

**Mastercard PrePaid Management Services (MPMS)**

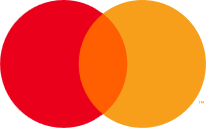
**FIS Payments One Card Processing Platform (P1C)**

**Solution Architecture Specification**

**Solution Definition – Hardware, Software, Configuration and Connectivity**

*US Data Centres: Little Rock, AR and Brown Deer, W, Chandler, AZ*

*US Cloud Environments: Azure US East, Azure US Central*

Icon

Description automatically generated

**Mike Albert**

**Monday October 23, 2022**

**Statement of Understanding**

This document contains confidential and proprietary information of Fidelity Information Services, LLC and/or its affiliates and subsidiaries (collectively “FIS”). In limited circumstances, this document may be copied and/or distributed to an FIS client and its employees on a “need to know” basis in order to fulfil their responsibilities. Any further copying, reproduction, or distribution outside of FIS without express written consent is strictly prohibited.

With or without FIS’ prior written consent, FIS accepts no liability whatsoever for any consequences arising from the reproduction of the information contained in or supplied with this document, or from its disclosure to any person or entity, including to the intended recipient. FIS additionally accepts no liability for the use of the information contained in, or supplied with this document, by the intended recipient, or by any other person or entity, with or without FIS’ express prior consent. The intended recipient shall not use any part of the information contained in, or supplied with this document, in any way to the competitive disadvantage of FIS, and will take all steps necessary to comply with this provision. FIS accepts no liability whatsoever for consequences arising from disclosure of information contained within this document to a third party.

©2022 Fidelity National Information Services, Inc. and its subsidiaries (“FIS”). All Rights Reserved.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version # | Date | Author / Editor | Version / Revision Comments |
| 0.x | 23 Oct 2022 | Mike Albert | Initial draft |
| 1.0 | 2 Nov 2022 | Mike Albert | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1. Introduction 6](#_Toc118299900)

[2. Executive Summary 7](#_Toc118299901)

[2.1 MPMS Specific Environments – Production and Non-Prod 7](#_Toc118299902)

[2.2 Dates – Production Implementations 8](#_Toc118299903)

[2.3 Volumes and Velocities 8](#_Toc118299904)

[3. High Level Architecture Description. 9](#_Toc118299905)

[3.1 Authorisation Processing 10](#_Toc118299906)

[3.2 API Processing 11](#_Toc118299907)

[3.3 Disaster Recovery (DR) Processing 11](#_Toc118299908)

[4. Component Architecture 12](#_Toc118299909)

[4.1) P1C Mainframe – Payments One Card. 14](#_Toc118299910)

[4.2) Data Express (Data Placement Manager = DPR). 14](#_Toc118299911)

[4.2.1) P1C Gateway Files. 15](#_Toc118299912)

[4.2.2) P1C Reports. 15](#_Toc118299913)

[4.3) MoveIT 15](#_Toc118299914)

[4.4) FICO® Falcon - Fraud Detection and Interdiction. 16](#_Toc118299915)

[4.5) FICO® Customer Communication Services for Fraud (CCS). 16](#_Toc118299916)

[4.6) MQ Series. 17](#_Toc118299917)

[4.7) Event Broker – (EB). 17](#_Toc118299918)

[4.8) P1C Service View – Customer browser portal access to P1C. 18](#_Toc118299919)

[4.9) P1C Infinity Connect. 21](#_Toc118299920)

[4.10) Exadata – P1C Infinity Connect. 23](#_Toc118299921)

[4.11) CBK – Charge Back Processing. 24](#_Toc118299922)

[4.12) Watch List Reporter- (WLR) 25](#_Toc118299923)

[4.13) IST Switch. 26](#_Toc118299924)

[4.14) MIPs – Mastercard Information Processors. 26](#_Toc118299925)

[4.15) HSMs – Hardware Security Modules. 26](#_Toc118299926)

[4.16) SPLUNK – Payments One Focus. 26](#_Toc118299927)

[5.) Critical Component Architecture 28](#_Toc118299928)

[5.1) Overview. 28](#_Toc118299929)

[5.2) Component Resiliency 28](#_Toc118299930)

[5.2.1) MIPs. 28](#_Toc118299931)

[5.2.2) IST Switch 30](#_Toc118299932)

[5.2.3) HSMs 32](#_Toc118299933)

[5.2.4) Falcon Fraud Manager (FFM) 34](#_Toc118299934)

[5.3) Summary 34](#_Toc118299935)

[6. P1C Core Mainframe Components 35](#_Toc118299936)

[6.1) Machine names and IP addresses. 35](#_Toc118299937)

[6.2) CICS Region Names by environment 35](#_Toc118299938)

[6.3) Data Set Naming Conventions 36](#_Toc118299939)

[6.4) Data Set Aliases. 39](#_Toc118299940)

[6.5) DB2 Database Considerations 40](#_Toc118299941)

[6.6) Storage – Mainframe Disk Considerations 41](#_Toc118299942)

[6.7) RACF – Mainframe Authentication and Authorisation. 42](#_Toc118299943)

[6.8) Endevor – Source Management System 42](#_Toc118299944)

[6.9) ZWS (IBM Z Workload Scheduler) – Job Scheduling 42](#_Toc118299945)

[6.10) CA View and CA Deliver – Job Listing and Reports 43](#_Toc118299946)

[6.11) Networking and Operating Systems 43](#_Toc118299947)

[7. CICSPlex® Architecture 44](#_Toc118299948)

[8. MPMS P1C Data Flow Diagrams 47](#_Toc118299949)

[8.1) Authorisation Flow 47](#_Toc118299950)

[8.2) Charge Back (CBK) data Flow 48](#_Toc118299951)

[8.3) API Flow 49](#_Toc118299952)

[8.4) Operational Data Flow 50](#_Toc118299953)

# Introduction

FIS and Mastercard Prepaid Management Services® (MPMS) have entered into a partnership agreement to process the MPMS portfolio of approximately 10M prepaid cards worldwide.

MPMS is a wholly owned subsidiary of Mastercard International servicing end-to-end prepaid card programme management solutions for issuers, governments, airlines and retailers.

MPMS are specialists in prepaid cards:

* Operating in 24+ countries
* Managing 565+ programmes
* Enjoying 20+ years’ experience in developing, launching, and managing prepaid programmes
* Millions of cardholders internationally

In addition, MPMS provide consumer and corporate solutions including travel, per diem, gift, compensation/pay-out, payroll, every-day spend and dual sided functionality cards to the largest brands and blue-chip corporations.

MPMS are seeking a phased migration of their multi-currency prepaid capability to FIS platforms with an initial “Friends & Family” pilot which will have key objectives of:

* Developing implementation processes between MPMS and FIS
* Enable workstreams to analyse and complete technical integration and validation
* Enable certification with end-to-end production validation
* Achieve business sign-off prior to phased migration events

Not all programmes will be migrated, and countries will initially be limited to 18, including the United Kingdom (UK), United Arab Emirates (UAE), Japan, Australia and New Zealand. In conjunction with the core processing capability, the proposed solution will include fraud management capabilities, chargeback management, and compliance activities such as Politically Exposed Persons (PEP) and Sanction screening.

# Executive Summary

This document describes the FIS Design Solution developed to service MPMS’ High Availability (HA), redundancy, and resiliency requirements. Much of the specific Architectural detail is contained in the embedded Architecture Diagrams. This document references the Production region.

The MPMS solution will be deployed across US Data centres with the Core ***Payments One Card*** (P1C) system running on a set of Little Rock Mainframes. There are currently two other deployments of P1C software operating at Little Rock and MPMS will be the third:

|  |  |  |
| --- | --- | --- |
| **Mnemonic** | **Name** | **Location / Mainframe** |
| EPC | P1C North America | Little Rock / P1C1 |
| FPC | P1C Latin America | Little Rock / P1C1 |
| MPC | **P1C MPMS** | Little Rock / P1C1 |

The MPMS (MPC) Instance of the software will run immediately adjacent to both existing instances.

