Devolutions

SOC 3®– SOC for Services Organizations: Trust Services Criteria for General Use Report

Report on the Devolutions Hub System
Relevant to Security.

Throughout the period January 1, 2023 to December 31, 2023

Devolutions

TABLE OF CONTENTS

INDEPENDENT SERVICE AUDITORS' REPORT

KPMG LLP
Chartered Professional Accountants
600, de Maisonneuve blvd. West
Suite 1500
Montreal QC H3A 0A3
Tel 514-840-2100
www.kpmg.ca

Independent Service Auditors' Report

To: Devolutions Inc.

Scope

We have been engaged to report on Devolutions Inc.'s (Devolutions) accompanying statement titled "Statement by Management of Devolutions" (the Statement) that the controls within Devolutions' Hub System (the System) were suitably designed and operating effectively throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Devolutions' service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA*, Trust Services Criteria.*

Devolutions' uses a subservice organization identified in management of Devolutions' Attachment C – Devolutions' Complementary Subservice Organization Controls (Attachment C). Management of Devolutions' Attachment C indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Devolutions, to achieve Devolutions' service commitments and system requirements based on the applicable trust services criteria. Management of Devolutions' Attachment C presents the types of complementary subservice organization controls assumed in the design of Devolutions' controls. Management of Devolutions' Attachment C does not disclose the actual controls at the subservice organization. Our engagement did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Management of Devolutions' Attachment D – Devolutions' Complementary User Entity Controls (Attachment D) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Devolutions, to achieve Devolutions' service commitments and system requirements based on the applicable trust services criteria. Management of Devolutions' Attachment D presents the complementary user entity controls assumed in the design of Devolutions' System. 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 complementary user entity controls.

Service Organization's Responsibilities

Devolutions 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

Devolutions' service commitments and system requirements were achieved. Management of Devolutions has provided the accompanying Statement about the suitability of the design and operating effectiveness of controls within the System. Devolutions is also responsible for preparing the Statement, including the completeness, accuracy and method of presentation of the Statement and the attachments to the Statement; providing the services covered by the Statement; selecting, and identifying in the Statement, the applicable trust service criteria; identifying the risks that threaten the achievement of Devolutions' service commitments and system requirements; and having a reasonable basis for the Statement by performing an assessment of the suitability of the design and operating 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 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 the Statement that controls within the System were suitably designed and operating effectively throughout the period to provide reasonable assurance that Devolutions' 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 the 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 Devolutions' service commitments and system requirements
- assessing the risks that controls were not suitably designed or did not operate effectively to achieve Devolutions' service commitments and system requirements based on the applicable trust services criteria
- performing procedures to obtain evidence about whether controls within the System were suitably designed to provide reasonable assurance that Devolutions would achieve its service commitments and system requirements based on the applicable trust services criteria if those controls operated effectively
- testing the operating effectiveness of controls within the System to provide reasonable assurance that Devolutions achieved its 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 are 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, the Statement that the controls within Devolutions' System were suitably designed and operating effectively throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that Devolutions' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

KPMG LLP

—
KPMG LLP, Chartered Professional Accountants

Montreal, Canada
April 5, 2024

STATEMENT BY MANAGEMENT OF DEVOLUTIONS INC.

Statement by Management of Devolutions Inc.

We are responsible for designing, implementing, operating, and maintaining effective controls within Devolutions Inc's (Devolutions) Hub system (the System) throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that Devolutions' service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in our attachment A – Devolution's Overview Services and the Hub System (Attachment A) and identifies the aspects of the System covered by our Statement.

Devolutions' uses a subservice organization identified in our Attachment C – Devolutions' Complementary Subservice Organization Controls (Attachment C). Our Attachment C indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Devolutions, to achieve Devolutions' service commitments and system requirements based on the applicable trust services criteria. Our Attachment C presents the types of complementary subservice organization controls assumed in the design of Devolutions' controls.

