ONESPAN SAAS SERVICE DESCRIPTIONS

These Service Descriptions are incorporated into and governed by the Master Terms at www.onespan.com/master-terms and the SaaS Subscription Schedule at www.onespan.com/saas-subscription-schedule. Terms not defined herein shall have the meaning given to them in the Master Terms or SaaS Subscription Schedule. Each of the Service Descriptions below apply to the particular Product indicated. Each SaaS Service is sold separately.

CHOOSE A PRODUCT FAMILY

Select a product below to jump directly to its Service Description.

SAAS PRODUCTS

Cybersecurity

DigipassONE Product Suite
- DigipassONE Authenticate
- DigipassONE Verify
- DigipassONE Insights
- DigipassONE Protect

OneSpan Cloud Authentication
authentication and signature validation via REST API

Intelligent Adaptive Authentication
risk analytics and orchestrated multi-factor authentication

Threat Fabric Mobile Threat Intelligence
curated mobile malware and fraud intelligence portal

Threat Fabric Fraud Risk Suite
malware, device and behavior risk indicators in real time

Digipass Management Portal
inventory, assignment and fulfillment tracking for Digipass devices

SAAS PRODUCTS

Digital Agreements

OneSpan Sign
e-signature platform, Virtual Room, Integration Platform, HYOK

OneSpan Notary
IPEN and Remote Online Notarization on the OneSpan Sign platform

Communication Hub
SMS OTP delivery, sold in Credits

OneSpan Identity Verification (IDV)
document verification, face comparison and OTP workflows

Each SaaS Service is sold separately. Product names and groupings are for navigation only and do not modify the terms of any Service Description, Order Document or the Contract.

DigipassONE Authenticate

DigipassONE Authenticate is OneSpan's passkey/FIDO authentication service sold either bundled with OneSpan Cloud Authentication ("DigipassONE Authenticate SaaS") or standalone ("DigipassONE Authenticate – Passkey Edition SaaS").
DigipassONE Authenticate provides customers with two different environments to support their development, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.

Production:

- Production usage of the current version of DigipassONE Authenticate
- Subject to the Service Levels detailed below

Staging:

- Integration, development and testing of the current version of DigipassONE Authenticate
- Not subject to the Service Levels, security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Staging environment

Pricing

DigipassONE Authenticate is sold based upon the committed number of Monthly Active Users. **"Monthly Active User"** or **"MAU"** means, for any calendar month, each individual, entity, or account that: (a) is issued a passkey by, or is authenticated in connection with, DigipassONE Authenticate; or (b) otherwise directly or indirectly accesses or uses a DigipassONE Authenticate, including access or use through Customer's services, applications, or software, whether by API call or otherwise.

The actual average number of MAUs during each twelve (12) month period during each annual term, shall be calculated at the end of such twelve (12) month period, and shall be calculated to be the average MAUs during such twelve (12) month period. If the actual average number of MAU in any year exceeds the maximum MAU indicated in the applicable Order Form, Supplier may invoice, and Customer will pay, for such excess actual MAU.

Unused MAU commitments do not carry over to the next month.

Additional SaaS Service Conditions

The use of passkeys typically depends on platform features. OneSpan cannot guarantee that platform features are present or remain present.
Notwithstanding anything to the contrary:

- DigipassONE Authenticate has not completed a SOC2 Type II assessment,
- some portions of the DigipassONE Authenticate components (e.g. firewalls and "nginx") generate logs in which some customer Data (such as IP addresses and authentication times) is not segregated,
- OneSpan DigipassONE Authenticate supports FIDO passkeys where supported by the User's platform. Actual functionality depends on the capabilities of the operating system and browser in use (such as Android, iOS, Windows, Chrome, Edge, or Safari), as well as any optional user-installed components (including password managers). OneSpan does not control and is not responsible for (a) the default features or limitations of third-party platforms or browsers, or (b) individual user configurations or installed components. As a result, OneSpan cannot guarantee compatibility or availability of FIDO passkey functionality across all user environments.
- The Availability of DigipassONE Authenticate is 99.95% measured on a monthly basis.
- Supplier may, during the Term, place the Data in a backup location within the System.
- Upon Customer's request, and subject to applicable fees, Supplier may extract backed up Data from the System and transfer and retain such Data to a Customer selected backup location, as set forth in the applicable Order Document.
- DigipassONE Authenticate contains Third Party Components. The list of Third-Party Components that process Personal Data for DigipassONE Authenticate can be viewed in the "OneSpan

Subprocessor" list available at www.onespan.com/privacy-center. For business continuity purposes, Supplier may alternate between Third Party Component providers at any time without notice to you. Third Party Component providers may mandate that additional terms are incorporated into this Contract. Those terms are available for review at https://www.onespan.com/third-party-terms and are hereby incorporated.

- Customers whose Order Documents specify "DigipassONE Authenticate SaaS: with OCA" are purchasing DigipassONE Authenticate bundled with OneSpan Cloud Authentication ("OCA"). Customers whose Order Documents specify "DigipassONE Authenticate – Passkey Edition SaaS: without OCA" are purchasing DigipassONE Authenticate – Passkey Edition as a standalone authentication solution and do not receive the OCA SaaS Service. The OCA SaaS Service Description can be reviewed below.

DigipassONE Verify

DigipassONE Verify is OneSpan's digital credential pillar that provides a single, standards-based integration layer that lets organizations issue and verify cryptographically signed verifiable digital credentials from digital identity wallets such as EUDI Wallets across onboarding, authentication, and transaction flows, providing an alternative to document-and-selfie identity proofing.

DigipassONE Verify provides customers with two different environments to support their development, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.
Production:

- Production usage of the current version of DigipassONE Verify
- Subject to the Service Levels detailed below

Staging:

- Integration, development and testing of the current version of DigipassONE Verify
- Not subject to the Service Levels, security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Staging environment

Pricing

DigipassONE Verify is sold based upon the committed number of Monthly Active Users. **"Monthly Active User"** or **"MAU"** means, for any calendar month, each individual, entity, or account that: (a) is issued a credential, or is authenticated in connection with, DigipassONE Verify; or (b) otherwise directly or indirectly accesses or uses a DigipassONE Verify, including access or use through Customer's services, applications, or software, whether by API call or otherwise.

The actual average number of MAUs during each twelve (12) month period during each annual term, shall be calculated at the end of such twelve (12) month period, and shall be calculated to be the average MAUs during such twelve (12) month period. If the actual average number of MAU in any year exceeds the maximum MAU indicated in the applicable Order Form, Supplier may invoice, and Customer will pay, for such excess actual MAU.

Unused MAU commitments do not carry over to the next month.

Additional SaaS Service Conditions

The use of credentials typically depends on platform features. OneSpan cannot guarantee that platform features are present or remain present.
Notwithstanding anything to the contrary:

- DigipassONE Verify has not completed a SOC2 Type II assessment,

- some portions of the DigipassONE Verify components (e.g. firewalls and "nginx") generate logs in which some customer Data (such as IP addresses and authentication times) is not segregated,
- OneSpan DigipassONE Verify supports digital wallets where supported by the User's platform. Actual functionality depends on the capabilities of the operating system and browser in use (such as Android, iOS, Windows, Chrome, Edge, or Safari), as well as any optional user-installed components (including credential managers or wallet applications). OneSpan does not control and is not responsible for (a) the default features or limitations of third-party platforms or browsers, or (b) individual user configurations or installed components. As a result, OneSpan cannot guarantee compatibility or availability of wallet functionality across all user environments.
- The Availability of DigipassONE Verify is 99.95% measured on a monthly basis.
- Supplier may, during the Term, place the Data in a backup location within the System.
- Upon Customer's request, and subject to applicable fees, Supplier may extract backed up Data from the System and transfer and retain such Data to a Customer selected backup location, as set forth in the applicable Order Document.
- DigipassONE Verify contains Third Party Components. The list of Third-Party Components that process Personal Data for DigipassONE Verify can be viewed in the "OneSpan Subprocessor" list available at www.onespan.com/privacy-center. For business continuity purposes, Supplier may alternate between Third Party Component providers at any time without notice to you. Third Party Component providers may mandate that additional terms are incorporated into this Contract. Those terms are available for review at https://www.onespan.com/third-party-terms and are hereby incorporated.