## 2.1 MPMS Specific Environments – Production and Non-Prod

MPMS will be deployed as a single tenant. Dedicated environments will be built out specifically for MPMS and will not be shared. FIS will build a total of 6 regions, 3 on the Production mainframe and 3 on the Non-Prod mainframe.

|  |  |  |  |
| --- | --- | --- | --- |
| **Region** | **Description** | **Mainframe** | **EcoSystem Connectivity**  **(Falcon, IST Switch, CBK, etc)** |
| PROD | Production | Prod P1C1 | Full connectivity, all EcoSystems |
| CNV1 | Conversion One | Prod P1C1 | None – Standalone P1C Instance |
| CNV2 | Conversion Two | Prod P1C1 | None – Standalone P1C Instance |
|  |  |  |  |
| UAT | User Acceptance Testing and Validation | Non-Prod P1Ct | Full connectivity, all EcoSystems |
| PFX | Production Fix | Non-Prod P1Ct | Internal Use Only – Limited Connectivity (P1C, Service View, Infinity Connect, MQ Series) |
| SIT | System Integration Test | Non-Prod P1Ct | Internal Use Only – Limited Connectivity (P1C, Service View, Infinity Connect, MQ Series) |

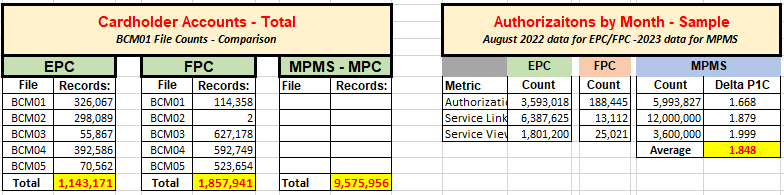
## 2.2 Dates – Production Implementations

Target dates for completion of the deployment are –

* Feb, 2023 – Friends and Family
  + This will be a subset of full functionality but will include at least:
    - The P1C Core Mainframe System
    - P1C Service View
    - P1C Infinity Connect
    - Falcon Fraud Manager
    - IST Switch
* Feb, 2024 – Production
  + MPMS (PTS) will work with FIS Conversion Teams to facilitate the inbound migration of cardholder accounts
  + All functionality will be available at this time.

## 2.3 Volumes and Velocities

MPMS are anticipated to have approximately 10M cards on file at the time of inbound conversion. Transaction volumes are anticipated at approximately 6M Auths per month. Additionally, MPMS are developing their own systems using P1C as the system of record and, as such will be a high Application Program Interface (API) user. API calls are anticipated to be about 12M per month. The table below shows comparative volumes between the existing EPC, FPC instances and our new MPC instance. The analysis shows the relative foot print for MPMS.



**Velocity information is not available at the time of writing.** We do not know traffic distribution patterns or peak Transaction per Second (TPS) rates for Authorisation processing, nor peak Calls per Second (CPS) rates for API calls.

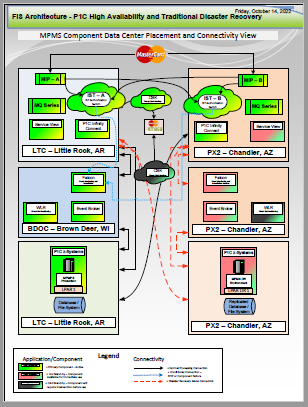
# High Level Architecture Description.

The design principles in developing FIS’ solution for MPMS processing have kept High Availability at the forefront of the design efforts. High Availability considerations were extended to both Authorisation processing and the API interfaces into the back-end systems. To meet the constraints of this level of availability, components have been distributed across all three of FIS’ Primary US data centres, and across two US Azure Cloud processing regions. Critical components have been mirrored and developed to run in an Active-Active configuration.

MPMS Solution Project Mnemonic: **MPS**

The diagram below shows the High-Level components, their Active/Stand-by status, and their locations.

**Note:** The diagram below does NOT reference the CICSPlex® configurations. These are addressed later in this document. See the section titled ***CICSPlex® Architecture.***



## 3.1 Authorisation Processing

The above diagram indicates the presence of mirrored IST Switches in the Azure cloud as Active-Active. All Authorisation processing from FIS’ on-premises Mastercard Information Processors (MIPs) will be routed to one of the two instances of IST Switch. In almost all cases, IST Switch will act as a simple pass-through routing the Authorisation Message to P1C for Authorisation processing. In the unusual instance that P1C is not available, IST Switch will Stand-In for P1C and respond to the Authorisation request on P1C’s behalf. When P1C again becomes available, messages that have been previously processed by IST Switch will be delivered to P1C as an advice.

Real time fraud processing will also be included in-line in the Authorisation flow. Fraud monitoring services will be provided by a call out to FICO®’s Falcon Fraud Monitoring product. Generally, all calls to Falcon will come from the P1C Authorisation system. During times that P1C is unavailable, however, IST Switch will be call out to Falcon to score the transaction.

## 3.2 API Processing

P1C external processing requests via API will be delivered directly to P1C Infinity Connect. The above diagram shows P1C Infinity Connect defined in an Active-Active configuration across two FIS data Centres. API calls to P1C Infinity Connect will be routed Round-Robin between the data centres to ensure the highest degree of resiliency. Additionally, the P1C Infinity Connect instances for MPMS will be deployed with the ***Infinity Connect Caching Option (ICCO)***. The ICCO retains a mirror of key data elements of the P1C database on a database local to P1C Infinity Connect. During normal processing, P1C Infinity Connect will generally pass update requests on to P1C for processing, however, in the event the P1C is unavailable, P1C Infinity Connect will service the request using the local database. Infinity Connect and P1C databases are kept in sync and P1C is the system of record.

## 3.3 Disaster Recovery (DR) Processing

**P1C** - The primary P1C mainframe systems are replicated to a geographically disparate location (Chandler, Arizona) and the replication keeps the DR system synchronized with the active Production system. Switching to the DR system will require a Declaration of Disaster and manual intervention will be required to switch processing to the DR site. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) criteria are defined in the service agreements.

**P1C Service View** – Is configured as a passive mirror to the primary site. As such, either site (but not both) can be active as the primary site. Switching the designation as to which site is the primary is via floating VIP and can be accomplished via automation. The primary site can be switched at a set interval to ensure both sites are operable and in sync, or can be used for software deployments or upgrades.

**CBK & WLR** – While both of these components are important, neither are viewed as critical in Authorisation and API processing. These are recovered under their external RTO/RPO guidelines.

**Falcon and Event Broker** – Both of these components have hot standby copies at the alternate site (Chandler, AZ). SLAs for their recovery are specified in their respective operations documentation.

# Component Architecture

While the core of the MPMS solution is the Payments One Card (P1C) software, there are many additional key components that will make up the MPMS Ecosystem. Many of the Ecosystem components are already in place and being used by other instances of P1C running at the LTC data centre (P1C North America and P1C Latin America). These existing components will be leveraged for the MPMS solution where possible.

The image below is a diagrammatic representation of these components and their interactions with both the P1C software and with each other. The significant components are described in this section. For detailed information, see the embedded Architectural Design diagram. The diagram shown below is for the Production environment only.

Embedded Architectural Design diagram below:

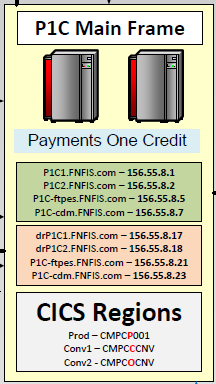


Diagram, timeline

Description automatically generated

## 4.1) P1C Mainframe – Payments One Card.

Both New and Leveraged Component – While the mainframe hardware is already in place, the MPMS solution will require the build out of a new instance of the P1C software, including file systems, database schemas, CICS regions, source management, job scheduling, etc.



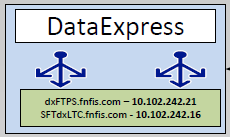
This is the central processing component for the solution. It is the FIS strategic go forward platform for credit processing in North America and card processing (including debit and prepaid) in international markets.

Authorisation processing, settlement, API servicing, statements and reporting, embossing file generation – and all other processing related to servicing MPMS’ 10M+ cardholders will be handled by this component.

P1C runs on a z/OS mainframe, is written primarily in COBOL and Assembler and utilizes VSAM/IAM, DB2 and flat files as a database repository. CICS is the primary data communications vehicle, using ServiceLink and MQ Series for external message communications. See the section on ***Mainframe Component Architecture*** below for more details.

## 4.2) Data Express (Data Placement Manager = DPR).

Leveraged Component



This component serves as a hub for file and report distribution. DPR uses SFTP protocol to send/receive files and is the primary staging area for report and data files going to the customer. DPR has the capability of splitting composite data files out, segregating one large file into smaller files specific to Clients, then transmitting the resultant file to the Client.

Communication between P1C and DPR will be via SFTP

### 4.2.1) P1C Gateway Files.

DPR will be used as the data transmission vehicle for Gateway files. For MPMS, Gateway files are produced by the nightly batch process and are produced as an aggregate of all for all Corps/Accounts in the region. With MPMS running in a desiccated region, rather than a shared environment, all data in the Gateway files will be for MPMS. P1C will transmit the full Gateway files to DPR and DPR will forward them, intact, to MPMS. No data segregation will take place.

