

ONESPAN CLOUD AUTHENTICATION (OCA) DATA MIGRATION PACKAGE DETAILS

1) Project Parameters

Maximum Service Hours included in this Package	Thirty two Hours (32)
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), OA Suite 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, OA Suite 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>). If Customer is migrating data from an unsupported version of OAS, they must also order the appropriate OAS upgrade package (available in a separate agreement).
- c) Packaged Services are performed remotely and during standard business hours of the Supplier office providing the Service ("Service Hours"), unless otherwise agreed in writing.
- d) Supplier can perform services outside of "Service Hours" at an additional expense through a separate agreement.
- e) Customer must have valid licenses for both the source (OASF, OA Suite or OAS) and target environments (Authentication Server,) and OneSpan Cloud Authentication.
- f) Customer will establish sufficient access to use Supplier's current remote services capability.
- g) 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 or OA Suite only), current OASF, OA Suite 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, OA Suite 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 Customer's OCA Staging environment. Customer is entitled to two (2) imports in the Staging environment.
 - iii) Supplier will migrate the Customer provided data into Customer's OCA Production environment.
 - iv) Supplier will provide engineering guidance to the Customer to verify all data was migrated successfully.

5) Project Deliverables

Deliverable #	Deliverable Description
0001	Migrated user and token data accessible in Staging and Production environments.

6) Exclusions



- a) Migration from an unsupported OASF, OA Suite or OAS solution
- b) Generate data export from Customer's existing OASF, OA Suite or OAS solution
- c) Upgrade of any existing OASF, OA Suite or OAS solution
- d) Configuration or programming of, or for, third party applications or hardware
- e) Software DIGIPASS provisioning
- f) Custom development
- g) Hardware security module extension
- h) Audit report
- i) No new product feature development or customization (available in a separate agreement).
- j) Creation of custom documentation or training materials
- k) Translation of any documentation
- l) 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
- m) Changes to workflows/outbound APIs
- n) Authentication to IAA through Active Directory. expressly addressed in this Package.
- o) Any Professional Services not expressly addressed in this Package.