

Sort Services B.V.

Key Technical setup and essential
components

Table of contents

1. INTRODUCTION	1
2. TECHNOLOGICAL ARCHITECTURE AND LOCATION OF INFRASTRUCTURE	1
2.1. SIMPLIFIED NETWORK DIAGRAM AND LOCATION	1
2.2. TECHNOLOGICAL INFRASTRUCTURE DATA CENTERS 1 & 2	1
2.3. NETWORK INFRASTRUCTURE	4
2.4. TECHNICAL SETUP RISK ASSESSMENT REPORT	7
3. APPLICATION ARCHITECTURE	7
3.1. GAMING ACCOUNT MANAGEMENT SYSTEM ARCHITECTURE	8
3.2. CUSTOMER FRONT-END WEBSERVER ARCHITECTURE	9
4. DATA ARCHITECTURE	10
5. SPECIFICATION OF THE RNG SYSTEM	ERROR! BOOKMARK NOT DEFINED.
6. SPECIFICATION OF INTEGRATION WITH PAYMENT GATEWAYS	10
6.1. BANK TRANSFERS	10
6.2. CREDIT CARDS	11
APPENDIX 1: SUMMARY OF THE APPLICATION SYSTEM.....	ERROR! BOOKMARK NOT DEFINED.

1. Introduction

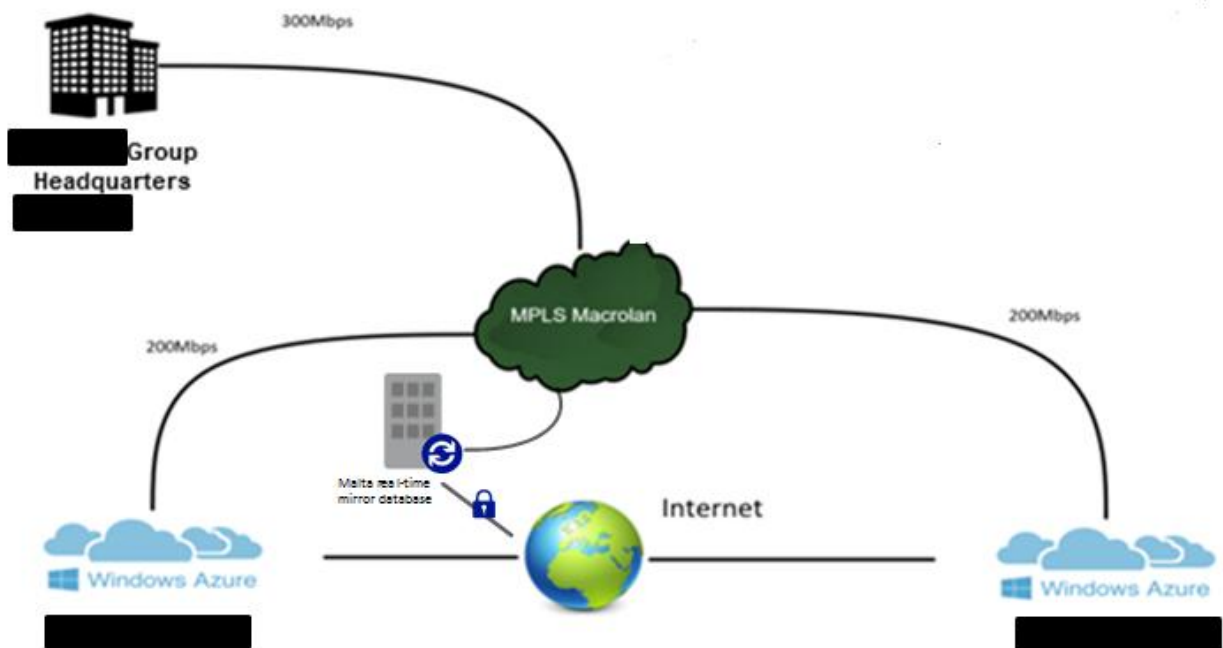
Sort Services's Gaming System is the group of systems, hardware, software, networks, databases, and other technical infrastructure used by the Company to provide the services necessary for the development, organization and operation through the internet of the Online Gaming System.

Sort Services's Gaming System consists of a self-developed system by the renowned software provider Anakatech for the Management of the Gaming Account and final user web front-end and also integrates the services of other B2B Gaming platforms.

