Devolutions

SOC 3 REPORT

Report on the examination of controls for the Devolutions Password Hub System relevant to security for the period of January 1, 2020 to February 28, 2021

TABLE OF CONTENTS

SECTION 1
INDEPENDENT SERVICE AUDITOR'S REPORT

Ernst & Young s.r.l./S.E.N.C.R.L.
Ernst & Young LLP
900, boul. De Maisonneuve Ouest
Bureau 2300
Montréal (Québec) H3A 0A8

Tél./Tel: +1 514 875 6060
Téléc./Fax: +1 514 879 2600
ey.com

Independent Service Auditor's Report

To the management of Devolutions Inc. (Devolutions)

Scope

We have examined management's assertion, contained within the accompanying Devolutions' Management Assertion (Assertion), that Devolutions' controls over the Devolutions Password Hub System (System) were effective throughout the period January 1, 2020 to February 28, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security (applicable trust services criteria) set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

The Assertion indicates that Devolutions' 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 Devolutions' controls are suitably designed and operating effectively, along with the related controls at Devolution. The Assertion presents the System; its controls relevant to the applicable trust services criteria; and the types of complementary subservice organization controls that the Devolution assumes have been implemented, suitably designed, and operating effectively at Microsoft Azure. Our examination did not extend to the services provided by Microsoft Azure and we have not evaluated whether the controls management assumes have been implemented at Microsoft Azure have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 1, 2020 to February 28, 2021.

Management's Responsibilities

Devolutions' management is responsible for its assertion, selecting the trust services categories and associated criteria on which the its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Devolutions Password Hub System and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- Identifying, designing, implementing, operating, and monitoring effective controls over the Devolutions Password Hub System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Devolutions' relevant security policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material

misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Devolutions' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations:

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Devolutions' principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion:

In our opinion, Devolutions' controls over the system were effective throughout the period January 1, 2020 to February 28, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, if the subservice organization applied the controls assumed in the design of Devolutions' controls throughout the same period.

Ernst & Young LLP [1]

Montréal, Canada
April 14, 2021

[1] CPA Auditor, CA, public accountancy permit no. A120370

SECTION 2
DEVOLUTIONS' MANAGEMENT ASSERTION

Devolutions' Management Assertion

Management's Report of its Assertions on the Effectiveness of Its Controls over the Devolutions Password Hub System Based on the Trust Services Criteria for Security

April 14, 2021

We, as management of, Devolutions Inc. are responsible for:

- Identifying the Devolutions Password Hub System (System) and describing the boundaries of the System, which are presented in **Attachment A**
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in **Attachment B**
- Identifying, designing, implementing, operating, and monitoring effective controls over the Devolutions Password Hub System to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

Devolutions uses Microsoft Azure (subservice organization) to provide PaaS (Platform as a Service) services. The boundaries of the System, which are presented in Attachment A, includes only the controls of Devolutions and excludes the complementary subservice organization controls. The boundaries of the System indicates that certain trust services criteria specified therein can be met only if complementary subservice organization controls assumed in the design of the Devolutions' controls are suitably designed and operating effectively along with the related controls at the Devolutions. Our assertion does not extend to controls of subservice organization.

However, we perform annual due diligence procedures for third-party sub-service providers and based on the procedures performed, nothing has been identified that prevents Devolutions from achieving its specified service commitments.

We assert that the controls over the system were effective throughout the period January 1, 2020 to February 28, 2021, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

_____

David Hervieux, President and CEO

Devolutions Inc.

ATTACHMENT A
PASSWORD HUB SYSTEM DESCRIPTION

Overview of Devolutions

Founded in 2010 and located in Lavaltrie, Canada, Devolutions is a leading provider of remote connections, network accesses, password and credential management tools for network administrators and IT executives.

An increasing number of organizations no longer consider their IT department as a source of expenses but rather as a strategic asset helping them to get an edge on the competition. Bearing this in mind, Devolutions takes pride in developing world class and intuitive technologies and products that address concrete challenges and concerns faced by IT departments in the course of their daily operations. Devolutions is committed to design and create down-to-earth, low-cost and easy-to-use IT solutions and management tools that have significant positive impacts on the productivity and security of customers throughout the world.

Devolutions' current range of solutions includes Password Hub Business, Password Hub Personal, Remote Desktop Manager, Devolutions Server, Wayk Bastion and the companion tools Web Login, Authenticator and Launcher.

Scope

This report has been prepared to provide information on internal controls of Devolutions relating to the security trust criteria.

This report describes the Devolutions' Password Hub System (System) for the period of January 1, 2020 to February 28, 2021. The three main components of the System are the Lucid component, used solely for authentication, the Password Hub Business component that allows customers and administrators to access and manage vaults, and the Password Hub Personal component that offers single user credential storage services.

