SOC 3®– SOC FOR SERVICE ORGANIZATIONS: TRUST SERVICES CRITERIA

Report on OneSpan's Description of its OneSpan Transaction Cloud Platform System and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security, Confidentiality, Availability and Privacy throughout the period January 1, 2022 to December 31, 2022

Table of Content

1. INDEPENDENT SERVICE AUDITORS' REPORT

KPMG LLP
KPMG Tower
Suite 1500
600, de Maisonneuve Blvd. West
Montreal, Quebec H3A 0A3
Tel.: 514-840-2100
www.kpmg.ca

Independent Service Auditors' Report

To: Management of OneSpan Inc.

Scope

We have been engaged to report on OneSpan Inc's (OneSpan's) accompanying statement titled "Statement by OneSpan Management" (statement) that the controls within OneSpan's Transaction Cloud Platform System (system) were effective throughout the period January 1, 2022, to December 31, 2022, to provide reasonable assurance that OneSpan's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

OneSpan is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that OneSpan's service commitments and system requirements were achieved. OneSpan has also provided the accompanying statement about the effectiveness of controls within the system. When preparing its statement, OneSpan is responsible for selecting, and identifying in its statement, the applicable trust service criteria and for having a reasonable basis for its statement by performing an assessment of the effectiveness of the controls within the system.

Our Independence and Quality Management

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies Canadian Standard on Quality Management Control 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility, under this engagement, is to express an opinion, based on the evidence we have obtained, on whether management's statement that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our engagement was conducted in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our engagement to obtain reasonable assurance about whether management's statement is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our reasonable assurance engagement included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve OneSpan's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve OneSpan's service commitments and system requirements based on the applicable trust services criteria
- Performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become ineffective because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's statement that the controls within OneSpan's Transaction Cloud Platform System were effective throughout the period January 1, 2022, to December 31, 2022, to provide reasonable assurance that OneSpan's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

*

KPMG LLP

*CPA auditor, CA, public accountancy permit No. A119819

Montreal, Quebec
May 18, 2023

2. STATEMENT BY ONESPAN MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within OneSpan Inc's (OneSpan's) Transaction Cloud Platform System (system) throughout the period January 1, 2022, to December 31, 2022, to provide reasonable assurance that OneSpan's service commitments and system requirements relevant to security, availability, confidentiality and privacy were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our statement.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2022, to December 31, 2022, to provide reasonable assurance that OneSpan's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). OneSpan's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We confirm that the controls within the system were effective throughout the period January 1, 2022, to December 31, 2022, to provide reasonable assurance that OneSpan's service commitments and system requirements were achieved based on the applicable trust services criteria.

OneSpan

E-SIGNED by Christian Vezina
on 2023-05-18 13:23:51 EDT

Christian Vezina, Chief Information Security Officer

May 18, 2023

ATTACHMENT A: ONESPAN'S DESCRIPTION OF THE BOUNDARIES OF ITS ONESPAN TRANSACTION CLOUD PLATFORM SYSTEM

Company Overview

OneSpan, the digital agreements security company™, helps organizations accelerate digital transformations by enabling secure, compliant, and refreshingly easy customer agreements and transaction experiences. OneSpan simplifies and secures business processes of organizations requiring high assurance security, including the integrity of end-users and the fidelity of transaction records behind every agreement, with their partners and customers. Trusted by global blue-chip enterprises, including some of the world's largest banks, OneSpan processes millions of digital agreements and billions of transactions in 100+ countries annually.

OneSpan Transaction Cloud Platform Description

For the purpose of this report, the OneSpan Transaction Cloud Platform is composed of the following solutions (the "Services"):

- OneSpan Sign (OSS);
- Identity Verification (IDV);
- Intelligent Adaptive Authentication (IAA);
- OneSpan Cloud Authentication (OCA); and
- Risk Analytics (RA).

OneSpan Sign (OSS)

OneSpan Sign is an e-signature solution that enables users to prepare, send and sign documents over the web electronically. This process typically requires five steps:

- Upload documents for the signature process;
- Add recipients who will either be signing or reviewing the documents;

- Define who will be signing and where the signatures will need to be applied;
- Select the authentication method (username/password, secret question/answer, one-time passcode (OTP), third-party authentication services); and
- Initiate signature process.