2. Technological architecture and location of infrastructure

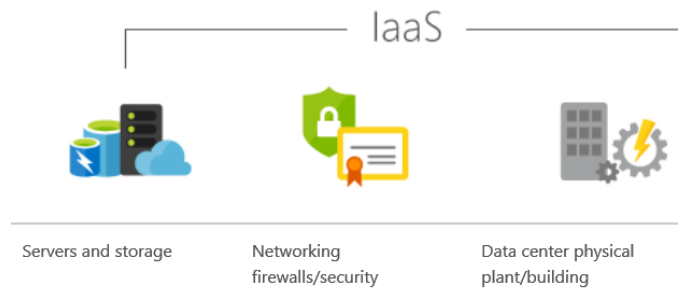
2.1. Simplified network diagram and location

The following image shows a simplified network diagram showing all the different geographical locations where the online gaming system is operated:



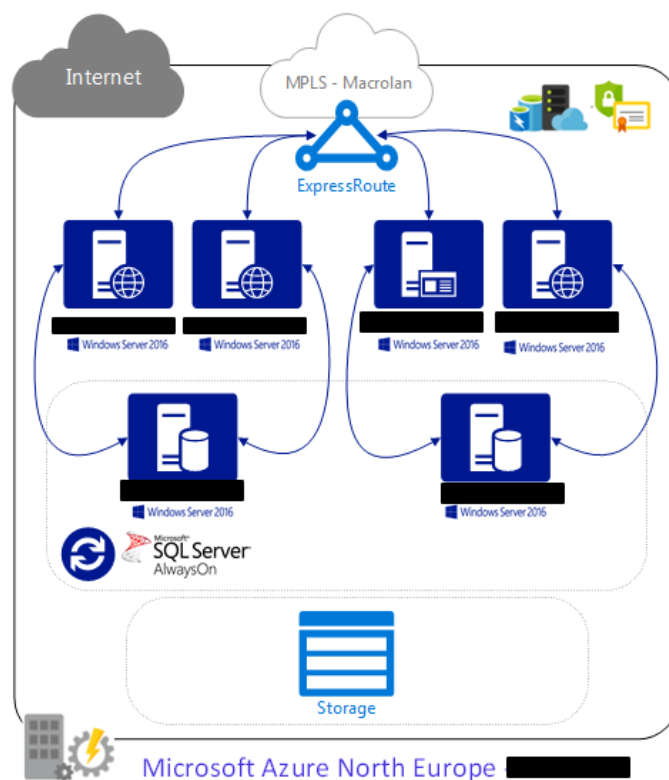
2.2. Technological infrastructure Data Centers 1 & 2

Data Centers 1 and 2 are located Curacao, based on an Infrastructure as Service agreement:



Both datacenters together form a high availability group, with replicated services and databases.

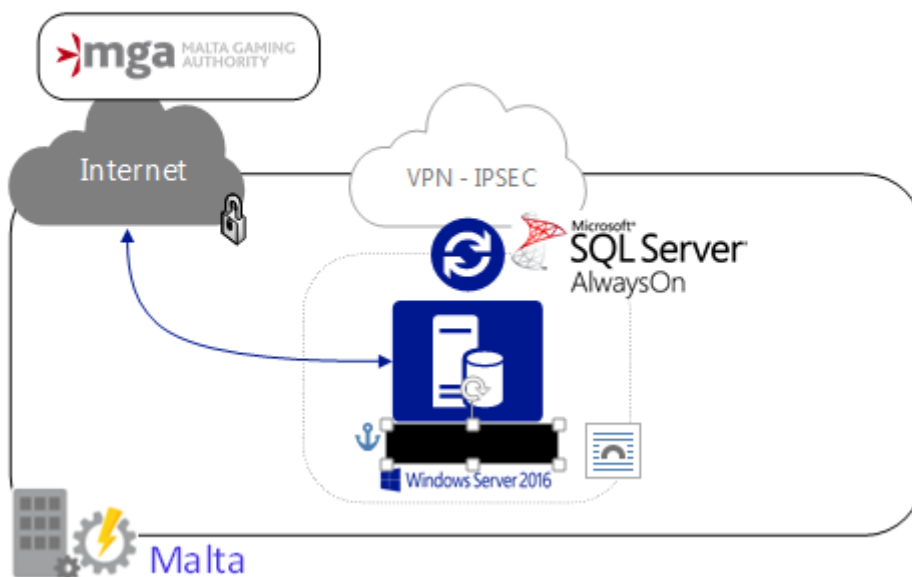
Real time replication of databases is done through the SQLServer 2016 AlwaysOn features.



