ONESPAN CLOUD AUTHENTICATION (OCA) DATA MIGRATION PACKAGE DETAILS

1) Project Parameters

Maximum Service Hours included in this Package	Eight Hours (8)
Expected Project Duration	Three (3) weeks
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 Cloud Authentication Data Migration Package ("Package") governs Supplier's provision of Professional Services aimed at migrating user and token data from one (1) existing OneSpan Authentication Server Framework (OASF) or OneSpan Authentication Server (OAS) to the OneSpan Cloud Authentication (OCA) solution. If Customer's requirements exceed those agreed to in this Package, Customer may enter into a Tailored Services SOW (as defined in the PS Schedule) with Supplier instead of this Package.
b) Customer must have an existing OASF or OAS solution in good operation (no pending support tickets) and have a version number that is still officially supported by Supplier (https://www.vasco.com/support/product-support/product-life-cycle.html)
c) If Customer is migrating data from a version of OAS older than v.3.20, they must also order the appropriate OAS upgrade package (available in a separate agreement).
d) Packaged Services are performed remotely and during standard business hours of the Supplier office providing the Service ("Service Hours"), unless otherwise agreed in writing.
e) Supplier can perform services outside of "Service Hours" at an additional expense through a separate agreement.
f) Customer must have valid licenses for OneSpan Cloud Authentication.
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 OAS or OASF system configuration and functionalities in use, state of existing DPX files, token types currently in use, format of database schema (pertains to OASF only), current OASF or OAS version installed.

4) Services

a) Data Migration Review Session
   i) Supplier will conduct a working session with the Customer to understand its current OASF or OAS data usage and data migration requirements.
   ii) Supplier will provide engineering guidance on how to export their OASF or OCA data for import into the OCA solution.
   iii) Supplier will explain the process for migrating user and token data into the OCA solution.
b) Data Migration Processing
   i) Supplier will provide engineering guidance to the Customer to export data from their existing solution.
   ii) Supplier will migrate the Customer provided data into one (1) OCA environment.
   iii) Supplier will provide engineering guidance to the Customer to verify all data migrated successfully.

5) Project Deliverables

Deliverable #	Deliverable Description
0001	Documented design of up to five (5) custom workflows.

6) Exclusions

a) Configuration of, or for, third party applications or hardware
b) Hardware security module extension
c) Software DIGIPASS provisioning
d) Audit report
e) DIGIPASS customization
f) Distribution and fulfilment services
g) Custom development
h) No new product feature development or customization (available in a separate agreement).
i) Mobile Security Suite (client-side) API competency development and engineering guidance (available in a separate agreement)
j) Mobile Authenticator Studio Base implementation, GUI configuration, and publishing (available in a separate agreement)
k) Creation of custom documentation
l) Creation of custom training materials
m) Translations
n) Direct configuration or programming of third-party or other applications/ hardware
o) Customized AWS data protection to allow relying parties to specify their own keys for encryption of data at rest. Supplier can implement this through an optional Bring-Your-Own-Key (BYOK) package
p) Mobile or web banking application development
q) Changes to workflows/outbound APIs
r) New product feature development or customization (available in a separate agreement).
s) Authentication to IAA through Active Directory. expressly addressed in this Package.
t) Operating System not supported by latest OneSpan Authentication Server.