Our Attachment D – Devolutions' Complementary User Entity Controls (Attachment D) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Devolutions, to achieve Devolutions' service commitments and system requirements based on the applicable trust services criteria. Our Attachment D presents the complementary user entity controls assumed in the design of Devolutions' System

We have performed an evaluation of the suitability of the design and operating effectiveness of the controls within the System throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Devolutions' service commitments and system requirements were achieved based on the applicable trust services criteria. Devolutions' 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 our Attachment B – Principal Service Commitments and System Requirements (Attachment B).

We confirm that the controls within the System were suitably designed and operating effectively throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Devolutions' service commitments and system requirements were achieved based on the applicable trust services criteria.

David Hervieux,
President and CEO
April 5, 2024

ATTACHMENT A
DEVOLUTIONS' OVERVIEW OF SERVICES AND THE HUB SYSTEM

Overview of Devolutions

Founded in 2010 and located in Lavaltrie, Canada, Devolutions is a 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 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 Remote Desktop Manager, Hub Business, Hub Personal, Devolutions Server, Devolutions Gateway 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' Hub system (System) for the period of January 1, 2023, to December 31, 2023. The three main components of the System are the Lucid component, used solely for authentication, the Hub Business component that allows customers and administrators to access and manage vaults, and Hub Personal component that offers single user credential storage services.

Lucid Component

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

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.

Hub Personal Component

This component is a secure and cloud-based password manager for individuals. It is based on the same technologies as the 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.

Companion tools

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

System Components

Infrastructure

The System uses Microsoft Azure (Azure) Platform-as-a-Service (PaaS) to deliver a robust and secure cloud-based solution for customers.

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 Application Services; and
- 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.

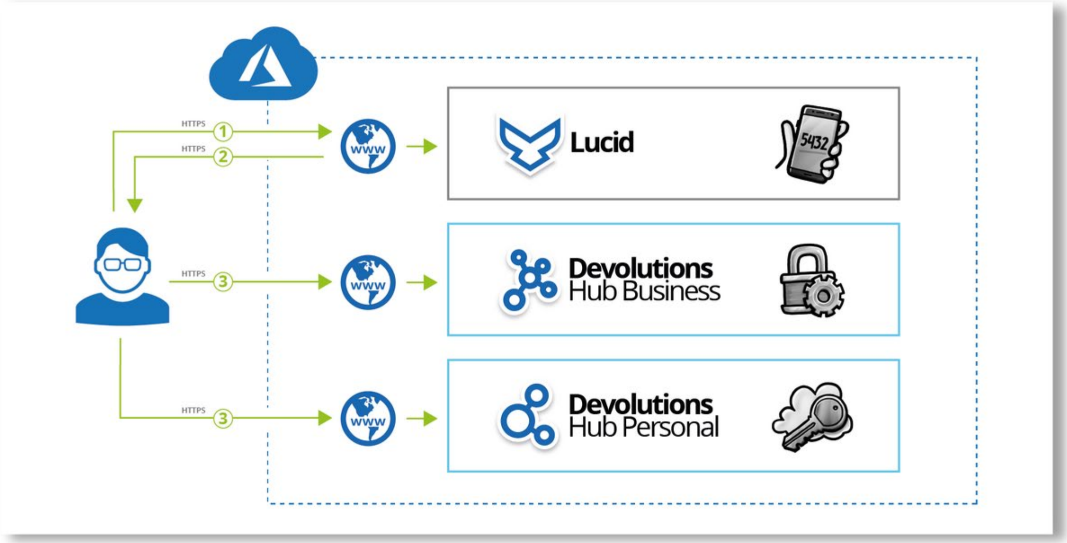

Diagram 1 - Password Hub Architecture Overview

Software

Both Hub Business and 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 activates the subscription and provides full administrative access to the logical instance (also called “Organization”) that 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 Hub Business or 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 that 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 Hub component (Diagram 1 Flow 3). Hub Business and 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. This access is granted as long as the session is valid and active.