Host Server Name	Function	Operatig System	Internal IP
xx	Web server 1	Windows 2016 Datacenter	xx
xx	Web server 2	Windows 2016 Datacenter	xx
xx	DB Server	Windows 2016 Datacenter	xx
xx	App Server	Windows 2016 Datacenter	xx
xx	DB Server	Windows 2016 Datacenter	xx
xx	Web server Online	Windows 2016 Datacenter	xx

External Web Server Sort Services-ip: Sort Servicesxx

Technological infrastructure Data Center 3 is a real-time mirror database.



Frequency of database log shipping is set to 30 seconds, meaning that incremental database backups are being created, sent, and restored on the remote site with that frequency. The infrastructure will, under normal conditions, be able to replicate key live system databases with a maximum lag of less than 2 minutes, as shown on the below screenshot. Threshold for alerts being sent to support team has been established at 15 minutes, meaning that if due to any extraordinary circumstances, logshipping latency is above that threshold, the support team would be alerted immediately.

Status	Primary Database -- Secondary Database	Backup			Copy	Restore				Last Bac
		Time Since Last	Threshold	Alert Enabled	Time Since Last	Time Since Last	Latency of Last File	Threshold	Alert Enabled	
Good						0 min	0 min	15 min	True	
Good						1 min	0 min	15 min	True	
Good						0 min	0 min	15 min	True	
Good						2 min	0 min	15 min	True	
Good						2 min	0 min	15 min	True	
Good						1 min	0 min	15 min	True	

Physical Database Server:

NS-HD85128 - Dell PowerEdge R620

Label name: xxxxx

Serial Number: xxxxx

IP Address: xxxxx

Network name: xxxxx xx

SQL Server version: 2016

RAM: 128 Gb

CPU: 2 Cores Intel Xeon

Storage 1: 4 x 1,6 Tb Raid 10

Storage 2: 8 x 1, Tb Raid 10

Physical firewall server:

Hardware Firewall - Dell PowerEdge R410

Label name: xxxxx

Serial Number: xxxxx

Firewall software: PFSense

Version/Model: PFSense 2.4.4

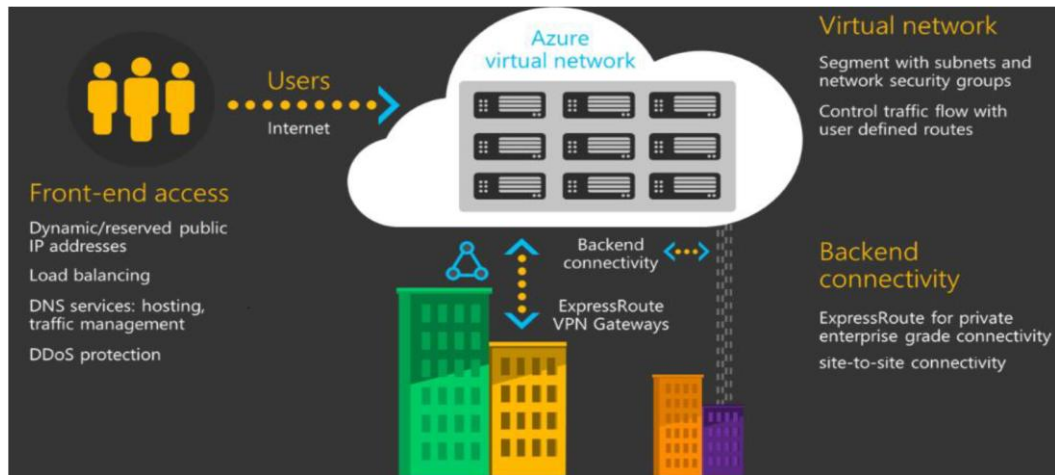
RAM: 8 Gb

CPU: 12 cores

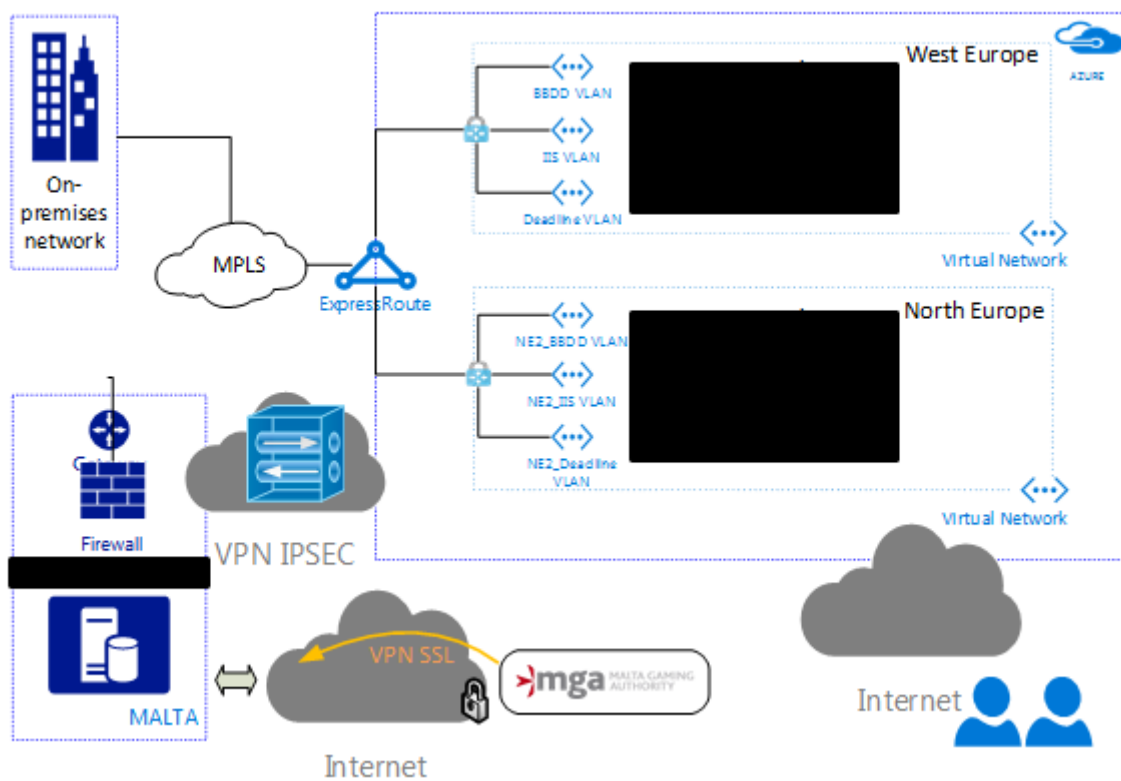
IP Address: Sort ServicesSort Services

2.3. Network infrastructure

Microsoft Azure includes a robust network infrastructure to support service connectivity requirements. Network connectivity is possible between resources located in Azure, between on-premises and Azure-hosted resources, and to and from the internet and Azure. The following diagram illustrates this infrastructure:



The Azure network infrastructure allows to securely connect Azure resources to each other by using virtual networks. A virtual network is a representation of a private network in the cloud, a dedicated logical isolation of the Azure cloud network.



FIREWALL

Serial number: xxxx

IP Address: xxxxx

Brand: PFSense

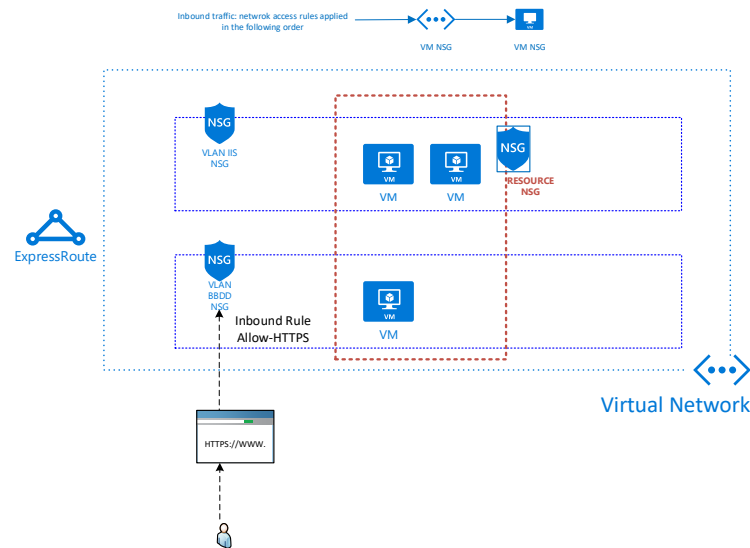
Model: PFSense 2.4.4

Memory: 8 Gb

CPU: 12 Cores

Virtual networks communicate with each other without going outside the Microsoft Enterprise Edge (MSEE) router. The worldwide Microsoft backbone is used to connect both virtual networks together. This network-to-network traffic between different Microsoft Azure datacenters (North and West Europe) uses the same ExpressRoute circuit.

