DSB Information Security

Frequently Asked Questions

Author: Derivatives Service Bureau
Date: 14 October 2017
Version: **1.1**

Contents

Preface

Change History

Date	Change	Version	Author	Revision Details
21 Sept 2017	Creation	1.0	Inder Rana	
14 Oct 2017	Addition	1.1	Inder Rana	Additional questions added

1 Introduction

1.1 Document Purpose

The purpose of this document is to detail the frequently asked questions and the corresponding answers posed by the industry. The purpose of this document is to provide clarity and enhance the already published DSB Information Security Document. We will periodically incorporate the items

1.2 Background

The DSB's core service is to provide ISINs for OTC derivatives. In January 2017, the DSB published a Technical & Operations Consultation paper. The responses received allowed the DSB to create an Information Security Policy in a form that would be useful to the Industry.

Since publishing the Policy the DSB has received further questions around the Information Security Policy. This document aims to answer those questions and will be a "living" document, updated as the DSB receive more requests for information. This document will be place on GitHub where is can be tracked by the Industry.

2 Frequently Asked Questions

2.1 Will/Does the Vendor utilise any Subcontractor(s) to provide the product(s) or service(s)?

There are two sub-contractors contracted to the Derivative Service Bureau. These being;

Contractor Name	Address	Service Provided
EtradingSoftware Ltd	City Tower 40 Basinghall St London EC2V 5DE	The Managed Service Provider to the DSB. Reporting to the DBS Board and liaising with the SPP for infrastructure operations functions.
Datapipe UK	East One 20-22 Commercial St, London E1 6LP, UK	Provides Infrastructure procurement and monitoring for the DSB.

2.2 How many Vendor employees are involved in providing the product(s) or service(s) dedicated to a Single Client?

There are no staff dedicated to servicing individual customers.

2.3 How many staff will be providing the service and where are they located.

Contractor Name	Location	Staff Number
Etradingsoftware LTD	UK & Philippines	Less than 20 in each location
Datapipe UK	UK, NA, Asia	355 worldwide

2.4 Where are the services hosted?

The infrastructure is designed as high availability and hosted in AWS cloud with the primary service located in EU-WEST-1 and the secondary US-EAST-1. The service is managed out of London and the Philippines.

2.5 Can the DSB be classified as a software service

Yes

2.6 Who does the DSB sub-contract to?

EtradingSoftware (MSP)

Datapipe (SPP) -> Amazon Web Services

2.7 Does the-DSB perform an ethical hack on the web interfaces?

Yes – Penetration testing

2.8 Can we see a copy of the report?

A formal request to see this information is required by the client

2.9 Which company performs the assessment?

GDS

2.10 How are passwords protected at rest?

Database stored with Hash values - PBKDF2 (Password-Based Key Derivation Function 2) is used

2.11 Which TLS cipher suites are used?

The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with P-256 (a strong key exchange), and AES_128_GCM (a strong cipher).

2.12 How is the DSB going to ensure connectivity is only from the user's network?

Security groups and dedicated port assignments for each user

2.13 What two-factor authentication method is being used and when?

RSA Tokens for all support staff when accessing BES servers & Bastion hosts

2.14 What does the-DSB mean by dedicated private stack in AWS?

Dedicated environment within AWS, separate instances of both hardware and software with synchronization back to shared hardware.

- Designed specifically for end users with a requirement for higher throughput rates + lower and/or consistent latency
- Offers enterprise users a level of insulation from performance of the shared infrastructure
- -The DSB facilitates release management
- No change to connectivity APIs
- The private stack is scalable & configurable – calibrated for the user's performance expectations

2.15 How are private keys stored?

Private keys are only available to the services that need them, or are stored in the Keepass database (for administrator access). Private keys/encryption keys used by the system itself (e.g S3, volume encryption, etc) are stored in Amazon Web Services' Key Management Service (KMS). As per documentation from AWS, the FIPS certification level is being evaluated for FIPS 140-2..

