Any enquiries regarding this publication should be sent to us at: MoJ Data Access Team Mailbox data.access@justice.gov.uk

HM Courts & Tribunals Service

M

Publishing & Information Service (P&I)
High Level Design

Future Hearings
REVIEWED – V1.2

Template Version V03

Table of Contents

1 Document Control

This section provides a history of how the document has been changed and how the changes have been governed.

1.1 Document History

The following provides a log of changes to this document:

Version	Date	Author	Notes
0.1	01/07/2021	Architect1	Initial Draft
0.2	16/08/2021	Architect1	P&I Project Team Review
0.3	22/08/2021	Architect1	Updates following socialisation review of 20/08/2021
1.2	8/11/2021	Architect1	PDG Approved Version (05/11/2021)

1.2 Document Authors

Role	Name	Responsibility
Author	Architect1	Solution Architect
Author		Technical Lead

1.3 Document Assurance

This document has been reviewed and approved by the following, the list has been grouped into different sections to aid readability as this document will be required at SDS PDG and possibly TDA.

Role	Description
Information	Shared for informational purposes including use as reference document for their domain's documentation and processes
Reviewer	Actively reviews the content to ensure alignment to guidelines and policies and technical accuracy, will contribute as required
Approver	Provides assurance that their domain is correct in context of the HLD

1.3.1 Publishing & Information Service (P&I Service) Project

Version	Date	Role	Reviewer/Approver	Responsibility
1.0	DD/MM/YY	*Reviewer*		PROJECT Delivery Manager
1.0	DD/MM/YY	*Reviewer*		PROJECT Business Analyst
1.0	DD/MM/YY	*Reviewer*		PROJECT Technical Lead
1.0	DD/MM/YY	*Reviewer*		PROJECT Lead Test
1.0	DD/MM/YY	*Reviewer*		Data
1.0	DD/MM/YY	*Reviewer*		Security
1.0	DD/MM/YY	*Reviewer*		Information Assurance
1.0	DD/MM/YY	*Information*		Lead Delivery Manager
1.0	DD/MM/YY	*Reviewer*	Architect1	Impacted Project Solution Architect
1.0	DD/MM/YY	*Reviewer*		FO/FH Integration Architect
1.0	DD/MM/YY	*Reviewer*		CFT Integration Architect
1.0	DD/MM/YY	*Reviewer*		Crime Integration Architect

1.0	DD/MM/YY	*Approver*		Future Hearings Lead Architect

1.3.2 Shared Services PDG

Version	Date	Role	Reviewer/Approver	Responsibility
1.0	DD/MM/YY	*Approver*		DACS - Lead SDS Architect
1.0	DD/MM/YY	*Approver*		SDS – Enterprise Architect
1.0	DD/MM/YY	*Reviewer*		Crime – Enterprise Architect
1.0	DD/MM/YY	*Reviewer*		CFT – Enterprise Architect
1.0	DD/MM/YY	*Approver*		Future Hearings - Lead Architect
1.0	DD/MM/YY	*Approver*		Future Operations – Lead Architect
1.0	DD/MM/YY	*Approver*		Security Architect
1.0	DD/MM/YY	*Approver*		Data Architect
1.0	DD/MM/YY	*Approver*		Integration Architect

1.3.3 TDA - IF Required

Version	Date	Role	Reviewer/Approver	Responsibility
1.0	DD/MM/YY	*Approver*		Chief Architect
1.0	DD/MM/YY	*Approver*		Shared Digital Services Lead Architect
1.0	DD/MM/YY	*Approver*		DTS Deputy Director (Acting)
1.0	DD/MM/YY	*Approver*		DTS Head of Digital Operations
1.0	DD/MM/YY	*Approver*		Deputy CISO
1.0	DD/MM/YY	*Approver*		Crime Programme Architecture Lead
1.0	DD/MM/YY	*Approver*		CFT Programme Architecture Lead
1.0	DD/MM/YY	*Approver*		DACS – Enterprise Security Architect
1.0	DD/MM/YY	*Approver*		DACS – Data Architect
1.0	DD/MM/YY	*Approver*		DACS – Platform Architect
1.0	DD/MM/YY	*Reviewer*		DACS –
1.0	DD/MM/YY	*Reviewer*		DACS –
1.0	DD/MM/YY	*Reviewer*		DACS – FH Lead Architect
1.0	DD/MM/YY	*Reviewer*		DACS – FO Lead Architect
1.0	DD/MM/YY	*Reviewer*		DCD Operations – Head of Live Services
1.0	DD/MM/YY	*Reviewer*		DCD Operations – Head of Platform Operations
1.0	DD/MM/YY	*Reviewer*		Crime Programme - Integration Lead
1.0	DD/MM/YY	*Reviewer*		CFT Programme - Integration Lead
1.0	DD/MM/YY	*Reviewer*		Government Digital Services (GDS)
1.0	DD/MM/YY	*Reviewer*		Government Digital Services (GDS)
1.0	DD/MM/YY	*Reviewer*		CPS Director of Digital Transformation
1.0	DD/MM/YY	*Reviewer*		Digital Product Management
1.0	DD/MM/YY	*Reviewer*		Lead Business Architect
1.0	DD/MM/YY	*Reviewer*		Service Design Authority representative

1.4 Document References

The following documents should be read in conjunction with this document:

Reference	Document	Version	Author	Source
DOCREF.01	Target Operating Model	2.0		Confluence
DOCREF.02	DACS Technical Guidance Library – Item 1			Confluence
DOCREF.03	DACS Technical Guidance Library - B2 Live Reporting and Management Information	NA	DACS	DACS Confluence
DOCREF.04	DACS Tech Debt Strategy	23/09/2019	DACS	DACS Confluence
DOCREF.05	Technical Design Authority (TDA) ToR	1.8	DACS	MS Teams
DOCREF.06	SDS PDG ToR			
DOCREF.07	DTS IT Services – Service Level Targets	1.3	DTS	Confluence
DOCREF.08	Host Security Pattern	NA		Confluence
DOCREF.09	DACS Technical Guidance Library – 2F. Security and Compliance	NA		Confluence
DOCREF.10	P&I MVP Requirements	N/A	Project	Teams
DOCREF.11	Availability Standards	N/A	Microsoft	Azure
DOCREF.12	DR Standards	N/A	Microsoft	Azure
DOCREF.13	Logging and Monitoring Policy	N/A	PlatOps	Confluence
DOCREF.14	Azure Database Storage	N/A	Microsoft	Azure
DOCREF.15	Drools Design Spike	N/A	Project	Confluence
DOCREF.16	Business Rules Decision Paper	2.0	Project	Teams
DOCREF.17	Azure Job Scheduler	N/A	Microsoft	Azure
DOCREF.18	IDAM Operations Manual	3.0	IDAM	Confluence
DOCREF.19	NCSC Cloud Security Principles	N/A	NCSC	Gov.UK
DOCREF.20	DTS DTU (BIAS) HLD	0.11	BIAS	Teams
DOCREF.21	DTS DTU (BIAS) LLD	0.9	BIAS	Teams
DOCREF.22	File Based Patterns	1.0	PDG	Teams
DOCREF.23	Cloud Infrastructure	N/A	DACS	Confluence
DOCREF.24	MyHMCTS Register Your Organisation	March 2020	MyHMCTS	Confluence
DOCREF.25	P&I Service Application Component Reuse	1.0	Project	Teams
DOCREF.26	HMCTS Media Guidance	March 2020	HMCTS	Gov.UK

2 Introduction

The Business Vision of the P&I Service is to support the delivery of HMCTS's commitment to open justice and to modernise and improve public access to information provided by HMCTS by publishing or displaying court/tribunal information (such as court and tribunal lists), according to the relevant policy requirements and business rules.

The service will provide a publishing platform which will enable the sharing or display of information provided by HMCTS and allow for updates of this information, as and when appropriate.

The publications & information service will simplify and streamline elements of the work currently required to publish lists, outcomes, judgments and enable information to be displayed via relevant presentation hardware, consistent with jurisdictional procedures and business rules.

This will improve HMCTS' commitment to open justice and enable the provision of transparent and consistent court and tribunal information across all jurisdictions.

When considering the publication of information there are a number of issues that need addressing, which may be summarised below:

1. Differing Formats
2. Differing routes for updates
3. Manual processes and interventions
4. Multiple places for updates
5. No single source or centralisation for publications online, in print or via communication channels

The Publication and Information (P&I) Service will ease the collection, representation and routing/distribution of updates to the channels ensuring that the most recent data is available and is both presented and formatted consistently.

2.1 Purpose

Currently there are inconsistencies across the landscape in how and what is being published by the various jurisdictions and the objective of this project is to bring these approaches together into one unified solution The core delivery partners and consumers will be within the Local Courts, Digital Delivery team and with partners (e.g. legal professionals), the press and the general public.

The current scope of the P&I Service, which is currently being driven from within Future Hearings, is to provide publication details of:

1. Lists (pre-hearing)
2. Live Case Status (during hearing)
3. Outcomes & judgments (post-hearing)

However, it is anticipated that this may be adopted more widely in the future (as part of subsequent programmes) to publish other official artefacts relating to hearings, cases and other topics. It is envisaged that this service will be used to make data produced by the Strategic Data Platform available to external parties.

2.1.1 In scope

1. Ability to publish:
    a) Court and Tribunal listing information across jurisdictions (Crime and CFT)
    b) Selected outcomes & judgments (to be selected with Crime and CFT)
    c) Live case proceeding updates (e.g. live case status accessible for Crown Courts providing URLs and views for in court screen displays – for Crime only at present)
    d) Hyperlinks where they are contained in documents will be toggled off when received (pending policy and legislation changes prior to becoming a live feature)
    e) Extensible to cover the needs of future data sources
2. Methods of access to published artefacts
    a) Single publication interface (web/mobile e.g. via a web redirect from gov.uk)
    b) Via gateway services (API)
    c) Via email (as an outbound subscription channel)
3. Users
    a) Unverified – Citizen users (e.g. the general public)
    b) Verified users (via IDAM)
        i. Internal (e.g. System Admins, HMCTS court staff, Digital Comms team, CTSC staff)
        ii. External (e.g. Partners such as Legal Professionals)
    c) Verified subscribers – Recipients of court e-emails (e.g. the press) or Systems via APIs
4. Access Management & Storage
    a) An Administration UI
    b) Storage & Subscription configuration interface

2.1.2 Out of scope

1. Publishing across wider HMCTS and MOJ, however, the design will be extensible for future data sources and receivers
2. Providing tactical solutions during transition from current case management systems to new systems, unless a solution appears to be suitable to do both without additional functionality
3. Any redaction of information MUST have been applied at source
4. There is no expectation to use the P&I Service to join a remote hearing from a list, which is handled by its own process through the courts, and the P&I Service will not have this capability
5. The negotiation of future contracts, i.e. transcription services, BAILII and purchasing legal books
6. Providing archiving facilities for transcription services or legal publications with the exception Employment Tribunals and BAILII which are currently archived through close relationship with HMCTS
7. Publishing of items not related to listing information, outcomes and judgments (e.g. academic reports/management information).
8. Changes to existing Court digital screen hardware
9. Any work on development of definition of the Hearing Management Interface (HMI) project other than feeding in and assuring P&I requirements on HMI (HMI only has limited use in P&I context for the S&L data source and is not the target API Gateway for the overall solution)
10. Customised formats for consumers (e.g. file formats suitable for data.gov.uk)

2.2 Intended Audience

The document is intended for technical and non-technical people looking to understand the purpose and operation of the Publishing & Information Service (P&I Service), particularly:

1. Senior Programme Management
2. Business Product Owners
3. Business Representatives
4. Delivery Managers
5. Business Architects and Business Analysts
6. Technical Architects
7. Security Architects

2.3 Definitions and Terminology

The following terms and abbreviations are used within this document.

Term	Meaning
API	An application programming interface is a computing interface which defines interactions between multiple software intermediaries. It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow.
APIM	API Management
DTS	HMCTS Digital Technology Services
DTU	The DTS Data Transfer Utility (also known as the DTS BAIS)
IDAM	Identity and Access Management
Judgment	A judgment is a decision of a court regarding the rights and liabilities of parties in a legal action or proceeding. Judgments also generally provide the court's explanation of why it has chosen to make a particular decision or court order. is a writeup of how the judge has reached their decision.
List	A list is defined as a set of ordered information that contains hearing details that can be published to different user groups based on permissions and information provided on the list templates. An example of a list would be a "public List" this would be published displayed by the court and highlight the hearings on the given parameters
MVP	Minimum Viable Product
Notification (If required)	Would allow verified users to receive a notification (likely email) to inform them that a list they are interested in has been published and they can log in to view that publication.
Outcome	An Outcome is the conclusion or result of a hearing (not necessarily the final outcome 'judgement for a case' as there can be many hearings for a case to conclude to a verdict).
RESTful	Representational state transfer - REST has been employed throughout the software industry and is a widely accepted set of guidelines for creating stateless, reliable web services.
S&L	Scheduling and Listing
SDP	Strategic Data Platform
Subscription	P&I subscription service will allow verified users to subscribe to lists of interest through (e.g. media who will use this to report on appropriate cases). Lists are attached to an email, which is automatically sent out when a list is available for publication.
Section 28	The law that provides for the ability to record vulnerable Witness Cross-examination prior to the actual Trial date so that it can present evidence during the Trial which may take place later..
Internal User	The person interacting with the PRE system that works for or are associated with the Court and or administration of a Court Hearing. This includes people from the following domains; 1. justice.gov.uk 2. ejudiciary 3. hmcts

External User	The person interacting with the PRE system that is associated with the case however does not have an account in the same domain as internal users.

2.4 Business Context

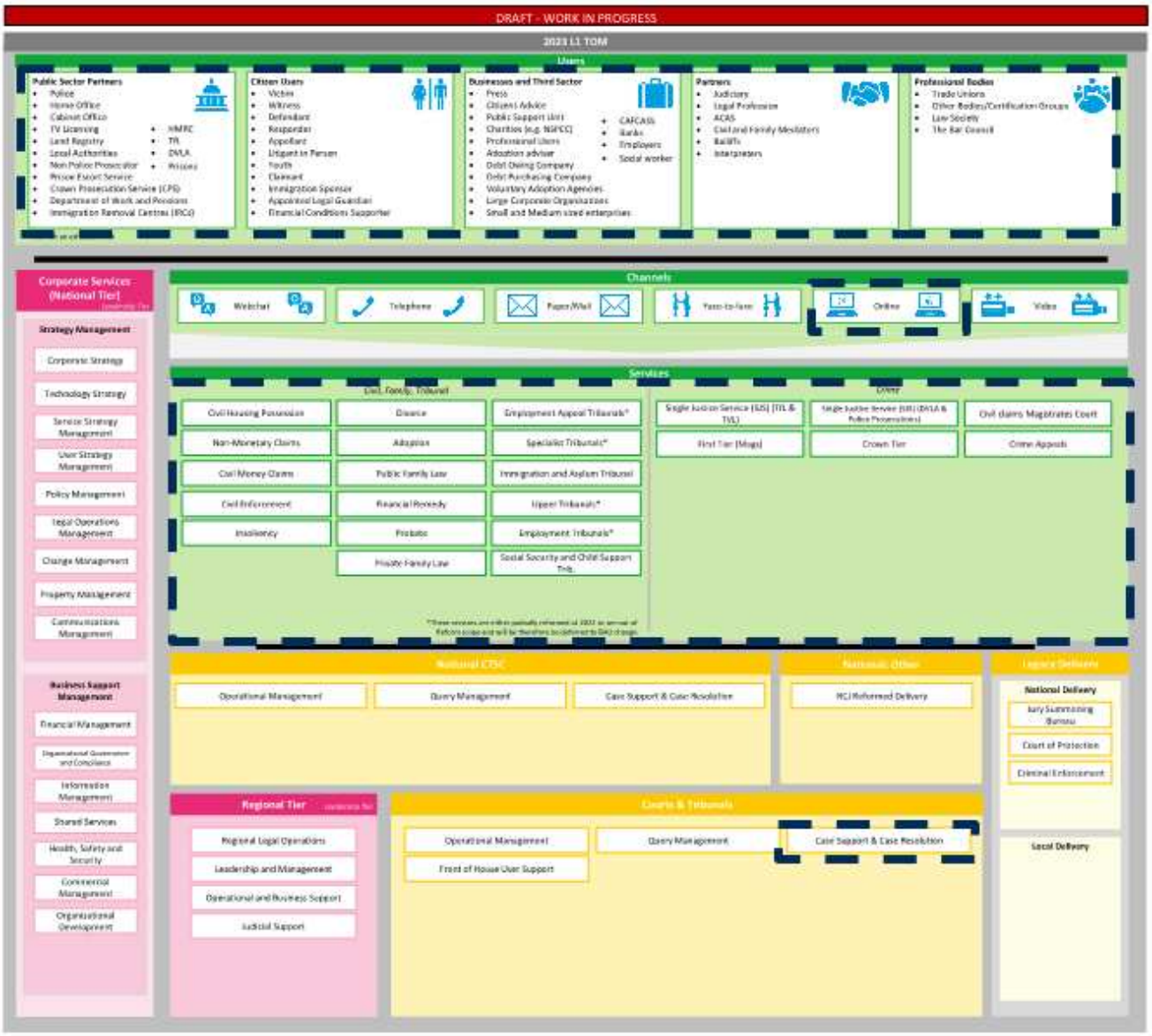
To support the delivery of HMCTS's commitment to Open Justice, to modernise and improve public access to information provided by HMCTS by publishing or displaying court/tribunal information (such as court and tribunal lists), according to the relevant policy requirements and business rules.

2.4.1 Target Operating Model

The areas of the Target Operating Model affected by the P&I Service are:

- L1 – Case Support & Case Resolution
- L2 – Publishing Management

The table below details the impacted areas. For completeness, the TOM has also been included, and the affected areas outlined with a dotted line.



Reference	Area	TOM Reference	Impact (Direct, Indirect)	Notes
TOM.01	Users	Public Sector Partners	Indirect	Subscribers or Non-Verified
TOM.02	Users	Citizen Users	Indirect	Non-Verified
TOM.03	Users	Business and Third Sector	Indirect	Subscribers or Non-Verified
TOM.04	Users	Partners	Indirect	Verified
TOM.05	Users	Professional Bodies	Indirect	Non-Verified (if not partner)
TOM.06	Channels	Online	Indirect	UI – Web/Mobile Gateway & Publication Services & Email
TOM.07	Services	CFT	Indirect	
TOM.08	Services	Crime	Indirect	
TOM.09	Direct	Case Support & Case Resolution Publishing Management	Direct	

2.4.2 Business Goals and Objectives

The table below outlines the high level business goals and objectives that are set out for the project.

Reference	Type	Goal/Objective
BGO.001	Goal	The P&I project will deliver a publishing platform which will enable us to share or display information provided by HMCTS into the public domain, in a single place, and allow for updates as and when appropriate.
BGO.002	Goal	Role based access to those who need enhanced case information e.g. Legal Professionals.
BGO.003	Goal	P&I (with S&L) will at end state replace capability currently provided by Xhibit and Libra. So, the P&I platform is a necessary component of Reform that contributes to being able to decommission Xhibit & Libra.
BGO.004	Objective	Ensure that information is made available within accepted timelines
BGO.005	Objective	Comply with Open Justice procedures and business rules
BGO.006	Objective	Simplify the processes to Publish lists, outcomes, judgments and Listing information to GOV.UK
BGO.007	Goal	Provide display information to court and tribunals buildings to display on relevant hardware
BGO.008	Goal	Provide data to existing external consumers across digital media channels and allow new consumers access as per business rules and permissions
BGO.009	Objective	Automate as much as possible the receiving of data from source systems
BGO.010	Objective	Provision for a wide range of potential known and unknown future data sources
BGO.011	Goal	Provide a reusable platform for the Publication of Information

2.4.3 Business Constraints

The following business constraints have been taken into consideration, as they may impact the delivery of the P&I Service.