### 4.2.2) P1C Reports.

DPR will also be used as the transmission mechanism for P1C Reports. P1C reports are generated out of the nightly batch, and reports from specific batch cycles are delineated by a date stamp suffix on the dataset name. P1C will transmit each of the selected report files for the processing date to DPR. DPR will then forward the report file to MPMS unaltered.

There will be no use of the report splitting or bundling capabilities of DPR/eReports and no reporting Portal is offered. These capabilities will be assumed by MPMS.

## 4.3) MoveIT

Leveraged Component

Application

Description automatically generated

Is a File Transfer hub used for staging files between P1C and internal consumers. The utility package has some sophisticated capabilities regarding file manipulation.

Communication between P1C and MoveIT will be via SFTP

For our MPMS implementation, we will be using MoveIT to forward extracts of the full database to WLR for inclusion in WatchList processing.

Embossing – Currently, P1C US is using the MoveIT connections to forward embossing files to the Card Production facilities. We will want to explore the best delivery options for our MPMS embossing files.

## 4.4) FICO® Falcon - Fraud Detection and Interdiction.

Leveraged Component

Diagram, text

Description automatically generated

Falcon will be our Fraud Solution for MPMS. The Falcon system will be In-Line in the Authorisation flow and score all transactions in Real Time mode. Falcon itself will not approve or decline an Authorisation request but will return a recommendation to decline a request that has a high likelihood of fraud. Falcon will be In-Line both for Primary Authorisation processing through P1C and for Stand-In processing from IST Switch when P1C is not available.

Communication between (P1C and Falcon) and (IST Switch and Falcon) will be over TCPIP

## 4.5) FICO® Customer Communication Services for Fraud (CCS).

Cloud Component

This optional component is not shown on the diagram. CCS is FICO’s cloud based automated dialer solution and interfaces with FIS’ on premises FRMC modules running at our BDOC/PX2 datacentres. CCS has the ability to contact cardholders via SMS/eMail to validate transaction activity and – based the response – take a set of actions.

At the time of writing – the CCS offering for MPMS has not been decided, and whether FIS would own the CCS Cloud relationship with FICO or MPMS would own that relationship.

To provide local calls in the UK, there is a CCS component in the USA and one in the UK. FIS’ FRMC will have an integration point with the US based CCS and FICO sets up the link between the US and UK. It’s been a few years since we set up the EMEA CCS so we may want to confirm with FICO if this is in fact the architecture used today.

## 4.6) MQ Series.

Leveraged Component

A picture containing text

Description automatically generated

Is our primary Message Processing hub and has redundant pairs of servers at Little Rock, AR and Chandler, AZ data centres. These instances of MQ Series are leveraged and MPMS will share them with other applications/users.

MQ will be the primary entry/egress point to the P1C mainframe for all message processing (excluding Authorisation messages). Components connecting thru MQ will be at least Service View, Infinity Connect and Event Broker.

Communication between (P1C and MQ) and (MQ and external Apps) will be via TCPIP

## 4.7) Event Broker – (EB).

Leveraged Component

Text

Description automatically generated

EB is a configurable message processing hub. It is defined as two sets of three redundant servers at FIS’ Brown Deer, WI and Chandler, AZ data centres. MPMS has requested notification be sent when a cardholder initiates or experiences certain conditions ( ie: change of address). The set of conditions is quite extensive. Additionally, all authorisation messages will be sent to MPMS. All this activity will be routed through EB. This will be high volume data transmissions and consideration will need to be given to the connection mechanisms between EB and MPMS.

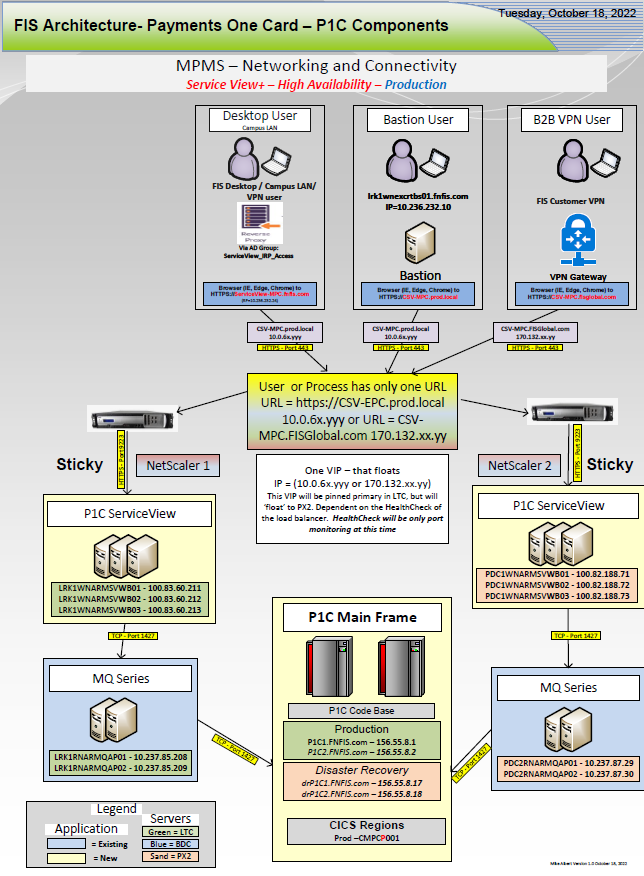
## 4.8) P1C Service View – Customer browser portal access to P1C.

New Build for MPMS Solution.

P1C Service View is P1C’s browser-based servicing portal for all customer service and back-office functions. This was built new for MPMS and consists of two sets of 3 servers at Little Rock, AR and Chandler, AZ data centres. The graphic below shows the servers, ports and connection configurations. For detailed specifics, refer to the embedded Architectural Design diagram.

Embedded Architectural Design diagram below:





P1C Service View requests are stateful and as such, it is built as an Active/Standby model. Both the LTC and PX2 sites are designated at Production, but only one of the two can be active at any point in time. The active site can be switched via alteration of the floating VIP.

There are three connection types to P1C Service View for MPMS:

* Desktop user – this is an individual within the FIS Network (either within a physical FIS facility, or on the FIS Internal VPN). The user access controlled via membership in an Active Directory group administered through a local reverse proxy server. Only the production region is available via this access method.

Application access controls require:

* + Inclusion in the AD Group
  + FIS Internal Network Access
  + Application User ID and Password

Browser URLs will be:

* + Production - <HTTPS://ServiceView-MPC.fnfis.com>
  + No lower environments
* Bastion User – Allows access only to FIS technical and Business Analyst personnel to the servers and applications. Users must be within the FIS Internal network (either onsite of on the Internal VPN) and must first log into the Bastion.

Application access controls require:

* + FIS Internal Network Access
  + Bastion access permissions
  + Application User ID and Password

Browser URLs will be:

* + Production - <HTTPS://CSV-MPC.prod.local>
  + UAT - <HTTPS://CSV-MPC-UAT.prod.local>
  + ProdFix - <HTTPS://CSV-MPC-PFX.prod.local>
  + SIT - <HTTPS://CSV-MPC-SIT.prod.local>
* Business to Business (B2B) Virtual Private Network – Will allow external customers to access the application via a dedicated B2B VPN link between FIS and MPMS. All access on this channel must come in only over the B2B VPN Link. MPMS will determine, at their discretion, access to the VPN link on their end – FIS will not filter any requests that come in over this channel.

Application access controls require:

* + Customer Permissions to access the B2B VPN Link
  + Application User ID and Password.

Browser URLs will be:

* + Production - <HTTPS://CSV-MPC.fisglobal.com>
  + UAT - <HTTPS://CSV-MPC-UAT.fisglobal.com>

Of note, the other two instances of P1C Service View offered for the EPC and FPC clients also permit open internet connections via Akamai. We will not be offering this to MPMS.