2.16 Is data encrypted in motion internally?

For frontend services, we encrypt data in motion via the use of HTTPS. For backend services, the principle is data is only decrypted on the device itself. For this we heavily use file encryption.

2.17 Has DSB done a security assessment of Amazon, can they share their findings?

Datapipe and AWS presented a combined proposal during the RFP phase. Datapipe is providing the managed service over AWS, an assessment was completed, but all vendor risk assessments are considered sensitive and proprietary in nature and are not provided to clients

2.18 How will DSB oversee AWS compliance with their security policy?

These protections are all to the overall master service vendor agreement in place with DP & Amazon.

2.19 What is the breakdown of security related responsibilities between DSB, Amazon and DSB Clients.

Infrastructure -> Datapipe (intrusion detection, virus checking, etc..)
Application stack -> DSB over the Datapipe managed service

2.20 Has a business continuity / disaster recovery plan been completed and tested, and what is the frequency of recurring tests going to be?

DR has been completed and tested. Frequency will be once a year for DR testing
3 Active Availability Zones (AZ's) in each region. Platform can operate on 2 Active. In the event of two AZ failure, regional DR is invoked

2.21 How is the user expected to comply with "Section 3.4b notes the User's responsibility for the installation and proper use of virus detection/scanning program. " considering the hosting is on AWS?

This is in relation to the client side infrastructure and the responsibility of the client to keep AV and intrusion detection up to date.

2.22 Who are Datapipe and eTrading and what is the relationship with them?

eTrading is a professional management services company contracted by the DSB board to run the DSB. Datapipe are contracted to the DSB and support and maintain the infrastructure including connectivity and networking

2.23 Datapipe maintains SOC 1, SOC 2, ISO 27001, FedRAMP, FISMA, PCI, and HITRUST compliance and security standards." Will the reports be made available to DSB's clients?

Yes, with an NDA in place, these documents will be made available to clients: SOC 1 & SOC 2 reports, ISO 27001 certificate, PCI ROC/AOC, and HITRUST myCSF report. We have internal policies that can be shared as well. Information concerning FedRAMP is only provided to Datapipe Government Solutions clients.

2.24 Generally which security assessments, reports, evaluations will be shared with clients? Clients may need to perform security assessments of the vendor on an ongoing basis, what transparency will be provided to facilitate that?

Information made available upon formal request. The DSB guaranties maintenance of the info sec policy and any additional information required by clients will be handled over mail

2.25 When DSB refers to PII (personally identifiable information), what are they referring to?

Contact information, user names, email address and client support contact information

2.26 How is Data leakage going to be managed?

Security alerts, monitoring, client communication. 2-factor authentication, can correlate logs to user access. Logs are monitored.

2.27 How will the destruction of devices be managed? How will our data be destroyed?

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800 - 88 ("Guidelines for Media Sanitization") as part of the decommissioning process.

Ref AWS Security White Paper:
https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

Keep data forever, unless not required. i.e. no maximum retention policy, only a minimum retention policy.

2.28 How and where will backups be managed?

For backups, encrypted EBS Volumes are snapshotted and storage in S3. Amazon EBS encryption handles key management. Each newly created volume is encrypted with a unique 256-bit key. Any snapshots of this volume and any subsequent volumes created from those snapshots also share that key. These keys are protected by AWS key management infrastructure, which implements strong logical and physical security controls to prevent unauthorized access. Data and associated keys are encrypted using the industry standard AES-256 algorithm.

2.29 Does Amazon have remote access to the applications and data (including encryption keys)?

No

2.30 How are logs protected from privileged users?

Segregation of duties, and 2-factor authentication

2.31 There is a one business day SLA for data breaches, why can't this be 24 hours? Will the DSB inform us of any other security events (e.g. DDOS attacks that may impact performance of our access)?

Yes, any material breach or downtime of services will be communicated to clients.