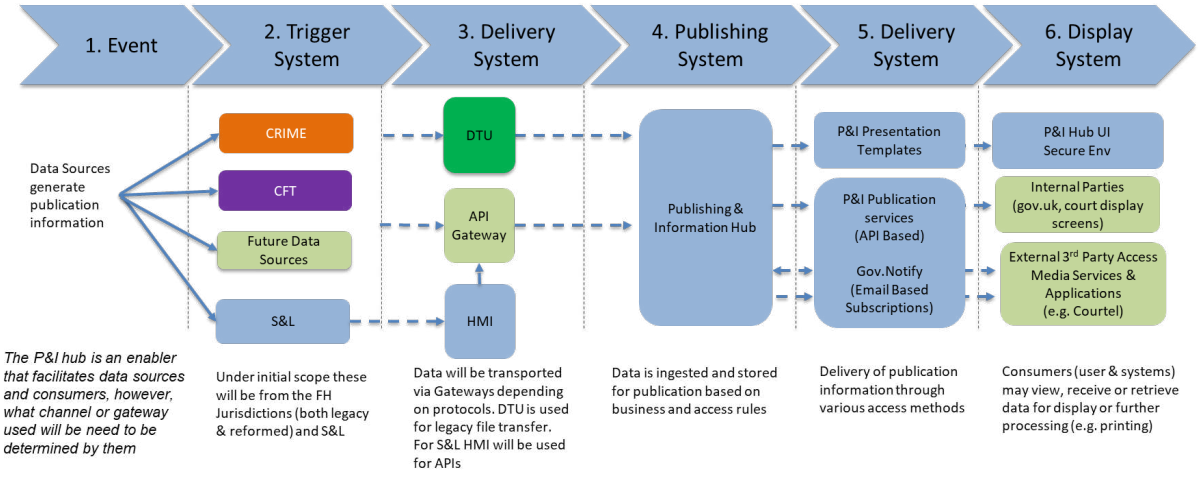
Reference	Constraint	Impact
BC.001	December Change Freeze	Cannot push all non-essential/use environments during this time so no changes to Prod environments during this time
BC.002	Training roll-out and roll out plans for cross site integrations.	Multiple sessions and communications needed, live training and wiki of support artefacts
BC.003	Resources required to operate dual processing during any transitions period will not be limited	Manual processing will increase and the resources would be stretched to fulfil the dual publishing processes
BC.004	Manual teams operating remotely need to be updated	Remote training, and updates for roll out and technical support
BC.005	Court Admin Resources to continue with Subscriber Validation and Recording Processes	Resourcing for existing manual process within Courts for validation Subscribers needs to remain in place
BC.006	Court staff to be available to verify Media Subscribers	Media subscribers will only be able to register when court staff are available

2.5 Vision

The vision of the P&I Service is to:

1. enable information that has been marked by business processes as "published" to be available to consumers.
2. support the delivery of HMCTS's commitment to Open Justice,
3. to modernise and improve public access to information provided by HMCTS by publishing or displaying court/tribunal information (such as court and tribunal lists), according to the relevant policy requirements and business rules.
4. as HMCTS modernises technology through Reform delivery, the P&I service will reduce the manual effort to produce lists and integrate applications across the infrastructure.
5. the P&I service UI to appear as a (click-though) service accessible from gov.uk (in a similar way to divorce or SSCS)
6. enable to onboarding of new data sources as part of an adoption process

The diagram below outlines the end to end flow envisaged for the P&I Service:



3 Compliance

This section covers the governance of the architecture and its compliance to programme principles and standards. The approach and rational behind the approach to the delivery of the architecture is explained along with key architectural decisions, and traceability to functional and non-functional requirements.

3.1 Approach

The project will conform to the architectural principles laid out within the Technical Guidance Library and it is not anticipated at this stage that any deviation will be required

As a data publisher, the P&I service is not the owner of the data it receives from its sources and as such it is incumbent on those sources to ensure that any information provided is correct and where necessary additional functions (i.e. redaction) have already been performed prior to receipt. Any business rules to be applied by the P&I service (i.e. dates to publish and retention periods) will be provided by data source owners for inclusion.

However, the P&I service will be building its own meta-data content, which it will master, so that information around access and MI is captured (e.g. audit logs & usage stats).

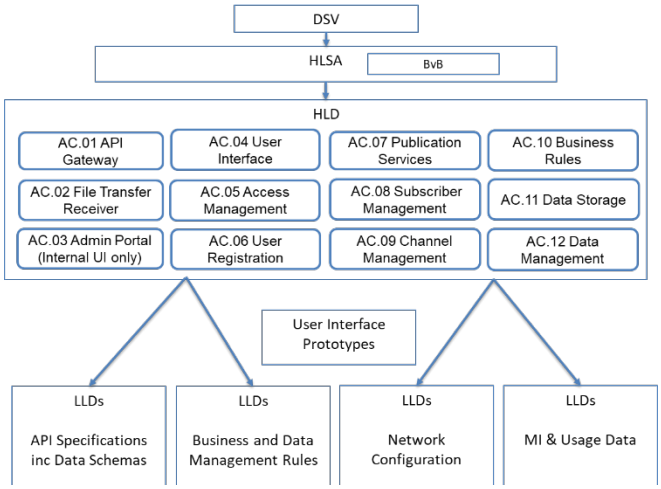
As part of a hybrid build approach existing services will be leveraged where possible. These have included:

Hearings Management Interface (HMI)	Reused scripts, templates, config, set-ups and devops including networking and certificates in building the API Gateway Logic for Gateway MI reporting Used by S&L as a mechanism to communicate with P&I
Data Transfer Utility (DTS DTU)	Utilising the DTU “Lift & Shift” pattern to support file ingestion from legacy sources
Design Guidelines	Following HMCTS & GOV.UK standards for governing UI design
CRIME & CFT IDAMs	Using existing CRIME & CFT IDAMs for User Authentication (where they host relevant users) and CRIME (Common Platform Change Team) and CFT MyHMCTS user/organisation registration processes
GOV.NOTIFY	Utilising existing approach for registration of subscriptions and sending of emails to subscribers
Legacy Specifications	Analysis of existing schemas from ingestion sources and consumers (e.g. Xhibit, Libra, Crime Portal & Courtel) to help create API Schemas
Crime Portal	Design time concepts and templates inc. analysis of REST specifications (as above) aiding understanding of process flows, typical rules, table structures, log contents and UI layouts. Further reuse was not applicable as a foundation for the P&I service, specifically as it was not designed to be a publication portal and would have needed significant rework and understanding of the embedded code base to remodel and rewrite which would have made it unviable
Strategic Data Platform (SDP)	Capturing of audit logs & reporting controls inc security events

How these apply to specific P&I components have been presented during DSV & HLSA phases.

3.1.1 Documentation Approach

The P&I Service is intended to be delivered as a componentised service with contributions and collaboration from a number sources, which may be worked on in parallel. However, these will all be defined within a single HLD that will act as an overarching document. However, due to the number of moving parts, LLDs will be delivered as component level documents that can be approved separately and worked on in parallel. Existing P&I services are carried out in a number of places and by a variety of publishers and it has been agreed not to document these as part of this project.



The following table provides a guide to P&I Documentation:

Doc Ref	Document Name	Format
PIHD001	DSV (Digital Solution Vision)	Confluence
PIHD002	HLSA (High Level Solution Approach)	Word Document
PIHD003	BvB (Buy vs Build)	Word Document
PIHD004	HLD (High Level Design)	Word Document
PIHD005	LLD - API Specifications inc Data Schemas	Word Document & YAML
PIHD006	LLD – Business and Data Management Rules	Excel
PIHD007	User Interface Prototypes	AXURE
PIHD008	LLD – Network Configuration	Azure
PIHD009	LLD – MI & Usage Data	Word Document (SDP template)

3.2 Architecture Principles

The following table explains how the project adheres to the REFORM programme architecture principles

A. Be user and business centric	Will align with other Reform UIs to deliver the best UX for user groups
B. Understand our Data	Provide meta-data definitions to control and secure our data Any API body and payloads will be well defined, relevant to the API call and logically structured to reflect relationships between data items.
C. Never compromise on Security and compliance	Publication Services and API & File Gateways will be developed and configured to make use of security standards and best practises as defined in the TGL and industry best practise.
E. Be Leading edge, not Bleeding edge	Making use of PAAS (Azure API Manager) and RESTful APIs which are all current technology patterns. Also, all stages of the development lifecycle are implemented on the Azure subscriptions (environments) using DevOps principles including CI/CD.
F. Cloud before on-premise	All components will be hosted on the Azure cloud
G. Be robust	The technologies selected (e.g. MS Azure API Manager), the patterns in use and the supporting technologies supporting technologies we will be using for application logging and monitoring (Dynatrace), security logging and monitoring (Log analytics workspaces/SPLUNK) will ensure that the solution built is stable and robust in design and operation.
H. Automate as much as possible	Data retention, user subscription and user housekeeping jobs will be fully configurable & automated Development and test processes will make use of DevOps processes and tools using CI/CD pipelines, version control and Infrastructure as Code.
I. Share and reuse knowledge	During design and build the project will be canvassing and sharing patterns and principles used.
J. Technical Guidance Library always prevails	The TGL will always be used as the 1st principle to adopt for the different areas of the design with exceptions sought where this is not possible.
K. Ingestion	Data sources MUST send atomic data objects that are self-contained and do not require data from other sources to fulfil their primary purpose.
L. Storage	All data will be stored as received - there will not be any manipulation in anyway, e.g. payloads will be held as blobs in the data store.
M. Presentation	Where required, presentation logic will contained in templates that will organise and format data from the data store for consumption. These will utilise HTML, CSS etc.

3.3 Policies and Standards

Where possible all policies and standards will follow TGL standards as outlined below. At the current HLSA phase no requirements for deviations have been identified.

Application Design	Will follow TGL guidelines: Applications & Core Technologies and will take account of other jurisdictions as they come on board
Service Design	Designed using TGL API Guidelines: API Strategy & Vision
UI Design	Following design and style guidelines: HMCTS Design System Standards And GOV.UK Design System Standards And following GDS service-assessments
Security	Will comply with all security policies and standards that apply to HMCTS/MoJ and be compatible with HMCTS/MoJ security systems and infrastructure Security & Compliance
Devops	Will follow TGL DevOps Guidelines DevOps Guidelines

3.4 Architectural Decisions

The following log explains the key architectural decisions made in the production of the architecture.

ID	Date	Decided By	Decision and Rationale
AD.01	27/04/2021	SDS PDG (DSV)	**The P&I Service will be a DRA Item for Publications** The P&I Service, whilst initially, being delivered for Future Hearings, will become a reusable DRA component for Publications
AD.02	04/05/2021	SDS PDG (BvB)	**The P&I Service will be delivered by a Hybrid Build Approach** As part of the Buy vs Build process a Hybrid Build Approach is to be taken to leverage existing functionality from currently deployed services (e.g. HMI & Crime Portal) to meet Crime MVP timescales
AD.03	27/04/2021	SDS PDG (DSV)	**Data Ingress to the P&I Service will always be via a Gateway** The usage of a Gateway will provide a standardised and controlled entry point to the P&I service to protect its boundary. This will include secure access, audit and throttling
AD.04	27/04/2021	Project	**HMI is to be used as the API Gateway for Future Hearings Information ONLY** The HMI (Hearings Management Interface) Gateway is the strategic tool of choice within FH for API based data transfer from S&L
AD.05	27/04/2021	SDS PDG (DSV)	**DTU is to be used for File Based Transfers** The DTU (DTS Data Transfer Utility) is the strategic tool of choice for File based transfer
AD.06	27/04/2021	Project	**Will ONLY accept API event based information in agreed standardised API schema formats** Standardised API Schema formats will be developed in collaboration with data sources during the LLD phases. Should data received fail validation a standard API error message (400) will be returned
AD.07	27/04/2021	Project	**Will NOT be responsible for any transformation work or other payload manipulation (i.e. conversions of document formats from .doc to .pdf)** The rendering of information will be the responsibility of the data consumer. Only locked file formats can be accepted P&I Service is not a master data source and does not have processes for validation and approvals, so will not update any information it receives. If an error is found by a user this should be corrected at source and resent as an update
AD.08	27/04/2021	Project	**The configuration of rules MUST be the responsibility of the Data Source Owner** The P&I service is the guardian of the data it holds and so will enforce any rules applied, however, it will not set them
AD.09	27/04/2021	Project	**Data sensitivity & classification relating to content MUST be provided by data sources** The P&I service must be provided with a data classification by its data sources so that it is able to apply rules to restrict access to sensitive data otherwise defaults will be applied
AD.10	11/08/2021	Project	**File Transfer will follow a lift and shift pattern** As per Arch Decision (File Based Patterns) PDG v1.0 file transfer will follow the Option 1: Lift and Shift Pattern. File to API type interaction is not required
AD.11	19/08/2021	Project	**Business Rules will be implemented using Java Code** This decision was reached further to the result of a design spike where the usage of Rules Engine (Drools), either as a new configuration or reused from existing Crime implementations, was considered against writing Java Code within the P&I service.
AD.12	15/07/2021	Project	**Business Rules and Definitions Evaluated using Decision Tree Logic**

ID	Date	Decided By	Decision and Rationale
			After assessment of business rules requirements and their complexity it was determined that the most appropriate way for them to be defined was to use decision tree type logic
AD.13	24/09/2021	IWG – Integration Working Group	**API Methods to follow HTTP Standards** POST – Additive transactions (inserts a new record every-time) PUT – Idempotent Transactions (controlled by data source either creating or overwriting an existing record)
AD.14	21/09/2021	Project	**Only Coarse Grained Access Control will be required for MVP** Whilst redaction will be carried out at source it MUST be applied at the artefact header level (and not the field level). If two versions of a document, redacted & non-redacted, are required then the source system MUST send them twice with appropriate data classifications and redaction having being applied
AD.15	30/09/2021	Security Architecture ()	**Usage of Verified/Un-verified Users Terminology** Verified Users being those having been either authenticated by an IDAM OR subscribers having had their e-mail addresses verified by Court Staff Un-verified Users being users that access the P&I service via the UI without having been authenticated
AD.16	27/09/2021	DWG – Data Working Group	**Housekeeping Service responsible for Removing Aged Artefacts and Inactive Subscriptions** Subscriber deactivation and artefact retention is driven by a scheduled housekeeping service as opposed to business logic that could be applied when a subscription is matched or an artefact is accessed.

3.5 Requirements Traceability

This section provides traceability to the functional and non-functional requirements that will be delivered by the architecture.

3.5.1 Functional Requirements

The following Functional Requirements are met by this architecture:

Ref	Functional Requirement	Category	Met
PIH001	The ability to receive listing publication data and information (automated feeds) as raw or pre-formatted information.	Ingestion- Data Collection	Yes
PIH002	The ability to receive outcomes publication data and information (automated feeds) as raw or pre-formatted information.	Ingestion- Data Collection	Yes
PIH003	The ability to receive judgments publication data and information (automated feeds) as raw or pre-formatted information.	Ingestion- Data Collection	Yes
PIH004	The ability to ingest data from reform and non-reformed services (HMCTS systems) for PIH Data and Document needs.	Ingestion- Data Collection	Yes
PIH005	The ability to manually upload data as a contingency should automated publishing functionality not be available.	Ingestion- Data Collection	Yes
PIH006	The ability to update a pre-formatted publication (e.g. PDF/word) through publication of a replacement (not via changing the payload)	Ingestion- Data Create/Update	Yes
PIH007	The ability to remove a certain field through invoking an update API method.	Ingestion- Data Removal	Yes
PIH008	The ability to remove an entire document.	Ingestion- Data Removal	Yes
PIH009	The ability to receive live case status information through automated feeds as raw information.	Ingestion- Data Collection	Yes
PIH011	The ability to send publications (pre-formatted or raw) to an external archive for superseded documentation. P&I may be involved in sending Judgments to The National Archives (TNA) which can be accessed by anyone (MOJ policy project currently in progress) & lists, outcomes and judgments to SDP which is accessed by academics – which could be a mixture of raw & preformatted information. *NB: This is not a definite requirement yet – P&I will have to work with MoJ as their project (Judgments storage and publication project) progresses to see how and if P&I can be involved in sending judgments to TNA*	Data storage & Access- Publishing Data Storage	Yes
PIH012	The ability to display data for specified periods of time as determined by the business rules.	Data storage & Access- Publishing Data Storage	Yes
PIH013	The ability to display labels on the user interface in Welsh or English.	Data storage & Access- Publishing UI Actors	Yes
PIH014	The ability for the general public to access and view the published data on external websites without any requirement to register in the service.	Data storage & Access- Account Management	Yes
PIH015	The ability to register a user.	Data storage & Access- Account Management	Yes
PIH017	The ability to provide identification and authentication controls.	Data storage & Access- Active Directory	Yes
PIH018	The ability to manage user accounts once registered, including the ability to reset passwords.	Data storage & Access- Account Management	Yes
PIH019	The ability to provide controls to restrict access to published data.	Data storage & Access- Data Permission Control	Yes

Ref	Functional Requirement	Category	Met
PIH020	The ability to validate an existing account is active or inactive.	Data storage & Access- Account Management	Yes
PIH021	The ability to restrict the names of individuals, who are included within any publication, from appearing in search engine results.	Data storage & Access- Security Policy	Yes
PIH022	The ability to configure access rules for user groups.	Data storage & Access- Rules Engine	Yes
PIH023	The ability to display data in accordance with Data Protection and GDPR requirements.	Data storage & Access- Data Policy	Yes
PIH025	The ability to display the latest data and published documentation.	Consumption- Publishing UI	Yes
PIH026	The ability to manage published list types. (place-holder awaiting Crime workshops - warned/firmed)	Ingestion- Publishing UI	Yes
PIH027	The ability to structure the data dependant on publication type (Lists, Outcomes, Judgments templates).	Consumption- Publishing UI	Yes
PIH028	The ability to allow or restrict printing from the browser.	Consumption- Publishing UI	Yes
PIH029	The ability for a user to confirm their agreement to T&Cs before downloading or printing from P&I User Interface.	Consumption- Auditing	Yes
PIH030	The ability to display data in accordance with the GDS Style Guide service standards.	Consumption- Publishing UI	Yes
PIH031	The ability for users to **search**, filter and sort data by specified criteria (Not for pre-formatted data).	Consumption- Publishing UI	Yes
PIH032	The ability to view publications on court screens.	Consumption- Publishing UI	Yes
PIH033	The ability for Criminal Justice Partners and Third Party commercial organisations to access the published data (in line with any data agreements made with HMCTS).	Consumption- Publishing Data	Yes
PIH035	The ability for live case status updates to be displayed via P&I online (HMCTS managed content pages which will be accessed via gov.uk). (Crown only)	Consumption- Publishing Data	Yes
PIH036	The ability to display lists in Welsh.	Consumption- Publishing Data	Yes
PIH037	The ability to subscribe to allow receipt to publications of interest being received via email attachment (See section 6.3.1.1 for more info on subscriptions)	Consumption- Publishing UI	Yes
PIH038	The ability to configure publication rules as defined by a set of business rules.	Data storage & Access- Rules Engine	Yes
PIH039	The ability to track manual intervention.	Data storage & Access – Auditing	Yes
PIH040	The ability to represent PDF formatted lists in the same format they are ingested	Consumption - Publishing UI	Yes
PIH041	The ability to format lists whereby the data is ingested in raw format using a template	Consumption - Publishing UI	Yes
PIH042	Will be visible on supported browsers and devices in a readable format in-line with the current GDS standards https://www.gov.uk/service-manual/technology/designing-for-different-browsers-and-devices	Consumption - Publishing UI	Yes
PIH043	The ability to notify users about publications of interest where there is a change or update by email	Consumption - Publishing UI	Yes

3.5.2 Non-Functional Requirements

The following Non-Functional Requirements are met by this architecture.