## 4.9) P1C Infinity Connect.

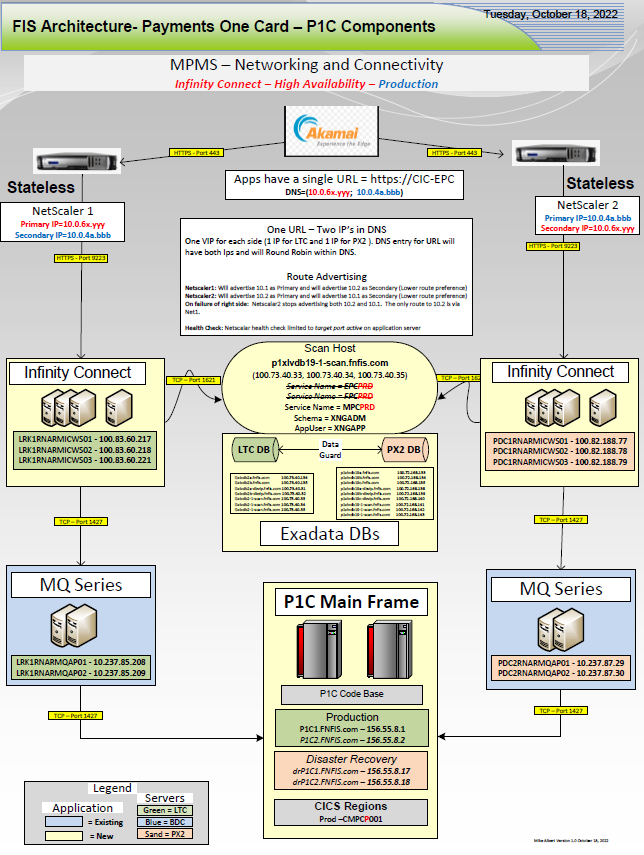
New Build for MPMS Solution.

API enablement for P1C. This includes tokenisation solution, APIs for all card servicing and back office functions, outbound Visa Claims Resolution (VCR), Visa Transaction Controls (VTC), 3D secure v2.0 for Secure Cardholder Authentication and Loyalty calls for Credit Card.

The schematic diagram image that follows shows the Architecture for P1C Infinity Connect. For greater granularity, see:

Embedded Architectural Design diagram below:





This was built new for MPMS and consists of two sets of three servers at Little Rock, AR and Chandler, AZ data centres. Infinity Connect will be built in an Active-Active configuration. API calls to Infinity Connect will be routed Round-Robin between the data centres. Entry/Egress of API calls from MPMS into FIS will be through Akamai. Akamai will be responsible for the Round-Robin load distribution between the FIS Netscalar load balancer pair. The Netscalars will then distribute the request traffic amongst one of the three active servers at their respective sites. This configuration will provide for the highest degree of resiliency and application availability.

Additionally, and further adding to the high availability of the solution, the P1C Infinity Connect instances for MPMS will be deployed with the ***Infinity Connect Caching Option (ICCO)***. This will offer seamless servicing of specified API requests even when the back end P1C system is unavailable. The data for ICCO will be housed in a pair of Exadata slices (see next item below). Account, Transactional and Authorisation data will be maintained in the Exadata databases. Under this configuration, the logic paths below will be followed.

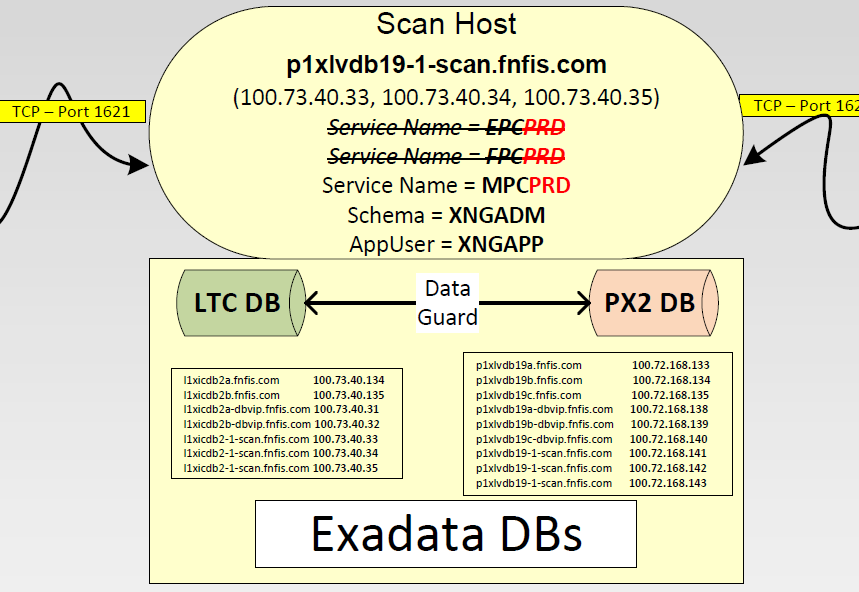
* When an **API inquiry** comes in, Infinity Connect will assess if the request can be serviced via the ICCO and, if so, results of the local query are immediately returned to the requestor.
* When an **API update** request comes in, Infinity Connect will assess weather the back end P1C system is active:
  + If so, forward the update to P1C. P1C would then apply the update returning the operation status code and message to Infinity Connect. P1C would then send, in near real time, an update back to Infinity Connect to mirror the update on the ICCO.
  + If not, Infinity Connect will perform the update locally on the ICCO and queue an update action to P1C (Store and Forward) to be applied when P1C returns.
* Finally, in the unlikely event that the underlying Exadata DB should become unavailable, Infinity Connect will route all requests directly to P1C for servicing. Responses from P1C for **API Update** requests will be queued (Store and Forward) for application to the Exadata DB when it again becomes available.

Utilizing the Round-Robin, Active-Active application server configuration, and employing the features of the ICCO option described above will provide the highest degree of availability possible to the MPMS Solution, for API processing.

## 4.10) Exadata – P1C Infinity Connect.

Leveraged Component.

Exadata slices at Little Rock, AR and Chandler, AZ have been procured specifically for P1C Infinity Connect. While these are dedicated to P1C Infinity Connect, they are shared across all three instances ( EPC, FPC and MPC ). Only MPC, however, is utilizing the ***Infinity Connect Caching Option (ICCO)***. The production instances of Exadata are being configured with 48GB memory (shared) and 3TB of storage. Since only MPMS will be using ICCO, almost all storage can be allocated to the MPC instance.



For resiliency, each site will have two active DB Nodes. Active at LTC are NodeA and NodeB, active at PX2 are NodeB and NodeC (NodeA is not used at PX2). Should there need to be database maintenance, the work can be staggered, scheduling one node at a time. Processing will continue seamlessly on the other node.

Additionally, the P1C Infinity Connect application, rather than connecting to the databases directly, will instead connect via a Scan Host. The Scan Host will insulate the application from underly database maintenance activity. In a situation where the Primary Database is switching from one data centre to the other (ie: LTC is Primary, PX2 is Secondary 🡺 Switch 🡺 PX2 is Primary, LTC is Secondary), simply, the Scan Host IP addresses would be updated to reflect the new datacentres slice.

**Note:** It will be important to coordinate any such work or other work resulting in possible database outage with the P1C teams to ensure we maintain availability to MPMS. As stated above, during the time the database would be unavailable, P1C Infinity Connect will route all requests directly back to the host P1C system. Database maintenance that might result in an outage must be coordinated so as not to coincide with any planned P1C unavailability.

Databases across both sites are kept in sync via replication.

## 4.11) CBK – Charge Back Processing.

Leveraged Cloud Component



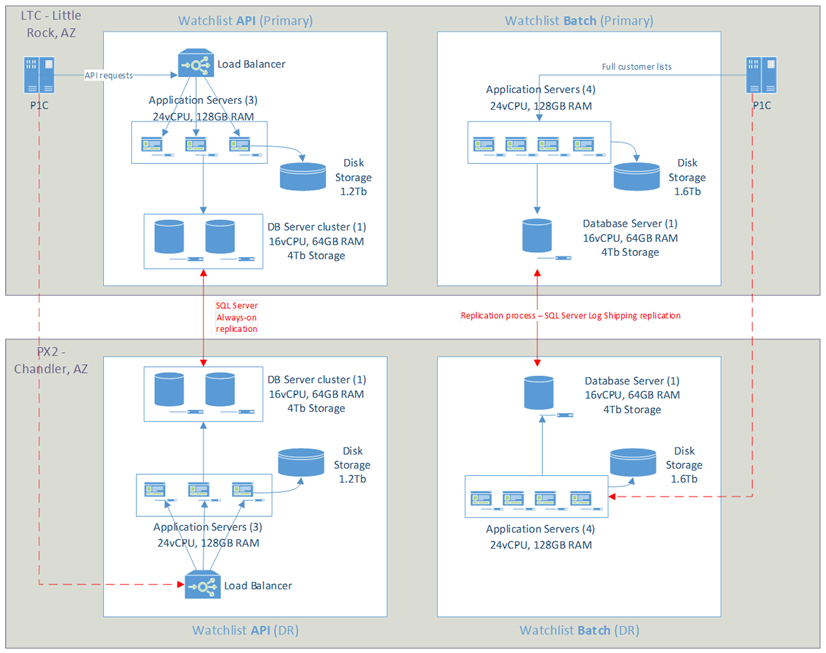
The MPMS solution will be leveraging an existing instance of CBK. This will be a cloud-based instance set up in the Azure Europe Cloud. CBK processing is not deemed to be critically time sensitive, so latencies from trans-Atlantic communications have been permitted without a lot of scrutiny. CBK processing will be initiated via a message being generated in P1C. The flow for CBK will be:

P1C 🡺 MQ Series 🡺 Event Broker 🡺 CBK

See the CBK design for specifics.

