Information Security Practises

AZURE APPENDIX

cegid

CONTENTS

1. Document version

Version	Date de publication
PAS_CEGID_SAAS_ANNEXE_AZURE_V201711	03 novembre 2017
PAS_CEGID_SAAS_ANNEXE_AZURE_V201802	02 février 2018
PAS_CEGID_SAAS_ANNEXE_AZURE_V201909	30 September 2019

2. Introduction

2.1 Purpose

This appendix to the ISP describes the data security commitments made by Cegid on the services operated on the Microsoft Azure platform.

2.2 Scope

This appendix only applies to the cloud elements of the Microsoft Azure platform which Cegid has integrated to deliver the application services selected by the Client in a secure and optimal way.

Cegid's Cloud Factory considers Azure as a critical supplier.

2.3 Definitions

ISO: International Organization for Standardization, whose purpose is to produce international standards in industrial and commercial fields

CSA STAR Certification: Certification by the 'Cloud Security Alliance' which combines the ISO 27001 certification and the Cloud Control Matrix

Microsoft Azure : The Microsoft Azure platform corresponds to the public cloud IT services such as Microsoft's PaaS and IaaS

SAN : Storage Area Network

2.4 Reference documents

I.S.P : Information Security Practises – Basic document describing the security policy implemented by Cegid for providing application services to its clients

Terms of Service : Document describing the specific conditions related to each of Cegid's SaaS services. These are available on www.cegid.com, Cegid's website

3. Certifications for the Microsoft Azure platform

Microsoft Azure holds a wide range of ISO and CSA certifications in order to have a highly comprehensive coverage of conformities.

A combination of these certifications on the Azure platform is effective and provides compliance with a large range of regulatory obligations.

The CSA STAR certification records can be viewed on:
https://cloudsecurityalliance.org/star-registrant/microsoft/

The ISO reports and associated certificates can be downloaded here:
https://servicetrust.microsoft.com/Documents/ComplianceReports

4. Presentation of Azure's security

To operate its client services on the Microsoft Azure platform, Cegid refers to Microsoft's experience and expertise.

Azure offers various security mechanisms to facilitate management and monitoring of cloud services and Azure's virtual machines.

Security of Microsoft Cloud's services is a collaborative effort and liability is shared between Cegid and Microsoft. Shared liability means that Microsoft is liable for Microsoft Azure and the physical integrity of its data centers (by using protection measures such secure doors, via badges, fences and guards). In addition, Azure provides high levels of cloud security on the software level, meeting Cegid's demanding requirements in terms of security, confidentiality and compliance.

Microsoft follows 10 main security principles which use the best security technology.

Details of these 10 principles can be found on: https://docs.microsoft.com/fr-fr/azure/security/azure-security

Cegid applies these baseline principles to the scope concerned by its business, i.e.:

- ✓ Network security
- ✓ Database security
- ✓ Storage security
- ✓ Operational security

These principles are applied in order to guarantee availability, integrity and confidentiality for data and client applications, but also compliance with best practices of Cegid's teams responsible for operating and releasing these applications.

4.1 Network security

Network security is focussed on the following points:

- Networking and architecture
  - Cegid builds different flexible architectures and customised to the applications of specific clients. These architectures are based on subnetting of the Azure virtual network and setting up DMZs.
  - In addition to Microsoft's native security, Cegid implements a level 7 firewall brick with IDS/IPS option.
- Controlling network access
  - Setting up a NSG (Network Security Group) gives full control of the different access to the different network components.
- Remote access and connectivity
  - The Express Route protocol is used to connect the different subscriptions.
  - UDR (User Defined Roads), Load Balancer and Application Gateway redirect the inflows to security bricks (Virtual Security Appliance)
  - The SaaS Production teams administer the solution via Express Route via an MPLS provider

4.2 Database security

Cegid used the main standards provided by Microsoft Azure, i.e.:

- The TLS/SSL protocol for the connection/authentication processes and for managing data in transit.
- Two encryption techniques can be implemented depending on the offers and architectures, i.e.:

  - PaaS offer: transparent encryption of the SQL database (TDE) by performing real-time encryption and decryption using a symmetric key called the database encryption key. This key is protected by an integrated server certificate. This certificate is unique for each SQL database server. These keys are stored in a digital safe with restricted access.
  - IaaS offer: direct encryption of the SAN envelope (storage area) without the need for an encryption key

4.3 Storage security

Cegid uses the following Azure bricks in order to administer the Azure platform.

- File Share and Blob Storage (storage and encrypted transport environment) for storing operating files (logs, scripts, etc.).
- RBAC (Role-Based Access Control) which secures the user account database of Cegid’s SaaS Production teams.
- VM Managed Disk Encryption

4.4 Operational security

Cegid uses the following Azure services:

- Azure Security Center: Prevention, detection and resolution of threats
- Azure monitor : Service monitoring tool
- Azure Network Watcher : Monitoring and diagnostics for the Azure network
- NSG : traffic flow and analysis
- Implementation of key vault (digital safe) for the storage of operational security elements (script passwords, etc.)

5. SPECIFIC OPERATIONAL ISSUES

5.1 Localisation

Cegid uses the following infrastructure of the Microsoft Azure Public Cloud: https://azure.microsoft.com/fr-fr/regions/

Data localisation may be defined contractually with the client (assigning a POD).

Description for access data process is describe at:

https://www.microsoft.com/fr-fr/trustcenter/privacy/who-can-access-your-data-and-on-what-terms

5.2 BCP & Resilience of SaaS services

As part of the Cegid Azure Cloud offerings, the implementation of the business continuity plan, defined in the Cegid ISP, is based in particular on the principles and mechanisms below.

From a technical point of view, the resilience of Cegid Azure Cloud solutions is based* on:

- Network load balancing mechanism (see Azure Load Balancer)
- Application load balancing mechanism (see Azure Application Gateway)
- High availability and scalability mechanism (see Azure Virtual Machine ScaleSet)
- High availability mechanisms (see Azure AvailabilitySet or Availability Zone depending on the offers)
- High availability of backup mechanism (see Azure Recovery Site and DPM)
- Multiple and distributed instances of application servers, firewalls / IPDS

** Please refer to the architecture documents of the corresponding business offerings*

The security and resiliency governance is based on the best practices defined by Microsoft Azure..

- https://docs.microsoft.com/en-gb/azure/best-practices-network-security

The SLAs of the corresponding services are accessible here:

- https://azure.microsoft.com/en-us/support/legal/sla/?v=17.42