NFR Ref.	NFR Section	NFR Sub-Section	Categorisation	Requirement Description	Priority
ACC-01	Accessibility	Accessibility	Requirement	All user interfaces within Reform must meet level AA of WCAG 2.1	Mandatory
ACC-03	Accessibility	Accessibility	Requirement	The System must not return any unhandled errors when responding to an error triggered by a user or system. Error messages must be identified by the System and explained to the user/interfacing system in order to understand the cause of the error.	Mandatory
ACC-05	Accessibility	Internationalisation	Requirement	Solution must be able to switch between Welsh language and English language for all static content and labels.	Mandatory
AUD-01	Audit	Audit Trail	Requirement	Audit entries must be stored for 6 years, and entries must be archived and/or deleted after this time.	Must
AUD-02	Audit	Audit Trail	Requirement	Audit trail records must be held against all reference data and data associated with business critical activity. Audit records must include: - The identity of the user; System date & time; - Identity of the host terminal/PC; - details of the transactional/event/user action; - Copies of the new and old values where data has been changed	Mandatory
AUD-03	Audit	Audit Trail	Requirement	The system must keep records of all failed, illegal and irregular events such as (but not limited to): - Failed log-ons; - Attempts to carry out actions for which the user is not authorised	Mandatory
AUD-05	Audit	Audit Trail	Requirement	The System must ensure that all user initiated create, update and delete actions are logged for auditing purposes. These use cases would be limited to P&I system administrators via the admin portal.	
AVL-01	Availability	Location	Requirement	The system must be accessible to office based and remote professional and HMCTS users	Mandatory
AVL-07	Availability	High Availability	Requirement	Typical failure scenarios should be identified in the detailed technical designs. The frequency and outage required for each failure scenario needs to be estimated	Mandatory
SUP-10	Supportability	Operational	Policy	Primary service hours are defined as 08:00 to 18:00. Secondary service hours are defined as 18:00 to 08:00. Service must be supported during the Primary service hours. Services must be available to end users during secondary service hours but will not be supported.	Mandatory

NFR Ref.	NFR Section	NFR Sub-Section	Categorisation	Requirement Description	Priority
AVL-11	Availability	Resilience	Policy	All transactions must be recoverable in case of failure to complete. Repeated running of a transactions must not lead to duplication.	Mandatory
AVL-12	Availability	Resilience	Principle	System should be designed to avoid single point of failure	Mandatory
DAT-02	Data	Data management	Requirement	All data accepted by a system interface must be validated before being processed or permanently stored. Transactions containing invalid data must be rejected and the error reported.	Mandatory
DAT-03	Data	Data management	Requirement	All data captured through a user interface must be validated on entry and invalid entries rejected by the user interface, with an explanatory reason to the user.	Mandatory
DAT-04	Data	Data management	Requirement	The System must enforce all the maximum and minimum data lengths where defined by the data domain.	Mandatory
DAT-05	Data	Data management	Requirement	The System must ensure that data values conform to the relevant data domain.	Mandatory
DAT-06	Data	Integrity	Requirement	All transactions that fail should be either recovered to a consistent state or rolled back in their entirety, so that data entry can be resumed or repeated with the sole use of the end-user applications.	Mandatory
INT-02	Interoperability	Integration	Requirement	All date/times & timestamps should be recorded using UTC. Date/times & timestamps should be converted to local datetime at point of display where required.	Mandatory
INT-03	Interoperability	Integration	Requirement	Solution must comply with Integration strategy and standards	Mandatory
MNT-02	Maintainability	Availability	Requirement	The system must be capable of handling routine business change in a Configurable manner without falling below the applicable Service Levels. Examples of such changes are alterations or additions to Courts, Magistrates, Fees, etc. Reference data specific to the project must be clearly identified and update processes documented.	Mandatory
OPR-02	Operability	Audit Trail	Requirement	Audit records must be available for online analysis for at least 90 days up to any legal requirements specified within the Business Requirements.	Mandatory
OPR-03	Operability	Audit Trail	Requirement	In order to facilitate the analysis of transactions that affect several components, the System must provide a single location and format for the recording of audit information, across all System components. Generic reporting facilities shall be available for the analysis of audit information.	Mandatory
OPR-04	Operability	Audit Logs	Requirement	The following metrics must be gathered daily and made available to support staff via a daily metrics report: • Daily business transaction counts by type • Daily counts of items transferred over each system interface • Daily counts of exceptions raised, by origin, type and severity	Mandatory

NFR Ref.	NFR Section	NFR Sub-Section	Categorisation	Requirement Description	Priority
OPR-06	Operability		Requirement	The System must make provision for reference data updates appropriate to that system, such as telephone prefix changes, Post Office Postcode changes or the like.	High
OPR-08	Operability		Requirement	Appropriate date-based processing must include consideration of Leap Years, Bank Holidays, Short and Long days in all the region(s) covered by the System.	Mandatory
PER-02	Performance	Response time	Requirement	System response times must be evaluated at maximum load, with a fully populated database and shall exclude the impact of network latency. In the assessment of response time, an operation must be timed from the moment the operation commences to when the operation is fully completed. Where a single user operation involves a number of System operations (e.g. invoking other service operations in a sequence), the response time must be assessed for the user operation as whole, not just for each System operation	Mandatory
PER-03	Performance	Response time	Requirement	Trivial user operations (e.g. tabbing between screen controls) must be instantaneous (less than 0.25 seconds)	Mandatory
PER-04	Performance	Bandwidth	Requirement	Citizen and 3rd party facing services must be tested with a bandwidth restriction of 1Mbps and achieve the response time targets	High
PER-05	Performance	Monitoring		The system must be capable of monitoring response times for business transactions and reporting both Network Request Time (NRT) and (Software Request Time (SRT).	Mandatory
PER-06	Performance	Response time	Requirement	The System must provide a screen response for each operation of • 90th percentile response time within 1 second • 95th percentile response time within 1.5 seconds • 99th percentile response time within 2 seconds unless specified otherwise within the Business Requirements for the system. This must be tested under realistic load conditions.	Mandatory
VOL-01	Volumetrics	Volume	Requirement	Whilst the P&I Service is a new product offering it is not anticipated to increase current publication demands or the user base requiring publication information. Therefore, the P&I Service MUST be able to support existing publication volumes. • In total there are 70k Journalists, however, those that report on courts are limited and it is expected that on average there will be 1k unique media users a month • There are currently 35k subscriptions (e-mails via gov.notify) for daily court lists	Mandatory

NFR Ref.	NFR Section	NFR Sub-Section	Categorisation	Requirement Description	Priority
				• Daily RCJ court lists distribution: 3,859 (combination of public, stakeholders and media) • SJP media court lists: issued to approx. 250 journalists • SJP public lists (on GOV.UK): 6,784 (unique views from 1 Jan 2021 to 30 June 2021 - combination of public, stakeholders and media) • E-alerts subscribers list 31,824 (combination of stakeholders, legal professionals and media) • Courtel have 50k00 of their members belong to the 'professional members' category i.e. solicitors, barristers, media • There are 93k users of existing publication service, which includes members of the public and are not unique, as there will be duplication across data sets. In total user numbers for the P&I service are expected to be less than 100k	
REL-01	Reliability	Integration	Requirement	Transport failure should not result in loss of data/transaction	Mandatory
REL-02	Reliability	Resilience	Policy	System design should ensure that single points of failure are avoided	Mandatory
REL-03	Reliability	Capacity	Requirement	Proactive monitoring should be in place to monitor disk use to ensure sufficient disk space is made available for logging, data files, table space etc.	Mandatory
SCA-01	Scalability	Infrastructure	Requirement	The system as a whole must be scalable in all respects including total number of users and/or core business data, for example User Accounts, with only configuration changes and no change to core system code and/or product set.	Mandatory
SCA-03	Scalability	Infrastructure	Requirement	The system should be able to scale up or down horizontally in a dynamic fashion (Elastic scalability) while still adhering to performance NFRs	Mandatory
SCA-04	Scalability	Costs	Requirement	Lower environments such as development and testing must be proactively monitored to optimise cost by releasing/terminating resources not used	Mandatory
SEC-01	Security	Access Control	Requirement	Technical restrictions must be in place to make sure that users can only access those areas of functionality that they are specifically authorised to do so.	Medium
SEC-02	Security	Access Control	Requirement	Technical restrictions must be in place to make sure that systems can only access those areas of functionality that they are specifically authorised to do so.	Medium
SEC-05	Security	Access Control	Policy	The allocation and use of privileges shall be restricted and controlled.	Mandatory
SEC-12	Security	Access Control	Requirement	All Default system / vendor accounts are removed, or the passwords changed, privileges revoked and account disabled	Mandatory
SEC-13	Security	Access Control	Requirement	The system should enforce HMCTS password policy	Mandatory
SEC-31	Security	Access Control	Requirement	The default period before an inactive session times out shall be 30 minutes.	Mandatory

NFR Ref.	NFR Section	NFR Sub-Section	Categorisation	Requirement Description	Priority
SEC-33	Security	Control	Requirement	All data transmission, except email, across untrusted networks are encrypted in accordance with HMG IA Standard 4(IS4).	Mandatory
SEC-34	Security	Control	Requirement	Integrity of data is maintained within the System and during data transmission.	Mandatory
SEC-36	Security	Control	Policy	The system shall comply with HMG Security Policy Framework	Mandatory
SEC-37	Security	Control	Policy	The System shall comply with the ~HMCTS Information Risk policy.	Mandatory
SEC-38	Security	Control	Policy	The system shall comply with the HMCTS Information Security policy	Mandatory
SEC-39	Security	Access Control	Policy	Direct access control to the primary servers or services via model connectivity	Mandatory
SER-04	Service Continuity	Continuity	Requirement	The solution should identify typical failure scenarios within the System's technical design specification, with for each failure scenario: • An estimate of the likelihood of such a failure • The state to which the System can be recovered (the recovery state) • The time taken to achieve such recovery (the recovery time) • The actions necessary to recover to that state whilst, highlighted here a full FMEA analysis will be carried out during LLD phase	Mandatory
SER-05	Service Continuity	Continuity	Requirement	Each component of the Service should be able to recover its hardware, database or application to the point of failure (e.g. via backups or re-do logs) with the agreed minimum loss of data	Mandatory
SUP-01	Supportability	Traceability	Requirement	In order to facilitate the analysis of transactions that affect several components, the system should be able to co-relate the audit trail (users) AND log entries (systems) to the transaction.	Mandatory
SUP-03	Supportability	Consistency	Requirement	All date/times & timestamps should be recorded using UTC. Date/times & timestamps should be converted to local datetime at point of display where required.	
SUP-06	Supportability	Monitoring	Requirement	It must be possible to configure new reports, views and alerts as part of continuous service improvement.	Mandatory
SUP-08	Supportability	Monitoring	Requirement	It must be possible to set defined thresholds for utilisation and capacity, after which warnings will be alerted to 1st Line Support staff.	Mandatory
SUP-09	Supportability	Monitoring	Requirement	The Solution must ensure that application and error logs are shifted to a searchable database.	Mandatory
SUP-10	Supportability	Monitoring	Requirement	The Solution must ensure that logs are separated into categories but not limited to: Application Logs Error Logs Audit Logs	Mandatory

NFR Ref.	NFR Section	NFR Sub-Section	Categorisation	Requirement Description	Priority
SUP-11	Supportability	Monitoring	Requirement	The solution must monitor resource utilisation at defined intervals and alert to utilisation in excess of defined thresholds to the 1st line support team.	Mandatory
SUP-12	Supportability	Monitoring	Requirement	The System must be able to categories the application and errors logs in below category but not limited to: • Severe • Error • Warning • Info • Debug	Mandatory
SUP-13	Supportability	Monitoring	Requirement	The System must be configurable to alert the different level of errors to the 1st line support staff.	Mandatory
SUP-14	Supportability	Monitoring	Requirement	The System must be configurable to store different levels of application and error logs.	Mandatory
SUP-15	Supportability	Monitoring	Requirement	The System must log all errors for the purpose of dealing with support incidents.	Mandatory
SUP-16	Supportability	Monitoring	Requirement	The System must log and store performance metrics, which must be captured and stored for 6 months for the purpose of trend analysis.	Mandatory
SUP-17	Supportability	Monitoring	Requirement	The System must report the below in the error logs/reports but not limited to: -Date / Time -Username -Human readable description of the error -Category (e.g. Error, Warning, Info).	Mandatory
SUP-18	Supportability	Monitoring	Requirement	The system must support remote monitoring of all critical components, such that the health of the system can be determined by support staff without manual intervention or reporting of issues by users.	Mandatory
SUP-19	Supportability	Monitoring	Requirement	All micro services must be observable, discoverable and calls between microservices traceable.	Mandatory
SUP-20	Supportability	Monitoring		Infrastructure performance metrics should be available in real-time and historically in one-minute increments over the last 24-hours covering at least the following key components. - Overall CPU usage per physical server - CPU details per CPU per physical server - CPU stats per process - Overall memory usage per physical server - RAM usage per process - Swap file size	Mandatory

NFR Ref.	NFR Section	NFR Sub-Section	Categorisation	Requirement Description	Priority
				- Overall heap usage per component instance - MB of free disk space on each partition - Number of active threads - Garbage collection stats per JVM - NIC utilisation per physical server - NIC utilisation per NIC per physical server	
USE-01	Useability		Requirement	When a business logic error occurs the user should receive an explanatory message indicating what they have done wrong.	Mandatory
USE-02	Useability		Requirement	When a system error occurs the user should receive an explanatory message indicating that there is something wrong with the system which has not been caused by them.	Mandatory
USE-03	Useability		Requirement	When an error occurs an indication as to what action the user should take should be given.	Mandatory

4 Risks and Issues

This section catalogues the architecturally significant assumptions, risks, issues and dependencies that have been identified.

4.1 Assumptions

The following assumptions have been made and are tracked within this architecture.

ID	Assumption	Actions	Status
A.01	All services will be able to consume the P&I Service API schemas	Publish API Specifications (LLDs)	Open
A.02	Access to Crime and CFT IDAMs for SSO by Legal Professionals	Validated with IDAM owners	Closed
A.03	There will be tactical solutions in place to enable Xhibit and Libra to communicate with the P&I Service	BAs to confirm as part of their analysis	Open
A.04	During the MVP the media will only have verified subscribers access and will be limited to non-verified UI access	Subscriber process confirmed with service design	Closed
A.05	Data Archiving will meet necessary standards even though they have not yet been fully captured and agreed	Work within the compliance guidelines for all published data to meet GDPR and Data Protection standards	Open
A.06	Publishing of items not related to listing information, outcomes and judgments (e.g. academic reports/management information) is out of scope	These will continue to be published as they are now, albeit, the design will not prevent it being included as part of future scope	Closed
A.07	Service Design Artefacts that this HLD is based on will be approved at DA.	Review document to ensure the most up to date information is available for DA Meeting.	Open
A.08	The service design artefacts will be approved at DA	If not then the HLD will need to be impact assessed against changes.	Open
A.09	Once Reference Data systems become available integration designs will be created	The HLD will need to be amended as well as LLD's to incorporate the relevant integration(s)	Open
A.10	CFT will be able to consumer P&I services prior to having provided their requirements	Based on the overarching objective being that the solution is to be generic in its nature and thus not customised bespoke to a service, this assumption implicitly has to exist.	Closed
A.11	As part of the strategic refresh of the IDAMs the P&I service will need to follow the transition steps of its user groups to their new locations	The P&I programme to be kept abreast of the strategic IDAM roadmap and have appropriate resource to be able to switch to the new strategic IDAM when appropriate	Open

4.2 Risks

The following risks and mitigations have been identified and are tracked within this architecture.

ID	Risk	Proximity	Likelihood	Impact	Mitigation	Status
R.01	Additional requirements may come from discussions with future data sources (e.g. CFT)	Unknown	M	M	Create an adoption roadmap with future data sources post MVP with a scalable architecture	Open
R.02	Data Archiving Requirements are not currently defined so the HLD is focusing on very high level assumptions based on good design practice.	Close	L	L	The HLD will need to be impact assessed when the requirements are ready, this could lead to changes but are not expected to be significant	Open
R.03	Data sources must provide accurate flags as without them to prevent incorrect/sensitive information being displayed	Close	M	M	In the case of missing flags default values will be provided within Business Rules. Default values will always err on the side of caution so that only public data will be displayed. In addition, update and delete functions will be provided to enable data sources to correct errors (both automatically via the API Gateway or manually via the Admin Portal)	Closed
R.04	Risks of seeing contradictory information being published by both P&I and existing services outside of P&I.	Close	L	L	Any external (to P&I) publication will have come via P&I and be sent from the service to the external source (e.g. Courtel). Therefore there will be no data that is more up-to-date outside of our own organisation. It is planned that any updates to data on P&I will also be shared with the external publisher(s). Therefore there will be no chance of "aged" information being available. As described per **I.02** the comms plan will ensure that there is no duplication between legacy systems and P&I. P&I is not decommissioning any systems but in may allow them to be decommissioned should that be appropriate (e.g. a legacy system that only exists to publish a list).	Closed

R.05	If the DA decide to challenge the service design artefacts this could result in rework and updates to the design in the HLD and re-submission for approval	Close	M	M	Validate the Impacts of any Design Artefacts being assessed , ensure the current understanding and SD Docs are correct. Post any decision provide an Impact Assessment of any challenges	Open
R.06	CFT does not currently have plans to use the P&I service and as such does not know whether it meets their requirements	Unknown	M	M	Create an adoption roadmap with CFT post MVP (driven by S&L)	Open

4.3 Issues

The following issues have been identified and are tracked within this architecture.

ID	Issue	Actions	Status
I.01	Which IDAM should Press be held on?	As part of the MVP media users will only have verified subscriber access with lists maintained within P&I having been validated by Court Staff. Should verified UI access be required a solution will need to be developed so that they can become fully authenticated users (e.g. via an IDAM)	Open
I.02	What Programme Comms are in place for adoption of the Service?	Hardware teams that support across jurisdictions will be readily informed and updated to any process changes required. P&I will looks to minimise change for integrations (for example links and URL data packets etc as today can and will be sent to the connected services and allow hardware to be maintained and configured to our service with minimal disruption).	Closed

4.4 Dependencies

The following dependencies have been identified and are tracked within this architecture.

ID	Dependency	Actions	Status
D.01	Gov.notify is required to deliver emails to subscribers	P&I will need registered and onboarded with GovNotify as the GovNotify service will be used to send communications to previously subscribed users. (This is not a hard dependency for the P&I service as it would remain up and running should GovNotify be down, just notifications would not be sent)	Closed
D.02	Approved list of verified subscribers to be collated from court admins for courts	Planned business processes will mitigate the absence of the lists	Open

ID	Dependency	Actions	Status
	involved in MVP. Will also require a list of those court admin users	however as a project insight is lost insight. The MVP is only currently looking at a single court to start with. This is a minor activity and will be an implementation activity as we rollout	
D.03	MyHMCTS and CFT & CRIME IDAMs must be available for registered user registration and access	Registered Users (& Organisations) to use the existing MyHMCTS service	Closed
D.04	Court Lists from Future Hearings so that appropriate style sheets can be developed for presentation via the UI or rendering emails for subscriptions	To be determined during LLD phase	Open
D.05	Verified user base needs to be maintained so that they can only access relevant information to their role via the UI or subscriptions	Crime & CFT IDAM owners/super users to maintain their user base Non-IDAM verified subscriptions will be created/updated by Court Staff as per existing processes, with house-keeping processes to remove inactive ones	Closed
D.06	Reference Data will be required to identify key attributes including Court Locations.	Sourcing and maintenance to be determined at LLD phase	Open

5 Baseline Architecture

Currently P&I service are carried out in a number of places by a variety of publishers and it has been agreed that under these circumstances not to document them. The new P&I service will be delivered as a target architecture, as outlined under section 6. It should be noted that adoption of P&I Service by Jurisdictions will be staged and defined and delivered by DTS post MVP go-live.

6 Target Architecture

This section describes the Target Architecture needed to meet the business outcomes, goals and objectives listed in Business Goals and Objectives and

Requirements Traceability.

6.1 Business Architecture

6.1.1 Business Capability View

The capabilities addressed in the designs are illustrated as business process flows and can be referenced to the core capabilities features. Such as Publish a List, Publish an outcome, Publish a judgment...

As part of the Service Design work the capabilities covered and delivered within the Publications and Information project are:

1) Publishing Lists before the day (publishing Management)
    A) External Publishing online
    B) Subscription and Notifications
2) On the Day management Maintaining Lists
    A) Update live case status information, including updates to on the day Lists (Time amendments and updates, locations etc)
3) Facilitation of Hearing
    A) Live status updates and lists on internal screens (e.g. publishing information to a URL)
4) Recording a Hearing Outcome, (publishing Management)
    A) Online updates for information on the outcomes and judgments for the case

The Business Capabilities are linked to the technical components within the Publications and Information's Project solution and will be defined more within the LLD documentation, the approach is to segment the components into Business logical features as well as core technical components such as Performance management and auditing capabilities within the application itself.

Business Capability	Technical Component	Description
Upload a File for publishing	AC.01 - API Gateway	The API Gateway will be the API based point of entry for the data sources and be responsible for protecting the boundary of the P&I service, carrying out functions such as authentication, throttling, white-listing etc, and validating any structured data against schema definitions.
	AC.02 - File Transfer Receiver	The File Gateway will enable data sources to provide unstructured and read-only file based information (e.g. PDFs). It will poll specific data source file locations on a scheduled basis and upload those files to the P&I Data Storage area
Access and view publications	AC.04 - User Interface	A user interface to allow users to search and browse information relevant to their user role
Manage Users, Content and control within the Application.	AC.03 - Admin Portal (Internal UI only)	Specific UI admin screens will be made available to users with admin roles so that they can maintain subscription and channels.
	AC.05 - Access Management	Ability to manage internal, admin and external users granting permissions to view information that is not available for general consumption based on user's roles and data sensitivity. Internal admin roles to allow for the configuration of rules and organisations
Request Access **Grant and approve access** **Validate users** **Manage Users, Content and control within the Application.**	AC.06 - User Registration	Partners will be maintained and configured via their respective organisations who will have followed a registration process and be assigned a user group that they will have admin control over
Request and manage content for publications	AC.07 - Publication Services	A service or set of services to support dissemination of information to various consumers
Subscribe to updates and notifications	AC.08 - Subscription Management	A configurable list to determine the onward transmission of publication information to registered subscribers (data consumers)
Send lists to third parties	AC.09 - Channel Management	Support and management of various channels that may receive publication services (e.g. email, API etc)
Manage rules for diverse types of publications.	AC.10 - Business Rules	Ability to support business rules that contain logic for the holding back of information that is not yet ready for publication or not publishing information that is not appropriate for a user role. This logic will be applied at a header level and not in relation to specific data within a payload. Any redaction of information MUST have been applied at source
Manage rules for diverse types of publications (restrictions, periods, and retentions)	AC.12 - Data Management	Ability to manage data based on data governance, retention and security policies. Including providing Usage Data & MI to SDP

6.1.2 Business Continuity View

In the event of a partial or complete IT failure there are various manual interventions which will cover these scenarios. In the event of partial failure, an internal member of staff with admin rights will have the capability to manually upload (to create or update) or delete publications from P&I using an administration login and UI. When the new publication is uploaded or deleted, this is mirrored wherever it is displayed by P&I. This will replace any automated inbound feed of raw data or pre-formatted publications received from source systems. Lists which are produced on source systems can be manually emailed out to distribution lists . Court Admins should notify the approved subscribers, from their records. If the partial IT failure is gov.uk only, then P&I would continue to provide Courtel with the data they need via API. This means that users could continue accessing electronic lists via the CourtServe website.

In the event of a complete IT failure, business operations will continue to print daily lists from the source systems, which is the current process alongside the electronic publication and distribution of lists. This means there would be no change to this part of the process but a reliance on paper lists rather than online lists for users who need guidance in court on the day. Users can also continue to contact the courts as they do today via telephone and email.