## 4.12) Watch List Reporter- (WLR)

Leveraged Component



Will be used as an ancillary function during account creation ( will not be in-line with the account creation process) and will have a batch component to periodically evaluate the entire MPMS cardholder base. Specifics of WLR servers have not yet been published.

Communications between P1C and WLR will be:

Account Creation – TCPIP

Batch Scanning – SFTP via MoveIT

Specific servers and IP addresses have not yet been made public for WLR.

## 4.13) IST Switch.

New Cloud Build for the MPMS Solution.

Authorisations; pass thru and Stand-In processing. IST switch is not shown on the diagram and is, instead referenced in the Authorisations container at the top left. Refer to the section ***Critical Component Architecture – IST Switch*** further down in this document.

## 4.14) MIPs – Mastercard Information Processors.

Leveraged Component

MIPs are not shown in this diagram but are referenced in the Authorisations container at the top left. Refer to the section ***Critical Component Architecture – Mastercard MIPs*** further in the document for details.

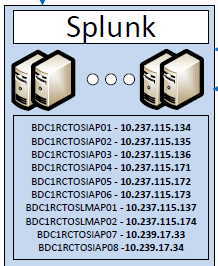
## 4.15) HSMs – Hardware Security Modules.

Leveraged Component

HSMs are not shown in this diagram but are referenced in the Authorisations container at the top left. Refer to the section ***Critical Component Architecture – HSMs*** further in the document for details.

## 4.16) SPLUNK – Payments One Focus.

Leveraged Component



Splunk is the single repository for logging, performance and operational data used to drive ***FIS’ Payments One Focus product***. Our MPMS solution will feed SPLUNK data from mainframe processing via the Ironstream for Splunk®. Ironstream runs as a started task on the P1Cx mainframes and will transmit mainframe log data detailing relevant activities for Authorisations, batch processing, file transmissions and the like. P1C Infinity Connect activity data will also be fed to Splunk, as will Service activities. Finally, IST Switch will be modified to provide log data to Splunk. All data feeds will be streaming and in near real time. The MPMS project teams will need to work with Splunk administrators to accommodate data volumes and any queries, dashboards alerts and reports.

# Critical Component Architecture

Critical components are those defined outside of the P1C Core software that are essential for Authorisation processing.

The MPMS solution has been designed with high availability Authorisation processing at the forefront. The resultant design presents the best solution to an ***Always Available*** Authorisation processing flow.

## 5.1) Overview.

General Message Flow

Issuing traffic will come to FIS via the MasterCard network and will be delivered to FIS via one of two MIPs located at geographically disparate data centres. MIPs are identified as 2AW at the Little Rock data centre and MIP = 1HIL at the Chandler DC. Messages will then be distributed from either of the MIPs to either instance of IST Switch.

Under normal processing:

* IST Switch will directly forward the message to P1C for Authorisation processing.
* P1C will call out to the HSM farm for message data element verification
* P1C will apply internal Authorisation parameters and call out to Falcon
* Falcon will score the transaction and return value for interrogation by P1C Authorisation system

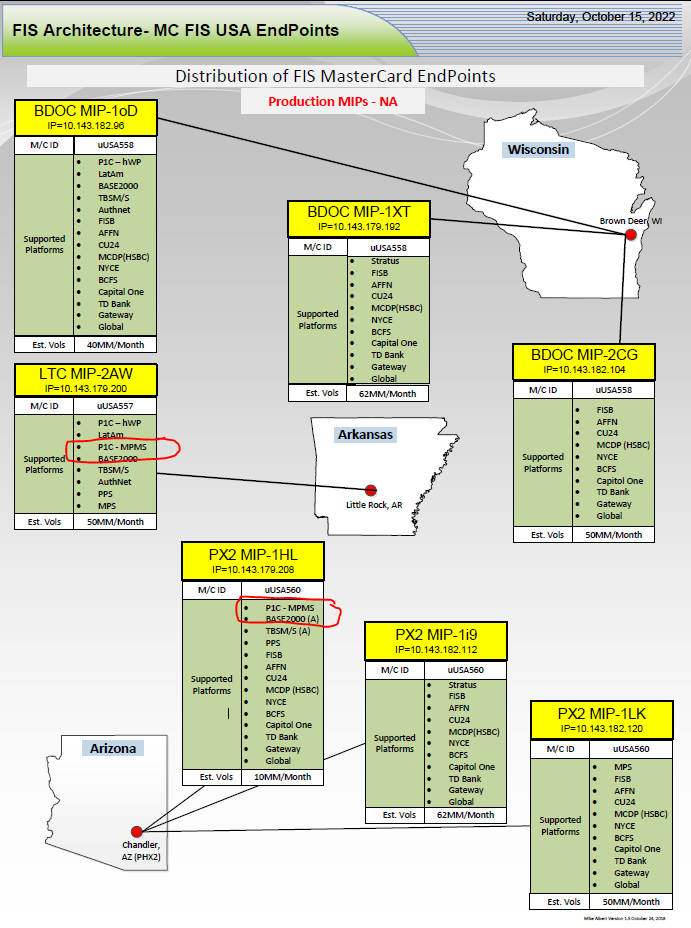
During Stand-In Processing (P1C is unavailable)

* IST Switch will perform Authorisation verification on a limited number of parameters
* IST Switch will call out to the HSM pool for data element verification
* IST Switch will call out to Falcon to transaction scoring

## 5.2) Component Resiliency

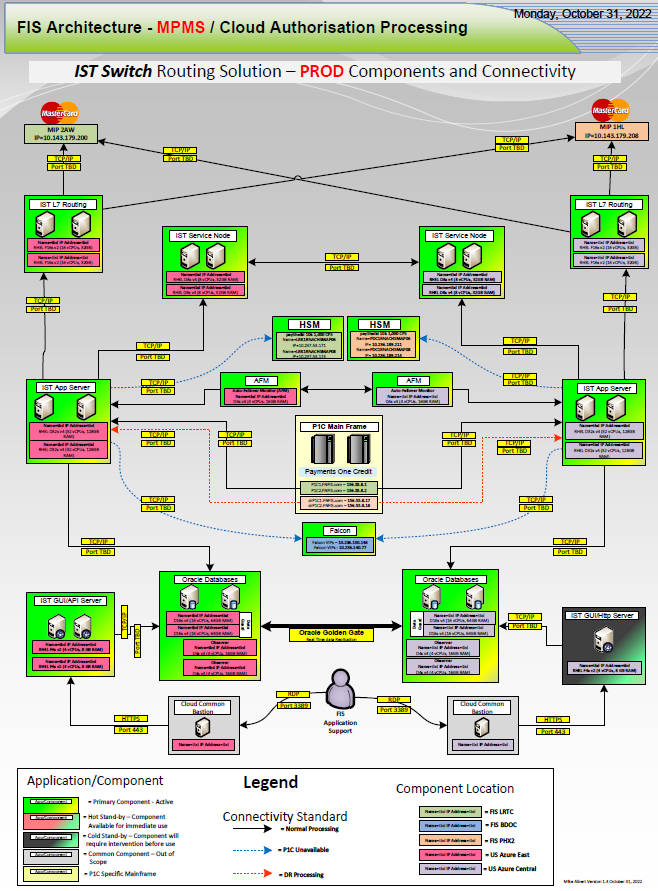
### 5.2.1) MIPs.

The MIP endpoints will be set up in a Round-Robin configuration, with Auto Enable/Auto Disable set for these Member IDs. IST Switch will also capitalize on MasterCard’s Advanced Session Management parameters where possible – details to be determined.



### 5.2.2) IST Switch

IST Switch is built as an Active-Active configuration across two separate regions of the Azure Cloud. The regions are identified as US Azure East and US Azure Central. IST uses a Service Node to ensue both instances of the software are in sync. Each critical component has local redundancy in each of the cloud regions ( ie: two App Servers in each cloud region). Further, the underlying Oracle databases have local redundancy; there are two local database servers (active-passive) and they are kept in sync via Data Guard. Finally, databases across the cloud regions undergo immediate database replication via GoldenGate. See the diagram below for a logical representation of the IST Switch build out.