DigipassONE Insights

DigipassONE Insights is an advanced analytics add-on for DigipassONE Authenticate or DigipassONE Verify, designed to make authentication performance measurable, actionable, and continuously improvable. It empowers organizations to optimize user experience and security by turning raw authentication data into meaningful insights.

DigipassONE Insights is an add-on to DigipassONE Authenticate and DigipassONE Verify. It is not sold independently and requires an active subscription to one of those products.
DigipassONE Insights usage is included within the Customer's DigipassONE Authenticate or DigipassONE Verify MAU commitment on a one-to-one basis. No separate MAU entitlement applies.

If Customer elects to use DigipassONE Insights, Customer grants Supplier a limited, non-exclusive right to process Customer Data to (a) compute authentication performance metrics for Customer, including average sign-in time, and (b) generate aggregated, anonymized benchmarking information. Benchmarking outputs will not identify Customer or its end users.

DigipassONE Protect

Definitions

"Analysis Data" means anonymized, aggregated (where appropriate), or otherwise de-identified Data. Analysis Data is part of the SaaS Service.

"**AI Feature**" means any functionality of DigipassONE Protect that utilizes or integrates artificial intelligence or machine learning technologies, including generative models, artificial intelligence algorithms, or machine learning models. AI Features are part of the SaaS Service.

"Derived Intelligence" means threat intelligence, security intelligence, attack indicators, detection patterns, false-positive analysis, device intelligence, environmental intelligence, model learnings, trends, benchmarks, analytics methodologies, and any other information, knowledge, insights, patterns,

correlations, or learnings generated, derived, or learned from Analysis Data or use of DigipassONE Protect. Derived Intelligence is part of the SaaS Service.

"Endpoint" means a distinct instance of a Protected Application installed on a device that is authorized to communicate with the DigipassONE Protect service. Each installation of the Protected Application on a device constitutes a separate Endpoint. If the same Protected Application is installed more than once (including reinstallation), or if different Protected Applications are installed on the same device, each installation is treated as a separate Endpoint.

An Endpoint is counted from the time the Protected Application is installed on the device and the associated authorization is issued by the DigipassONE Protect technology. It remains countable for so long as the associated authorization issued remains valid. Such authorization is subject to periodic renewal and expiration as part of its normal operation. As a result, Endpoint counts may increase or decrease over time, including where: (a) an installation is removed from a device but remains countable until the associated authorization expires, or (b) a subsequent installation on the same device creates a new Endpoint before a prior authorization has expired.

"Excess Limit Fee" means the price per Endpoint listed for the Product on the applicable Order Document that is charged for Endpoints in excess of the Annual Commitment.

"Next Gen App Shielding Intellectual Property" means the DigipassONE Protect Product including its AI Features, Analysis Data, and Derived Intelligence and any derivations, improvements or enhancements, and all intellectual property rights therein.

"Protected Application" means a mobile application that Customer has integrated with the DigipassONE Protect technology.

"Training" means the use of Analysis Data or other information to develop, train, retrain, fine-tune, adapt, test, validate, evaluate, improve, optimize, or otherwise enhance the AI Features.

Product Information

DigipassONE Protect is a mobile application security platform that provides in-app protection, active hardening, threat intelligence monitoring, server-side attestation, and backend integration capabilities designed to help protect Customer's mobile applications against tampering, reverse engineering, and runtime threats. DigipassONE Protect is comprised of the following modules, each of which is sold separately and may be combined based on Customer's requirements:

In-App Protection

- **No Code with Active Hardening SaaS**: In-app protection applied without any code changes, including Active Hardening SaaS. Customer receives access to the no code shielding portal. In addition to the SaaS Service, a mobile SDK component is included.
- **Master Code with Active Hardening SaaS**: In-app protection delivered as an SDK integration with a complete feature set, including Active Hardening SaaS Service. Deliverable is SDK delivery. In addition to the SaaS Service, a mobile SDK component is included.
- **Step Code with Active Hardening SaaS**: In-app protection delivered as an SDK integration with a limited feature set, including Active Hardening SaaS Service. Deliverable is SDK delivery. In addition to the SaaS Service, a mobile SDK component is included.

Threat Intelligence Monitoring

- **TraceBoard SaaS – Core**: Core web console for monitoring mobile app threats, app activity, and alerts. Customer receives access to the TraceBoard web portal.
- **TraceBoard SaaS – Premium**: Premium web console for monitoring mobile app threats, app activity, and alerts, with the ability to take remote action on compromised app instances. Customer receives access to the TraceBoard web portal.
- Notwithstanding anything to the contrary, TraceBoard is only provided from the European Union.

Server-Side Attestation & API

- **DeviceAttest SaaS**: Server-side attestation that automatically validates device integrity and enforces configurable rules based on predefined policies, with no coding required. Customer receives access to the DeviceAttest web portal.

- **BuildAPI REST SaaS**: REST API for integrating threat intelligence, remote actions, and cryptographic key management directly into Customer's backend applications.
- **BuildAPI Streaming SaaS**: Streaming API for integrating threat intelligence directly into Customer's SIEM or fraud engine.

DigipassONE Protect provides customers with two environments to support their needs. The environment and its characteristics may change at Supplier's discretion.
Production:

- Production usage of the current version of DigipassONE Protect
- Subject to the Service Levels

Testing:

- Integration, development and testing of the current version of NGAS;
- Not subject to the Service Levels, security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Testing environment.

Pricing

DigipassONE Protect is priced based upon the number of annual Endpoint committed in the applicable Order Document ("**Annual Commitment**"). Customer may exceed the Annual Commitment, but then must pay for Endpoints in excess of the Annual Commitment. Endpoints in excess of the Annual Commitment will be charged Excess Limit Fees. Excess Limit Fees are invoiced at the end of each contract year (annual true-up); however, Supplier may elect to aggregate Excess Limit Fees over more than one period prior to invoicing for administrative convenience. Unused Endpoint commitments do not carry over to the next year.

Additional SaaS Service Conditions

- Notwithstanding anything to the contrary, DigipassONE Protect does not have a SOC 2 assessment, but rather it is ISO 27001 certified.
- Notwithstanding anything to the contrary, Customer Data is automatically stored in the data center that Supplier deems optimal, unless otherwise specified in the applicable Order Document; provided that such data centers are located solely within the European Union or the United States. Customer may specify either of these regions in the Order Document, and no other data center locations are available for this Service.
- DigipassONE Protect modules include both a mobile SDK and the associated SaaS Service.
- The AI Features incorporated into the DigipassONE Protect Product analyze telemetry, user device information, Customer application event data, and related operational information to identify patterns, improve detection accuracy, reduce false positives, and generate dashboards, analytics, insights, recommendations, and reporting regarding application security and performance. Customer acknowledges and agrees that use of Analysis Data to operate, maintain, improve, validate, test and enhance AI Features, including through Training activities, is an essential component of DigipassONE Protect and is necessary for OneSpan to provide the Product. Accordingly, Supplier may use Analysis Data for Training. Such use of Analysis Data cannot be disabled or opted out of while Customer uses DigipassONE Protect. Supplier has no obligation to delete existing Analysis Data or Derived Intelligence upon expiration or termination of the Contract.
- Supplier may use and disclose information derived from Data, Analysis Data, Derived Intelligence, or operation of the DigipassONE Protect Product, provided such information does not identify Customer or any individual as the source.
- Customer retains all right, title, and interest in and to Data. As between the parties, Supplier owns and retains all right, title, and interest in and to Next Gen App Shielding Intellectual Property.
- Subject to the Contract, Customer may access, use, reproduce, and distribute Derived Intelligence generated from Data solely for Customer's internal business purposes and only in connection with its authorized use of DigipassONE Protect.
- DigipassONE Protect contains Third Party Components. The list of Third Party Components that are utilized to provide DigipassONE Protect can be viewed in the "OneSpan Subprocessor" list available at

www.onespan.com/privacy-center. For business continuity purposes, Supplier may alternate between Third Party Component providers at any time without notice to you. Third Party Component providers may mandate that additional terms are incorporated into this Contract. Those terms are available for review at https://www.onespan.com/third-party-terms and are hereby incorporated.