Business Continuity:

1. When will the service be affected by an intrinsic outage
    a. Lists services out of action (OOS for P&I)
        i. S&L
        ii. CP
        iii. CFT
    b. P&I Is not responding (API Gateway not reachable)
        i. How to publish
        ii. Fall back solutions
    c. Courtel not available (OOS for P&I)
        i. From P&I
    d. P&I is not visible in the browser
        i. 404
        ii. 50X
    e. Service partners are non-responsive (OOS for P&I)
        i. Gov.UK
        ii. Gov.Notify
        iii. API GW non responsive
        iv. URL changes
        v. 3rd party non responsive

Expectation:

Currently the Publication services operate a very manual trigger process and highlight services that are often non joined or disparate in interoperability. The list production is maintained by the integrations of the legacy and 3rd party solutions currently and distributed by a manual process of management for email and call to action triggers on functions from the Case management systems (inter-linked by CP to Xhibit to Court-serve(Courtel)

Impacts:

As current process is limited we are only producing an on the day record of lists and manually emailing and generating from the case management solutions the lists that are sent to courts or subscribers, as a way of introducing the P&I services we will look to decouple dependency and maintain fall back processes utilising the current delivery partner and service through court-serve (Courtel's publishing product). Where today the email subscriptions and lists are sent via a mailing list, and automated processes via API are done through to Courtel (email failsafe) we will expect to maintain these processes maniually if a service is unresponsive within the P&I solution. Additionally the introduction of a court list (report) within List Assist (S&L Strategic) will also be

available for print and download, thus minimising any on the day information impacts to the information available.

Immediate vs delayed:

Publications are sent in advance of any communication for the publics consumption, those involved in the case are in receipt of location, times and proceedings ahead of any appearance and as P&I is an information service for those not necessarily directly involved within the case or hearing, the details of which are readily available to defence/prosecution and court clerks via Case management, case progression processing and communications of dates and times ahead, the impact of P&I services going down across the board is limited and not a severity 1 in terms of daily operation of hearings. This being said there is a need to ensure continuously serviced feeds of data are shown but with any failure there will be a support ticket logged and raised automatically inline with DTS processes and ratings to properly identify, report and fix any issues within the service and dependent to / from services along the delivery chain.

Resolution:

The resolutions are defined in three categories:

1) Ingres(inbound) services
    a. Any solution utilising P&I for a delivery will send a trigger, data or request to P&I.
    b. Where P&I are not able to receive (internal failure – see type 2 below) else outside of P&I scope and resolution is with the sending party or failed function pre ingress call at sending party.
2) Internal Services
    a. Internal components producing the deliveries' to externals and responding to requests from within P&I.
    b. Within scope and will raise tickets through SNOW and manage through DTS partner
3) Egress(outbound) services
    a. Processes that send outbound communications from P&I to the wider services, such items are internal and external services within the products remit, including 3rd party providers
    b. Where P&I cannot send due to internal error (see point 2 above) else partner service or supplier are notified and expect a ticket to be raised with P&I logs for supporting identification of failure

The table below highlights example scenarios and resolution methods and current expectations: Severity is assumed at present, we are a convenience service at current take so the necessity of severity will be minimum. Sev 1 being a catastrophic failure and government cannot operate its function or service intrinsic to public service, Sev 2 is a mediocre issue but will not affect operationally the processes that are required for core activity to proceed, I.e. hearings can still take place, Sev 3 is a disturbance but again not a n operational issue and will not impact if the service isnt returned to normal within a week or so forth... (these are examples and used to articulate the levels of severity expected in the failure table below)

Ref	Outage	Description	Severity	Resolution
001	Inbound service	LA is not able to send list data	2	Outside of P&I Scope. Service ticket raised within S&L
002	Inbound service	Case management solution is not able to send data	2	Outside of P&I scope. Service ticket raised by CMS
003	Internal Failure	P&I cannot produce list or publication within internal component	3	Ticket raised to SNOW and DTS monitor and pick up failure to be resolved within 24 hours
004	Outbound Failure	P&I send information to HMCTS services (gov.notify) and failure to respond	3	Outside of P&I scope, Ticket should be raised by service, DTS process to notify service of issues and logs to support from P&I are sent

Step Scope	Potential Failure Mode	Potential Effect	Severity	Causes	Freq %	Control
Ingestion of data via API to P&I	Calling to API GW of P&I	Files and data cannot be received by P&I	Minor	API GW down, upstream systems and sources not available	<1	External controls in source systems, audit and health check on gateway
Control	User Auth Failure	Users access is granted, revoked in error	Medium	Auth systems communications are not available	<1	HTTPS return codes will identify and audit monitoring and alerts from external systems of any catastrophic failures
Core	Generation of Publications (Lists) (Court Screen updates) (Outcomes) (Judgements)	Publications fail to produce and are not sent or published	Major	In terms of service but not operationally, this would be an internal issue and need audit logging to be validated and a potential	<1	Internal health checks and maintenance, logging of errors in audit logs
Dependant services	Notify doesn't send Courtel is down Domain services are offline IdAM service N/A Cloud features/partner provider is non responsive	End to end failures or access errors for publishing, reviewing and updating online	Major to service but not to operational	External delivery and capabilities are non-responsive and return errors	<1	External Management of components and logging/reporting
Consumption	External partners cannot be reached, or consume	Data (as no stored archive) will be removed and updates wont be resent at a later date	Operational Minor	Not our concern and any bounce backs should be notified to us not from us, unless our service is reported to be erroring (external again) then we will investigate	<10	External notifications or internal failures and logging

6.2 Data Architecture

6.2.1 Conceptual Data View

Both structured events and unstructured files (e.g. PDFs) will be received from the P&I data sources. Unstructured data will be received as read-only format files (e.g. PDFs) and structured data will be received as events.

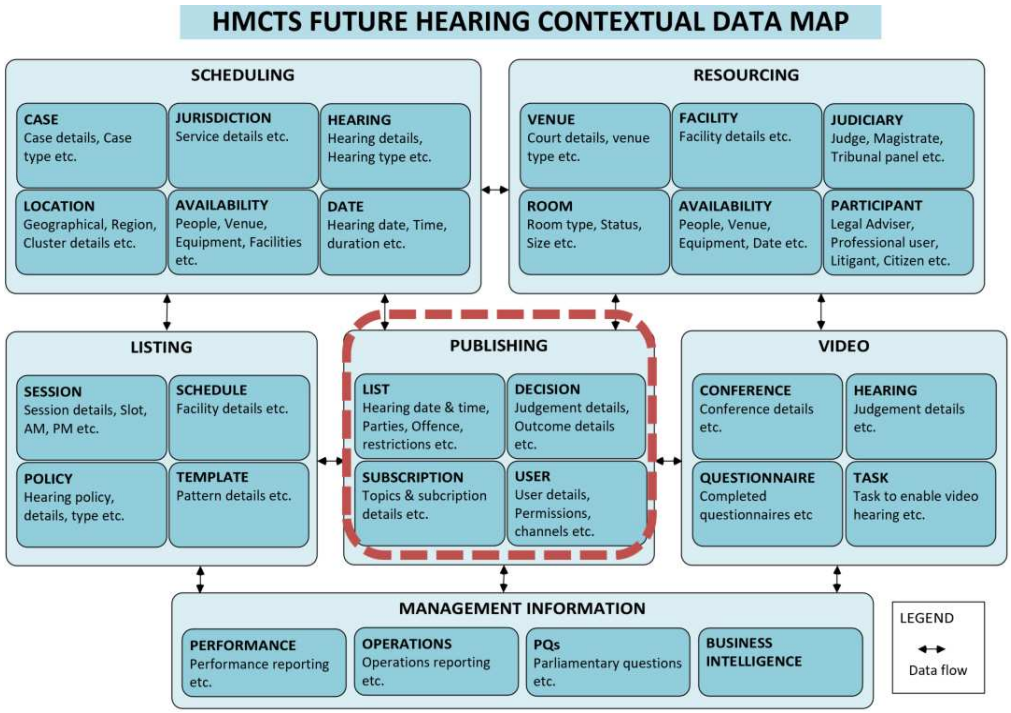
In either case the key artefacts will be those that sit within the Publishing context and will include:

1. Lists (Pre-Hearings)
2. Live Case Updates (During Hearings)
3. Decisions/Outcomes & Judgements (Post Hearings)

However, as a generic platform the P&I service is designed to allow for future artefacts to be added.

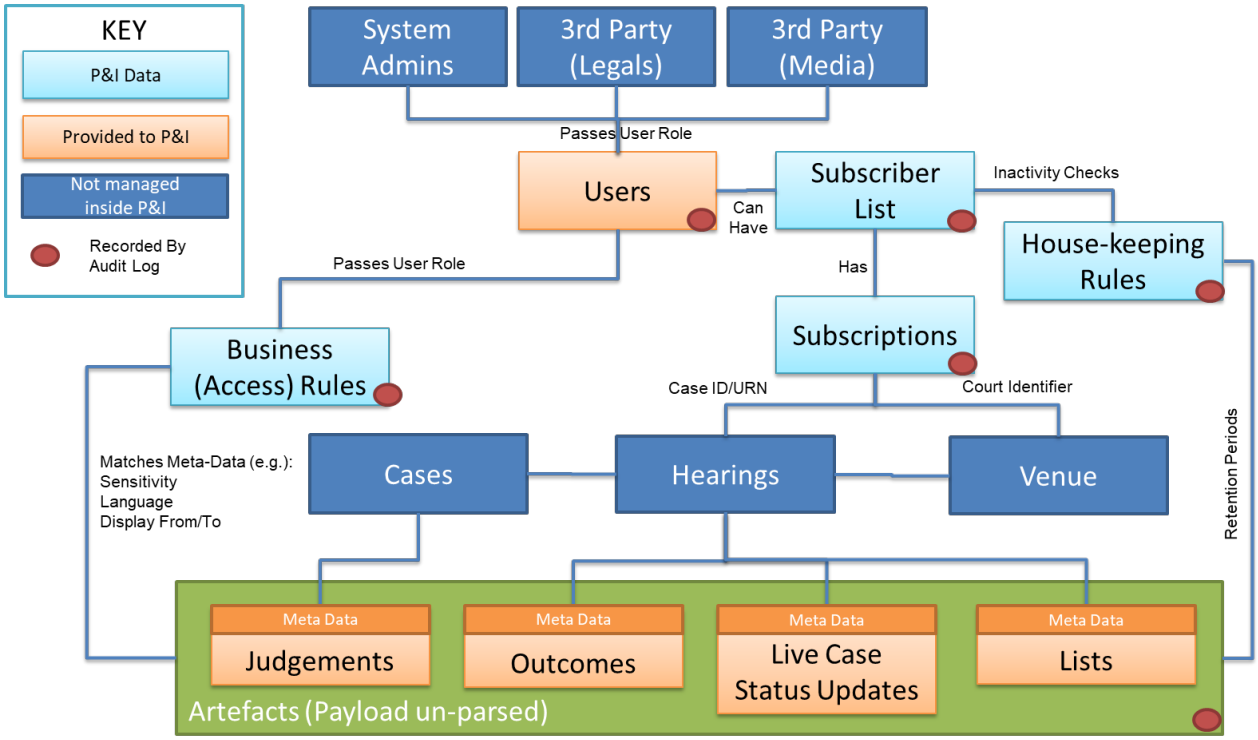
In addition, the P&I service will also use the following entities to control access and subscriptions:

1. Subscriptions
2. Users
3. Meta-Data provided by Data Sources (Information Producers)



Provided on 15/04/2021:

Conceptual Data Model



6.2.2 Logical Data View

Primary functionality within the P&I service will be driven from meta-data supplied by the P&I data sources. This will enable it to apply data management rules when storing data and its subscription and business rules to the consumers that wish to access it. The meta-data required will include:

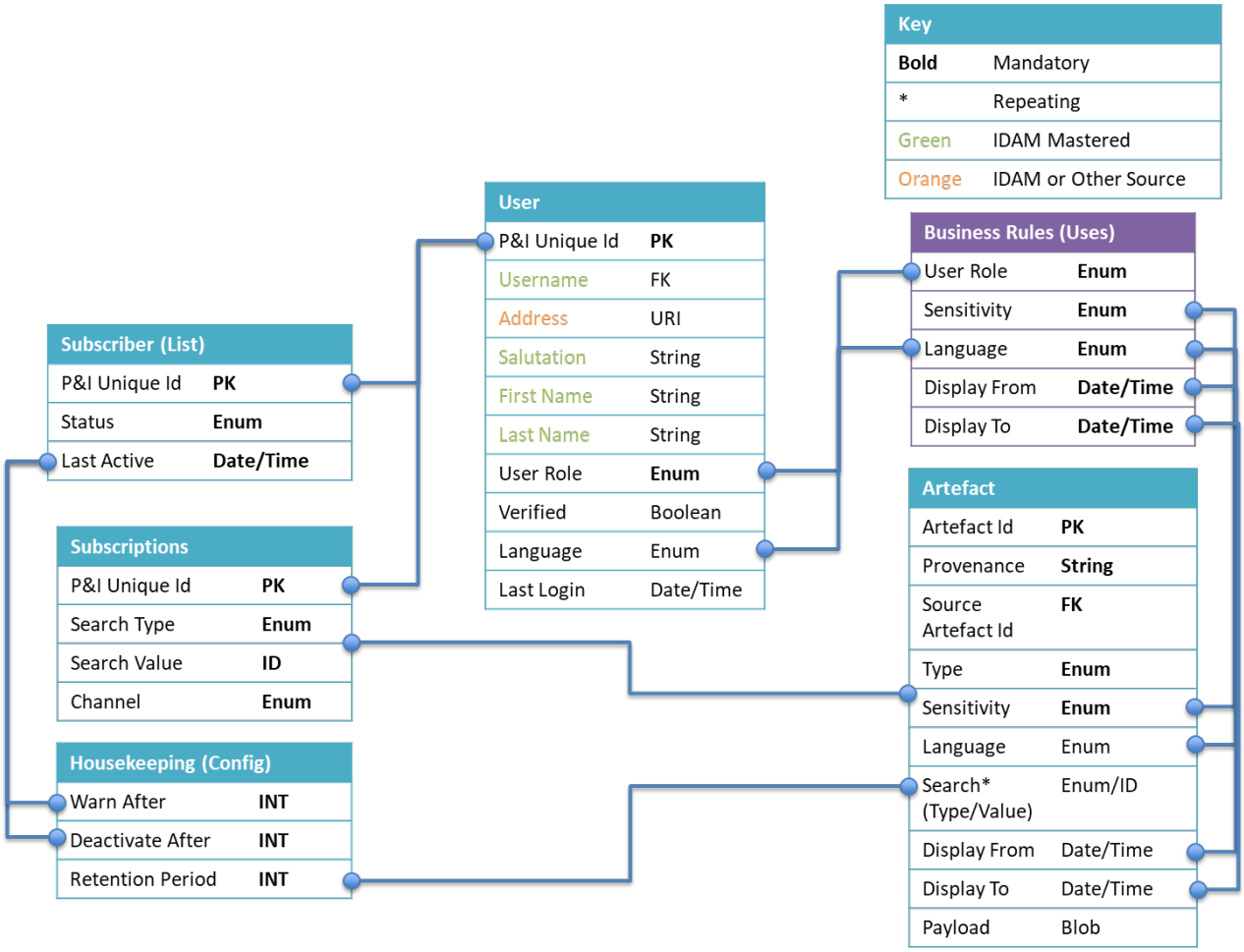
1. Restricted data flags indicating data sensitivity and classification
2. Dates and times for publications to indicate when publications can be viewed from and how long they should be retained (aka Retention Periods)
3. Language, particularly for Welsh Language (specification of which will align to Welsh Language Support)
4. Ability to align to a court via location specified data references (including Welsh names)
5. Specific requirements such as role based permissions and restrictions (i.e. legal professionals to see enhanced information and the public not etc...)

This is at a high level and as further requirements are derived after stakeholder sessions and confirmations the solution designs will be looked at further to specify specific meta and attribute values or characteristics for design.

It is imperative that data sources provide accurate flags as without them there is a risk that incorrect/sensitive information could be displayed.

Audit Information e.g. CreatedDateTime (Initial Ingestion datetime) will be recorded by the API Gateway and Authenticated User Access via the appropriate IDAM. There is no requirement to record viewing of artefacts.

6.2.3 Logical Data Model



Enumerated Values (Enums)						
Sensitivity*	**User Role***	**Search Type**	**Language**	**Artefact Type**	**Channel**	**Subscriber Status**
Public	P&I Admin	Case Id	English	List	Email	Registered
Standard	System	Case URN	Welsh	Outcome	URL	Active
Warned	Public Sector Partner	Court Id**	Bi-Lingual	Judgement	HTML	Inactive
	Citizen User			Status Updates		De-activated
	Business and Third Sector					
	Partners					
	Professional Bodies					

* Cross References will be required between Jurisdiction Specific Values and P&I Values

** There will be reference data dependencies that will need to be synchronised e.g. Court Ids

6.2.4 Data Dissemination View

The P&I Service is a publisher and not the owner of data. As such it is not a system of record or the master of any data, aside from any it holds for specific logging/auditing requirements. This data will be made available for consumption by the Strategic Data Platform (SDP). The data it holds is provided by its data sources that come CFT, Crime and other potential HMCTS sources. It is the responsibility of those data source owners to be responsible for the content of both the data and meta-data they send to the P&I service.

Data will be exposed via a GDS compliant web portal and also via API based publication services used for third party access.

Data will be stored within the P&I service and availability of publications will be driven by retention periods provided by the data sources in their meta-data (e.g. from/to dates – as described above).

Redaction will not be handled in terms of the obfuscation of data or removal of the data received through unstructured formats (e.g. PDFs). Where publications need to be provided to different user roles it is expected that the data source will provide separate drafts that are flagged in the meta data for the correct recipients, such that P&I will have a draft for Legal Professions vs a draft for General Public.

Alternatively, if structured data is provided (e.g. within the payload of an event) then a flag could be required to be provided at attribute level to determine if a field has restricted access view (e.g. Legal Professionals may see names but anyone outside restricted or confirmed permission levels would only see blank fields).

However, during MVP redaction will only be applied at the artefact header level (and not the attribute level). If two versions of a document, redacted & non-redacted, are required then the source system MUST send them twice with appropriate data classifications and redaction having being applied

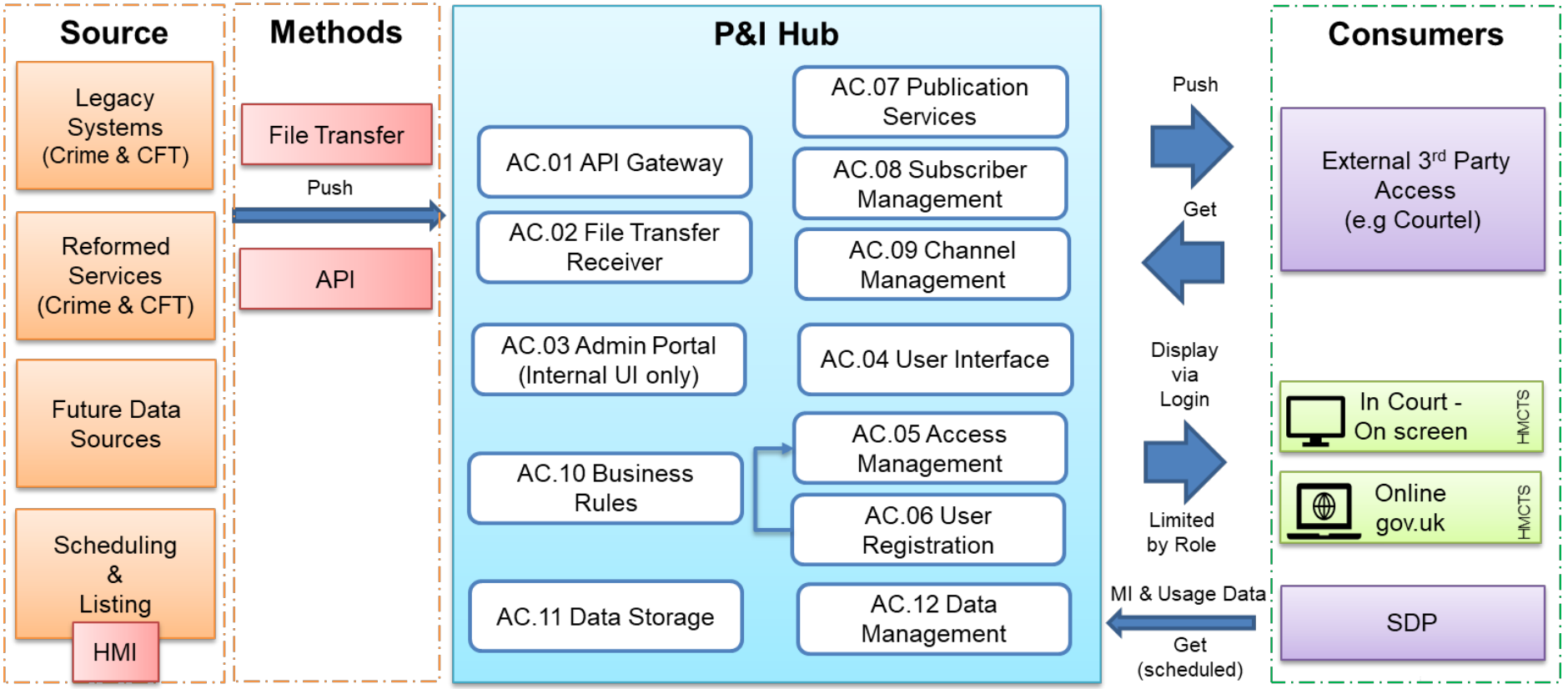
The Information assets owners are from CFT, Crime and other potential future sources. The information asset ownership remains with the service owner of the originating source throughout the process .

