SILANIS TECHNOLOGY

SERVICE ORGANIZATION CONTROLS (SOC[SM]) 3 REPORT-TYPE II

On SILANIS TECHNOLOGY'S Description of its eSignLive System on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security (Version 10.13)

Throughout the Period January 1, 2016 to December 31, 2016

May 5, 2017

Table of Contents

KPMG LLP
600 de Maisonneuve Blvd. West
Suite 1500
Tour KPMG
Montréal, Québec H3A 0A3

Telephone 514-840-2100
Fax 514-840-2187
Internet www.kpmg.ca

Independent Service Auditor's Report

Chief Information Security Officer
SILANIS TECHNOLOGY INC.
8200 Decarie Blvd, Suite 300
Montreal, QC
H4P 2P5

We have examined management's assertion that during the period January 1, 2016 through December 31, 2016, SILANIS TECHNOLOGY maintained effective controls over the eSignLive system V10.13 to provide reasonable assurance that:

- the system was protected against unauthorized access (both physical and logical), use, or modification;

based on the AICPA and CPA Canada trust services security criteria set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*).

SILANIS TECHNOLOGY's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the SILANIS TECHNOLOGY's eSignLive system V10.13 covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of SILANIS TECHNOLOGY's relevant controls over the security of the SILANIS TECHNOLOGY's eSignLive system; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, SILANIS TECHNOLOGY's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA and CPA Canada trust services *security* criteria.

KPMG LLP

May 5, 2017
Montreal, Quebec

SILANIS TECHNOLOGY Management's Assertion regarding its eSignLive system throughout the period January 1, 2016 to December 31, 2016

May 5, 2017

The management of SILANIS TECHNOLOGY INC. ("SILANIS") makes the following assertion pertaining to the eSignLive V10.13 Deployment:

SILANIS maintained effective controls over the eSignLive system V10.13, during the period January 1, 2016 through December 31, 2016, in Montreal based on the AICPA and CPA Canada Trust Services security, criteria set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) to provide reasonable assurance that:

- the eSignLive system was protected against unauthorized access (both physical and logical), use, or modification

The attached description of the eSignLive system identifies those aspects of the system covered by our assertion.

Very truly yours,

SILANIS TECHNOLOGY

e-Signed by Christian Vezina
on 05/05/2017

Christian Vezina
Chief Information Security Officer

Description of SILANIS TECHNOLOGY's eSignLive system for the period January 1, 2016 to December 31, 2016

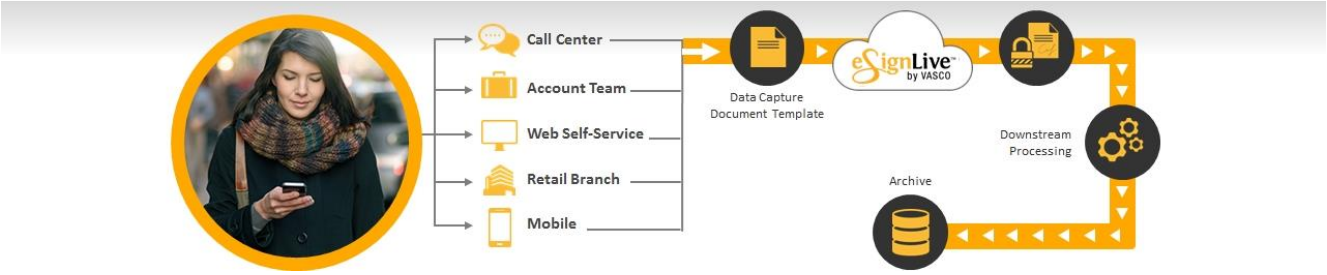
Company Overview

Since 1992, eSignLive has delivered e-signature solutions to organizations of all sizes, including banks, credit unions, insurers, pharmaceutical companies and government agencies. Built on a single SaaS platform that can be deployed in the cloud or on-premises, eSignLive offers a flexible and scalable solution to help organizations to digitize business processes and conduct secure enterprise transactions that touch the customer.

As of November 25, 2015, SILANIS TECHNOLOGY INC. is a subsidiary of VASCO Data Security (NASDAQ: VDSI), which allows more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions and protect assets across financial, enterprise, e-commerce, government and healthcare markets.

Product Introduction

eSignLive is an e-signature solution that enables users to electronically prepare, send and sign documents over the web. The figure below depicts a typical e-signature transaction workflow.



With eSignLive, customers have the ability to authenticate the user's identity using a variety of methods including email, 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 does not require connection to the eSignLive Service.

In addition, eSignLive offers a patented active audit trail called "e-Witness" that captures everything that occurs during a transaction, from beginning to end. This provides businesses with stronger customer insight and evidence than is possible with paper. Organizations can then reproduce the entire e-transaction for litigation, regulatory and internal control purposes.

Components of the System Providing the Service

People

All SILANIS TECHNOLOGY employees are bound by a non-disclosure agreement, as well as VASCO's 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 or customer data. The system is operated by a team of senior administrators with a strong security background and all accesses are granted based on a strict least privilege principle.

Senior Management's philosophy on the importance of protecting customer information is reflected in SILANIS TECHNOLOGY's control environment. SILANIS TECHNOLOGY 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 all employees at hire time and again annually, or as required. Multiple roles are clearly defined, along with their responsibilities, such as Chief Information Security Officer, Information Security Director, 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

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

Technology and Infrastructure

By leveraging best-of-breed cloud partners, eSignLive can leverage all the required infrastructure resources whenever the need arises. SILANIS TECHNOLOGY's cloud partners have extensive global data center networks. This provides eSignLive with a robust environment that is highly available with a quick disaster recovery capability to another geographic region. Utilizing cloud technology ensures eSignLive can quickly be scaled up and expand operations to meet its customers' growing needs.

SILANIS TECHNOLOGY's cloud partners provide extensive physical and environmental security controls, and they have implemented comprehensive compliance programs to provide their customers assurance about the security of their underlying infrastructure. SILANIS TECHNOLOGY regularly reviews its cloud partners' compliance to validate that the controls in place are sufficient to meet SILANIS TECHNOLOGY's requirements.

As per best practices, infrastructure is split into multiple network segments and firewall technology is used to control all network traffic and only allow what is required. All system instances are securely hardened to ensure that only required services are running. Administrative access to the system requires complex multifactor authentication. All user accesses are logged and controlled, and mechanisms are in place to prevent system abuse.

eSignLive is monitored on a 24/7 basis, including through the use of intrusion detection tools. All events are centrally correlated, providing system administrators with continuous visibility over, and automated notifications in case of any potential incidents, including with regards to system health or security.

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

Data

The system captures and stores all the data necessary to carry the electronic signing of documents. Data remains within the system's boundaries at all times and is not shared with any third parties. All traffic over the Internet is encrypted using TLS/SSL technology, and all data at rest is encrypted for increased security.

Complementary User-Entity Controls

SILANIS TECHNOLOGY's 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 SILANIS TECHNOLOGY's controls to achieve the customer's security or business requirements in regard to the use of the system.