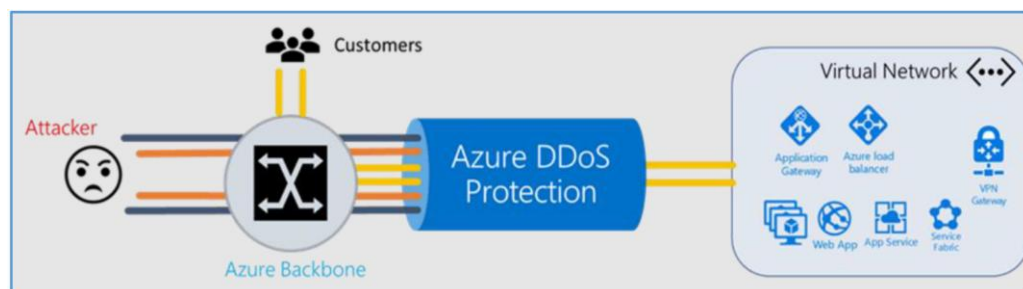
Azure supports dedicated WAN link connectivity between Sort Services's corporate MPLS network and an Azure virtual network with ExpressRoute. The link between Azure and Sort Services's corporate MPLS does not go over the public internet. ExpressRoute connections offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the internet.



Within each virtual network, segmentation and traffic filtering is achieved through configuration of Network Security Groups. Each NSG contains multiple inbound and outbound security rules that are used to filter traffic by source and destination IP address, port, and protocol.

Azure DDoS protection, combined with application design best practices, provide defense against DDoS attacks. Azure DDoS protection provides a basic service tier automatically enabled as part of the Azure platform. Always-on traffic monitoring, and real-time mitigation of common network-level attacks, provide the same defenses utilized by Microsoft's online services. The entire scale of Azure's global network can be used to distribute and mitigate attack traffic across regions. Protection is provided for IPv4 and IPv6 Azure public IP addresses.

The following diagram shows how Azure DDoS protection works:



Azure Load Balancer delivers high availability and network performance to internet facing applications. It's a Layer 4 (TCP, UDP) load balancer that distributes incoming traffic among healthy instances of services defined in a load-balanced set.

2.4. Technical Setup Risk Assessment report

As part of the Information Security Management System in place on the scope of all online gaming system managed by Sort Services, an information security risk assessment is done and reviewed at least yearly, and a risk treatment process is followed, all in accordance with ISO 27001:2013 standards.

Before the introduction of the Cloud technical Setup that will be used to provide remote gaming services under the Curacao jurisdiction, a review of that analysis has been performed, basically assessing new potential risks that the operation of a gaming system which, with a similar setup, is already in production on non-cloud premises. Therefore, the risk analysis report performs an assessment of the new potential risks introduced by the usage of a Cloud Setup. For every new risk assessed determined as unacceptable, new security controls were introduced to mitigate those risks.

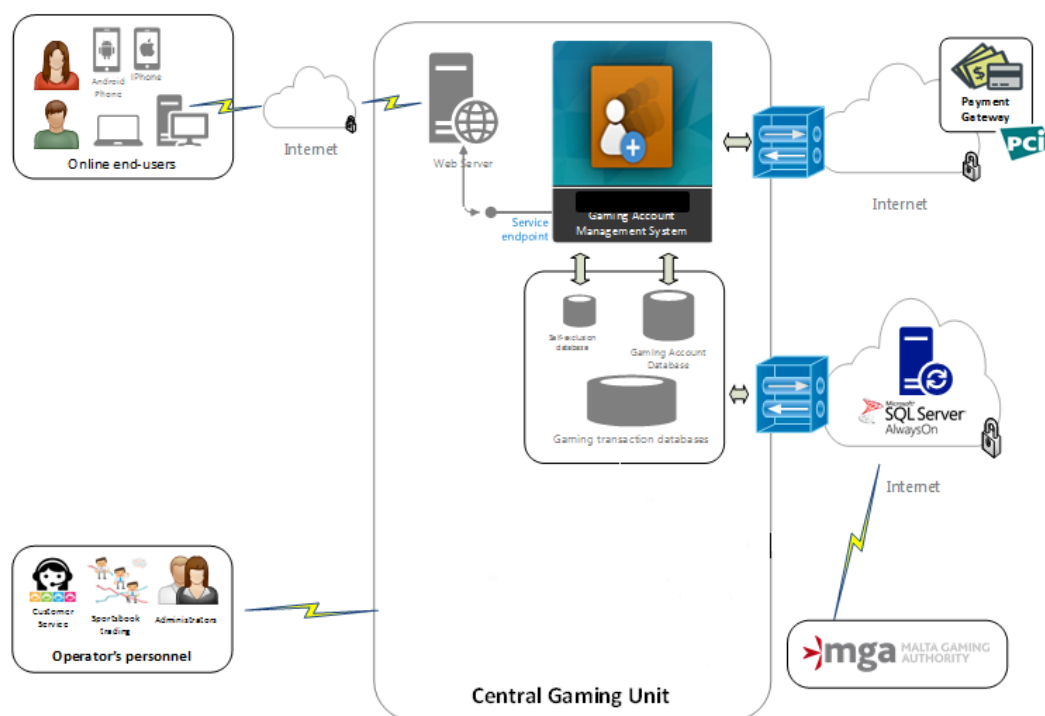
Complete risk assessment report is attached as a separate document.