6.2.5 Data Migration View

There will be no planned data migration of publication information as data sources will begin populating the P&I Service on go-live. However, subscriber information will need to be migrated from existing systems, including Libra and Xhibit.

6.3 Application Architecture

6.3.1 Application Component View



Where possible existing technology components are reused from a variety of sources, which are described here:

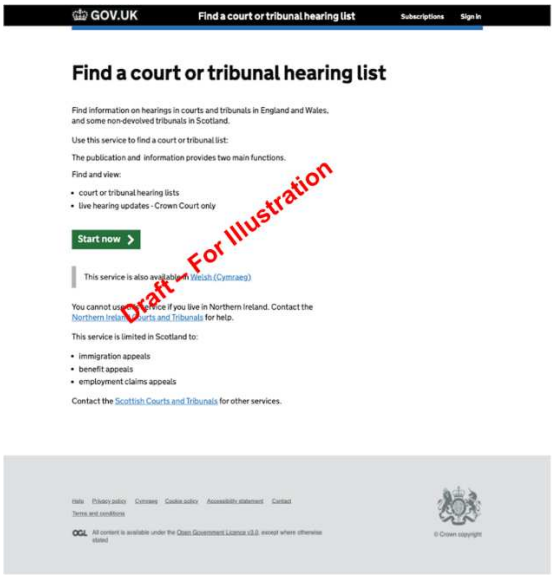
P&I Service - Application Component Reuse.pptx

ID	Component	Description
AC.01	API Gateway	The API Gateway will be the API based point of entry for the data sources and be responsible for protecting the boundary of the P&I service, carrying out functions such as authentication, throttling, white-listing etc, and validating any structured data against schema definitions.
AC.02	File Transfer Receiver	The File Gateway will enable legacy data sources to provide unstructured and read-only file based information (e.g. PDFs). It will poll specific data source file locations on a scheduled basis and upload those files to the P&I Data Storage area
AC.03	Admin Portal (Internal UI only)	Specific UI admin screens will be made available to users with admin roles so that they can maintain subscription, channel, business and data management rules
AC.04	User Interface	A user interface to allow users to search and browse information relevant to their user role. This will follow GOV.UK Design Standards using GDS components
AC.05	Access Management	Ability to manage internal, admin and external users granting permissions to view information that is not available for general consumption based on user's roles and data sensitivity Internal admin roles to allow for the configuration of rules and organisations
AC.06	User Registration	Verifies users to enable enhanced access. The user registration process outside of P&I and handled by the MyHMCTS service (*described in more detail below AIP01a*)
AC.07	Publication Services	A service or set of services to support dissemination of information to various consumers
AC.08	Subscription Management	A configurable list to determine the onward transmission of publication information to registered subscribers (data consumers). *Further detail provided below*
AC.09	Channel Management	Support and management of various channels that may receive publication services (e.g. email, API etc)
AC.10	Business Rules	Ability to support business rules that contain logic for the holding back of information that is not yet ready for publication or not publishing information that is not appropriate for a user role. This logic will be applied at a header level and not in relation to specific data within a payload. *Further detail provided below*
AC.11	Data Storage	A data persistence area to store publications and configuration rules giving frequent access over a specified retention period
AC.12	Data Management	Ability to manage data based on data governance, retention and security policies. It will also maintain and collect reference data (e.g. Subscribers) Any redaction of information MUST have been applied at source. Usage Data & MI sent to SDP

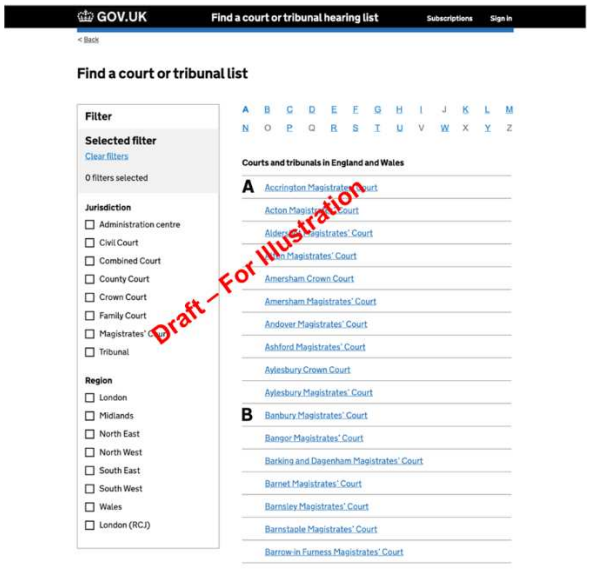
6.3.1.1 User Interface (AC.04)

The P&I Service will provide a user interface that will be made available through web/mobile which would be typically accessed via a web redirect. The UI/UX design is proto-typed through the AXURE rapid proto-typing tool which replicates GDS components and is then created by the development team using JavaScript, Node.js, HTML & CSS using the GOV.UK Design System components (https://design-system.service.gov.uk/)

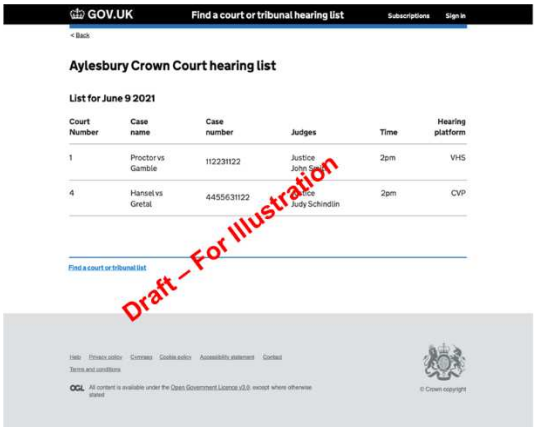
Sample screens are included as follows (note these are for illustration only):



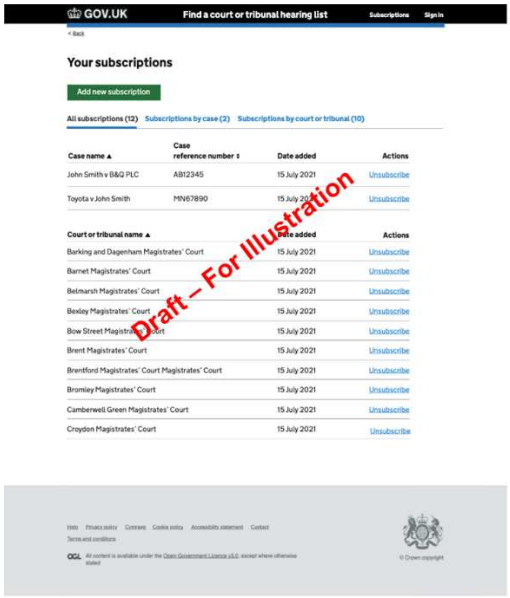
Start Page



A-Z Index



Hearing List



Manage Subscriptions

Where new artefacts are created additional screens will be defined that will use a corresponding template/style sheet to display the data payload received via a defined API schema

6.3.1.2 Access Management (AC.05) & User Registration (AC.06)

The P&I Service will enable access of publication information through its UI for a variety of user roles:

1) Unverified - Citizen users (e.g. general public)
2) Verified users (via IDAM)
   a) Internal (e.g. System Admins, HMCTS court staff, Digital Comms team, CTSC staff)
   b) External (e.g. Partners)

At present the IDAM Landscape is currently undergoing a refresh and, as such, User Groups using P&I will need to follow a transition to a strategic IDAM solution and will be implemented as part of the P&I Service MVP using an interim step. Note there will be no single IDAM solution, but the right solution per user group. Therefore, at a time post-Reform the professional users of CFT and Crime maybe combined together

The User Groups are detailed in the table below and indicate the Interim IDAM that will be used and the proposed future location.

User Group	User Role	Interim IDAM	Strategic IDAM
Member of the Public	Unverified	N/A	N/A
Professional User (Crime)	Verified (External)	Crime	3rd Party IDAM
Professional User (CFT)	Verified (External)	CFT	3rd Party IDAM
Media Users	Verified (External)	N/A – **Subscribers ONLY for MVP**	TBD as part of the Strategic IDAM refresh (see I.01)
HMCTS Staff (standard)	Verified (Internal)	N/A – should only access publications via internal HMCTS systems (such as CMS & ListAssist)	N/A – as interim
HMCTS Staff (P&I Admins)	Verified (Internal)	MoJ justice.gov.uk	MoJ justice.gov.uk

As part of a federated IDAM approach authentication will be carried out as follows:

1. Crime & CFT registered users on their own specific IDAMs
2. P&I Admins (i.e. HMCTS staff) to use SSO via their Justice Accounts.

Whilst Professional Users may exist in one or more IDAMs (Crime & CFT) the granularity of the business rules is such that it is only necessary to understand that they are legal professionals and not the type of legal professional they are

Externally verified users will be required to follow the MyHMCTS registration process, which is an existing capability outside of the P&I Service (MyHMCTS Register Your Organisation - User Guide March 2020.pdf)

6.3.1.3 Application Component AC.08 – Subscription Management

Subscribers will be set-up through a subscriber registration process (described below AIP01b) and details will be held within a subscribers table within the data store (AC.11). This will contain the following information:

- Subscriber Details
  - Group (e.g. Partner, Professional Bodies, Businesses & Third Sector)
  - Organisation
  - Email Address
  - Last Update (Date)

A registered subscriber may update their subscriptions via the User Interface (AC.04), which will follow the Information Subscriptions Process (described below AIP03c). The subscriber record in the subscribers table will include the following subscriptions information as a repeating group:

- Subscriptions, filtered by:
  - Court Name
  - Case IDs
  - Case Name

ANY or ALL subscription filters may be applied.

Publication Information will be sent following the Information Subscribers Process (described in AIP03d). Subject headers will be applied to contain the following information:

- Court Name
- Listing Type
- Date
- “Preference Trigger”

The “Preference Trigger” is generated on the unique filtering of matches retrieved by the subscription process so that information is only sent once. i.e. If two competing filters return the same information, such as one filter may ask for all listings by Court Name and another ask for a Case Name that may be being heard in that court. Order of preference would be Court Name -> Case IDs -> Case Name so in this matching example only the Court Name match would be returned with a “Preference Trigger” of Court Name.

Housekeeping process (see AIP04b) will be applied so that a Subscriber will be removed if they are inactive for a configurable period of days. Prior to being made inactive they will be sent a warning pending their response to renew their access (see AIP01c). Inactivity will be determined by their last update (e.g. their registration, updating of their subscriptions or response to an inactivity warning)

6.3.1.4 Application Component AC.10 - Business Rules

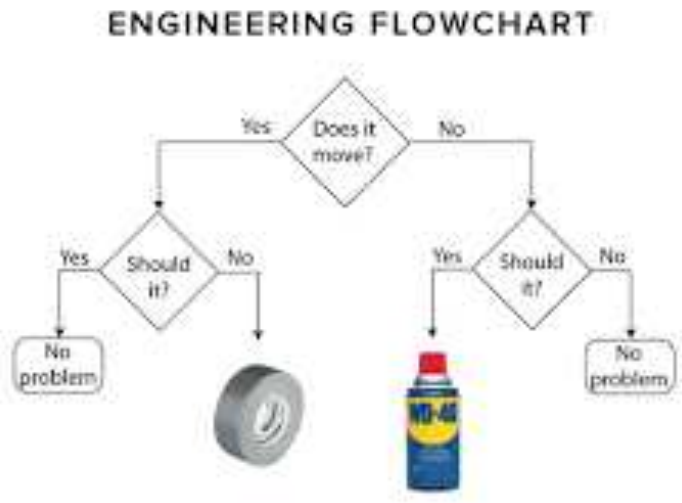
The purpose of the Business Rules Component (AC.10) is to provide control to the storage and access of Publication Information.

It is required by the following Consumption processes:

AIP03a – Information Consumer (UI Based)
AIP03b – Information Consumer (API Based)
AIP03c – Information Subscriptions

It is dependent on the Data Management (AC.12) and Access Management (AC.05) components to provide it with its input parameters and carry out housekeeping functions

The Business Rules component uses Decision Trees to evaluate and return a token based on true/false logic e.g.



The decision tree logic is realised through the use of Truth Tables, where each row is evaluated as a complete branch and the table is exited when a true expression is found:

Does it move?	Should It?	Token
Yes	Yes	**No Problem**
Yes	No	**Gaffer Tape**
No	Yes	**WD40**
No	No	**No Problem**

Definition of Terms

Term	Description
Decision Tree	Set of questions that evaluate to true/false branches
Truth Table	Realignment of a Decision Tree into a table, where columns contain questions and rows evaluate to true answers
Parameters	Data Inputs
Source	The data source of a parameter
Token	Return Value
Intermediary Tables	Additional Truth Tables that may be used to evaluate calculated parameters to simplify overall decision logic

Principles

Principle	Reason
All questions MUST be positive	Negative and double-negative questions lead to confusion and table logic not being formulated correctly
Default Parameters MUST be provided	If a value is not provided by a Data Source a default parameter must be provided to enable a decision to be evaluated, even if the default is no value
Table logic should be STATIC and driven by DYNAMIC parameters	The control of logic should be driven by the parameters provided by the data sources, with the tables providing simple matching logic
An evaluated exit to the table MUST be provided	When no positive results are found a graceful exit should also be provided indicating that no matches have been found or that an error has occurred
Intermediate tables should be used to reduce complexity	The number of combinations of answers (rows) should be reduced by using intermediary tables which in turn reduces complexity
Intermediate tables may use parameters as well as enumerated values	Where parameters may have static enumerated data sets they maybe used for questions (column headers)
Intermediate tables should only match a single question	Intermediate tables should be kept simple and be used to match a single question or a question set defined by enumerations. More complex logic should be handled using multiple Intermediary tables
Intermediary tables may be used by multiple tables	An intermediary table should be able to be used by more than table and may form nested groups
Wildcards maybe used	<ANY> maybe used as a wildcard to indicate any further response would evaluate to TRUE. <NONE> maybe used to indicate that a result maybe valid if no value is provided

Parameters (EXAMPLES)

The parameters table defines fields within the message that provide inputs to the business rules.

The values may be provided by either the data source (within its header or message body) or from the user via their login details or through their preferences. Values are validated and stored on receipt/login by the Data Management and User Management components respectively from the source location specified.

Parameters may ONLY be applied at the header level for file based interfaces but maybe applied at the attribute level for API based events

Parameter	Source	Default	Type	Comment
RetentionTo	/header/retentionTo	Now + 30 Days	DateTime	How long should a publication be retained for
DisplayFrom	/header/displayFrom	Now	DateTime	From when should the publication be displayed
DisplayFromMedia	/header/displayFrom/media	Now + 10 Days	DateTime	From when should the publication be displayed for a specific role
Sensitivity	/header/sensitivity	“Private”	String (Enum)	What level of data sensitivity does the publication contain
Sensitivity	/body/defendantName/sensitivity	“Classified”	String (Enum)	Data sensitivity set against a specific attribute within the publication
Language	/header/language	“English”	String (Enum)	What language has the publication used
ExcludedUserIds	/header/user/excludedIds	“”	String	An Id or a repeated list of Ids that may not view a publication
UserId	/user/userId	“Anonymous”	String	The login Id authenticated against a user
UserRole	/user/userRole	“Citizen User”	String (Enum)	What role does the user have
UserLanguage	/user/userLanguage	“English”	String (Enum)	What is the user language preference

Intermediary Tables

As a pre-cursor to the main truth table, intermediary truth tables maybe used to return calculated parameters

Each line should be evaluated sequentially and the table exited on the first true statement found

Parameter OR Enumeration matches maybe used

As an example of parameter matching the table below shows an input of Language as meta-data received from the data source matched against the language preference of the user. The resulting token indicates with there is a full, partial or no match between the two

Language	User Language	Preferred Language
English	English	**Match**
Welsh	Welsh	**Match**
English	Welsh	**Partial**
Welsh	English	**Partial**
<ANY>	<ANY>	**No Match**

As an example of enumeration matching the user role parameter is matched against enumerated columns for data sensitivity. The data sensitivity value received from the data source as part of the meta data is matched against the appropriate column and the row against the user role to give a “Cleared” token.

E.g. If the data sensitivity received is “Classified” then only P&I Admin & Public Sector Partners may view the data and so if a User Role of “Partners” was identified the “Cleared” Token returned would be FALSE so the user would not be able to view the publication

	Data Sensitivity				
User Role	**Public**	**Private**	**Classified**	**Internal**	**Cleared**
P&I Admin	<ANY>	<ANY>	<ANY>	<ANY>	**TRUE**
Public Sector Partner	<ANY>	<ANY>	<ANY>	NO	**TRUE**
Citizen User	<ANY>	NO	NO	NO	**TRUE**
Businesses and Third Sector	<ANY>	<ANY>	NO	NO	**TRUE**
Partners	<ANY>	<ANY>	NO	NO	**TRUE**
Professional Bodies	<ANY>	NO	NO	NO	**TRUE**
<ANY>	<ANY>	<ANY>	<ANY>	<ANY>	**FALSE**

NB: The table above is provided as an example and finalised config will be defined within the LLD.

The Truth Table (Example)

As with the intermediary truth tables each line should be evaluated sequentially and the table exited on the first true statement found

Parameters may be direct or from intermediate tables

DisplayFrom	RetentionTo	Cleared	Preferred Language	Token	Action
<= Now	>= Now	True	Match	Display	**Display publication**
<= Now	>= Now	True	Partial	Display&Warn	**Provide message "Publication not available in preferred language**
> Now	>= Now	True	<ANY>	Warn	**Provide message "Publication not available yet"**
<ANY>	< Now	True	<ANY>	Warn	**Provide message "Publication no longer available"**
<ANY>	<ANY>	False	<ANY>	Warn	**Provide message "Publication not available to your UserRole"**
<ANY>	<ANY>	<ANY>	<ANY>	Fail	**Provide message "Publication not found"**

6.3.2 Application Interaction View

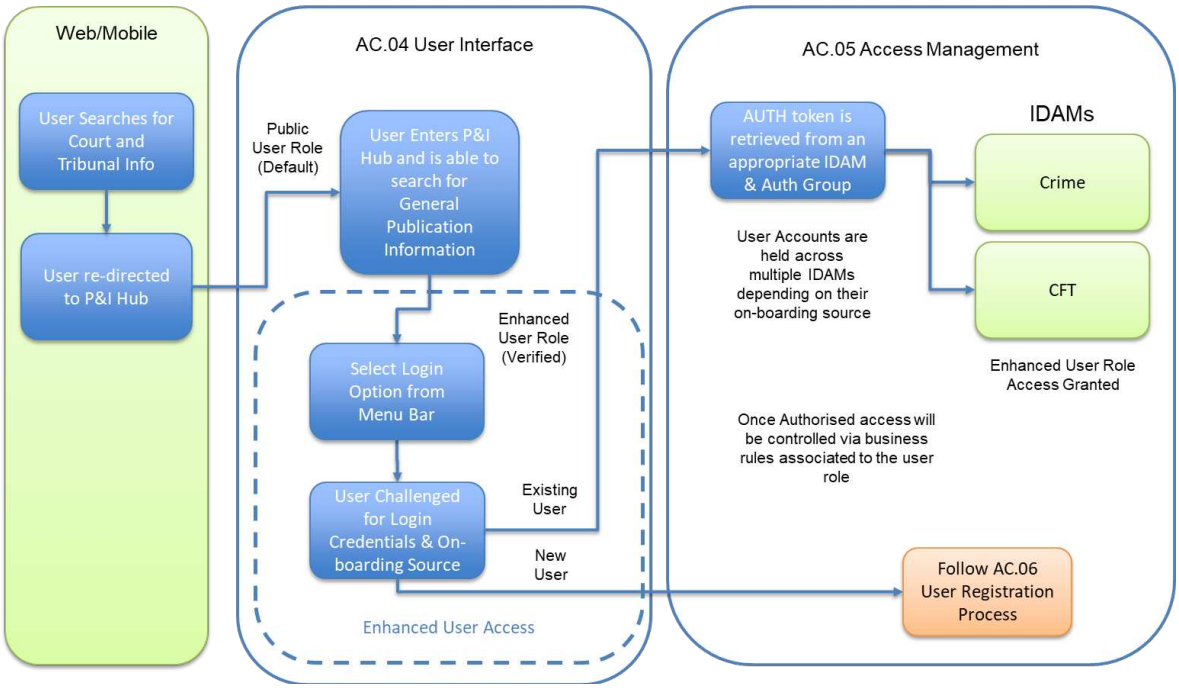
Within the P&I application, interaction processes can be broken down into four key areas:

REF	Process Group	Process Name
AIP01a	Core Processes	User Access Process
AIP01b		Subscriber Registration Process
AIP02a	Ingestion (How P&I data sources provide their information)	Information Producer (API Based)
AIP02b		Information Producer (File Based)
AIP03a	Consumption (How P&I consumers view and receive information)	Information Consumer (UI Based)
AIP03b		Information Consumer (API Based)
AIP03c		Information Subscriptions
AIP03d		Information Subscribers
AIP04a	Maintenance Processes	Maintenance of Rules and Overrides via the Admin Console
AIP04b		Housekeeping Jobs & Scheduling
AIP04c		Maintenance by Information Producers

6.3.2.1 Core Processes

AIP01a - User Access Process

The outline user access process is described below, however as mentioned above, access management takes account of existing solutions within Crime and CFT.



