SOC 3®– SOC for Services Organizations: Trust Services Criteria

Report on OneSpan's Description of its OneSpan TID Platform on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security, Confidentiality Availability, and Privacy throughout the period July 1, 2021 to December 31, 2021.

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 Management of OneSpan" (statement) that the controls within OneSpan's TID System (system) were effective throughout the period July 1, 2021, to December 31, 2021, 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*).

The description of the boundaries indicates that OneSpan's controls can provide reasonable assurance that certain service commitments and system requirements 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. Our engagement did not include complementary subservice organization controls, and we have not evaluated the suitability of the design and operating effectiveness of such controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at OneSpan, to achieve OneSpan's service commitments and system requirements based on the applicable trust services criteria. The description presents OneSpan's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of OneSpan's controls. Our engagement did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

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 Control

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 Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, and accordingly maintains a comprehensive system of quality control including documented policies and 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.

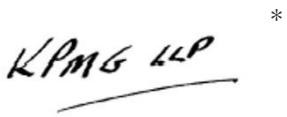
Inherent Limitations

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 Environment, Health, Safety and Quality Management system were effective throughout the period July 1, 2021, to December 31, 2021, 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.



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

Montreal, Quebec
June 1, 2022

2. STATEMENT BY ONESPAN MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within OneSpan Inc's (OneSpan's) TID System (system) throughout the period July 1, 2021, to December 31, 2021, 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 July 1, 2021, to December 31, 2021, 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.

Our description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at OneSpan, to achieve OneSpan's service commitments and system requirements based on the applicable trust services criteria. Our description of the boundaries does not extend to controls of the subservice organizations.

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 July 1, 2021, to December 31, 2021, 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 2022-05-31 16:32:24 GMT

Christian Vezina, Chief Information Security Officer

June 1, 2022

ATTACHMENT A: ONESPAN'S DESCRIPTION OF THE BOUNDARIES OF ITS TID SYSTEM

Company Overview

OneSpan helps protect the world from digital fraud by establishing trust in people's identities, the devices they use, and the transactions they execute. OneSpan's security solutions reduce digital transaction fraud and enable regulatory compliance for more than half of the top 100 global banks and thousands of financial institutions worldwide.

Our next-generation solutions are delivered on a cloud-based platform, from risk-based adaptive authentication to digital identity verification and e-signature.

Products depending upon the OneSpan TID Platform

Intelligent Adaptive Authentication (IAA)

The Intelligent Adaptive Authentication (IAA) solution secures web applications of Relying Parties 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. Relying Parties 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.

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).

Cloud Authentication (CA)

The OneSpan Cloud Authentication (OCA) solution secures web applications of Relying Parties 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, Relying Parties are financial institutions or enterprises that wish to protect access to their web applications.

Identity Verification (IDV)

OneSpan Identity Verification (IDV) digitizes the customer journey for digital identity verification while capturing and managing all supporting evidence.

IDV is hosted on the TID Platform and comprised of the following modules

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

The figure below depicts the high-level components of the service

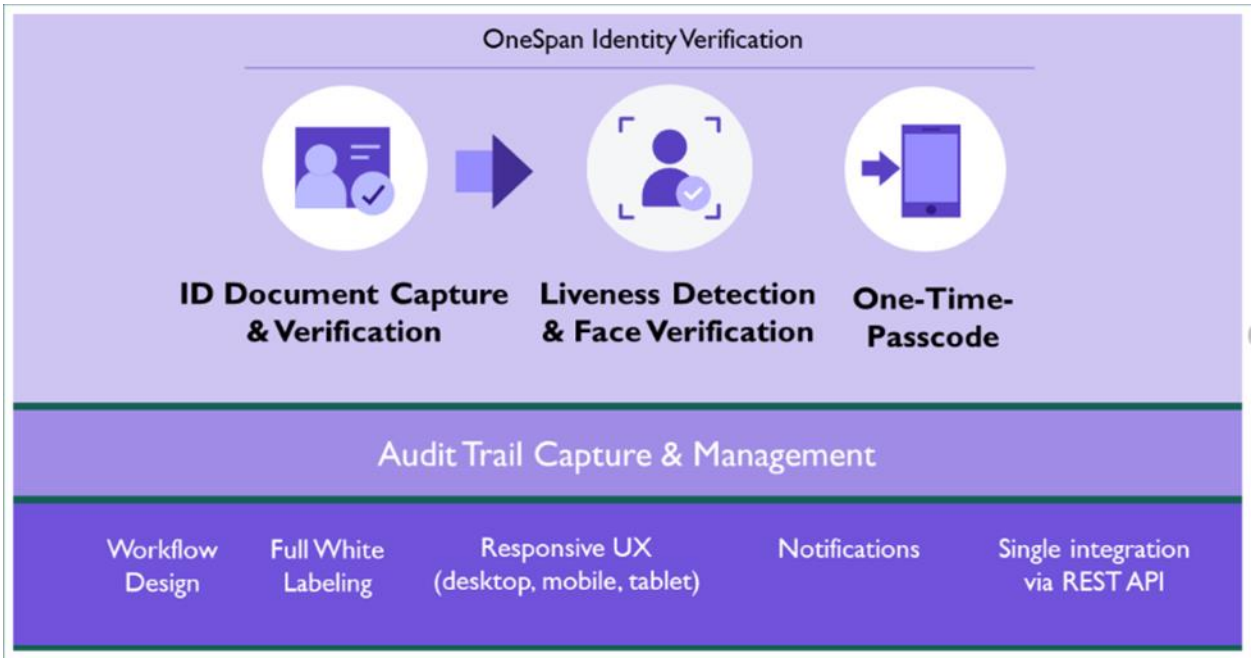


Figure 1 Functional structure of IDV Service

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
- 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.