OneSpan Cloud Authentication

Definitions

"Annual Commitment" means the number of annual Users committed in the applicable Order Document.
"Excess Limit Fee" means the price per User or per Transaction listed for the Product on the applicable Order Document that is charged for use in excess of the Annual or Monthly Commitment.
"Monthly Commitment" means the number of monthly Transactions committed in the applicable Order Document.
"**Transaction**" means an individual API request for User authentication or signature validation.

Product Information

OneSpan Cloud Authentication ("**OCA**") leverages OneSpan multi-factor authentication to provide both User authentication and signature validation. OCA provides a real-time validation of a OneSpan authentication credential used for either User authentication or signature validation through a REST API interface. Several features and options are available through OCA including, but not limited to (as further described in the OCA Documentation):

- REST API to perform User authentication and signature validation
- REST API to perform device and User administration
- Centralised management interface for Users and authenticators
- Mobile authentication capabilities
- Secure User mobile onboarding and activation

OCA provides customers with three different environments to support their development, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.

Production:
- Production usage of the current version of OCA
- Subject to the Service Levels

Staging:
- Integration, development and testing of the current version of OCA
- Not subject to the Service Levels and security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Testing environment

Sandbox:
- Development access to functionality planned in the next upcoming major release and regression testing of integrations before the new major release is deployed in production
- Not subject to the Service Levels and security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Development environment

Pricing

- Transaction Based Pricing
  - Transaction Based Pricing for OCA is based upon the Monthly Commitment.
  - Excess Limit Fees are invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one quarter prior to invoicing for administrative convenience.
  - Unused Transactions do not carry over to the next month.
- User Based Pricing
  - User Based Pricing for OCA is based upon the Annual Commitment of the maximum number of Users registered in the SaaS Service during the applicable year.
  - Users processed in excess of the Annual Commitment will be charged Excess Limit Fees. Excess Limit Fees are invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one quarter prior to invoicing for administrative convenience.
  - Unused User commitments do not carry over to the next year.

Additional SaaS Service Conditions

- Supplier may, during the Term, place the Data in a backup location within the System.

- Upon Customer's request, and subject to applicable fees, Supplier may extract backed up Data from the System and transfer and retain such Data to a Customer selected backup location, as set forth in the applicable Order Document.
- OCA contains Third Party Components. The list of Third Party Components that are utilized to provide OCA can be viewed in the "OneSpan Subprocessor" list available at www.onespan.com/privacy-center. For business continuity purposes, Supplier may alternate between Third Party Component providers at any time without notice to you. Third Party Component providers may mandate that additional terms are incorporated into this Contract. Those terms are available for review at https://www.onespan.com/third-party-terms and are hereby incorporated.

Intelligent Adaptive Authentication

Definitions

"Annual Commitment" means the number of annual Users committed in the applicable Order Document.
"Customer Application" means a web-based, offline, mobile or other software application functionality that is provided by Customer or a third party and interoperates with the SaaS Service.
"Excess Limit Fee" means the price per User or Transaction listed for the Product on the applicable Order Document that is charged for use in excess of the Annual or Monthly Commitment.
"Monthly Commitment" means the number of monthly Transactions committed in the applicable Order Document.
"Session" begins upon a User's login to a Customer Application and terminates i) when the Customer Application times out; or 2) the User logs out of the Customer Application. A User's return to the Customer Application after an expired Session constitutes an additional Session.
"**Transaction**" means a unique Session.

Product Information

Intelligent Adaptive Authentication ("**IAA**") leverages multi-factor authentication, machine learning-powered risk analytics, and application security to help reduce account takeover fraud. IAA provides real-time analysis of User, device and Transaction data, resulting in a risk score that triggers an automated security workflow in the Customer Application which applies the security workflow for each Transaction. Several features and options are available through IAA which may include (as further described in the IAA Documentation):

- Account takeover fraud detection/prevention
- New account fraud detection/prevention
- Real-time detection of an untrusted device
- Real-time analysis of device risk
- Real-time, continuous monitoring of transaction risks
- Identify new fraud scenarios and suspicious account payees
- Policy configuration to support low, medium and high risk actions
- Case management to create, investigate and update suspicious activity
- Role-based access control via a centralized management console
- Interactive fraud relationship visualization
- Reporting
- Web based API (REST Interface)
- Authentication orchestration
- Mobile authentication capabilities
- Secure User mobile onboarding and activation

IAA provides customers with three different environments to support their development, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.

Production:

- Production usage of the current version of IAA
- Subject to the Service Levels

Staging:

- Integration development and testing of the current version of IAA
- Not subject to the Service Levels, security requirements or safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Testing environment

Sandbox:

- Development access to functionality planned in the next upcoming major release and regression testing of integrations before the new major release is deployed in production

- Not subject to the Service Levels, security requirements, or safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Development environment

Pricing

(a) Transaction Based Pricing
- Transaction Based Pricing for IAA is based upon the Monthly Commitment of Transactions.
- Transactions processed in excess of the Monthly Commitment will be charged Excess Limit Fees. Excess Limit Fees are invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one quarter prior to invoicing for administrative convenience.
- Unused Transactions do not carry over to the next month.

(b) User Based Pricing
- User Based Pricing for IAA is based on the Annual Commitment of the maximum number of Users registered in the SaaS Service during the applicable year.
- Users processed in excess of the Annual Commitment will be charged Excess Limit Fees. Excess Limit Fees are invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one quarter prior to invoicing for administrative convenience.
- Unused User commitments do not carry over to the next year.

Additional SaaS Service Conditions

Supplier may, during the Term, place the Data in a backup location within the System. Upon Customer's request, and subject to applicable fees, Supplier may extract backed up Data from the System and transfer and retain such Data to a Customer selected backup location, as set forth in an applicable Order Document.

IAA contains Third Party Components. The list of Third Party Components that are utilized to provide IAA can be viewed in the "OneSpan Subprocessor" list available at www.onespan.com/privacy-center. For business continuity purposes, Supplier may alternate between Third Party Component providers at any time without notice to you. Third Party Component providers may mandate that additional terms are incorporated into this Contract. Those terms are available for review at https://www.onespan.com/third-party-terms and are hereby incorporated.

Threat Fabric Mobile Threat Intelligence

Definitions

"**Annual Commitment**" means the number of annual Named Users committed in the applicable Order Document

"**Excess Limit Fee**" means the price per Named User listed for the Product on the applicable Order Document that is charged for use in excess of the Annual Commitment.