Devolutions also uses various software applications to support the system, including:

- A ticket management application used for change management, work order, and bug tracking; and
- Corporate application for HR, internal messaging, project management etc.

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 the strategic and tactical sectors of the System’s information security;
- **Director of Legal affairs, Risk and Privacy** owns all legal, risk and privacy practices within the organization including their integration through all System components, development, deployment and usage;
- **Director of Development** is responsible for organizing, planning and tracking the software development lifecycle (SDLC) according to Devolutions and industry standards;
- **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 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. The person approves and prioritizes development tasks and determines the development schedule;

- **Development Team** is responsible for the development of system. 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 the intended behaviour. Any gaps identified are 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 the Cloud Operations Team on security incidents as well as every other function to provide the best level of security for the System; and
- **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.

Processes and 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.

A comprehensive set of policies and procedures have been put in place by Devolutions which cover the following topics:

Information Security

- Risk Management;
- Information Security;
- Data Classification and Destruction;
- Password Management;
- Cryptography;
- Access Control;
- Incident Management;
- Vulnerability Management;
- Backups Management; and
- Security Awareness & Training.

Human Resources

- Code of Ethics;
- Human Resources; and
- Security Controls.

Development

- Software Development Lifecycle (SDLC); and
- Change Management.

Policies, plans and directives are made available to personnel on the Devolutions' internal knowledge base platform. Policies and plans are reviewed and approved on a regular basis by appropriate stakeholders, before being communicated to personnel. Security processes are updated as required and communicated to relevant personnel.

Data

Data relating to the System constitutes the following:

Customer data

- Hub Business and Hub Personal manage the customer data related to vaults, entries, credentials, documents, and configurations; and
- Lucid manages 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
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Principal 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/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. 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.

In the context of the present report, Devolutions' security commitments are to deploy and manage security measures in order to help protect the system from unauthorized physical and logical access.

ATTACHMENT C
COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Complementary Subservice Organization Controls

Devolutions uses a subservice organization, Microsoft Azure, to provide PaaS and IaaS hosting.

This table below describes the subservice organization and the types of controls Devolutions assumed to be in place at Microsoft Azure when designing their control set.

Subservice organization (carved out)	Services Provided / Complementary Subservices Organization Controls
Microsoft (Azure)	Microsoft Azure is responsible for providing, operating, maintaining and protecting the platform and infrastructure that runs the HUB system in the Azure Cloud environment. This platform and infrastructure are composed of the hardware, software, networking, and facilities that run Azure Cloud services. Azure is responsible for: • Protecting logical access credentials; • Installing, configuring, and managing physical and virtualized infrastructure; • Maintaining the logical separation of Devolutions' deployments and data from those of other customers; • Encrypting data at rest and in flight; • Protecting stored encryption keys; • Physical security for data centers in which the services are hosted; • Destroying physical data storage assets securely; • Security event detection and reporting; • Vulnerability compliance monitoring and reporting; • Automated database & storage account backup; • Geographic separation for cloud hosting regions; and • Developer Operations console and related workflows.

ATTACHMENT D
COMPLEMENTARY USER ENTITY CONTROLS

Complementary User Entity Controls

The Devolutions' processes and controls are designed under the assumption that certain controls will be implemented by it clients ("user entities"). The complementary user entity controls presented below should not be regarded as a comprehensive list of the controls that should be employed by user entities.

Complementary User Entity Controls
Customers' access to Hub is restricted to authorized personnel, usernames and passwords are kept confidential, strong passwords are used, and access is revoked promptly upon users leaving the user entity.
Users immediately notify Devolutions' customer service of any suspected or confirmed System abuse, unauthorized use or access, system vulnerability or security incident.
Customer account management is managed by the customer and the customer is the only party responsible for the user's account management and configurations.

Devolutions