Lucid Component

Lucid is a robust authentication and identification service. Its goal is to provide identities throughout the entire Password Hub ecosystem and facilitating identity security by providing a strong authentication mechanism for users. Lucid is developed to use OpenID Connect and OAuth2 protocols.

Password Hub Business Component

This component is a secure and cloud-based password manager for teams. It empowers organizations to easily and securely vault and manage business-user passwords, along with other sensitive information, through a user-friendly web interface that can be quickly, easily and securely accessed via any supported browser.

Password Hub Personal Component

This component is a secure and cloud-based password manager for individuals. It is based on the same technologies as the Password Hub Business component and uses the same operational and security processes and policies. Its purpose is to provide easy and secure access to a credential vault owned by a single user. Access is provided through a user-friendly web interface that can be accessed using any of the supported browsers.

This component was officially released on October 1, 2020. Thus, this report only addresses the controls for this component for the period of October 1, 2020 to February 28, 2021.

Companion tools

To increase functionality, efficiency and performance, the System can be enhanced with multiple companion tools such as Launcher, Web Login and Authenticator. Those companion tools are out of the scope for this report.

System Components

Infrastructure

The System relies on Microsoft Azure (Azure) Platform-as-a-Service (PaaS) features to deliver a robust and secure cloud-based solution for customers. Microsoft Azure (Azure) is a world leader in terms of cloud infrastructure, with a comprehensive compliance program that provides its customers with a high level of assurance about the security of its underlying platform. In that respect, Azure publishes on its Trust Center (https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide) a series of attestation and compliance reports amongst which: Service Organization Control (SOC) 1 (SSAE 18 and ISAE 3402), SOC 2 and SOC3 reports, PCI DSS, and ISO 27001, 27017, 20000 and 9001 certifications. The controls defined in the Azure SOC 2 Type 2 report cover both the Trust Services Criteria and the CSA CMM Criteria. Azure controls are not included in the scope of this report.

On an annual basis, Devolutions obtains and reviews a SOC report for Microsoft Azure, and when appropriate. Devolutions requests and reviews bridge letters from Microsoft Azure to obtain assurance that the cloud service provider has been maintaining effective complementary subservice providers controls. During its review of the reports, Devolutions considers the scope, timing and assurance provided, adequacy of the identified security controls, potential impact of any noted deficiencies or exceptions, and what actions if any may be required to address any noted issues and concerns.

The affected criteria are included below along with the expected minimum controls in place at the subservice organization.

Criteria	Controls expected to be in place at the subservice organization
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Access to data centres are restricted and controlled.
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Controls are in place to prevent and act upon the introduction of unauthorized or malicious software.
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The production environment is patched on a regular basis.
CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	System components are configured according to Azure recommended settings. Rationale is documented for security setting(s) not configured according to the Azure recommended settings.

By using Azure's PaaS services listed below, Devolutions is taking advantage of Azure's fully managed services thus alleviating the burden of managing the underlying infrastructure needed to support the operation of the System.

- Azure Kubernetes Services
- Azure Storage Accounts
- Azure Traffic Manager
- Azure Key Vault
- Azure SQL Server
- Azure SQL Databases
- Azure Application Services
- Azure Functions

The infrastructure architecture overview of the System is shown in Diagram 1 below and depicts the services and technologies used by the System.

