NEXT GEN APPLICATION SHIELDING MASTER CODE SAAS STARTER PACKAGE DETAILS

1) Project Parameters

Maximum Service Hours included in this Package	Hundred and four (104) Hours
Expected Project Duration	Three (3) Month
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 Next Gen Application Shielding **Master Code SaaS** Starter Package (the "Packaged Services") describes Supplier's provision of Professional Services to Customer to support Customer's implementation of OneSpan Next Gen Application Shielding Master Code on SaaS for one (1) mobile app on iOS and Android.
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 expenses billed separately.
e) Customer must have valid licenses for:
    i) Next Gen App Shielding - Master Code with AH SaaS (mandatory)
    ii) Optionally, licenses for add-ons
f) Supplier will provide services to assist with configuration of only the following mobile in app functionalities (only when applicable and if Customer has valid license)::
    i) In-app threat detection
    ii) In-app threat response
    iii) Crypto keys management
    iv) Obfuscation
    v) REST API protection
    vi) Crypto utils
    vii) Malware protection
    viii) User interface protection
    ix) Secure PIN (Android only)
    x) Secure channel PCI
g) Supplier will provide services to configure only the following optional add-on for SaaS threat intelligence functionalities (only when applicable and if Customer has valid license):
    i) "TraceBoard"
    ii) "DeviceAttest"
    iii) "BuildAPI"
h) Customer is deemed knowledgeable on mobile development (Java, Objective C, SWIFT, Kotlin, and other applicable mobile development programming languages)
i) Customer will establish sufficient access to use Supplier's current remote services capability (MS Teams).
j) Customer will arrange for mobile test devices
k) Customer is proficient in C development (for Secure PIN)
l) Customer is deemed knowledgeable about operating the Docker platform
m) Customer commits to the dedicated availability of the following profiles: Project Manager, Enterprise/Security Architect, Product Owner, Mobile Developer, Business Tester.

4) Services

a) Project kickoff conference call
    i) Supplier will:
        (1) Conduct a project kickoff call to explain the overall approach, set objectives and explain project phases and scope
        (2) Verify that all prerequisites and requirements for the provisioning of Services are fulfilled
        (3) Share relevant product information: access to on-line documentation and sample code
        (4) Perform a high-level mobile SDK walkthrough

(5) Perform a high-level SaaS threat intelligence walkthrough
(6) Share Kick Off slides and next steps

ii) Customer and Supplier to agree on:
(1) Success criteria for the engagement
(2) Project controls (communication cadence, schedule, escalation paths)
(3) Next steps

b) Application Shielding Solution Design Session
i) Supplier will conduct a solution design session with Customer covering:
(1) Overall solution overview
(a) Mobile in-app protection
(b) Active hardening
(c) Threat intelligence and response
(2) Explain mobile SDK integration approach, architecture, and compatibility with the Customer's technology stack.
(3) Provide guidelines for SaaS deployment and configuration
(4) Deliver the solution design diagrams

ii) Customer will
(1) Validate the solution design with bank's enterprise, security, and compliance architecture.

c) Next Gen App Shielding In App Competency Development
i) Supplier will:
(1) Provide competency development to Customer on the required SDKs
(2) Share training materials

d) Next Gen App Shielding Setup And Configuration
i) Supplier will:
(1) Configure the Customer entity in the Staging and Production SaaS environments
(2) Support Customer with initial SDK integration and server config
(3) Assist on the definition of the rule set

ii) Customer will:
(1) Allow connectivity to SaaS backend

e) Next Gen App Shielding Threat Intelligence Competency Development
i) Supplier will:
(1) If applicable and provided Customer has a valid Product license, provide competency development to Customer on SaaS modules TraceBoard and/or DeviceAttest and/or BuildAPI
(2) Share training materials

f) Guidance During Development And Integration
i) Supplier will:
(1) Guide Customer with the integration of the SDKs
(2) Perform intermediate reviews of the integration
(3) Advice on best practices for integration

ii) Customer will:
(1) Integrate the client SDK into mobile app and handle configuration and development testing
(2) Ensure correct integration using SDK and backend analytics systems.

g) Guidance During End User Testing
i) Supplier will:
(1) Monitor SaaS environment in relation to the tests being executed

ii) Customer will:
(1) Define the relevant test scenarios
(2) Validate the use cases and business flows
(3) Regression tests on existing flows

h) Validation of Mobile Application Before Publication
i) Supplier will:
(1) Review the implementation of the final mobile application
(2) Review security configuration

ii) Customer will:
(1) Apply corrections and revalidate use cases on a relevant range of mobile devices and OS versions
(2) Provide a sign off that the functionalities in scope of this engagement have been implemented as expected

i) Next Gen App Shielding Go-Live Support
i) Supplier will:
(1) Assist in release to Production
(2) Provide post-go-live support for a period of five (5) calendar days
(3) Arrange for a handover to OneSpan Customer Support.

5) Project Deliverables

Deliverable #	Deliverable Description

0001	Solution design recommendations and diagrams
0002	SaaS backend configured in Staging and Production
0003	In app and threat intelligence competency development training materials

6) Exclusions

The following are excluded from these Packaged Services:

a) 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)
b) Any OneSpan solution software deployed on premise
c) Services for unlicensed modules
d) Services related to version upgrades after project end
e) Services related to monitoring or trend evolution of the SaaS environment
f) Custom documentation
g) More than one (1) mobile application (Available through separate add-on offering)
h) Support for mobile application penetration testing
i) Services for mobile development
j) Application publishing or publishing Support
k) Definition or execution of test scenarios
l) Storage by OneSpan of publishing/signing keys
m) Configuration of any out-of-scope functionalities
n) Development of any new features or functionality not expressly described in the Documentation in effect at the time of purchase
o) Any Professional Services not expressly addressed in this Package