"**Content**" means all information, reports, bulletins, data, indicators, malware intelligence, metadata, enrichment, and other materials made available by Supplier to the Named Users via the Portal. Content does not constitute security advice, guarantee protection, or ensure compliance with any regulatory standards

"**Named Users**" means the employees designated by Customer from time to time who are authorized to access the Portal on a individual-Named User basis, each with unique credentials. Customer may replace or reassign Named Users at its discretion, provided that the total number of Named Users does not exceed the Named User Annual Commitment

"**Portal**" means the hosted MTI portal made available through the internet, through which Named Users access the Content.

Product Information

Threat Fabric Mobile Threat Intelligence ("MTI") provides Customer access to a software as a service curated mobile threat intelligence (including reports, indicators, alerts, and analyses) regarding mobile malware and related fraud strategy and customer awareness campaigns for internal informational purposes, available via the Portal.

MTI allows a customer to:

- share Content internally with employees and contractors on a need-to-know basis for informational purposes;
- summarize the Content for internal use; and
- include limited extracts of the Content for internal security purposes.

Pricing

MTI is priced based on the number of individual Named Users set forth on the applicable Order Document.

Named User Based Pricing

- Named User based pricing for MTI is based upon the Annual Commitment of the maximum number of Named Users during the applicable year.
- Named Users processed in excess of the Annual Commitment will be charged Excess Limit Fees. Excess Limit Fees are invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one quarter prior to invoicing for administrative convenience.
- Unused Named User commitments do not carry over to the next year.

Additional Restrictions on Use

In addition to the restrictions set forth in the Service Use Guidelines, Customer will not (and will not permit any third party to):

- remove proprietary notices or attribution.
- share Named User credentials
- use the Content to develop or train any machine learning or AI models

Threat Fabric Fraud Risk Suite SaaS

Definitions

"Annual Commitment" means the number of annual Users committed in the applicable Order Document.
"Excess Limit Fee" means the price per User listed for the Product on the applicable Order Document that is charged for use in excess of the Annual Commitment.
"User" means any individual end-user of the Customer who is authorized to access and use any Customer mobile application or web application into which the Supplier's solution is implemented, regardless of whether such end-user undertakes any transaction within the application. A User includes any individual who has the ability to log in to the protected application during the Subscription Term, and excludes only those individuals who do not have access rights to such application**.**

Product Information

Threat Fabric Fraud Risk Suite ("FRS") includes risk indicators shared in real-time with Customer's in-house or third-party risk engine to enable authentication, application fraud or payment fraud monitoring. FRS has the following modules:

- **Malware Risk** detects presence of known mobile malware on a device during mobile banking sessions for the purposes of preventing fraud
- **FRS Device Risk** is an extension of FRS Malware Risk to detect device-level fraud indicators, such as remote access tools, live calls, screen sharing, emulators, jailbroken devices, rooted devices and other device insecurities from mobile and web sessions. Includes all FRS Malware Risk detections.
- **FRS Behavior Risk** is An extension of FRS Device Risk to detect user-level anomalies in digital behavior (e.g. keystroke, navigation, mouse movements, touch, rotation, motion) that are indicative of social engineering or unauthorized user access. Includes all FRS Device Risk detections and FRS Malware Risk.

Pricing

User Based Pricing

- User Based Pricing for FRS is based upon the Annual Commitment of the maximum number of Users during the applicable year.
- Users processed in excess of the Annual Commitment will be charged Excess Limit Fees. Excess Limit Fees are invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one quarter prior to invoicing for administrative convenience.
- Unused User commitments do not carry over to the next year.

Digipass Management Portal

Definitions

"**Portal**" means the hosted Digipass Management Portal made available through the internet, through which Users can manage their Digipass Hardware Devices.

Product Information

The Digipass Management Portal is an online administrative service that enables Customer to manage and oversee the distribution of DIGIPASS Hardware Devices (the "**Device(s)**") by OneSpan through a centralized web-based interface.

The Portal is designed as an operational management tool and does not perform authentication, cryptographic operations, or identity verification. It does provide the following features:

- **User-to-Device Assignment**
  Track DIGIPASS Devices to Users
- **Inventory Management**
  View inventory levels, allocation status, and historical tracking
- **Order and Fulfillment Visibility**
  Track orders, shipments, and fulfillment progress (where available)
- **Reporting and Monitoring**
  Access dashboards showing Device shipment, Device consumption, and Device mix that has been shipped
- **Role-Based Access**
  Control administrative permissions and access rights.

The Portal provides Customer with two different environments to support their development, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.

Production:

- Production usage of the current version of the Portal
- Subject to the Service Levels

Demo:

- Integration development and testing of the current version of the Portal
- Development access to functionality planned in the next upcoming major release and regression testing of integrations before the new major release is deployed in production
- Not subject to the Service Levels, security requirements, or safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Demo environment

Pricing

The Portal pricing is a flat annual fee that is priced based on the annual Device shipment capacity tier set forth on the applicable Order Document.

OneSpan Sign

OneSpan Sign is a software platform for creating and managing the execution of digital transactions with electronic signing and delivery of Documents. Several features and options are available through OneSpan Sign. Refer to the Documentation available for review on OneSpan's Community Portal at https://community.onespan.com for more details. Other, optional functionalities that Customer may choose to add-on to existing product capacities ("**Components**") are available for purchase as detailed in this SaaS Service Description.

Definitions

"Completed Transactions" means any Transaction listed as "Completed" or "Archived" on the OneSpan Sign application dashboard.
"Document" means a single file representing a form, document or other record, not to exceed 10 megabytes of Data (the "**Document Limit**"), and capable of being viewed, electronically signed, sent or received or stored through the SaaS Service. Any Documents in excess of the Document Limit will create one or more additional new Documents
"Incomplete Transaction" means any Transaction that is not listed as a Completed Transaction on the OneSpan Sign application dashboard.
"**Named User**" means Customer's employee or agent who has been given login access credentials to the Account by the Administrator for purpose of accessing the SaaS Service. A Named User must be identified by a unique email address and user name, and two or more persons may not use the OneSpan Sign Service as the same Named User.
"Recorded Session" means a recording of the Virtual Room session with audio/visual experience.
"Session Participant" is any person joining a Virtual Room session, including but not limited to signers and hosts.
"Session Participant Unit ("SPU") is equivalent to thirty (30) minutes per Session Participant in an active Virtual Room session.
"**Transaction**" means a container or package created or sent by a User associated with a unique transaction identifier and comprised of a maximum of ten (10) Documents (the "**Transaction Limit**") created or sent through the SaaS Service (includes both Incomplete and Complete Transactions). Any Documents in excess of the Transaction Limit will create one or more additional new Transactions.
"Virtual Room" combines electronic signature, video-conferencing, co-browsing, and recording capabilities into a single solution .

Product Information

OneSpan Sign includes the following (as further defined in the OneSpan Sign Documentation) as part of the subscription fee:

- Web-based e-signing process that provides options for the presentation and review of Documents, methods of signature capture and user authentication, data capture and form fields.
- Workflows, reminders and notifications, attachments and e-delivery of the Documents to Users.
- Transaction management features for preparing and sending documents manually through the user interface or using transaction templates, and the ability to monitor and manage documents that are in progress or completed.
- Electronically signed Documents in PDF format with each e-signature digitally signed for comprehensive security and detection of any Document changes along with an embedded audit trail.
- An Evidence Summary Report is provided and both the electronic evidence and summary are protected by digital signing.
- A REST API along with Java and .Net SDKs to allow integrating third party and custom applications with the SaaS Service.
- Support for native mobile applications and pre-built connectors to applications such as Salesforce and Microsoft Dynamics.

- If Customer chooses to deploy it, the SaaS Service offers a geolocation feature that allows for disclosure of a signatories' geolocation on the Transaction evidence summary report. Geolocation accuracy is dependent upon the browser and device used and Supplier is not responsible its accuracy.

OneSpan Sign provides customers with two different environments to support their development, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.