3. Application architecture

The basic elements of SORT SERVICES's Gaming System are:

- A) Central Gaming Unit. Is the group of Technical elements allowing the operation of online gaming. Has two main groups of components:
 - a. Gaming platforms. Is the group of technical gaming platforms which allow registration, storage, processing and management of the gaming transactions performed by end users. Each platform incorporates all the logic of the games included on it, and stores a user identifier, dissociated from the user's personal information, necessary for gaming transaction management.
 - b. Gaming Account Management System. Is the group of technical elements allowing full identification and storage of all gaming account activity related to the user. Manages and stores all information related to the user profile and the funds deposited on the corresponding gaming account. Maintains an interface with each of the Gaming Platforms, allowing using the available funds to participate on its games, and recover all winnings or reimbursements resulting from gaming transactions, if any. It also manages the interface to all payment gateways for all payment methods used for deposits and withdrawals to/from the gaming account.
- B) Web front-end. Is the group of interfaces allowing access to the gaming account and games through the internet, using a Web Browser, from an end-user-owned device (personal computer, smartphones, iPads, etc.)
- C) Payment Gateway. Is the group of components allowing fund deposits and withdrawals on gaming accounts, using authorised payment means, and managing the technical interfaces to the financial entities providing such payment methods.
- D) Self-exclusion database. Keeps the information on all end-users who have themselves excluded from gaming. It is shown here as an independent component, even though technically it's management is done by the software components of the Gaming Account Management System.

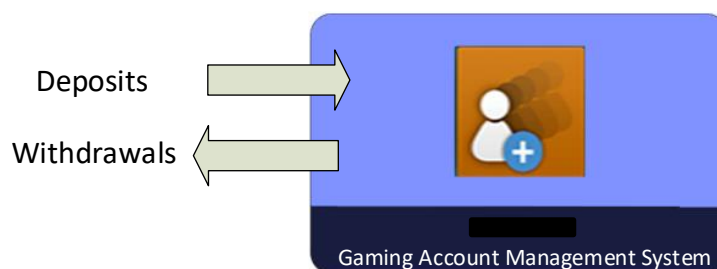
Next image shows a simplified software architecture of the Gaming System to be used by Sort Services for the provision of online gaming services:



Interactive online channel

The Central Gaming Unit provides access through the internet, using most common personal devices, with a differentiated interface for personal computers, optimized for the most common web browsers; and another one for intelligent mobile devices (smartphones and tablets) of most common operating systems (Android, iOS, Windows Phone). All connections between web clients and web server are done through secure channels using SSL certificates with 4096 bit RSA keys.

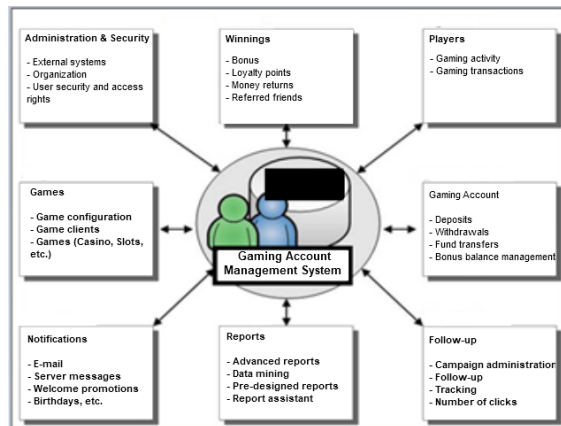
The customer can, at any moment, make fund deposits and withdrawals to/from his gaming account, using any of the available payment methods.