An email is sent to each signer, inviting them to e-sign the document(s). If Users are face-to-face with the signer, they can use their computer or mobile device to capture the signer's signature. Each signer is guided step-by-step through the signing process. Once the documents are signed, they can be downloaded. The e-signed documents can then be downloaded for retention in the User's record system and deleted from OneSpan Sign.

The e-signed documents are standard PDF files that can be viewed in Adobe Reader and other PDF readers.

OneSpan Sign provides a flexible and scalable solution to support signing needs. OneSpan Sign was designed to be easy to use for stakeholders: signers, reviewers, senders and developers. There are several ways in which an organization can consume e-signatures. This largely depends on their use case – and whether they need e-signatures embedded inside of an application.

Organizations can get up and running with OneSpan Sign in three ways:

- Standalone web-based service (Professional Plan): This option largely satisfies the most common signing workflows and e-contracting use cases– for example, getting contracts and agreements electronically signed. Users simply upload a document, select their signers and begin e-signing in minutes;
- Integration (Enterprise Plan): Our solution gives users the ability to add e-signing capabilities into their own applications – whether that's through their website, mobile app, or even their home-grown or legacy system. We have an open, industry-standard REST API and fully supported SDKs for Java, .NET, APEX, iOS and Android – to help users embed e-signing capabilities in ANY one of their applications; and

- Pre-built connectors for 3rd party applications: Users can send and sign documents without ever leaving 3rd party applications. We've done all the integration work with these connectors – no coding or IT resources are needed to get started with e-signatures inside these business applications that users know and use every day.

OneSpan Sign E-Signature Workflow

The solution was built for businesses and projects of all sizes – making e-signatures available to everyone, regardless of deployment preference, budget or IT resources. Users simply create and send out digital documents and e-forms to clients for signing. OneSpan Sign manages the online signing process so that electronic contracts and records are enforceable, compliant and secure. In addition, customers can monitor all in-progress transactions, identify bottlenecks and empower users to take action to keep digital processes moving forward. See Figure 1 below for a typical e-signature transaction workflow.

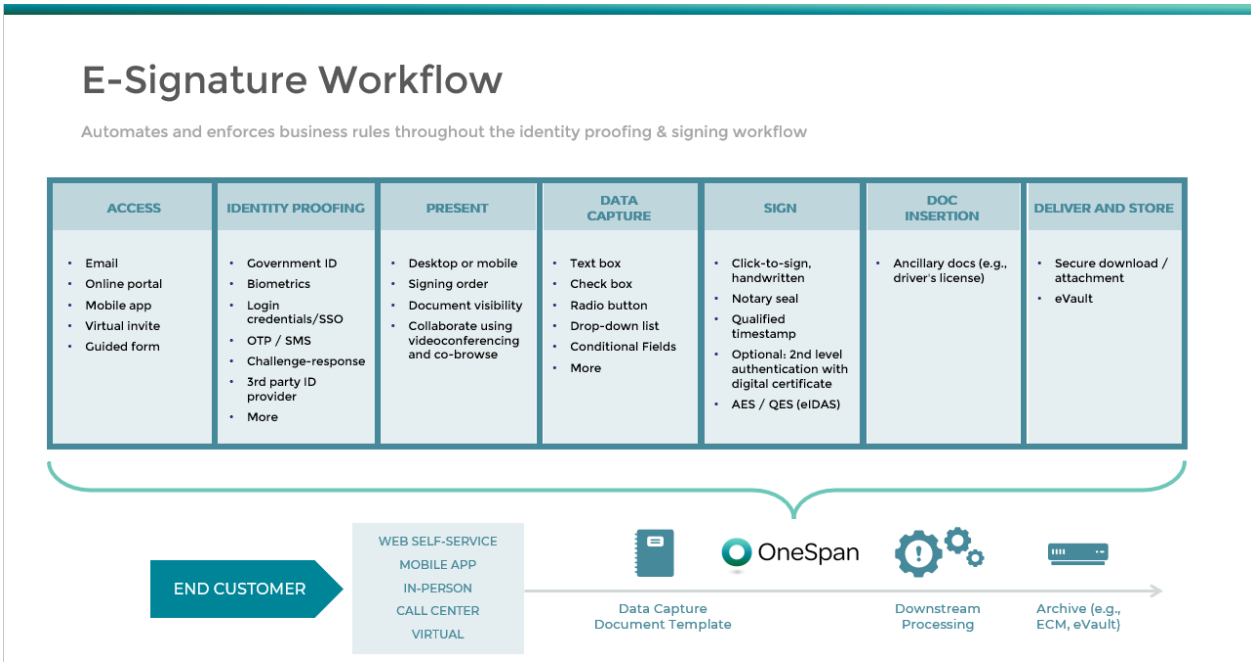

Figure 1: E-signature transaction workflow with OneSpan Sign

including email, ID Verification, SMS, Question/Answer, and third-party authentication services. Digital encryption securely seals each signature block after signing, and the embedded audit trail reports on who signed, in what order, at what time and in what locations. This audit trail travels with the e-signed document and can be verified with one simple click to ensure the document's integrity.