Components of the System Providing the Service

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

Infrastructure

By leveraging cloud partners, OneSpan's Trusted Identity (TID) platform can scale the required infrastructure resources whenever the need arises. OneSpan's cloud partners have extensive global data center networks. This provides the TID platform with a robust environment that is highly available with a quick disaster recovery capability to another geographic region. Utilizing cloud technology ensures the TID platform 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 TID 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 TID platform 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:** The Relying Party applications access this layer. It is built from microservices, which are small, loosely-coupled, independent applications. The microservices are deployed as docker containers and communicate with Relying Party applications via a REST-based API. The API microservices are exposed to Relying Party applications. The integration microservices provide more fine-grained functionality. Workflow orchestration allows Relying Parties to customize the logical flow to implement specific API microservices.
- **Application layer**: This layer controls the TID platform's functionality. It consists of multiple functional components, including OneSpan Authentication Server (CA), OneSpan Risk Analytics (RA) and a push notification server.

- **Persistence layer**: This layer manages the storage and retrieval of data from databases. The TID platform uses different databases such as Oracle, Couchbase and Aurora MySQL.

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 service. All of 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 OneSpan TID platform 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 TID platform 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.

OneSpan uses the infrastructure services of AWS to host the TID platform and customer data.

For the control objectives listed below, OneSpan uses AWS to support the achievement of control objectives identified in this report. The subservice organization controls presented below should not be regarded as a comprehensive list of all of the controls that should be employed by the subservice organizations.

Subservice Organization	Complementary Subservice Organization Control	Control Objective Reference	AICPA SOC2 criteria
AWS (Amazon Web Services)	The external connectivity points to AWS' computing environment should be restricted to the level of network access that is required.	AWSCA-3.1 AWSCA-3.2 AWSCA-3.3	CC6.1
	The AWS KMS should provide secure key management services. The keys should be issued using strong cryptographic algorithms and be protected in transit and at rest.	AWSCA-4.5 to AWSCA-4.15	CC6.1
	The physical access to the AWS data centers where the System is hosted should be limited to properly authorized individuals only, reviewed on a quarterly basis by appropriate personnel, and revoked within 24h of their deactivation.	AWSCA-5.1 AWSCA-5.2 AWSCA-5.3	CC6.4
	AWS should protect the physical entry points of the data centers where the System is hosted with electronic access control devices, closed-circuit television cameras (CCTV) and electronic intrusion detection systems	AWSCA-5.4 AWSCA-5.5 AWSCA-5.6	CC6.4
	AWS should securely decommission and physically destroy media such as hard drives at the end of their functional life.	AWSCA-5.13	CC6.5
	AWS-owned data centers and third-party colocation service providers used by AWS should have environmental controls in place, including fire detection and suppression systems, HVAC systems, uninterruptible power supplies, and generators that are monitored and maintained to protect computer equipment used for the System.	AWSCA-5.7 AWSCA-5.8 AWSCA-5.9 AWSCA-5.10 AWSCA-5.11 AWSCA-5.12	A1.2
OneLogin	OneLogin must protect the security and confidentiality of submitted OneSpan user credentials.	C1.1 C1.2	C1.1 C1.2

Subservice Organization	Complementary Subservice Organization Control	Control Objective Reference	AICPA SOC2 criteria
	OneLogin must protect the availability of their service to ensure OneSpan can continuously log on to their outsourced services.	A1.1 A1.2 A1.3	A1.1 A1.2 A1.3
Mitek	Mitek must protect the communication between the TID platform and its web services. Mitek must protect personal data provided by the TID platform for identity verification. Identity verification partners must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.	C1.1 C1.2 P3.1 P4.3	C1.1 C1.2 P3.1 P4.3
Veridas	Veridas must protect the communication between the TID platform and its web services. Veridas must protect personal data provided by the TID platform for identity verification. Identity verification partners must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.	(ISO 27001) A.13.2.4 A.18.1.4	C1.1 C1.2 P3.1 P4.3

Changes since the Date of the Last Report

No changes occurred during the period of July 1, 2021, to December 31, 2021.

Complementary User-Entity Controls

The TID platform 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 TID 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 TID Platform service, 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 TID Platform 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 the following commitment related to percentage uptime and connectivity for TID Platform, as well as commitments related to service credits for instances of downtime. Except for maintenance windows, the SaaS Service will be available continuously at least 99.9% of the time on a monthly basis. The SaaS Service is considered unavailable when the SaaS Service is not accessible through the Internet at the point the data center connects to the public Internet for a reason other than a Force Majeure for a period of at least five (5) minutes.

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 Service is designed and developed, how the System is 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 TID Platform.