3.1. Gaming Account Management System architecture

The architecture of this component is based on the standard Microsoft CRM tool, extended for management of gaming accounts and the integration of all the different gaming platforms.

The following image shows the main functions performed by Account Management System:



Present Microsoft Dynamics CRM version is:

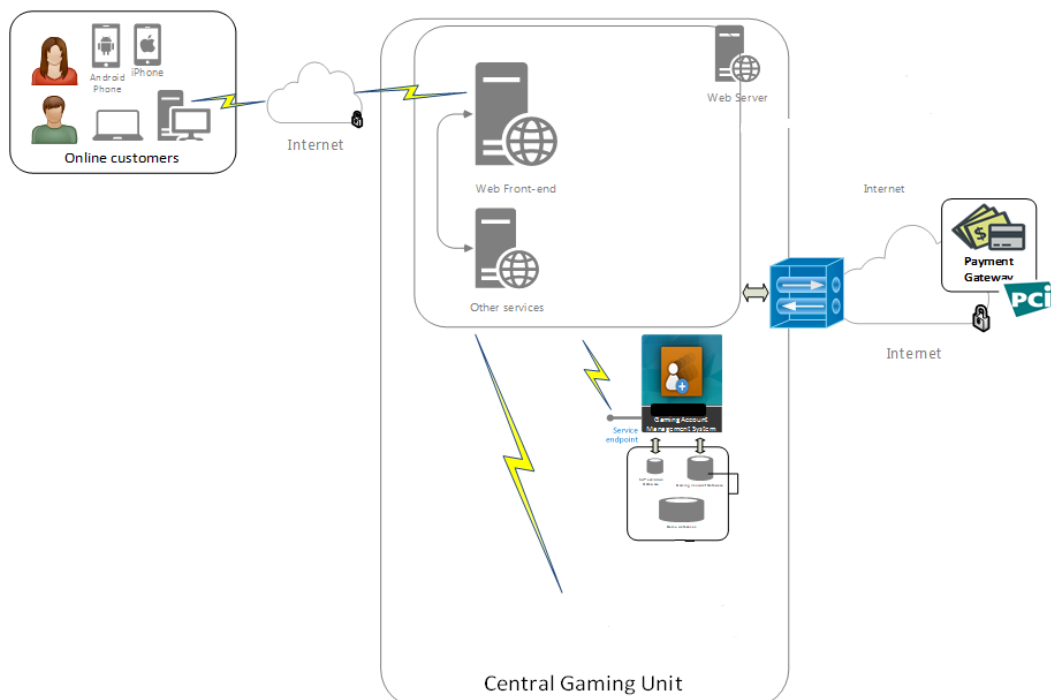


3.2. Customer front-end Webserver architecture

The WebServer servicing the online channel consists of three major components:

- Web Front-end. Provides the presentation layer for all customer web applications.
- Event information concentrator. Concentrates and manages all information on real events coming from the SBS Service, and distributes it to all the different user session opened through the web front-end.
- Other services: Session Management, Payment Gateway Management, etc.

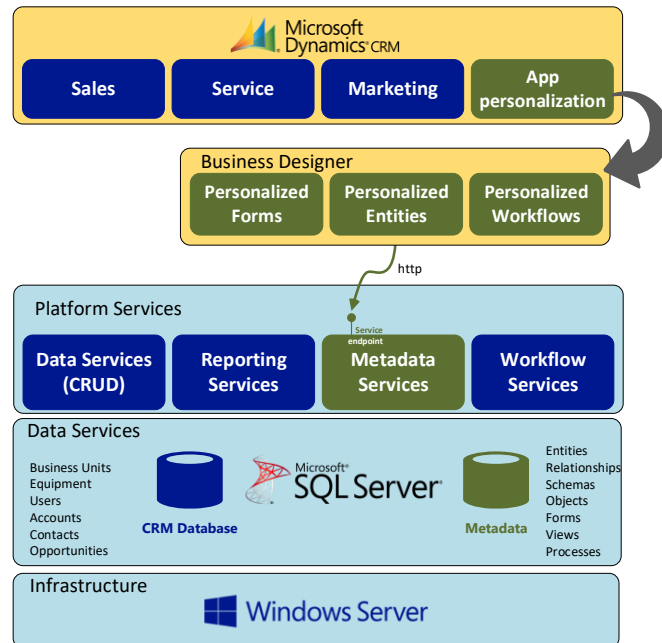
The following image shown the main functions of this Web Server and its relationship to other components of the Central Gaming Unit:



4. Data architecture

The data architecture of Sort Services gaming system is based on the data architecture of the underlying Microsoft Dynamics CRM data architecture.