When a user lands on the P&I UI (AC.04) they will be by default be given a public user role. This role has an unverified status and as such would have business rules (AC.10) applied restricting the data they were able to see. They would also not be granted access to any enhanced admin functions (AC.03)

If they wanted to perform additional functions (e.g. system admins adding subscriptions) or have access to restricted data (e.g. legal professionals) they would require verified access.

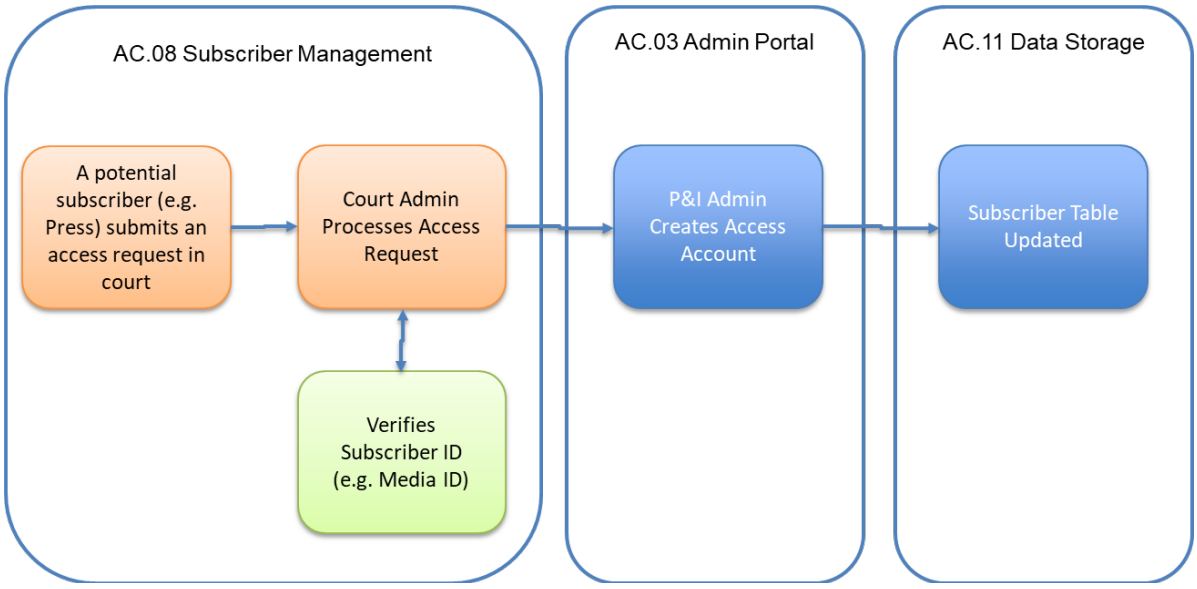
For verified access a user would be required to provide both login details and their on-boarding source (e.g. Crime or CFT) and based on this would be redirected to their appropriate IDAM. Access would be granted via an AUTH token retrieved from the IDAM associated with their Authorisation Group. This would then assign a user role enabling access to enhanced functions (such as the admin portal) and to restricted data applicable to that role.

A federated approach will be taken to access management (AC.05) and will align with existing IDAM services currently in use in both CFT and CRIME.

The User Registration Process (AC.06), which includes registration of both Users, Super Users, Auth Groups and Organisations is part of the service provided outside of the P&I Service by MyHMCTS or the Common Platform Change Team who are responsible for the CFT and Crime IDAMs respectively.

AIP01b - Subscriber Registration Process

Subscribers (i.e. those users who are sent publication information via email, such as the Media) who are not verified through an IDAM must follow a subscriber registration process and have their email address verified by court staff . This subscriptions process is summarised as follows:



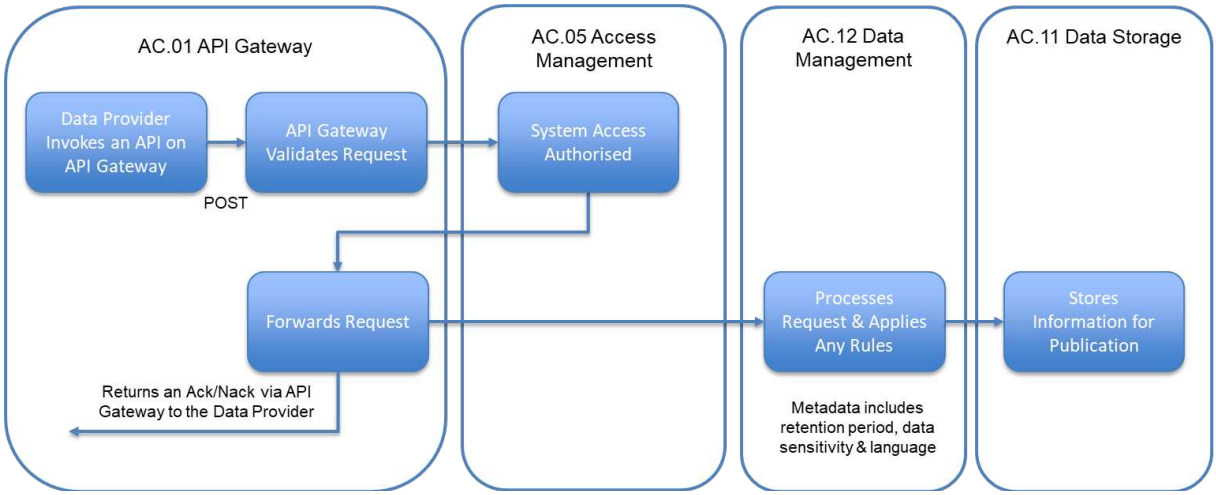
The subscription email address for those user verified via an IDAM will be taken from the email they have registered on their IDAM profile.

6.3.2.2 Ingestion Processes

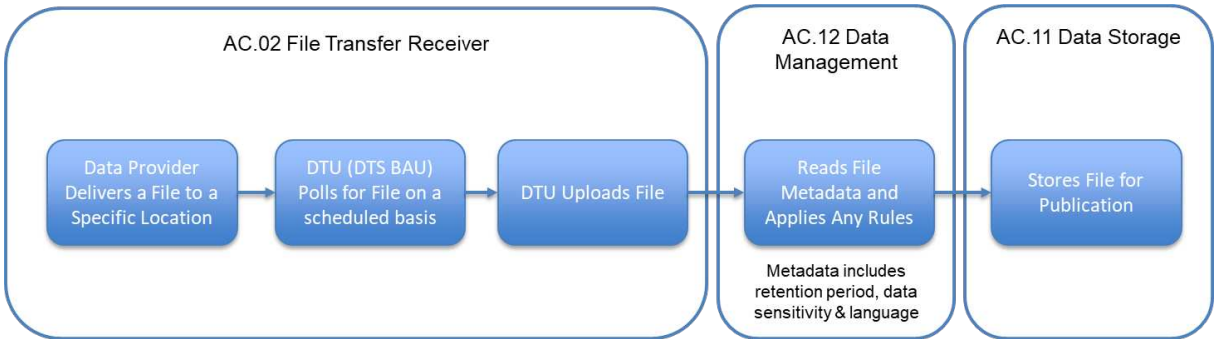
Two primary methods of ingestion will be provided to allow for file and API based transfer. In both cases a Gateway will be the point of entry for the data sources and be responsible for protecting the boundary of the P&I service. In the API Gateway case it will also carry out functions such as authentication and throttling etc, and will validate any structured data against schema definitions.

Once forwarded to the P&I service, it will apply any processing logic, using meta-data supplied by the data source, against its data management rules (e.g. data sensitivity, language, retention periods etc) and store the information for publication.

AIP02a - Information Producer (API Based)



AIP02b - Information Producer (File Based)

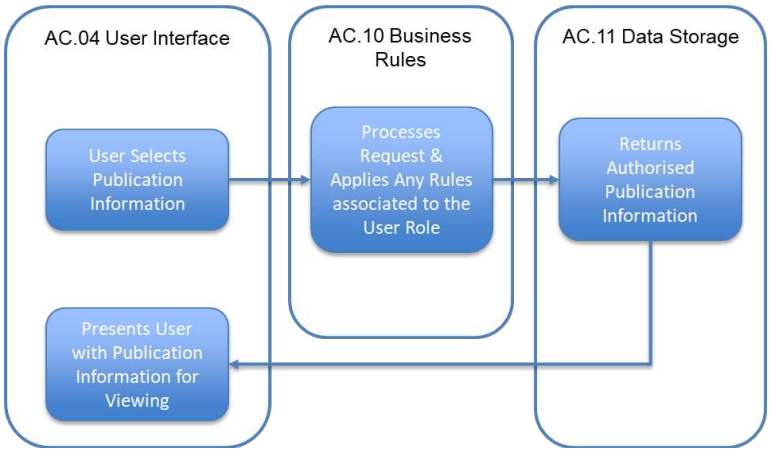


6.3.2.3 Consumption Processes

There are four primary ways that consumers may view and receive information. In all cases no charges will be applied for consumption.

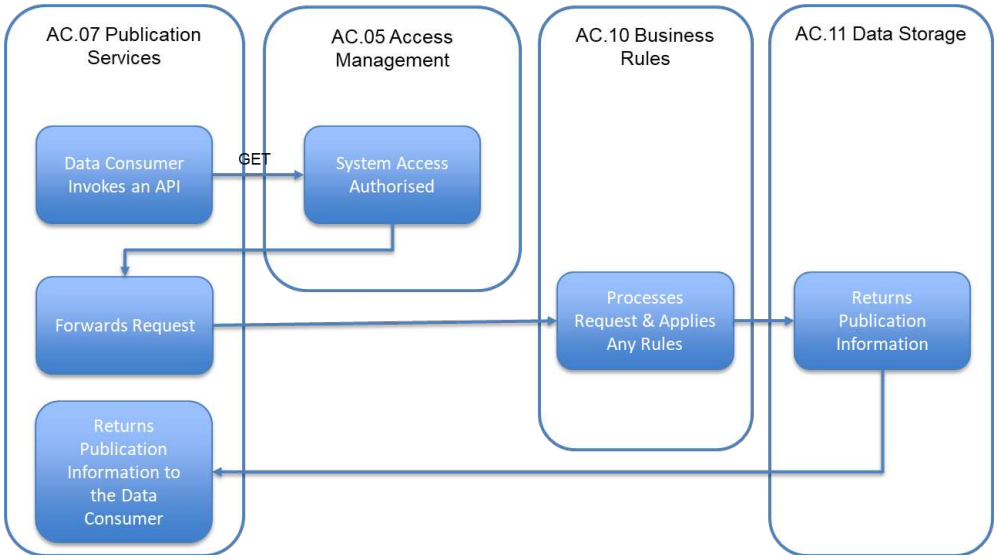
AIP03a – Information Consumer (UI Based)

Within the UI (AC.04) a user is presented with lists of available Publication Information, determined by retention periods, that they may search and filter against. On selecting a specific Publication Item business rules (AC.10) are checked to ensure that the Information they wish to retrieve is appropriate to their user role and is then returned from the data store (AC.11) for viewing through the UI. Within the data store similar versions of the same Publication Information may exist that may be either presented in other languages (e.g. Welsh) or have different levels of redaction. The business rules will ensure that the correct Publication is returned based on metadata held against the publication and the user preferences and user role



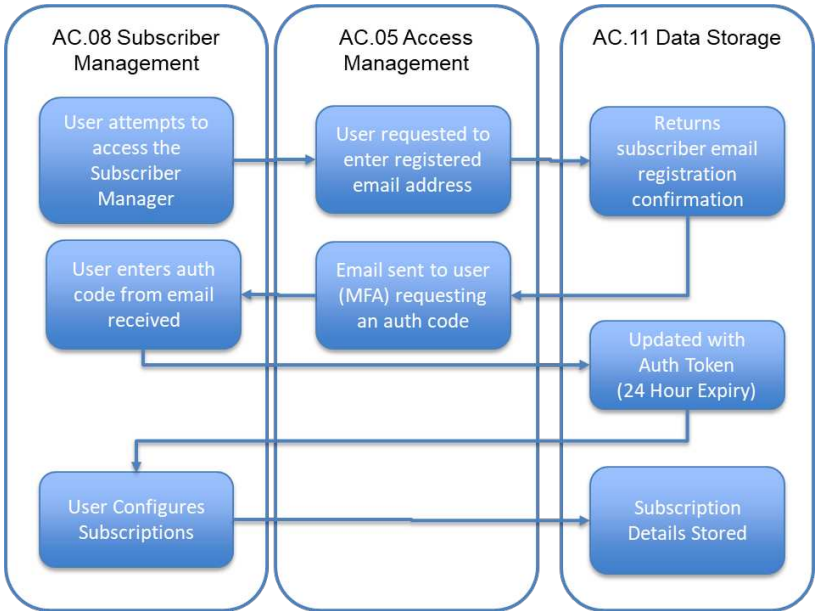
AIP03b - Information Consumer (API Based)

Publication Services are available to enable consuming system to retrieve Publication Information. Similar search & filtering criteria is applied to any request and appropriate business rules applied against the system user in terms of the Publication Information they are allowed to access. System Access, as a user role level, is controlled via User Access Management (AC.05)



AIP03c - Information Subscriptions

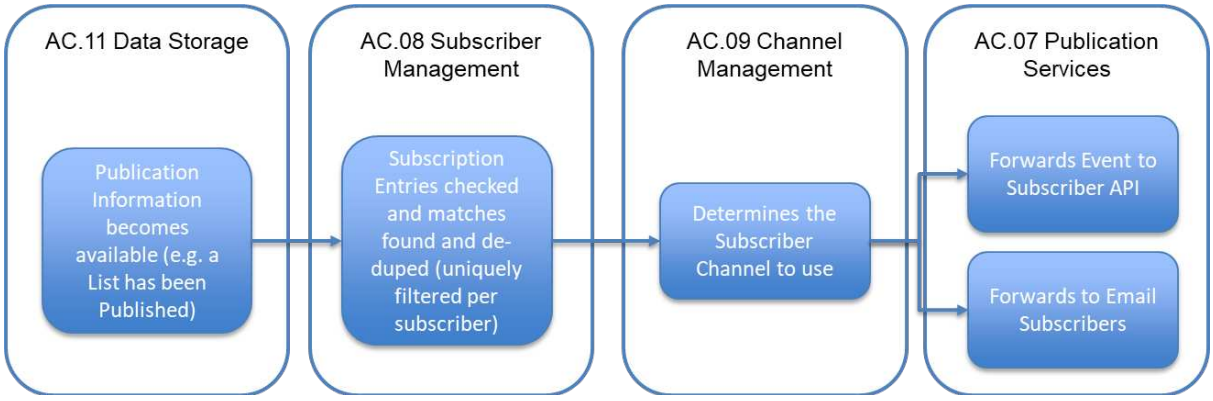
Users may add subscriptions so that they are sent publication information once it becomes available. To achieve this they must both register as a subscriber (see AIP01d) and configure their subscription in the Subscriber Manager (AC.08).



To access the subscription manager, via the UI (AC.04), the subscriber must first confirm their email address through an MFA challenge. They are then presented with their current subscriptions and are able to either create new subscriptions or manage their existing ones (update or remove) which are held in a Subscriber Table in the Data Store (AC.11)

AIP03d - Information Subscribers

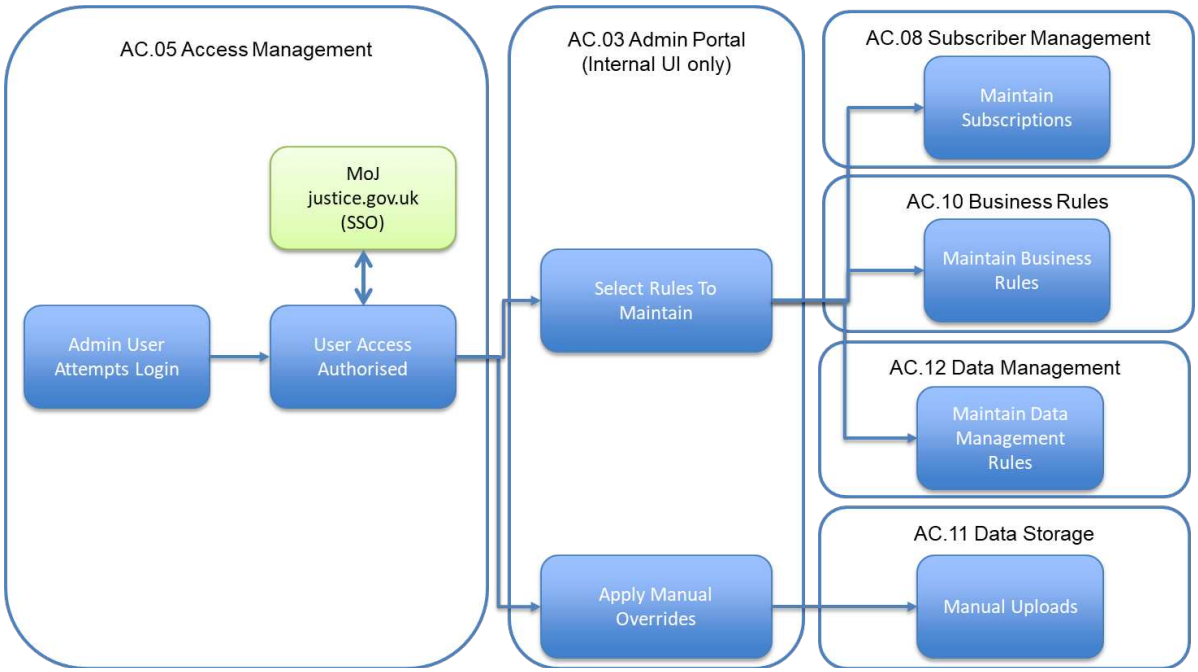
When Publications become available within the Data store (e.g. a new event has arrived or a viewed from date has passed) the Subscriber Manager (AC.08) will retrieve the Publication Information, determine a subscriber list, filter for unique subscriptions (e.g. so a subscriber does not get multiple events) and forward it to the matched subscribers over their selected channel. This might be via an email or sent as an event via the Publication Services for System Users.



6.3.2.4 Maintenance Processes

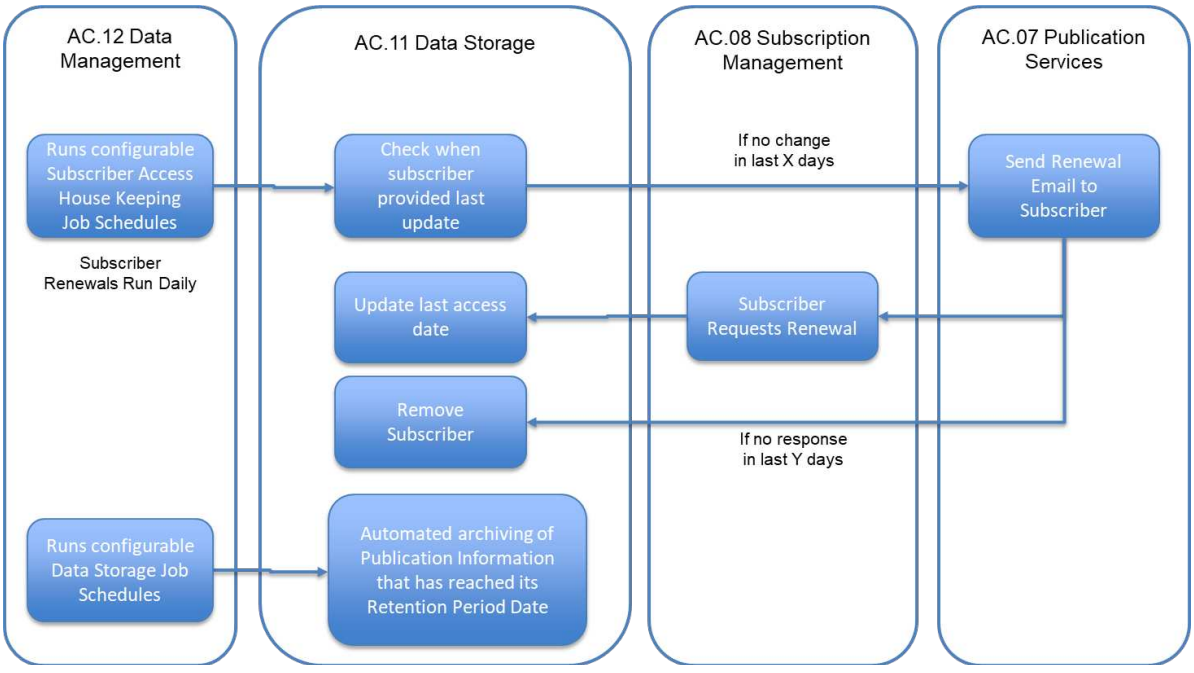
AIP04a - Maintenance of Rules and Overrides via the Admin Portal

Enhanced functions will be provided to Admin users to allow them to administer business, data management and subscription rules. The admin console will also allow Admin users to provide manual overrides to either update meta-data (e.g. changing of start dates and retention periods) or upload files should other ingestion or maintenance functions be unavailable.



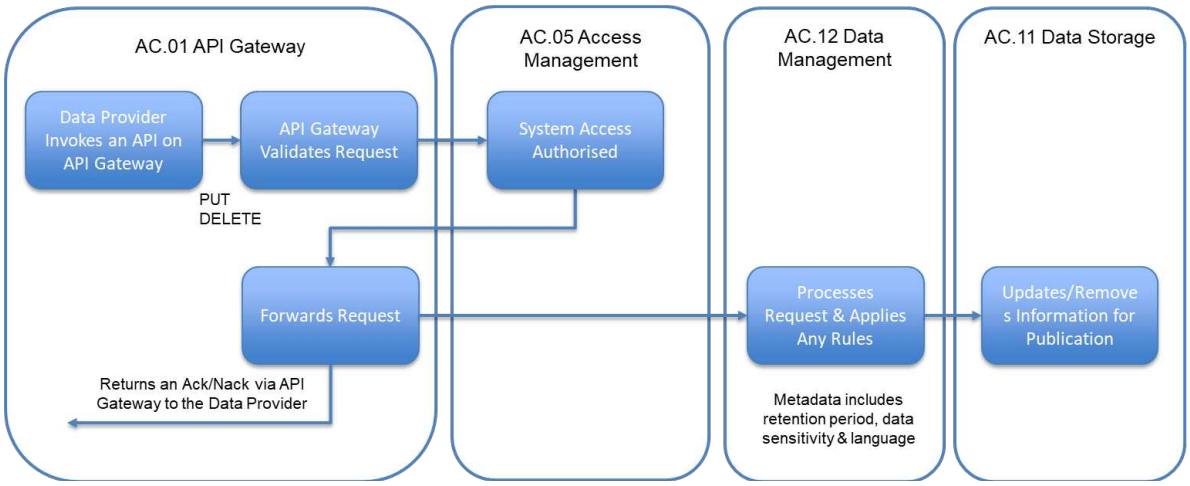
AIP04b - Housekeeping Jobs & Scheduling

The Data Management component has the ability to run configurable job schedules for the house keeping of data, that may relate to both Subscriber and Publication Information.



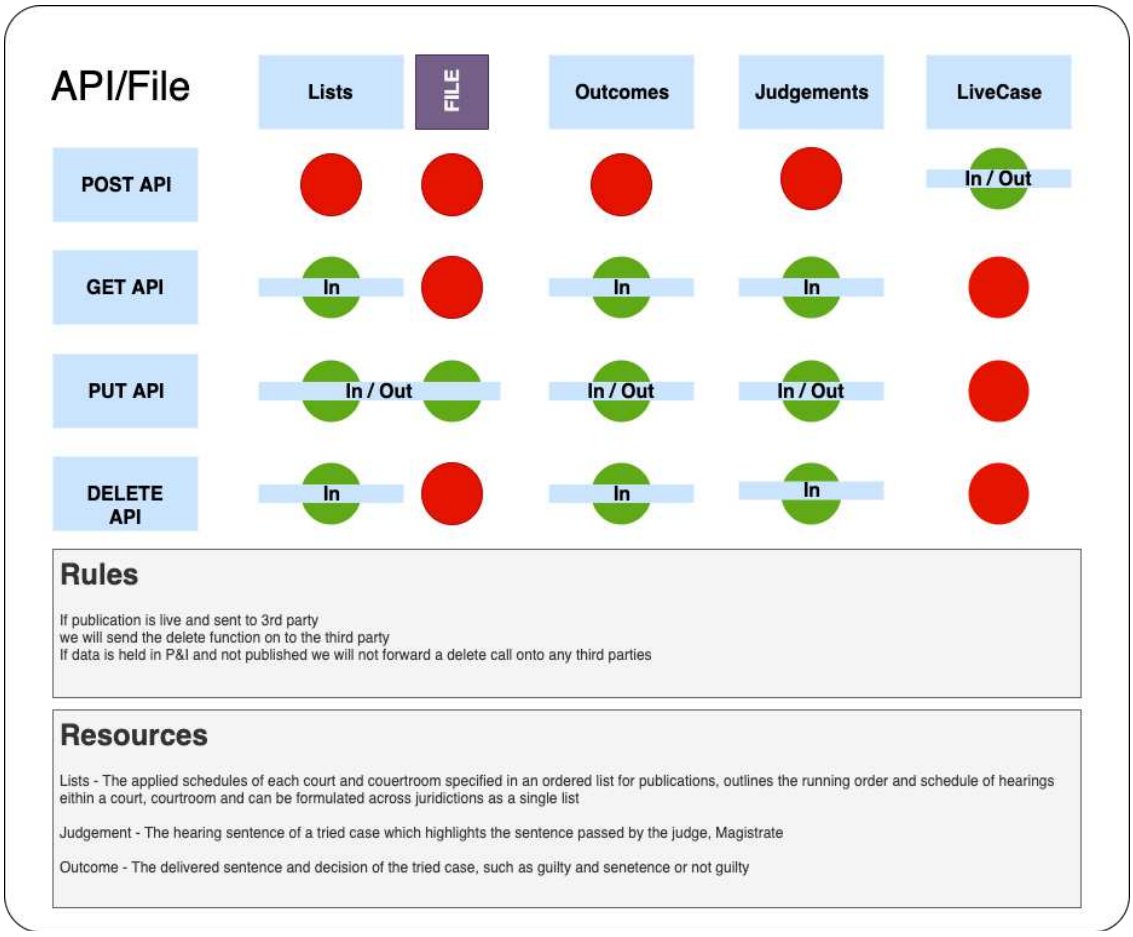
AIP04c – Maintenance by Information Producers

Using a similar method employed by the API based ingestion process and Information Producer may also issue PUT (update) and DELETE (remove) methods to either update or remove Publication Information they have previously sent. File Based methods updates may also by employed in a similar way by providing the same file name as an existing file, which may also make a file inactive by setting a retention period in the past.



6.3.3 Application Integration View

6.3.3.1 API Methods and Resources



Source – Link

The table above defines the resources and methods that will be made available through the API Gateway for both data sources, data consumers and subscribers. It shows those methods and resources that will be built as part of the Crime MVP rollout but it is intended that these will be extensible over time as more data sources and consumers adopt the service and introduce wider requirements.

- POST – Additive transactions (inserts a new record every-time)
- PUT – Idempotent Transactions (controlled by data source either creating or overwriting an existing record)
- DELETE – Permanently removes a record
- GET – Retrieves a record

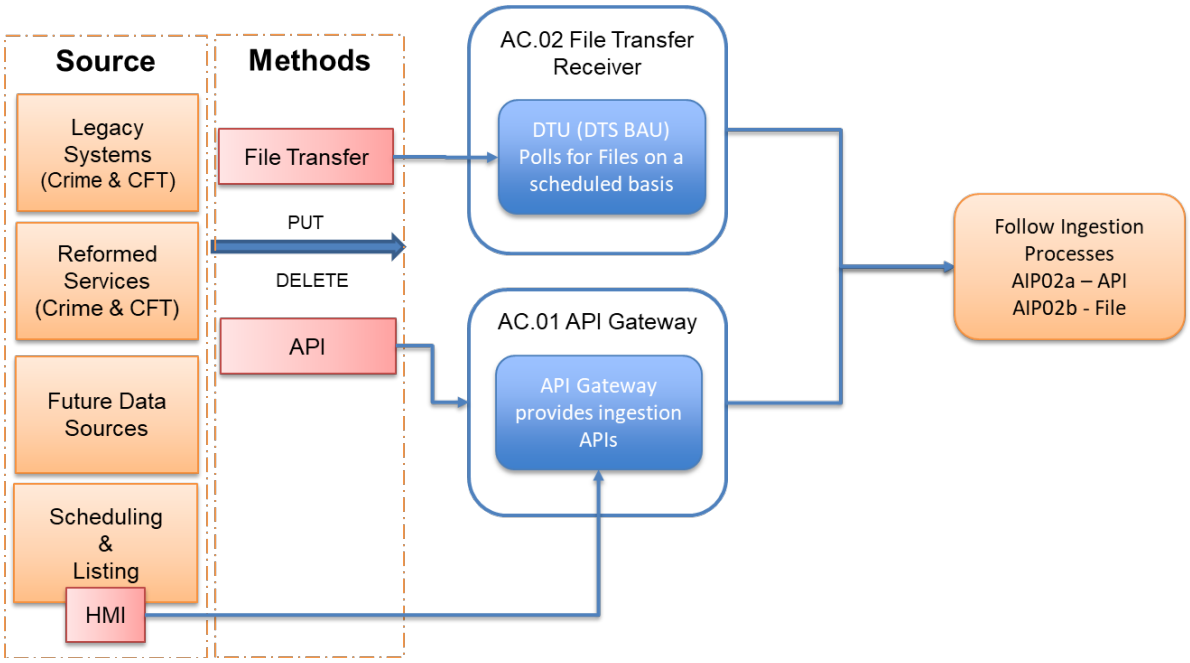
APIs which are offered via the API Gateway are labelled as “In”. This relates to either data sources publishing (or updating) information to P&I for ingestion or data consumers (which may include the P&I service itself) retrieving information from the P&I data store.

APIs which are offered to subscribers are labelled as “Out”. This relates to data consumers who P&I will forward information onto by invoking their APIs.

For each new resource an API schema will be defined.

6.3.3.2 Ingestion Methods

The P&I service will provide two primary methods for data ingestion, namely API & File Based, to handle both structured and unstructured data.

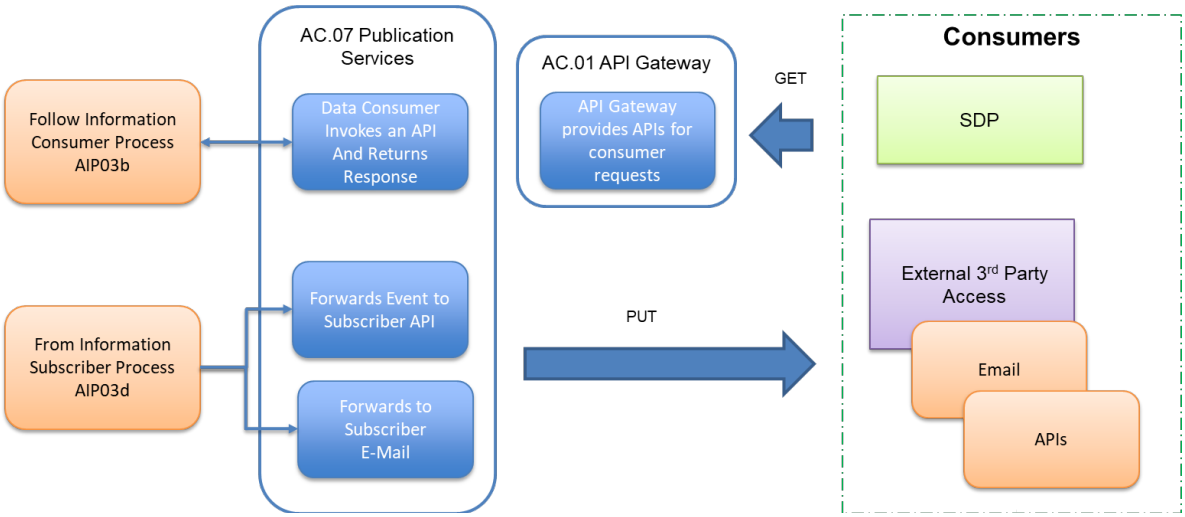


At a high level the APIs will provide standard PUT and DELETE type methods applied to Listing and Decision Data Objects, which will be detailed at the schema level during the LLD phase. This will provide data sources with the ability to create, update and remove the structured information that they either want to publish or have previously published.

For legacy systems, and those without API capability, a file based mechanism is provided to enable those data sources to provide their publishing information in a unstructured file format. The formats of these files should be a “locked” format (e.g. PDFs).

6.3.3.3 Consumption Methods

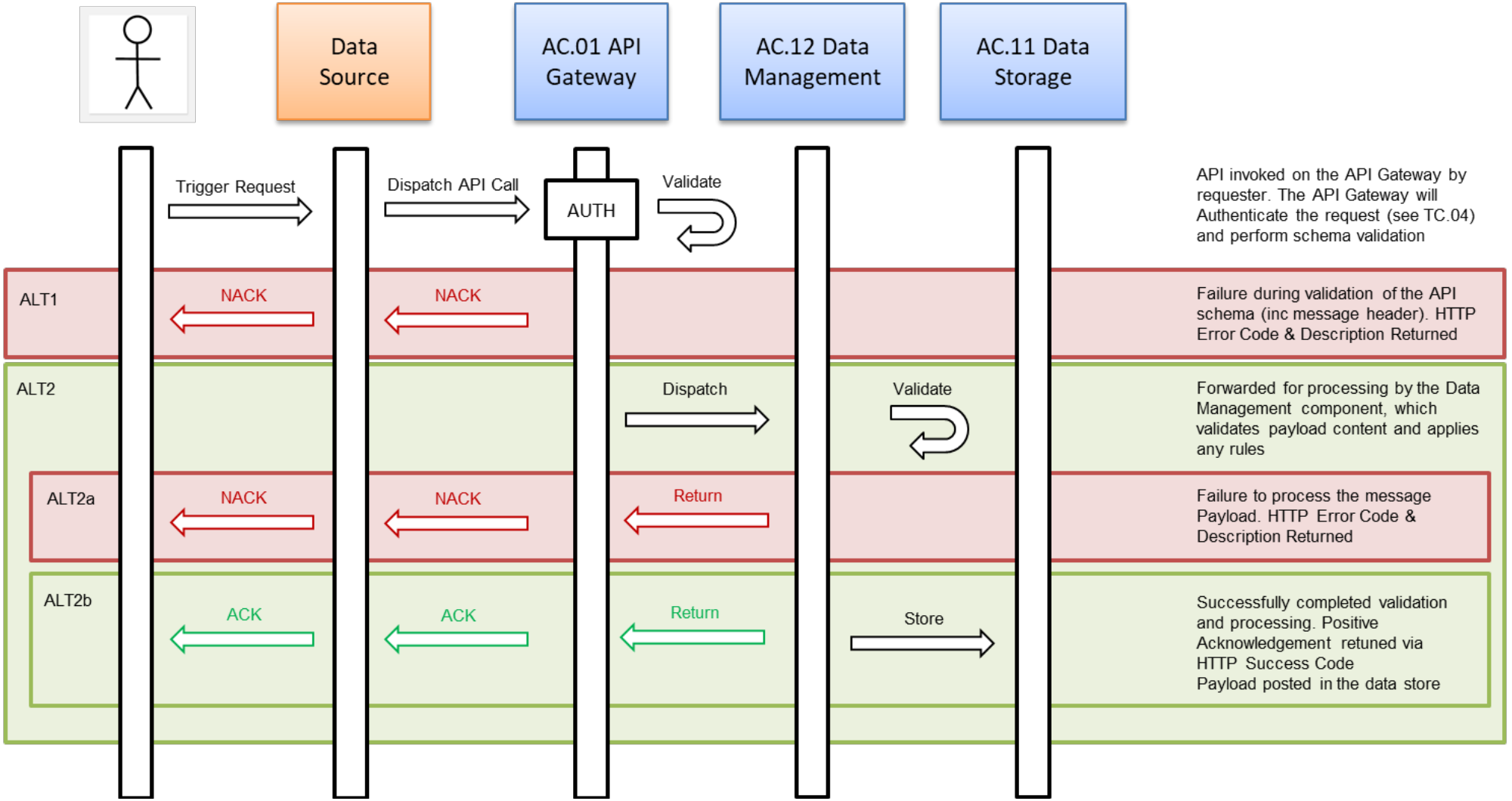
The P&I service provides a number of mechanisms (outside of its UI) for 3rd Party systems to consume publishing information, which include both API and Email based methods, through its Publication Services.



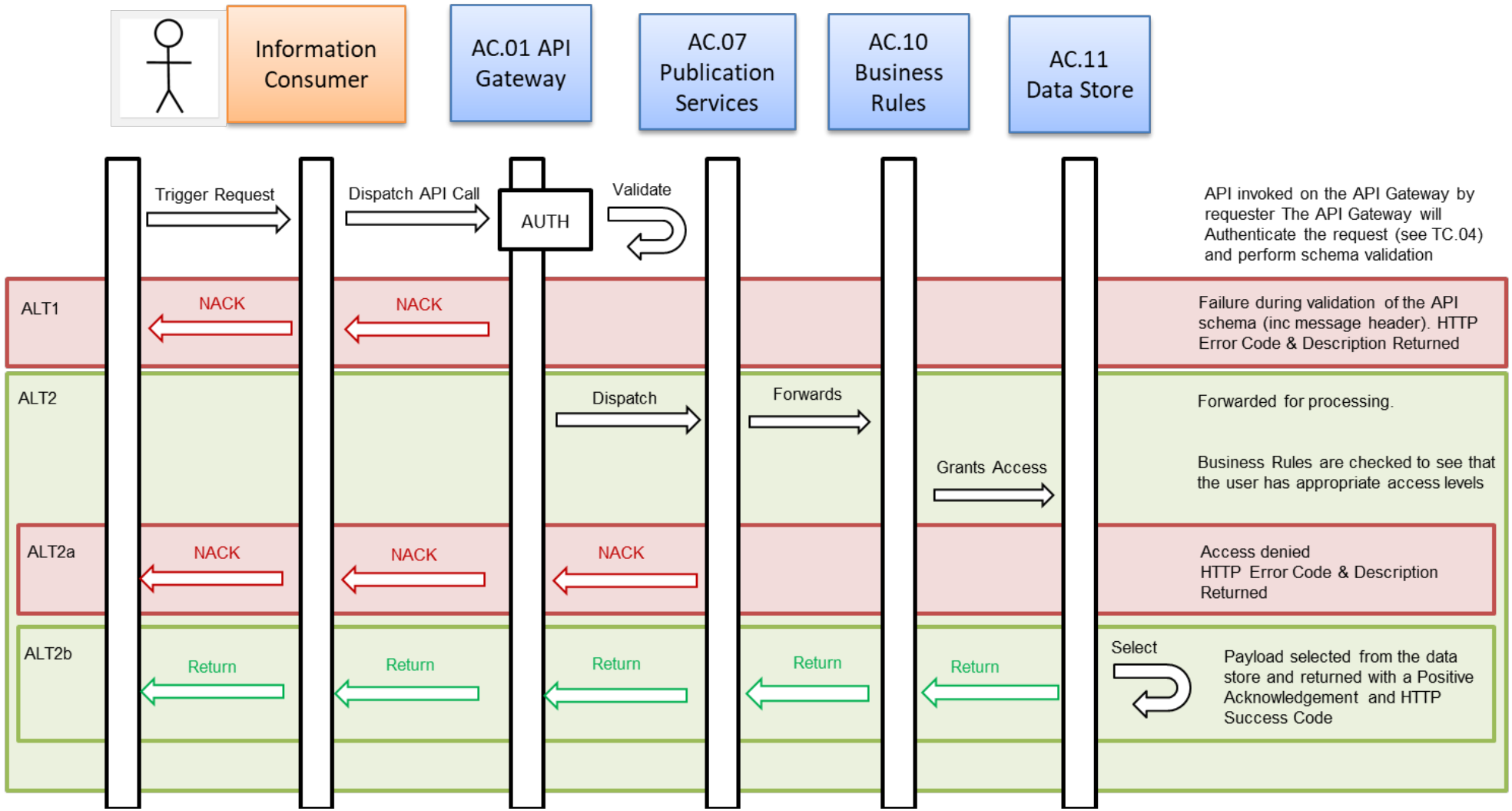
For API access a PUT method is provided for systems registered as subscribers and also a GET method for systems to retrieve specific structured publishing information.

In addition, individuals may subscribe to information via email so that they can received information as it is published. They may view this information within the email received or via access it via the UI.