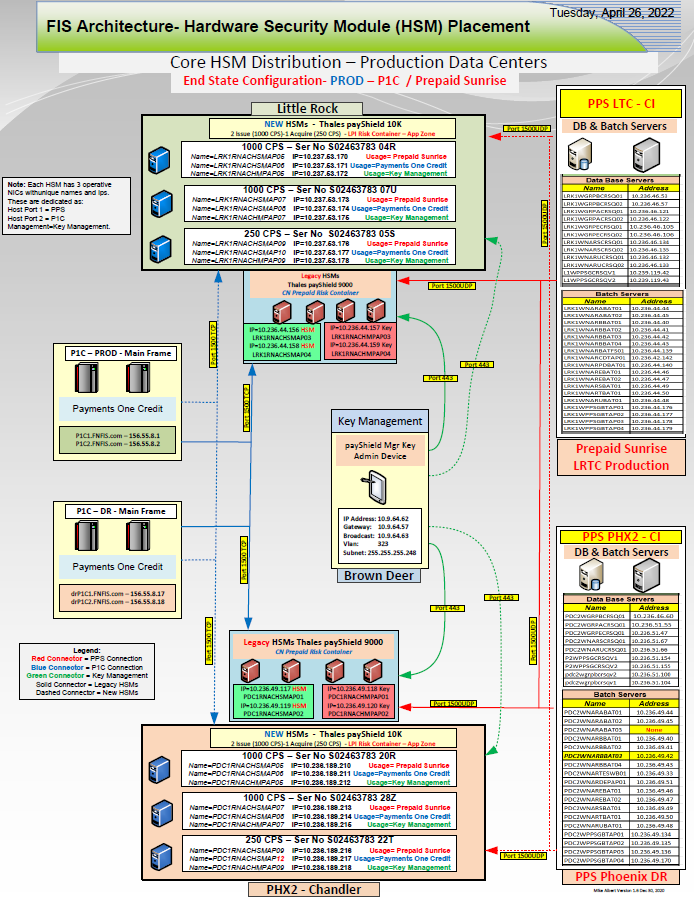


### 5.2.3) HSMs

HSMs are critical and in-line to Authorisation processing. The MPMS Solution will be leveraging a pool of HSMs for Authorisation call outs either from P1C (normal processing) or IST Switch (during STIP processing). The HSMs in use are Thales paySheild 10k, and are running the Premium Command package. There are 4 HSMs in the pool available for issuer processing and these are separated in pairs across two geographically disparate data centres – Little Rock and Chandler.

This local redundancy and inter datacentre redundancy provide for maximum availability of the HSMs. Note that these devices are shared with other Lines of Business (LOBs) – the other primary user is Prepaid Sunrise (PPS).

See the diagram below for details



### 5.2.4) Falcon Fraud Manager (FFM)

Falcon Fraud Manager (FFM) – runs as a composite of servers across multiple data centres and provides the highest degree of resiliency within its own product suite. FFM is in-line in Authorisation processing for all switches in FIS North America and covers processing for EMEA B2K and P1C. FFM is well capable of volumes exceeding 1,000 TPS. Resiliency of the FFM platform, aside from the assertions above, is left out of this document.

## 5.3) Summary

To ensure maximum availability of the Authorisation flow and develop, is as much as possible, the ***Always Available*** state for MPMS Authorisation processing, redundancy and resiliency have been developed along each stage of the processing path. Additionally, designing and permitting cross connection between the entities along the flow path further mitigates any disruption from the failure of any individual component.

The net product of this effort will provide the highly available Authorisation system that can meet our Customer SLA’s.

# P1C Core Mainframe Components

## 6.1) Machine names and IP addresses.

Machine names for the MPMS mainframes are defined as:

|  |  |
| --- | --- |
| **Function** | **Name** |
| Production (Current) | P1C1.FNFIS.com |
| Production (CICSPlex) | P1C2.FNFIS.com |
| Disaster Recovery (Current) | drP1C1.FNFIS.com |
| Disaster Recovery (CICSPlex) | drP1C2.FNFIS.com |
| All Non-Prod | P1Ct.FNFIS.com |
|  |  |

IP addresses are assigned for specified usage. A summarized view of the IP address assignments is shown in the table below:



## 6.2) CICS Region Names by environment

A new set of CICS regions will be required for this build.

**Note:** This does not reference our CICSPlex® build out; rather this is an SRO specification. For CICSPlex® CICS region names, please refer to the section titled ***CICSPlex® Architecture*** below.

CICS Names for our SRO deployment will be built out as one region per environment. Three of the regions will reside on the Production Logical Partition (LPAR), the other three on the Non-Prod LPAR. Summary shown below

|  |  |  |
| --- | --- | --- |
| **MPMS** CICS Region Names - **All Regions** ***STC Namings by Region, LPAR*** | | |
|  |
|  |
|  |
| **LPAR** | **Region Name** | **Environment** |  |
| P1C1 | CMPCP001 | Production |  |
| P1C1 | CMPCC001 | Conv One |  |
| P1C1 | CMPCO001 | Conv Two |  |
|  |  |  |  |
| P1CT | CMPCA001 | UAT |  |
| P1CT | CMPCF001 | Prod Fix |  |
| P1CT | CMPCS001 | SIT |  |
|  |  |  |  |

## 6.3) Data Set Naming Conventions

MPMS will operate on a unique set of files specific only to MPMS. The data sets will follow the standard naming conventions for applications on the P1C1/P1Ct Sysplex. The conventions for the new datasets are shown below. For display purposes only, they are broken into 3 groups by environment –

* Production and UAT
* SIT and Prod Fix
* Conversion One and Conversion Two

**Production and UAT Environments -**



**SIT and Prod Fix Environments –**



**Conversion One and Conversion Two Environments –**



## 6.4) Data Set Aliases.

A new set of catalogue Aliases will be required for this project. These aliases will be similar to those previously created for the EPC and FPC instances but will reflect the naming conventions shown above. A listing of the required new Aliases is as below:



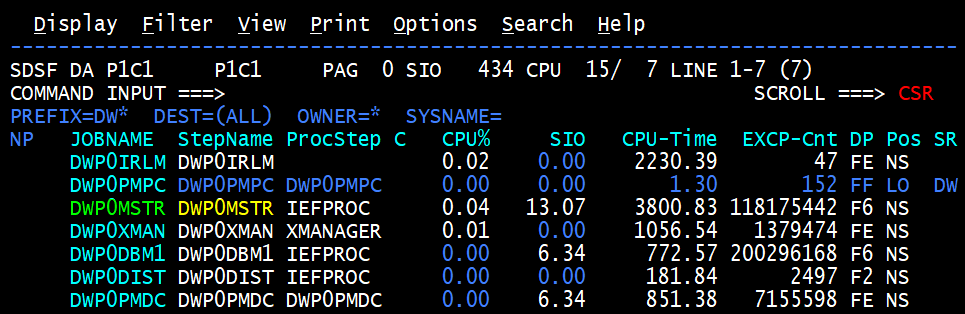
## 6.5) DB2 Database Considerations

The MPMS deployment will use the existing DB2 Subsystems currently running on the P1C1 and P1CT LPARS. MPMS data will be segregated by Schema within the same subsystems.

Current subsystems are DWP0 running in Production on P1C1 and DWN0 running for the non-production environments on P1CT.

**Note:** This does not reference our CICSPlex® build out; rather this is an SRO specification and does not address possible data sharing requirements for DB2. For CICSPlex® specifications, please refer to the section titled ***CICSPlex® Architecture*** below.

Production



Non-Production

A screenshot of a computer

Description automatically generated with medium confidence

## 6.6) Storage – Mainframe Disk Considerations

Additional storage will be required for the full MPMS conversion, however, for the anticipated initial implementation of the friends and family deployment, additional storage requirements will be minimal.

Analysis will be required to determine the exact amount of additional storage, and the appropriate timing to bring the storage on-line, and the specific numbers are not available at the time of writing. We do have, however, relative sizing when comparing to the known footprint of the adjacent instance of the software – EPC.

Specific storage requirements will come out of the detailed analysis.

Graphical user interface, text, application, email

Description automatically generated

New storage allocations for MPMS will be defined in advance as RLS Capable in advance of the CICSPlex work to follow. Additionally, all volumes will be enabled with Pervasive Encryption. All datasets under these storage pools will meet the 2024 Pervasive Encryption requirements of PCI.

## 6.7) RACF – Mainframe Authentication and Authorisation.

A new set of controls will be defined for MPMS. These will be delivered as Roles with permissions defined to the specific roles. First line production support will be delivered by the North America mainframe card production support teams. These are the same teams that currently support the EPC and FPC environments. As such, it may be possible simply to ALTER their role definitions to further permit access to the MPMS environment.