The adaptation of Microsoft Dynamics CRM for the Management of gaming account has been done through the standard extension mechanisms provided by the tool and shown on the following image:



Through the Business Designer, all entities, relationships, schemas, objects, forms, views and processes have been created, extending the base system for the Management of gaming accounts, and the metadata necessary for integration with other gaming platforms.

5. Specification of integration with Payment Gateways

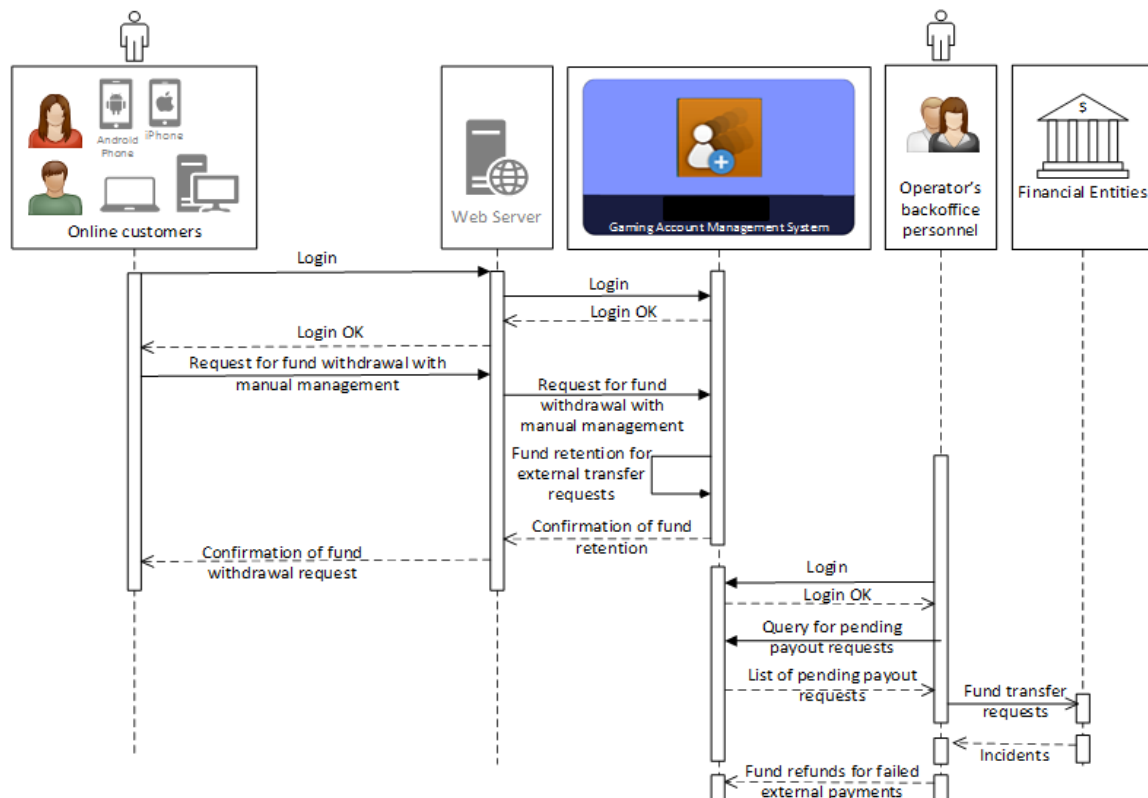
The Gaming System will initially integrate three payment methods to allow customer deposits/withdrawals on their gaming accounts:

- 1) Fund withdrawal through bank transfers to regular banking accounts.
- 2) Fund deposits through debit and credit cards.

Each of the payment methods is integrated with the Gaming Account Management System using a different approach, as follows.

5.1. Bank transfers

Bank transfers are requested to the Operator's financial entity manually. The Gaming System facilitates this through backoffice tools, as the following image summarizes:



5.2. Credit Cards

For credit card deposits the system integrates a Payment Gateway, completely externalized with a PCI DSS homologated provider, **TTT**. Neither the B2B gaming services provider, nor the B2C gaming licensee store, process or sends any credit/debit card information.

All elements of the payment web pages sent to the customer's web browser are sourced exclusively by **TTT**.

The following image shows a simplified diagram of this type of payments:

