and recommendations to the Customer based on the application workflow review including:
      (1) OASF SDK function calls and parameters
      (2) The data model used to store OASF related objects
      (3) Kernel parameters validation
      (4) Customer's use of OASF security features and best practices
      (5) The Data Model for Digipass related data
      (6) The flows related to Digipass
      (7) Every piece of code using OASF
      (8) Every parameter being used or returned by an OASF API
      (9) The Kernel Parameter values

d) Integration validation report
   i) Supplier will provide feedback and recommendations to the Customer based on the workflow review
   ii) Supplier will create a solution validation and OASF integration validation report documenting the feedback and recommendations from the integration validation review.
   iii) Customer will apply corrections to remarks flagged as 'Critical' within one (1) month from receipt of the integration validation report.
e) Validation 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 validation report.
0002	Validation of Customer's correction of remarks flagged 'Critical' subject to completion of requirement in section 4(d)(iii).

6) Exclusions

a) Build or modification of Customer's application.
b) Integration support or training on OASF subject of a separate Service Package.
c) Any development by OneSpan.
d) Validation of Critical issues if Customer does not apply corrections within one (1) month after the Integration validation report has been delivered.
e) Integration validation of Customer's mobile application(s) using Mobile Security Suite (MSS).
f) Coding style – unless it weakens the application or breaks a functionality.
g) Parts of the code not related to OASF.
h) Installation, configuration, backup or management of any 3rd 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).
i) Any Professional Services not expressly addressed in this Package.
j) Operating System not supported by latest OneSpan Authentication Server.