Production:

- Production usage of the current version of OneSpan Sign;
- Documents are not watermarked;
- Subject to the Service Levels.

Sandbox (Staging):

- Integration, development and testing of the current version of OneSpan Sign;
- Documents are watermarked to make them unsuitable for production usage;
- Not subject to the Service Levels and security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Sandbox environment.

Pricing

Enterprise:

- **Pricing**: OneSpan Sign Enterprise is priced based upon the number of annual Transactions committed in the applicable Order Document("**Annual Commitment**"). Customer may exceed the Annual Commitment, but then must pay for Transactions or Documents in excess of the Annual Commitment.
- **Incomplete Transactions**: Incomplete Transactions may be retained on the System up to one-hundred and twenty (120) days from the Transaction creation date, after which such Incomplete Transactions will be permanently deleted from the System.
- **Unlimited Annual Commitments:** Notwithstanding anything to the contrary, unlimited Transactions are non-transferable and may only be initiated by a Named User within Customer's or its authorized Affiliates' organization (i.e. Customer cannot share it's Account with third parties).

Professional:

- **Pricing**: OneSpan Sign Professional is priced based on the number of individual Named Users set forth on the applicable Order Document. Professional Plans are limited to one thousand (1,000) Transactions per Named User per annual term, usage in excess of which will result in an additional Named User license fee.
- **Incomplete Transactions**: Incomplete Transactions may be retained on the System up to one-hundred and twenty (120) days from the Transaction creation date, after which such Incomplete Transactions will be permanently deleted from the System.

Optional OneSpan Sign Components

*OneSpan Sign Virtual Room ("**Virtual Room**"):*

- Virtual Room is priced based on the number of annual Session Participant Units committed in the applicable Order Document (the "**Virtual Room Annual Commitment**"). Customer may exceed the Virtual Room Annual Commitment, but then must pay for Session Participant Units in excess of the Virtual Room Annual Commitment.
- Customer must download a Recorded Session within seven (7) days of the date the recording is available for download, after which time Supplier will delete the Recorded Session.
- Customer receives 400 free Sandbox (Staging) Session Participant Units (SPU) per year. Use in excess of this limit will be charged Session Participant Units.
- Supplier recommends Virtual Room Users maintain Internet speed of 3 Mbps or higher for optimal Product performance.
- A OneSpan Sign subscription is required for Virtual Room.

Communication Hub

- for use with OneSpan Sign

- see Communication Hub Service Description.

OneSpan Identity Verification

- for use with OneSpan Sign
- see OneSpan Identity Verification Service Description.

OneSpan Integration Platform

- OneSpan Integration Platform allows you to connect OneSpan Sign to your desired business application.
- For paid OneSpan Integration Platform business applications, OneSpan Integration Platform is priced on the number of annual Transactions committed for processing through the Integration Platform (the "**Integrated Platform Annual Commitment**"). Customer may exceed the Integrated Platform Annual Commitment for an additional fee. Please note some OneSpan Integration Platform business applications are supported free of charge. Please contact your sales representative for details.
- A OneSpan Sign subscription is required for Integration Platform.
- The Integration Platform operates with or uses APIs and/or other services operated or provided by third parties. Customer may use a third party's applications, software, interfaces, APIs, products, services or websites that interoperate with the Integration Platform (collectively, "**Third-Party Applications**"). Customer is responsible for acquiring the license and rights to use the Third-Party Applications and accepting and complying with the applicable terms and conditions and privacy policy of the Third-Party Applications. Notwithstanding anything to the contrary: (a) Customer is solely responsible for its use of such Third-Party Applications and any data loss or other losses it may suffer as a result of using such Third-Party Applications, (b) Supplier does not warrant or support any Third-Party Applications or control the privacy practices of any Third-Party Application to which data may be sent or from which data may be retrieved, whether or not they are recommended by Supplier or designated by Supplier as preferred, certified or otherwise, and shall have no responsibility, liability or indemnification obligations for any claims, losses or damages arising out of or in connection with Customer's use of any Third-Party Applications, (c) Supplier does not guarantee compatibility with any Third-Party Application, and (d) Supplier shall not be responsible for any changes or new developments in Third-Party Applications which may interrupt Customer's use or interaction with the Integration Platform.

OneSpan Sign SMS Notifications

- SMS Notifications provide senders with the ability to send transaction notifications directly to signers through text SMS, in addition to the traditional email notification option.
- OneSpan SMS Notifications are billed per OneSpan Sign Transaction that uses this feature. Customer may exceed the SMS Notification Annual Commitment but then must pay for Transactions that use SMS Notification in excess of the Annual Commitment.
- To comply with the Telephone Consumer Protection Act (TCPA) and other applicable laws governing SMS communications, Customer must ensure that each SMS recipient provides express consent to receive SMS messages prior to initiating any transaction that includes SMS delivery. Such consent must be obtained directly from the SMS recipient before sending any SMS message.
- If you elect to send or receive SMS messages through OneSpan Sign, you represent and warrant that you are the subscriber of the mobile number provided or have the subscriber's authorization to receive SMS messages at that number. Standard message and data rates may apply as determined by the mobile service provider. Supplier does not control mobile service provider networks and is not responsible for any issues arising from such services, including, without limitation, delivery failures, transmission delays, or service changes impacting SMS messaging when using the Service.
- Each OneSpan Sign Transaction is limited to 50 SMS notifications. Once this limit is reached, an alert will appear in the user interface, and no further SMS messages can be sent for that Transaction.

OneSpan Sign Hold Your Own Key:

OneSpan Sign Enterprise Customers may participate in the Hold Your Own Key program subject to the Contract and the following terms:

- "Hold Your Own Key" or "HYOK" allows the Customer to use a Private Customer Master Key with the SaaS Service. "Private Customer Master Key" means an encryption key unique to the Customer provided by Supplier

to encrypt data stored at rest. Supplier has no access to Private Customer Master Keys without Customer's permission.

- Pricing for Hold Your Own Key is on per configured self-managed key management service ("KMS") basis. For example, if Customer has twenty accounts, ten of which are in the US, and ten of which are in Canada, but they all point to the same HYOK KMS, then only one (1) HYOK fee is charged. However, if the same Customer has the US accounts pointing to one HYOK KMS and the Canadian accounts pointing to another, then the Customer will be charged two (2) HYOK fees.
- At Customer's option, and not automatically included in the SaaS Service, Customer may elect to use a Private Customer Master Key for encryption of data at rest in OneSpan's database which can consist of Documents, recorded evidence of the signing process, form fields entered by signers, passwords (hashed), signer authentication information, and ancillary documents. One (1) Private Customer Master Key is provided to Customer free of charge for Customers that purchase more than 100,000 Transactions annually. Customer must pay a fee for each additional key used annually. Customer may set up sub Accounts using the same Private Customer Master Key without additional charge. Customers that purchase less than 100,000 Transactions annually must pay a fee for each key used annually. Private Customer Master Key is not available for Professional Plans.
- As a condition of the HYOK program, Customer agrees that notwithstanding anything to the contrary in the Contract:
- CUSTOMER IS LIABLE TO AND SHALL NOT SEEK RECOVERY FROM SUPPLIER FOR ANY AND ALL CLAIMS, ACTIONS OR PROCEEDINGS (INCLUDING MISSED SERVICE LEVEL COMMITMENTS) BASED ON OR OTHERWISE ARISING OUT OF OR IN CONNECTION WITH Private Customer Master Keys UNDER THE HOLD YOUR OWN KEY PROGRAM, WITHOUT LIMITATION. Customer agrees to indemnify and defend Supplier and its Affiliates, and their respective officers, directors, employees and agents from and against any claim, suit, proceeding, or action and pay any liabilities, damages and costs, including reasonable attorney's fees, arising out of or in connection with Customer's provision and use of Private Customer Master Keys.

Additional SaaS Service Conditions

- Non-prepaid fees such as fees for excess usage and excess storage are invoiced quarterly in arrears; however, Supplier may elect to aggregate these fees over more than one quarter prior to invoicing for administrative convenience.
- A Maximum of 100 signatories per Transaction are allowed, signatories in excess of this amount create an additional Transaction.
- Unused annual Transactions, Documents, Session Participant Units and participant counts may not be carried over to the next annual term.
- OneSpan Sign contains Third Party Components. The list of Third Party Components that are utilized to provide OneSpan Sign can be viewed in the "OneSpan Subprocessor" list available at www.onespan.com/privacy-center. For business continuity purposes, Supplier may alternate between Third Party Component providers at any time without notice to you. Third Party Component providers may mandate that additional terms are incorporated into this Contract. Those terms are available for review at https://www.onespan.com/third-party-terms and are hereby incorporated.
- To the extent Supplier makes available any artificial intelligence, machine learning, generative AI, or AI-assisted functionality in connection with the OneSpan Sign Service including its Virtual Room, Commination Hub and OneSpan Identity Verification components, Customer's use of such functionality shall be subject to the OneSpan AI Terms available at www.onespan.com/da-ai-terms, as may be updated from time to time, which are hereby incorporated into the Contract by reference.

OneSpan Notary

Definitions:

"Completed OneSpan Sign Transactions" means any e-signature Transaction listed as "Completed" or "Archived" on the OneSpan Sign application dashboard.

"Document" means a single e-signature file representing a form, document or other record, not to exceed 10 megabytes of Data (the "**Document Limit**"), and capable of being viewed, electronically signed, sent or received or stored through OneSpan Sign. Any Documents in excess of the Document Limit will create one or more additional new Documents

"Incomplete OneSpan Sign Transaction" means any e-signature Transaction that is not listed as a Completed Transaction on the OneSpan Sign application dashboard.

"IPEN" or **"In-Person Electronic Notarization"** is the process of a State approved Notarization that occurs in-person; however, the documents are signed and notarized electronically using electronic signature electronic notarial journals and other record keeping processes

"**Notary**" means Customer's employee, contractor or agent who has been commissioned by a particular state, jurisdiction, or territory of the United States to perform in-person electronic notarizations or remote online notarial acts, who has the required certifications and training to perform IPENs or RONs, and who has been given login access credentials to OneSpan Notary by the Administrator for purpose of performing Remote Online Notarizations.

"Notarial Evidence" means the Recorded Session, OneSpan Sign Transaction, Notarial Journal and other electronic artifacts created during the Notary Transaction.

"**Notarial Journal**" means the record of notarial acts performed by the Notary as mandated by applicable law.

"**Notarization**" means the authorized notarial act performed by a Notary in compliance with applicable law.

"**OneSpan Notary**" means Supplier's IPEN and RON SaaS Service that allows Notaries to perform In-Person Electronic Notarizations and Remote Online Notarizations on the OneSpan Sign platform.

"**Participant**" means a person or company, internal or external to Customer, identified and invited by a Notary to participate in a Notary Transaction.

"Recorded Session" means a recording of the Notary Transaction with audio/visual experience.

"**Remote Online Notarization**" or "**RON**" is the process of a State approved Notarization that occurs remotely via the Internet using electronic signature, identity verification, virtual rooms, electronic notarial journals and other record keeping processes.

"**Notary Transaction**" and "**Notary – RON – Transaction**" means a session within the OneSpan Notary Service.

"**OneSpan Sign Transaction**" means an e-signature container or package created or sent by a User associated with a unique transaction identifier and comprised of a maximum of ten (10) Documents (the "**OneSpan Sign Transaction Limit**") created or sent through the OneSpan Sign Service (includes both Incomplete and Complete OneSpan Sign Transactions). Any Documents in excess of the OneSpan Sign Transaction Limit will create one or more additional new OneSpan Sign Transactions.

OneSpan Notary Product Information

The OneSpan Notary is a SaaS Service that enables commissioned Notaries employed by business entities to perform In-Person Electronic Notarizations and Remote Online Notarizations. OneSpan Notary includes the following (as further defined in the OneSpan Notary Documentation) as part of the subscription fee (some features may not be used in an IPEN session due to the nature of an IPEN):

- Web-based e-signing process that provides options for the presentation and review of Documents, methods of signature capture and user authentication, data capture and form fields.
- Workflows, reminders and notifications, attachments and e-delivery of the Documents to Participants.
- OneSpan Sign Transaction management features for preparing and sending Documents manually through the user interface or using OneSpan Sign Transaction templates, and the ability to monitor and manage Documents that are in progress or completed.

- Electronically signed Documents in PDF format with each e-signature digitally signed for comprehensive security and detection of any Document changes along with an embedded audit trail.
- An Evidence Summary Report is provided for the e-signature experience and both the electronic evidence and summary are protected by digital signing.
- Recorded Notary Transaction capabilities that combine e-signature, video-conferencing, co-browsing, and recording capabilities into a single solution.
- Identity verification capabilities that incorporate the components necessary to facilitate the automated verification of a Participant's identity see OneSpan Identity Verification for terms specific to this feature.
- Notarization capabilities including, but not limited to, Notary onboarding, the Notarial Journal, digital certificates, ability to upload notarial seal, and Participant authentication.

OneSpan Notary provides customers with two environments to support their integration, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.

Production:

- Production usage of the current version of OneSpan Notary;
- Documents are not watermarked;
- Subject to the Service Levels.

Sandbox (Staging):

- Integration, development and testing of the current version of OneSpan Notary;
- Documents are watermarked to make them unsuitable for production usage;
- Not subject to the Service Levels and security requirements and safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Sandbox environment.

Pricing

- Pricing is based upon either the annual number of IPEN or RON Notary Transactions ("Annual Commitment"). Customer may exceed the Annual Commitment, but then must pay for IPEN or RON Transactions in excess of the Annual Commitment. Each Notary may only have one (1) commission.
- Notaries may only create Notary Transactions, they may not use OneSpan Sign as a standalone product independent of a Notarization act. Customer may purchase OneSpan Sign as a standalone product separately.
- Notwithstanding anything to the contrary, unlimited Notary Transactions are non-transferable and may only be initiated by a Notary within Customer's or its authorized Affiliates' organization (i.e. Customer cannot share it's Account with third parties).
- Customer receives 300 free Sandbox (Staging) Notary Transactions per year. Use in excess of this limit will be charged as a Notary Transactions.

OneSpan Notary General Terms

The use of OneSpan Notary by Customer and its Users is subject to the following conditions:

a. Compliance with Law

Customer understands and agrees that:

i. not all jurisdictions allow In-Person Electronic Notarization and Remote Online Notarization and Customer is responsible for ensuring that its use and its Notaries' use of OneSpan Notary is authorized for its particular notarial acts.

ii. Customer is responsible for the method, adequacy, accuracy and compliance of the notarial act with applicable federal, state, and local regulations including, but not limited to, the applicable state's IPEN and RON laws. Customer will require that its Notaries perform all Notary Transactions in compliance with applicable law and is responsible for its Notaries failure to do so.

iii. when required by a particular jurisdictions applicable law, Supplier may share lists of active and non-active Notaries with the appropriate state agency.

iv. many jurisdictions require that Notarial Evidence is stored for a prescribed period of time (typically ten (10) years from Notarization). It is the Customer and/or Notary's responsibility to ensure that the Notarial Evidence is stored, maintained , and made accessible with the applicable jurisdiction(s) in compliance with applicable law.

v. notwithstanding anything to the contrary in the Contract, Supplier may disclose Data Breaches to applicable legal authorities when required to do so by law.

b. Commissions

Customer represents and warrants that:

i. its Notaries have a valid IPEN or RON commission in the applicable State and, where applicable, its Notary has notified the Secretary of State (or other state required authority) (including by providing a certification if required) of the Notary's intent to use OneSpan Notary to perform IPENs and/or RONs, as applicable.

ii. because Notaries are responsible for the accuracy of their commission in OneSpan Notary, Customer requires that: i) its Notaries update the commission information, as needed, and ii) if a Notary leaves Customer's employment or their commission expires, the Notary will de-register from OneSpan Notary as soon as possible. A Notary whose commission has expired in OneSpan Notary will be prevented from participating in Notary Transactions until they update their commission information in OneSpan Notary.

iii. it requires that its Notaries refrain from any act or omission that would be grounds for suspension or revocation of their commission.

iv. it will require Notaries located in jurisdictions that require exemplars to file an exemplar with the Secretary of State (or other state required authority) in compliance with applicable law

c. Digital Certificates

Supplier may supply digital certificates as part of OneSpan Notary; however, Customer is responsible for ensuring that its Notaries use digital certificates that meet the appropriate jurisdiction's digital certificate requirements. This means that in some cases the Customer or Notary may be required to purchase a digital certificate from the applicable State or trusted certificate authority. Supplier is not responsible for the cost or adequacy of digital certificates.

d. Electronic Signatures and Seals

Customer represents and warrants that:

i. the electronic signatures configured by the Notary for use with OneSpan Notary conforms to the Notary's name as shown on their commission.

ii. the Notary's seal conforms with the applicable state requirements and is embedded in and visible on all displays of the notarized Documents upon completion of the Notary Transaction.

e. Notarial Certificates

Customer understands and agrees that its Notaries are responsible for the accuracy and conformance of the notarial certificate with applicable State law.

f. Authentication

Customer may elect to deploy third party features within OneSpan Notary designed to verify the identity of the Participants ("**Identity Verification Measures**"). Supplier: (i) will apply only those Identity Verification Measures (if any) selected by Customer, (ii) makes no representations or warranties regarding the appropriateness of such Identity Verification Measures and whether Users have the necessary knowledge or ability to successfully meet such Identity Verification Measures, and (iii) assumes no liability or responsibility for the circumvention by any Participant or other person of any Identity Verification Measures.

g. Notary Transaction

i. Customer and its Notaries are responsible for the conduct Notary Transactions, including recording the required information for each notarial act.

ii. Customer must require that its Notaries terminate any Notary Transaction if at any time the Notary believes the communication technology is inadequate or the Session otherwise fails to meet applicable IPEN or RON laws.

iii. Customer and its Notaries are responsible for the accuracy of all IPEN and RON Participant information, including but not limited to, name, addresses, contact information, and identification details.

iv. Customer ensures (and will require that its Notaries ensure) that the Notaries and IPEN and RON Participants are physically located in the jurisdiction required by applicable law.

v. Customer's Notaries are responsible for confirming that the credentials presented by the IPEN or RON Participant or credible witness meet the applicable state requirements.

vi. For RON, Customer must download Notary Transaction recordings within seven (7) days of the Notary Transaction, after which the recording will be permanently deleted.

vii. Supplier recommends maintained Internet speeds of 3 Mbps or higher for optimal Product performance.

h. Notarial Journal

i. Customer and its Notaries are responsible for the accuracy and completeness of the Notarial Journal, and Supplier makes no representation or warranty that the Notarial Journal is sufficient to meet the Customer and Notaries' needs.

ii. Notwithstanding anything to the contrary, Supplier shall store the Notarial Journal until the earlier of (a) the expiration or termination of the Customer's OneSpan Notary subscription, or (b) the expiration of the Notary's commission (each a "**OneSpan Notary Termination Event**"). It is Customer's responsibility to download copies of the Notarial Journal prior to a OneSpan Notary Termination Event.

iii. Customer warrants that it has a process in place to (a) provide access to its Notaries' Notarial Journals if a Notary becomes incapable of performing their duties or their commission is terminated, is revoked or expires, and (b) to export Notarial Journal entries within thirty (30) days of a OneSpan Notary Termination Event.

iv. Customer consents (and will require that its Notaries and Participants consent) to Supplier sharing the Notarial Journal and IPEN or RON System documents with applicable State Secretaries of State or other reviewing government agencies in charge of notary commissions, when so required.

v. Certain jurisdictions may require that the Notary sign the Notarial Journal. OneSpan Notary allows Notaries to do this by signing the Notarial Journal using OneSpan Sign upon the completion of the Notary Transaction.

Additional SaaS Service Conditions

- Unless agreed otherwise in a signed amendment referencing this section, OneSpan Notary is only suitable for the United States market.
- Unused Notary Transactions may not be carried over to the next annual term.
- Non-prepaid fees such as fees for excess usage and excess storage are invoiced quarterly in arrears; however, Supplier may elect to aggregate these fees over more than one quarter prior to invoicing for administrative convenience.
- Incomplete OneSpan Sign Transactions may be retained on the System up to one-hundred and twenty (120) days from the OneSpan Sign Transaction creation date. Complete OneSpan Sign Transactions may be retained on the System up to one-hundred and twenty (120) days from the Transaction completion date. OneSpan Sign Transactions retained on the System beyond these time frames will either be deleted by Supplier or charged overage charges per month of retention per OneSpan Sign Transaction.
- For SMS one-time-passcode services, Customer is responsible for providing the correct phone numbers that are capable of receiving texts for applicable Participants. Customer warrants that it has obtained Participants' consent to receive SMS text messages.

- Supplier may, during the Term, place the Data in a backup location within the System. Upon Customer's request, and subject to applicable fees, Supplier may extract backed up Data from the System and transfer and retain such Data to a Customer selected backup location, as set forth in an applicable Order Document.
- Customer will notify Supplier immediately, but in no case less than forty-eight (48) hours after discovery, if they become aware of any loss, unauthorized use or compromise of the Notary's electronic seal, e-signature, or unique credentials to access the IPEN or RON System, and will require that its Notaries notify Customer of the same.
- Some jurisdictions require that Supplier provide a list of Notaries onboarded and offboarded from OneSpan Notary from time to time. Customer consents to Supplier's provision of this list to the applicable jurisdiction authority.
- Some jurisdictions have IPEN and RON specific data breach notification requirements, it is Customer's responsibility to understand and comply with these notification requirements and other applicable state data privacy laws as it applies to its particular use case.
- OneSpan Notary contains Third Party Components. The list of Third Party Components that are utilized to provide OneSpan Notary can be viewed in the "OneSpan Subprocessor" list available at www.onespan.com/privacy-center. For business continuity purposes, Supplier may alternate between Third Party Component providers at any time without notice to you. Third Party Component providers may mandate that additional terms are incorporated into this Contract. Those terms are available for review at https://www.onespan.com/third-party-terms and are hereby incorporated.
- To the extent Supplier makes available any artificial intelligence, machine learning, generative AI, or AI-assisted functionality in connection with the OneSpan Notary Service, Customer's use of such functionality shall be subject to the OneSpan AI Terms available at www.onespan.com/da-ai-terms, as may be updated from time to time, which are hereby incorporated into the Contract by reference.

Communication Hub

Definitions

"Annual Commitment" means the number of annual Credits committed in the applicable Order Document.
"Credit" means the unit purchased in order to access and use Communication Hub services.
"Excess Limit Fee" means the price per Credit listed for the Product on the applicable Order Document that is charged for Credits in excess of the Annual Commitment.
"SMS OTP" means a text message containing a one-time access code, which the User must enter in order to gain access to the applicable Customer application, OneSpan Product, or other relevant application.

Product Information

OneSpan's Communication Hub (the "**Communication Hub**") is a global service allowing the use of SMS OTP to transmit information or features to registered Users.
Communication Hub uses Credits in order to access any of the possible combinations.

Communication Hub provides customers with two different environments to support their testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.
Production:

- Production usage of the current version of Communication Hub
- Subject to the Service Levels

Testing/Sandbox (Preview):

- Integration development and testing of the current version of Communication Hub
- Not subject to the Service Levels, security requirements or safeguards set out in the Contract; as such, Customer acknowledges that no production Data is to be uploaded to the Testing environment
- Subject to Pricing requirements below and as indicated in the companion OneSpan Product Service description herein

Pricing

Pricing for Communication Hub is based upon Annual Commitment allocated as follows:

SMS OTP: Credits based on the User's telephone number geographic location as indicated below. For a list of Tiers see www.onespan.com/smsotp-tiers.

1. Tier 1: one (1) Credit
2. Tier 2: two (2) Credits
3. Tier 3: three (3) Credits

Credits processed in excess of the Annual Commitment will be charged Excess Limit Fee. Excess Limit Fees are invoiced quarterly in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one quarter prior to invoicing for administrative convenience.

Unused Credits do not carry over to the next year.

For OneSpan Sign, Customer receives up to one percent (1%) of the SMS OTP Communication Hub Credits purchased by Customer in production environment for use in the Sandbox (Staging) environment provided free of charge. Use in excess of this amount in Sandbox (Staging) will result in Excess Limit Fees.

Additional SaaS Conditions

- Customer is responsible for providing correct phone number for applicable User. SMS OTPs sent to incorrect phone numbers will incur applicable Credits.
- The phone number provided by Customer must be able to receive SMS text messages. SMS OTPs sent to phone numbers unable to receive SMS text messages will incur applicable Credits.
- Customer warrants that it has obtained Users consent to receive SMS text messages.
- Communication Hubb contains Third Party Components. The list of Third Party Components that are utilized to provide Communication Hubb can be viewed in the OneSpan Sign list "in the "OneSpan Subprocessor" list

available at www.onespan.com/privacy-center. For business continuity purposes, Supplier may alternate between Third Party Component providers at any time without notice to you. Third Party Component providers may mandate that additional terms are incorporated into this Contract. Those terms are available for review at https://www.onespan.com/third-party-terms and are hereby incorporated.

OneSpan Identity Verification (OneSpan IDV)

Definitions

"Annual Commitment" means the annual Component commitments as indicated in the applicable Order Document.

"Component" means an optional set of functionalities that Customer may choose to purchase based on their requirements. The Component has a specific pricing structure and may give access to features that are specific to the Component.

"Excess Limit Fees" are fees charged for each particular Component used in excess of the Annual Commitment.

"Transaction" means a Workflow initiated by Customer in the SaaS Service for a particular User(s) and is comprised of one or more Components.

Product Information

OneSpan Identity Verification ("OneSpan IDV" or "IDV") incorporates the Components necessary to facilitate the automated verification of a User's identity. IDV is deployed with a single integration, allowing customers to specify only the features they require. Several options are available for configuration by working with OneSpan Professional Services (subject to the Professional Services Schedule at www.onespan.com/professional-services and the applicable SOW), which may include:

- Configurable Workflows: Customer works with Supplier's Professional Services to combine workflow components in multiple ways (a "**Workflow**")
- Digital Identity Verification: Digital identity verification utilizing the SaaS Services' identity document verification Component ("**Identity Document Verification**") or combining this with facial comparison of a 'selfie' (and liveness detection) with the photo from the identity document ("**Identity Document Verification with Face**") or using the one-time-passcode ("**OTP**") Component .
- End-to-End Audit Trail: The SaaS Service collects a complete audit trail, showing what actions the User took at each stage of the Workflow
- Notifications: SaaS Service allows Customer ability to subscribe to several notifications to track User progress through the Workflow
- Localization: Workflow configurations can be defined for many languages; Customer decides the languages required and specifies the text to use so that Transactions are presented in the language requested
- White-Labelling: Allows Customer to customize language and branding, dialog boxes, buttons and navigation
- Responsive design: User interface adjusts for web-browsers on desktop, tablet and mobile devices
- Data Retention: subject to storage limitations, Customer controls incomplete and completed Transaction storage periods and may erase Transactions at any time.

IDV provides customers with two environments to support their integration, testing and production needs. Each environment serves a specific purpose and has its own characteristics. These environments and their respective characteristics may change at Supplier's discretion.

Production:

- Production usage of Workflows on the current version of IDV
- A/B testing may be performed here
- Subject to the Service Levels and subscription Fees

Staging / Testing and Development:

- Integration development, system integration testing of Workflows on the current version of IDV
- The Staging/Testing and Development environment is not subject to the Service Levels and data security requirements; as such, Customer acknowledges that Personal Data and production Data provided as testing data IS NOTWITHSTANDING ANYTHING IN THIS CONTRACT: PROVIDED "AS-IS", WITHOUT ANY WARRANTY, SERVICE LEVELS, LIABILITY OR INDEMNITY OBLIGATIONS; may be accessed by OneSpan and third party personnel; and may be accessed, processed and stored by a third party service provider in the US and the European Economic Area.

Pricing

- Pricing for IDV is based upon the Annual Commitment.
- IDV Components are priced as follows:
  - **Platform Component Fee**: Fee assessed once for each Transaction at the time of Transaction creation.
  - **Identity Document Verification Component Fee**: Fee assessed for each Identity Document Verification request attempt made by a User at the time the attempt is made within the Transaction.
  - **Identity Document Verification with Face Component Fee:** Fee assessed for each Identity Document Verification with Face request attempt made by a User at the time the attempt is made within the Transaction (there are no additional charges for liveness detection).
  - **OTP Component Fee**: Fee assessed for each OTP attempt made by a User at time the attempt is made within the Transaction. One Transaction may have multiple OTP Component Fees.
- Components processed in excess of the Annual Commitment are charged Excess Limit Fees. Excess Limit Fees are invoiced on the annual anniversary in arrears; however, Supplier may elect to aggregate Excess Limit Fees over more than one annual period prior to invoicing for administrative convenience.
- Unused Annual Commitment does not carry over to the next year.
- For OneSpan Sign:
  - Customer receives up to one percent (1%) of the production environment Annual Commitment for use in the Sandbox (Staging) environment free of charge each annual term. Use in excess of this amount in Sandbox (Staging) will result in Excess Limit Fees.
  - If Customer purchases IDV for use with OneSpan Sign, Customer is not charged a Platform Component Fee or an OTP Component Fee.

Additional Saas Service Conditions

- Supplier may, during the Term, place the Data in a backup location within the System. Upon Customer's request, and subject to applicable fees, Supplier may extract backed up Data from the System and transfer and retain such Data to a Customer selected backup location, as set forth in an applicable Order Document.
- IDV contains Third Party Components. The list of Third Party Components that are utilized to provide IDV can be viewed in the "OneSpan Subprocessor" list available at www.onespan.com/privacy-center. For business continuity purposes, Supplier may alternate between Third Party Component providers at any time without notice to you. Third Party Component providers may mandate that additional terms are incorporated into this Contract. Those terms are available for review at https://www.onespan.com/third-party-terms and are hereby incorporated.
- To the extent Supplier makes available any artificial intelligence, machine learning, generative AI, or AI-assisted functionality in connection with the OneSpan Notary Service, Customer's use of such functionality shall be subject to the OneSpan AI Terms available at www.onespan.com/da-ai-terms, as may be updated from time to time, which are hereby incorporated into the Contract by reference.