Other users, BA’s and Roles specific to MPMS will need to be explicitly defined. These definitions are typically delivered by the Software Deployment Teams.

## 6.8) Endevor – Source Management System

FIS’ P1C instance of Endevor will be utilized for the MPMS project. We will define an new environment group for the MPMS copy of the source code and executables. Since P1C is a global code base, the source code in the library should be the same as that for the EPC and FPC instances, however, best practice dictates that we create a separate copy for MPMS.

Endevor Administrators will build the MPMS environment within the current Endevor instance, the source will be loaded by the Software Deployment Teams.

## 6.9) ZWS (IBM Z Workload Scheduler) – Job Scheduling

We will leverage our current existing instances of ZWS on the production and non-production mainframes. Specific schedules for MPMS will have to be build and accommodations made for the GMT base, offsetting US run times by 5 hours.

The ZWS administration teams will be responsible for the build of the new schedules. The ZWS schedules themselves are generally delivered by the Software Deployment Teams.

## 6.10) CA View and CA Deliver – Job Listing and Reports

Specifics will need to be specified for job class specifications or naming specifications unique to MPMS to allow for population into CA-View/CA Deliver. The CA View/CA Deliver teams will need to work with the project teams to determine the best approach to add MPMS. We will also need to consider additional space or processing requirements imposed on CA View/CA Deliver by the addition of the MPMS volumes.

## 6.11) Networking and Operating Systems

IST Switch Communications will be a net new add to the P1C Sysplex. This will require port selection and assignment and need to be coordinated between the Mainframe teams, the P1C teams and the IST Teams.

Excepting IST Switch, additional port assignments for MPMS should not necessary. Rather, it is anticipated that MPMS will be able to leverage existing communication channels already in place. Still though, a review of all current port allocations and expected use would be prudent.

# CICSPlex® Architecture

This section describes the CICSPlex® Architecture at a high level and in general terms. Specifics of the rollout, deployment and testing of the CICSPlex® will be covered under a separate project. Detailed design documentation will be delivered as part of that effort. Of note, the MPMS delivery teams will attempt to minimize re-work between the standard deployment and the follow on CICSPlex® deployment.

**Overview**

The CICSPlex® Architecture will provide for additional resiliency in the mainframe platforms by providing a locally redundant LPAR within the same data centre. Current Architecture has our instances of P1C processing on a single LPAR at the Little Rock, AR data centre (LRTC), namely P1C1. The CICSPlex® Architecture will introduce the definition of a second LPAR to exist immediately adjacent to the current primary LPAR, also at LRTC, to be named P1C2.

This will allow for seamless continuity of processing of the P1C Mainframe application during times of scheduled IPLs of the mainframe systems. IPLs (Initial Program Load – or reboot of the mainframe) of the LPARs would be staggered, so as that – while P1C1 reboots, all processing would be shunted to P1C2. Then, once completed and both LPARs are again available, the process would be repeated for P1C2.

The two LPAR concept began at inception of the first install of the P1C Code for the Payments One Card North America (EPC) instance. Much of the work in the definition of the EPC instance was done with the foresight of the eventual existence of the P1C2 LPAR. Much of the routing and firewall work for the second LPAR should already be in place.

In addition to the second LPAR, the CICSPlex® Architecture will require a shift from Single Region Operation (SRO) to Muti-Region Operation (MRO). In the SRO configuration, as we have it today, there is only one CICS region, so all work of any type is routed to the same place. In the MRO configuration, there is not only dual Application Owning Regions (AORs), but also other regions defined to perform specific functions. Work is routed, then, not only between active AORs, but also routed to other regions based on type of work (ie: Terminal Owning Region (TOR) or Gateway Owning Region (GOR)).

The SRO 🡺 MRO change, and other factors, requires additional logic in the application code, and therefore enhancements by the P1C development teams.

Both the technical environment for CICSPlex® and the application code modifications to support it must be in place before we can utilize the enhanced functionality.

CICSPlex® proposed deployment steps needed to pursue this development.

We will first deploy our CICSPlex® Architecture on out test systems. Currently at LRTC, there are only three mainframe LPARs defined and only two of those are active as below:

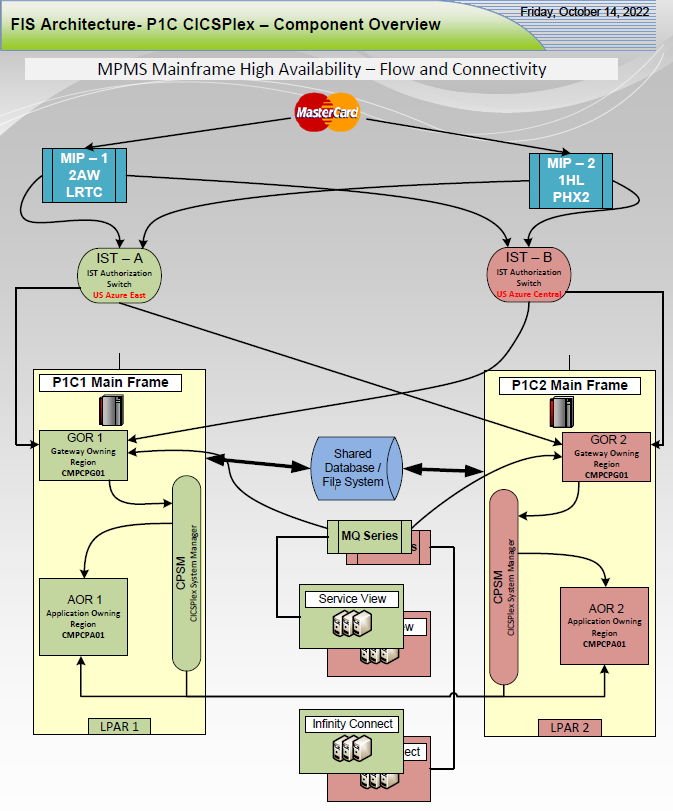
* P1C1 – Production Mainframe – Active
* P1C2 – Production Mainframe – placeholder – yet to be defined
* P1Ct – Non-Prod or Test Mainframe – currently active for test and UAT
* ***P1Cu – New LPAR to be created for CICSPlex® work***

Initially, we will need to define a second test system – P1Cu – to operate as the mirror in the pair for Non-Prod development work for CICSPlex®. Work might commence on the SIT regions, for example, by defining the CICS regions below on both the P1Ct and P1Cu LPARs.

* CMPCSA01 – Application Owning Region
* CMPCSG01 – Gateway Owning Region
* CMPCST01 – Terminal Owning Region

There will be significant technical considerations to deploying the CICSPlex® solution after the installation of the initial SRO defined MPMS regions. The teams will have to solve for the overlap of filenames and aliases, database naming, etc.

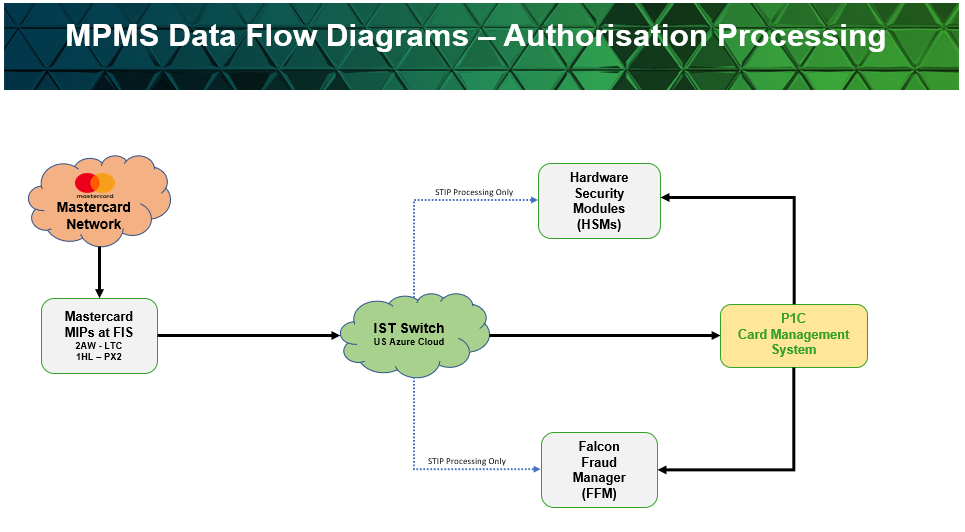
DB2 Data Sharing – will also have to be considered across the pair of LPARs.