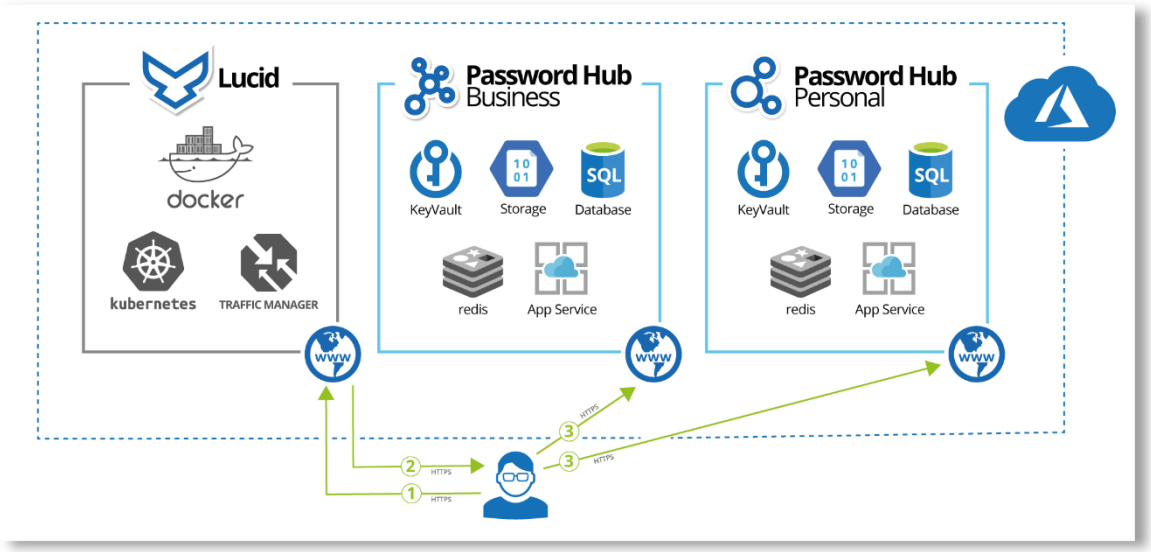

Diagram 1 - Password Hub Architecture Overview

Software

Both Password Hub Business and Password Hub Personal are web applications using secure HTTPS protocol. They provide logical repositories known as "vaults" that store "entries" of various types. An entry stores credentials used to access a remote service such as RDP, SSH or WEB. Vault storage and configuration settings tied to a specific user entity are stored in a dedicated SQL database.

Once subscribed to the System, a dedicated link is sent to the user entity that activated the subscription and provides full administrative access of the logical instance (also called "Organization") which includes the vault, the configuration and the user management. Cryptographic keys are also generated to protect the Organization's stored data.

To manage or access an Organization, the user must use the Password Hub Business or Password Hub Personal over secure TLS protocol. If the user doesn't have an already valid and active session, he/she is redirected to the identity management component, Lucid (see Diagram 1 Flow 1). This component hosts a web application over secure TLS protocol which requires users to authenticate with their username, password and, if enabled by the customer, second factor

challenge-response. Users without a Lucid account must create an account through the registration process with a valid e-mail. Once authenticated, Lucid provides the user a security token that attests the user's identity (see Diagram 1 Flow 2) and redirects the user to the desired Password Hub component (Diagram 1 Flow 3). Password Hub Business and Password Hub Personal components authorize the user based the identity provided (security token) and is granted access to the organization's vaults with the privileges assigned by the organization's administrators

People

Devolutions staff involved in the design, development, support and operation of the System are organized into the following roles or functional areas:

- **Executives and Senior Management:** provide vision for the company and products at the overall corporate level, with a strong focus on System security and performance, as well as quality and continuous improvement of customer experience.
- **Chief Security Officer (CSO)** oversees Devolutions' information security management system and security governance activities. The CSO's role extends to all strategic and tactical sectors of the System's information security.
- **Cloud Operations Team** is responsible for the implementation and maintenance of the environments capable of supporting the System's requirements according to the existing policies and procedures. They are also responsible for contacting Microsoft Azure support service for any issue under their own responsibility.
- **Human Resources Team** is the owner of the Devolutions' Code of Ethics and is responsible for its communication to and acknowledgement from all personnel at onboarding and yearly onwards. They make sure only capable, screened and well-trained personnel are assigned to the System's development, delivery, operations, and security functions.
- **Product Owner** has overall responsibility for the product, its development, testing, deployment and support in different environments. Approves and prioritizes development tasks and determines the development schedule.
- **Development Team** is in charge of System development. Developers update the source code through the source control system to meet the requirements approved by the Product Owner. Developers are also responsible for reviewing code developed by other members of the team.
- **Software Quality Assurance Team** is responsible for testing the resulting software and ensuring it respects to the intended behaviour. Any gaps identified is communicated to the appropriate team for remediation.
- **Information Security Team** is responsible for the security operations, code and architecture security validations, and monitoring production access. They work closely with Cloud Operations Team on security incidents as well as every other function to provide the best level of security for the System.
- **Support Team** is responsible for customer-facing communications and troubleshooting. They are the main point of contact for the customer, and they manage their requests from start to finish with any relevant assistance from other teams.

Procedures

As part of its governance, Devolutions has developed and communicated the directives and procedures related to the security of the System to its personnel, who understand their individual roles and responsibilities with regards to information security. Changes to these directives and procedures are made, as required, by the Chief Security Officer with the participation of the relevant teams and are approved by the executive management.

Data

Data relating to the System constitutes the following:

Customer data

- Password Hub Business and Password Hub Personal manage all the customer data related to vaults, entries, credentials, documents, and configurations.
- Lucid manages all data related to the identity of users such as usernames, derived passwords, and multi-factor secrets.

Non-Customer data

- Logging, audit and error information are collected by Azure services and the System to monitor performance and identify anomalies.

ATTACHMENT B
SERVICE COMMITMENTS AND SYSTEM REQUIREMENT

Service Commitments and System Requirements

Devolutions designs its processes and procedures related to the System to meet its objectives for its password management services. Those objectives are based on the service and security commitments that Devolutions makes to user entities, which are documented and communicated in its Terms of Online Services and other customer agreements, on the security section of the public website (available at *https://devolutions.net/legal/security),* as well as in the general description of its service offering also provided on its public website.

Devolutions established operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Devolutions' system policies, procedures and documentation, as well as its customer agreements. Information security policies define an organization-wide approach to how systems and data are protected. These include directives and procedures 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 processes required in the operation and development of the System.