End-User Access to the System

Users can access the System in a standalone fashion via its secure web interface using their unique username (email address) and password. Integrated customers can also access the service through its Application Programming Interface (API) using an API key. All connections are made over HTTPS (TLS 1.3 by default) encrypted using secure ciphers, such as AES-256.

Identity Verification (IDV)

OneSpan Identity Verification (IDV) digitizes the customer journey for digital identity verification while capturing and managing all supporting evidence. IDV is comprised of the following modules:

- Workflow Management;
- Identity Verification Hub; and
- Audit Trail Capture and Management.

The solution provides the following functionality:

- Digital identity verification validates the authenticity of an identity document (e.g., passport, identity card, driver's license). It checks whether the person presenting the identity document is the genuine owner of the document via facial comparison;
- Secure document signing, which digitally signs documents for account opening and financial transactions; and
- Digital audit trails of the entire agreement process, including identification checks and all actions performed by the customer. This includes recording all web pages presented to the customer during the agreement process. Supports web page replay with an event timeline to reveal precisely what the customer did and saw during the agreement process.

Intelligent Adaptive Authentication (IAA)

The Intelligent Adaptive Authentication (IAA) solution secures web applications of customers by providing easy integration of authentication functionality into these web applications.

The authentication functionality secures logins into web applications and transactions, or payments initiated from the web applications. The solution dynamically assesses which authentication or transaction security measures are appropriate for each unique end-user at any given moment, taking into account the characteristics of the user or transaction as well as the user's behaviour and devices. Customers are typically financial institutions that want to protect access to their online banking applications and ensure a smooth, frictionless authentication experience for their end-users.

OneSpan Cloud Authentication (OCA)

The OneSpan Cloud Authentication (OCA) solution secures web applications of customers by providing easy integration of authentication functionality into these web applications. The authentication functionality secures logins of end-users into web applications as well as transactions initiated by end-users from the web applications.

In the context of this solution, customers are financial institutions or enterprises that wish to protect access to their web applications.

Risk Analytics (RA)

The Risk Analytics (RA) solution provides fraud detection and management to payment service providers and financial institutions. It allows monitoring of online banking applications and payment processing across multiple channels, such as online banking, mobile banking, and banking via ATMs, and assigning a risk score to financial transactions and user sessions. In addition, it helps payment service providers and financial institutions protect against anti-money-laundering (AML) and online banking fraud and comply with regulations, such as the European Union's revised Payment Services Directive (PSD2).

Components of the System Providing the Services

This section describes infrastructure, software, people, procedures, data, and privacy practices used to deliver the Services.

Infrastructure

By leveraging cloud partners, the OneSpan Transaction Cloud Platform can scale the required infrastructure resources whenever the need arises. OneSpan's cloud partners have extensive global data center networks. This provides OneSpan with a robust environment that is highly available with a quick disaster recovery capability to another geographic region. Utilizing cloud technology ensures OneSpan's Services can quickly be scaled up and expand operations to meet its customers' growing needs.

OneSpan regularly reviews its cloud partners' compliance to validate that controls in place are sufficient to meet OneSpan's requirements.

As per good practices, infrastructure is split into multiple network segments and firewall technology is used to control network traffic and allow required traffic. System instances are hardened to help ensure that required services are running. Administrative access to the system requires multifactor authentication. User accesses are logged and controlled, and mechanisms are in place to help prevent system abuse.

The OneSpan Transaction Cloud Platform is monitored on a 24/7 basis, including through the use of intrusion detection tools. Events are centrally correlated, providing system administrators with continuous visibility over, and automated notifications in case of potential incidents, including system health or security.

Vulnerability scanning and intrusion tests are performed periodically through the use of tools to detect areas that require patching or other remediation to help protect against outside threats. Patches are applied regularly to help ensure the system stays up to date and secure.

Software

The system is designed based on a 3-tier architecture approach, comprised of different types of instances. Unless otherwise indicated, instances are built from standardized Images and are hardened as per OneSpan's hardening guidelines.

- **Presentation layer**: This layer is running public-facing instances in the form of load balancers, outbound proxies, and microservices to allow secure inbound traffic to the system and outbound traffic to integrated customers and interfaces to external third-party services.
- **Application layer**: This layer controls the OneSpan Transaction Cloud Platform's functionalities. It hosts the system's front-end web services and back-end instances handling all the business logic associated with the Services, including the API requests.
- **Database layer**: Database instances supporting the system are running in this layer. Databases reside on encrypted volumes for data protection. Backups and replication of the data are performed in multiple zones and datacenters for high availability and disaster recovery purposes.

People

OneSpan employees are bound by a non-disclosure agreement, as well as a Code of Conduct & Ethics, which they are asked to acknowledge on a yearly basis. A criminal background check is required for employees with access to production systems.

Senior Management's philosophy on the importance of protecting customer information is reflected in OneSpan control environment. OneSpan has developed an extensive set of security policies, standards and processes to help employees understand their individual roles and responsibilities with regards to information security and protection of customer information. Policies are communicated to employees at hire time and again annually, or as required. Multiple roles are defined, along with their responsibilities, such as Chief Information Security Officer, Data Protection Officer, Cloud Operations Director, Change Manager, Human Resources Manager, Product Management team, System Owner, Product Owner, Release Manager, R&D team, Senior Developers, Software Quality Assurance team, etc.

Procedures

OneSpan has developed procedures and processes to restrict logical access to the system and protect customer data. These procedures and processes are communicated to employees, and reviewed and updated as required to maintain system security. They cover multiple aspects, such as risk management, access controls, secure development, system hardening, change management, patch

management, vulnerability management, business continuity, disaster recovery, and incident response.

Data

The system captures and stores all the data necessary to provide the Services. This data is coming through to the system via its REST API over secured HTTPS connections.

Privacy Practices

OneSpan accesses, processes and stores customer data in accordance with the relevant agreement between customers and OneSpan. Customer data is retained according to the relevant agreement with its customers. OneSpan has no direct control or ownership of the personal information it processes under the direction of its customers.

Identified System Incidents

OneSpan has not experienced significant security incidents related to the system that either (a) were the result of controls that were either not designed or operating effectively to achieve commitments or system requirements, or (b) otherwise resulted in a failure in the achievement of commitments or system requirements.

Complementary Subservice Organization Controls

The system was designed with the assumption that certain control objectives can be achieved only if complementary subservice organization controls assumed in the design of OneSpan's controls are suitably designed and operating effectively, along with the related controls at OneSpan.

The boundaries of the OneSpan Transaction Cloud Platform System did not extend to the complementary subservice organization controls and policies and procedures at the subservice organizations.

Complementary User-Entity Controls

The system was designed with the assumption that certain policies, procedures and controls would be in existence or implemented by user entities. These controls should be in operation at the user entities to complement OneSpan's controls.

ATTACHMENT B: THE PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

OneSpan designs its processes and procedures related to OneSpan's Transaction Cloud Platform to meet its objectives. Those objectives are based on the service commitments that OneSpan makes to its user entities, applicable laws and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that OneSpan has established for the Service.

Service commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, such as the OneSpan Terms and Conditions, which are published online (onespan.com). Service commitments include the following:

Security:

OneSpan has made commitments related to designing and implementing controls to help support the protection of the system and customer data. These commitments are addressed through controls such as data encryption, authentication mechanisms, network security and other relevant security controls.

Availability:

OneSpan has made commitments related to percentage uptime and connectivity for the system, as well as commitments related to service credits for instances of downtime.

Confidentiality:

OneSpan has made commitments related to designing and implementing controls to help support the confidentiality of customers' data through data classification policy, data encryption and other relevant security controls.

Privacy:

OneSpan has made commitments related to designing and implementing controls to help support the protection of personal information and complying with applicable privacy laws and regulations.

OneSpan has established operational requirements that support the achievement of service commitments, compliance with applicable laws and regulations, and other system requirements. Such requirements are communicated in OneSpan's policies and procedures, system design documentation, and contractual agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the system is designed, developed, and operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the system.