****

# MPMS P1C Data Flow Diagrams

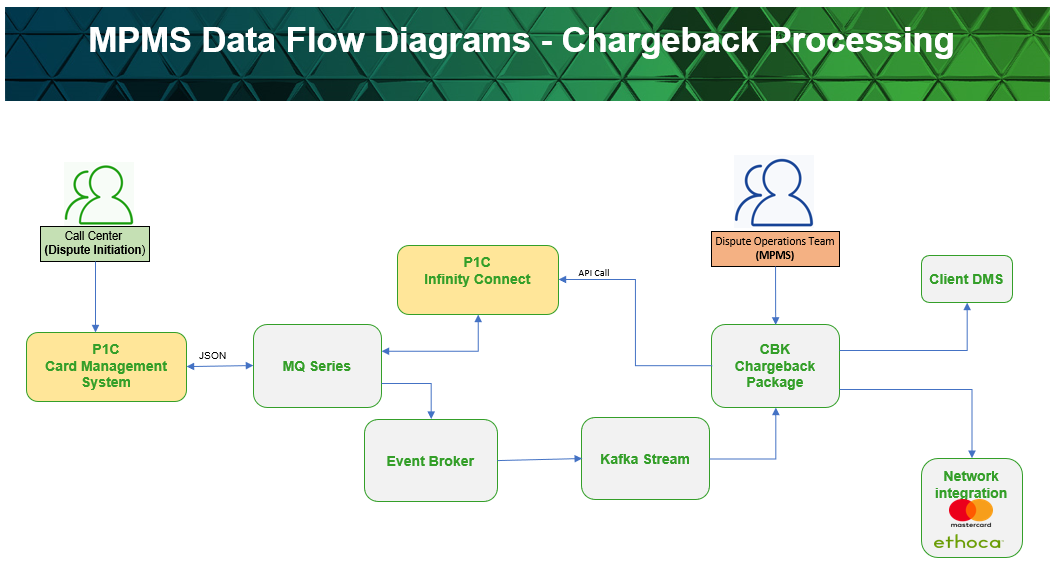
## 8.1) Authorisation Flow

Authorisations will come into FIS from the Mastercard Network as issuing traffic. Authorisation messages will first be received and one of the two Mastercard MIPs hosted at the FIS datacentres. Messages will be forwarded from the MIPs to the MPMS Instance of IST Switch hosted in the US Azure Cloud, then forwarded on to P1C. In the event of STIP processing, IST Switch will call out to the HSMs and Falcon Fraud Manager as part of the stand-in Authorisation processing.



## 8.2) Charge Back (CBK) data Flow

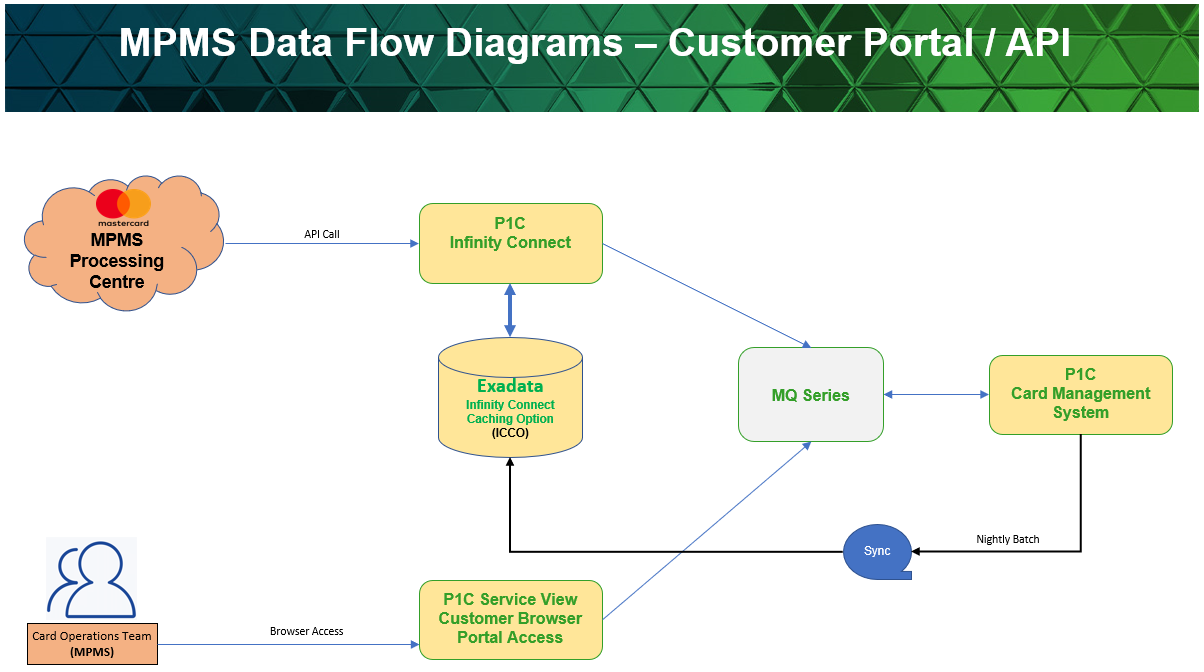
Chargeback processing will be initiated out of P1C. Once a chargeback is saved in P1C, it will be pushed out to CBK via Event Broker. CBK will communicate back to P1C via API Calls through P1C Infinity Connect.



## 8.3) API Flow

For API calls, MPMS will access the P1C system via P1C Infinity Connect. Calls will originate from MPMS data centres or cloud processing regions. P1C Infinity Connect will service Inquiry requests from the local Exadata ICCO. Update requests will either be passed directly on to P1C or, if P1C is not available, processed on the ICCO database and queued for delivery to P1C.

User Customer access will be via the browser portal provided by P1C Service View. The browser will provide both inquiry and update access for cardholder functions.



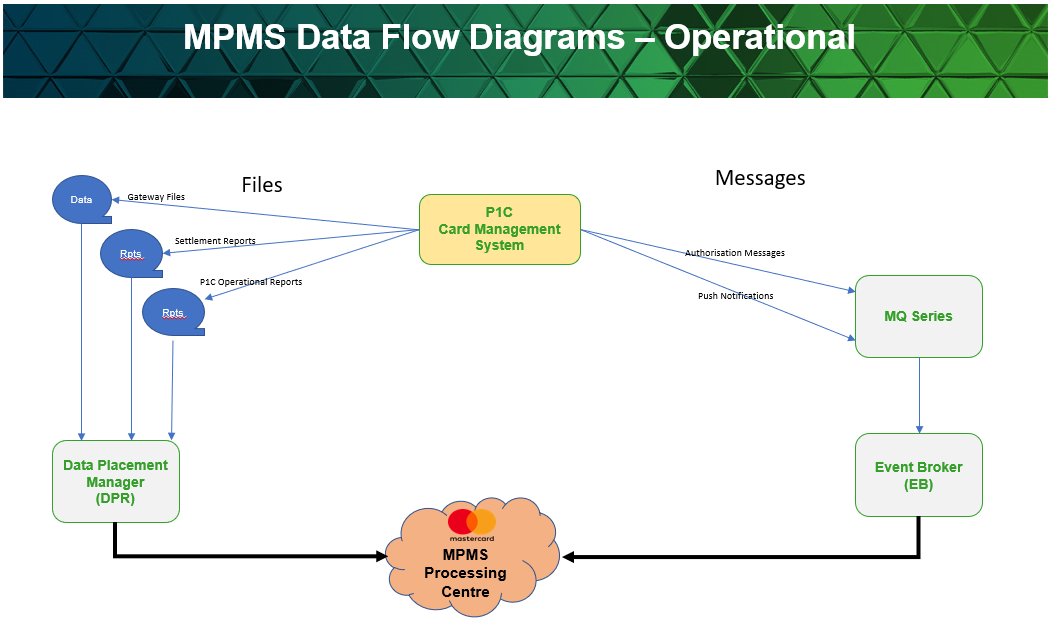
## 8.4) Operational Data Flow

Data delivery to MPMS from P1C will be via two channels

* Batch File delivery
* Near Real Time (NRT) Messages

Gateway files, settlement files and P1C Reports will be delivered to MPMS via an SFTP feed from Data Placement Manager (DPR). As part of the nightly batch process, P1C will push relevant files to DPR for subsequent distribution to MPMS.

Authorization messages and push notifications will be delivered to MPMS via an NRT feed from P1C to Event Broker via MQ Series. Event Broker (EB) will delivery messages directly to MPMS. If MPMS is unable to consume messages, EB will queue messages for delivery when MPMS is again able to consume them.



How do they interact?

High level overview of the application

Mpc overflow?

Troubleshoot

Database instances

Database names

Important tables to look into database