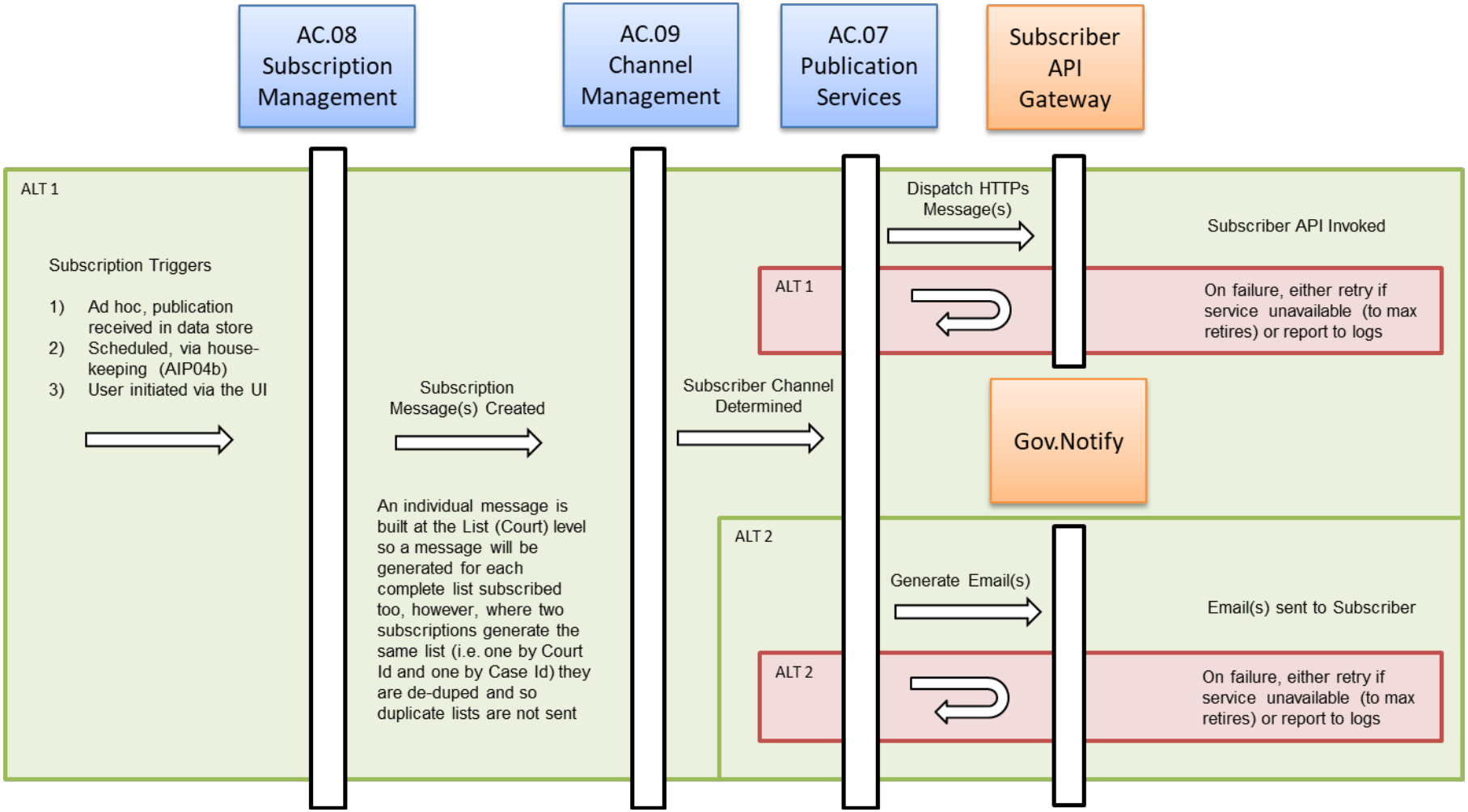
6.3.3.4 Information Producer (API POST/PUT/DELETE)



6.3.3.5 Information Consumer (API GET)



6.3.3.6 Information Subscriber (API POST/PUT, Email)



6.4 Technology Architecture

6.4.1 Technology Component View

The following technology components will be required:

ID	Technical Component	Application Component(s) Supported
TC.01	API Gateway	AC.01 API Gateway AC.07 Publication Services
TC.02	File Transfer Utility	AC.02 File Transfer Receiver
TC.03	User Interface	AC.03 Admin Portal (Internal UI only) AC.04 User Interface
TC.04	Identify and Access Management	AC.05 Access Management AC.06 User Registration
TC.05	Job Scheduler	AC.08 Subscription Management AC.12 Data Management
TC.06	Rules Engine	AC.08 Subscription Management AC.09 Channel Management AC.10 Business Rules
TC.07	Database	AC.11 Data Storage
TC.08	Email Capability	AC.07 Publication Services AC.08 Subscription Management

6.4.2 Infrastructure View

We will follow standard practices as set out by Digital Architecture and Cyber Security's policy on Cloud Infrastructure:
[removed]

The P&I service will be hosted on Azure and built using Platops 'Shared Development Services' (SDS) and will conform to current standards

TC.01 API Gateway

Component	Description
Azure Gateway	The endpoint that: 1. Accepts API calls and routes them to backends. 2. Validate API call headers and message content 3. Verifies API keys, certificates, and other credentials. 4. Enforces usage quotas and rate limits. 5. Transforms APIs on the fly without code modifications. 6. Caches backend responses where set up. 7. Logs call metadata for analytics purposes
Azure Portal	Administrative interface to: 1. Define or import API schemas 2. Package APIs into products 3. Set up policies like quotas or transformations on the APIs. 4. Get insights from analytics 5. Manage users
Azure Front Door	The Azure Front provides an application delivery network as a service and includes the following features: 1. Layer 7 load balancing for applications 2. Dynamic site acceleration 3. TLS/SSL offloading and end to end TLS 4. A Web application Firewall (WAF) which can be used to set rate limiting rules 5. URL based routing for appropriate backends 6. URL redirection such as directing traffic received on HTTP to HTTPS, this also includes different hostnames and paths.

TC.02 File Transfer Utility

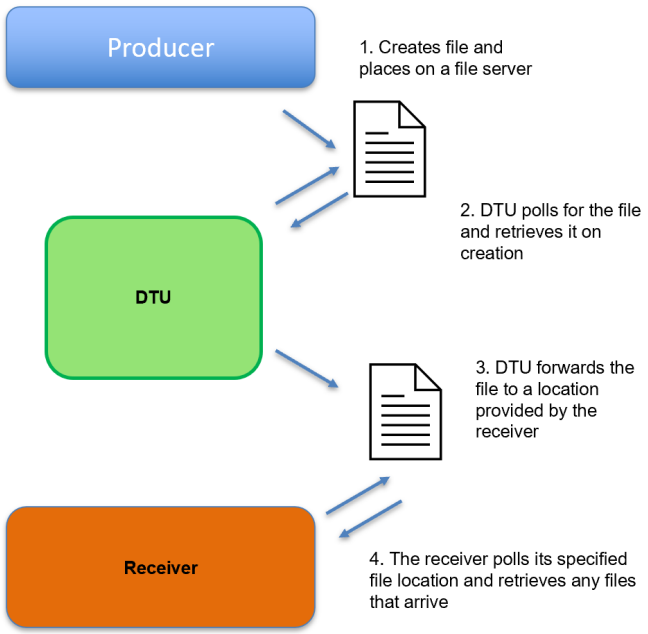
File transfers will reuse the DTS DTU Data Transfer Utility. It will be used for any file transfer activities, including polling, transfer and any protocol conversions.

As per Arch Decision (File Based Patterns) PDG v1.0 it will follow the Option 1: Lift and Shift Pattern. File transfer capability is provided to support legacy applications that can only deliver file based interfaces. Should these applications be upgraded to use APIs then the API Gateway would be used instead. Therefore, other File Based patterns are not relevant

Option 1: Lift & Shift
Managed file transfer (MFT) type functionality is carried out by the Data Transfer Utility (DTU) where it provides a mechanism to poll for a file created by a producer and transfers it to a location specified by a receiver

KEY POINTS

1. A producer creates a file containing multiple records and places it in a file location
2. DTU uses a file polling mechanism to retrieve the file
3. DTU forwards the file to a location specified by the receiver
4. The receiver polls its specified file location to retrieve any files that arrive



Further information regarding the DTS DTU product (as delivered through the BIAS project) maybe found here:

HLD - HMCTS Azure BAU Integration HLD - HMCTS.BAU.xxx.HLD.011 - Tracked v11.docx
LLD - PD.6500 - HMCTS BAIS_LLD v0.9 TC.docx

TC.03 User Interface

UI is written in Node.js with HTML & nunjucks for presentation, all hosted on Azure as per HMCTS standards (https://design-system.service.gov.uk/)

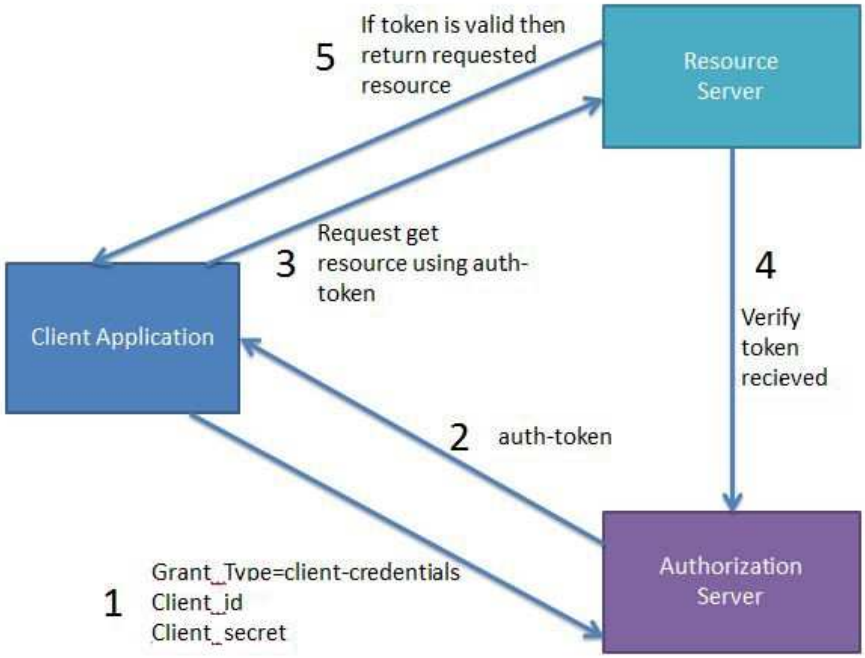
TC.04 Identity and Access Management

As per NCSC guidelines, OAuth2 has been selected as an authentication mechanism as it is one of the best practices for securing, not only public users of web applications but API access.

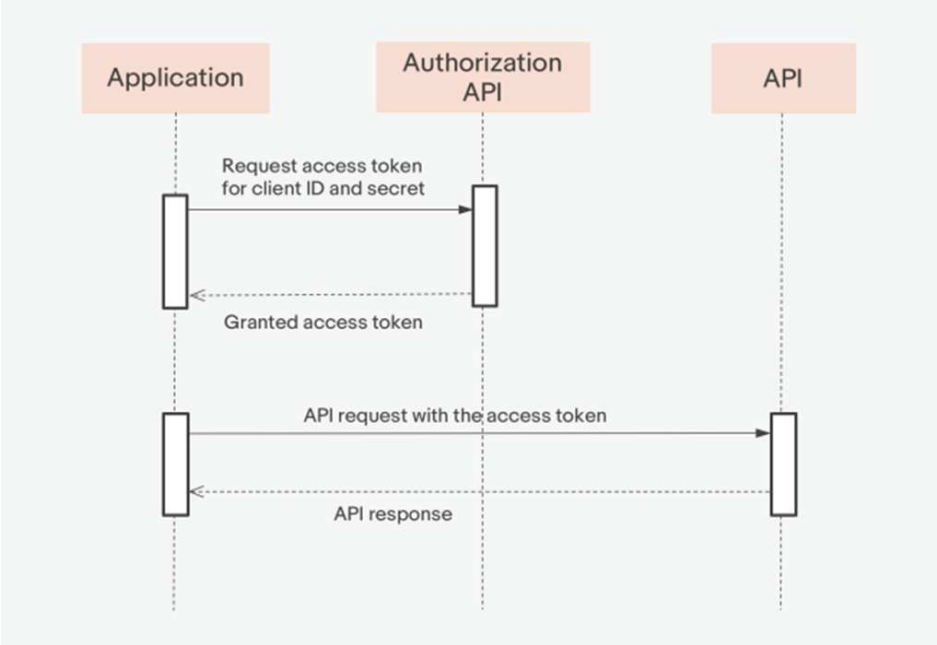
https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles/identity-and-authentication

This pattern has been adopted by HMCTS and continues to be the de-facto mechanism for authentication for both APIs and web users.

This will be realised using the OAuth2 Client Credentials grant type which is the most appropriate for system to system authentication and authorisation. The diagram below shows the high level sequence of calls involved in a typical OAuth 2 Client Credentials grant type implementation.



The pre-requite steps are that the Client application (API Consumers) need to be first registered as an Application in the Authorisation server as an application. A Client Id and client secret will be generated. The sequence diagram below further shows the calls an application would make with this grant type.



Verified user access will be controlled via user authentication against their appropriate IDAM. The IDAM that a user is verified against will be dependent on their on-boarding source, which may have been via CFT, CRIME or via the P&I IDAM.

The user will be required to select the correct on-boarding option and will then be directed to the corresponding IDAM that they were registered on.

In the case of CFT an Open ID connect approach is taken and once successfully authenticated they will be redirected back to the P&I URL with an access token. The user roles on the Crime and CFT IDAMs are held at a lower level of granularity than required by P&I business rules and a lookup will be required to map between roles. These mappings will be non-bijective and so original values will also be held against the user role for traceability.

e.g.

Case Worker – Divorce – Solicitor (CFT) -> Solicitor (P&I service)

TC.05 Job Scheduler

Job schedules will be used primarily for housing keeping functions described by AC.12 Data Management. Schedules will be configuration based and utilise the Azure Scheduler:

https://docs.microsoft.com/en-us/azure/scheduler/migrate-from-scheduler-to-logic-apps#schedule-recurring-jobs

TC.06 Rules Engine

As per architectural decisions AD.12 Business Rules will be implemented within P&I using Java Code.

TC.07 Database

The P&I service will be using a Azure database to store data it receives from both its data sources and the data it masters itself. This data includes:

- Event Data (e.g. Lists received from the data sources via APIs)
- File Data (e.g. PDFs & other lockable file formats received from the data sources)
- Configuration Data (e.g. Subscriptions & Channel Management)
- User Information & Preferences (e.g. Media User details & Welsh Language)

Business Rules will be captured and held within the Rules Engine (TC.06)

App Insights will log all Audit Information (e.g. when a user last logged in and the information being looked at) based on the assumption that this will only need to be held for 90 days. SDP will be responsible for retaining any information for a longer period.

The Azure Database technology used will be Blob Storage:

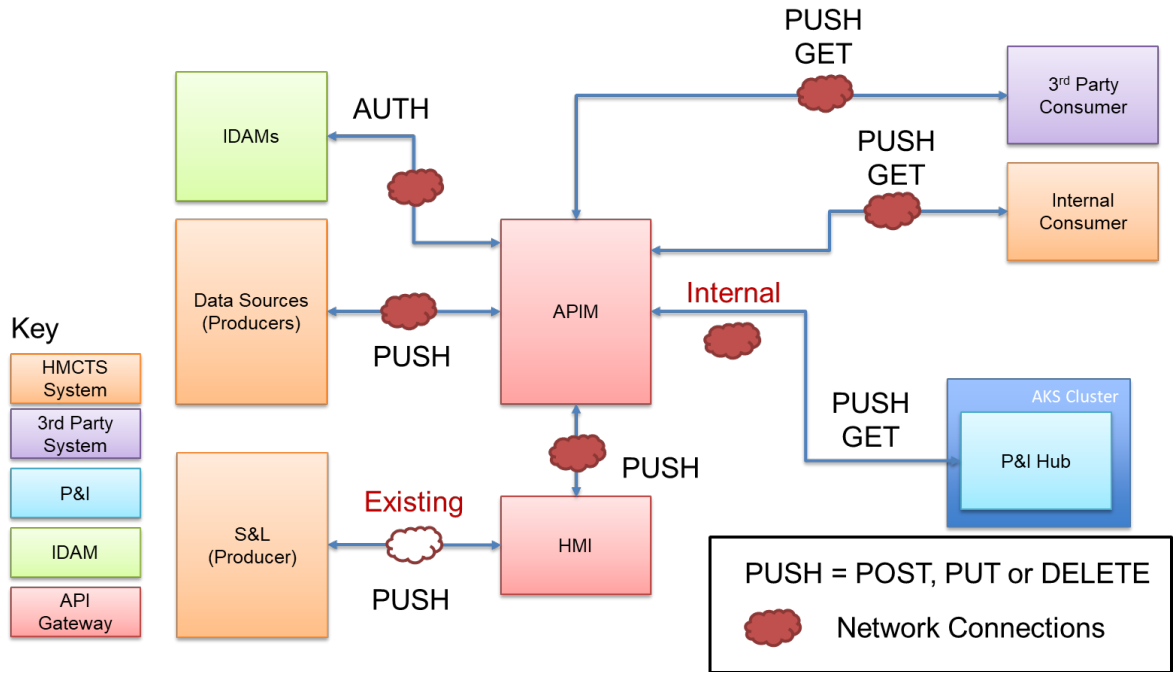
https://azure.microsoft.com/en-gb/product-categories/storage/

TC.08 Email

Email services will use Gov.Notify for the generation of outbound emails to subscribers of publication information.

6.4.3 Network and Communications View

Logical Network Component Diagram



The P&I service is not looking to introduce new components and will be using standard patterns, It is simply going to re-use existing resources configured in a different way which forces new routes of traffic through existing infrastructure, namely:

- P&I APIM -> P&I Application: Existing connectivity from SDS APIM instance to SDS AKS cluster
- P&I APIM -> IDAM: Existing connectivity in place, no change.
- S&L will ONLY communicate via HMI APIM which in turn will communicate with the P&I APIM

However, it will require the following configuration:

- New P&I Frontdoor URL for 3rd party consumers
- New P&I APIM URL

Data sources -> P&I APIM: full list has not yet been identified and therefore network designs will need to be done on a case by case basis as part of onboarding each data source. The network routes & ranges to connect to the P&I APIM will be discovered and implemented following standard hub/spoke pattern.

Network Component Diagram

Physical Network Implementation

6.5 Security Architecture

6.5.1 Confidentiality, Integrity, Availability View

The information and assets within scope of this architecture have been assessed.

Item	Rating	Assessment
Confidentiality	4 – High	The API management gateway is a generic facility for data of all levels of classification. Therefore, the highest classification must be taken into account. Disclosure of this information could lead to reputational damage to HMCTS and potential harm to individuals (both judicial and public).
Integrity	3 – Medium	Corruption of information within API calls could lead to incorrect judgements or outcomes being published. Business processing that fails to match the correct information with the stakeholders (e.g. case identifier, name and address) could lead to multiple complaints and claims for compensation and hence reputational damage.
Availability	2 – Low	The API management gateway is common to all API's and therefore unavailability would affect many functions. Partners would have a lower opinion of HMCTS. Only if an embarrassingly long outage were to be made public could reputational damage occur.

6.5.2 Security Controls View

Control ID	Category	Description
001	Developer Authentication	Individual user IDs must be used to maintain accountability, any access to the system and its components must be separate from one another and provided to devops in a controlled process.
002	Developer Authentication	Passwords must never be stored, displayed or transmitted in cleartext, they must be stored in a separate location to system data.
003	Developer Authentication	Accounts must be locked after 5 incorrect login attempts
004	Developer Authentication	Complex passwords must be enforced that comply with the MOJ password policy
005	Developer Authentication	Role Based Access Controls (RBAC) and entitlements based on the principle of least privilege must be enforced
006	Developer Authentication	Multifactor Authentication must be used for access to the system
007	App Sec	The application must be designed and implemented to prevent common security attacks such as the OWASP Top 10
008	App Sec	Applications must validate all data input, and reject input that: - is not formatted as expected - falls outside the bounds - contains code and characters other than expected - contains embedded queries that include illegal characters - contains any other unexpected content
009	App Sec	All the request must be made over a secure channel, Insecure services, protocols, etc. must not be used
010	App Sec	Full penetration test must be performed before go-live and annually thereafter in accordance with detailed scope and test plans
011	Encryption	Data in transit must be encrypted using at least 128-bit TLS with v1.2 preferred
012	Encryption	Data at rest must be encrypted
013	Encryption	Applications must never use self-signed certificates
014	Encryption	Wildcard certificates are not permitted in the production environment. All certificates must match the Fully Qualified Domain Name for internet facing services
015	Data Management	The use of production data for testing must be explicitly authorised
016	Asset Management / Dev Access	Assets must be identified, classified and documented within an asset inventory with a defined owner
017	Asset Management	Access to sensitive/confidential data must be restricted to those with a valid business need and for a specified time period
018	Incident Management	Events must generate an alert to the centralised Security Incident and Event Monitoring (SIEM) tool
019	Incident Management / Dev Access	Privilege account usage must generate log events and these events must be reviewed periodically by the Security team
020	Logging	Access to logs must be restricted to those who have an appropriate business requirement
021	Logging	Applications must log the following security-related events with userID and date/timestamps: - authentication (success of failure) - authorisation/permission granting - all configuration changes performed using a privilege account - e.g. admin

Control ID	Category	Description
		- data access attempts - data deletions - data transfers - user lockouts
022	Hosting	The server must be configured running only the required services. All unrequired services must be disabled to lower the attack surface
023	Hosting	The environments (i.e. production, staging, test) must be logically isolated from one another.
024	Account privileges	All accounts (user or system) must be configured to provide the least privileges

6.5.3 Protective Monitoring View

The following protective monitoring views must be adhered to:

1. Success and failure of job execution must be reported.
2. Login failure must be recorded and reported on.
3. Privileged access must be logged and reported on.
4. Data exports must be logged and reported on.

Both CFT and Crime IDAMs monitor user logins and log each user attempt, and if it was successful or unsuccessful, which will also be captured within the P&I service

The egress endpoints to external systems will have monitoring in place to record each external request. This will record the service token of the requesting service, along with what records it was attempting to retrieve. Platform Operations should be able to provide further details on each request if necessary.

6.6 Systems Management

6.6.1 Environments and Automation

The P&I project will use the standard HMCTS DevOps approach to the use of environments and the respective activities of build, test, deploy (https://hmcts.github.io/ways-of-working/#ways-of-working)

Azure subscriptions will be used for the environments needed with Continuous Integration and Continuous Development (CI/CD) approach adopted using the Azure DevOps component to manage the CI/CD pipeline tasks.

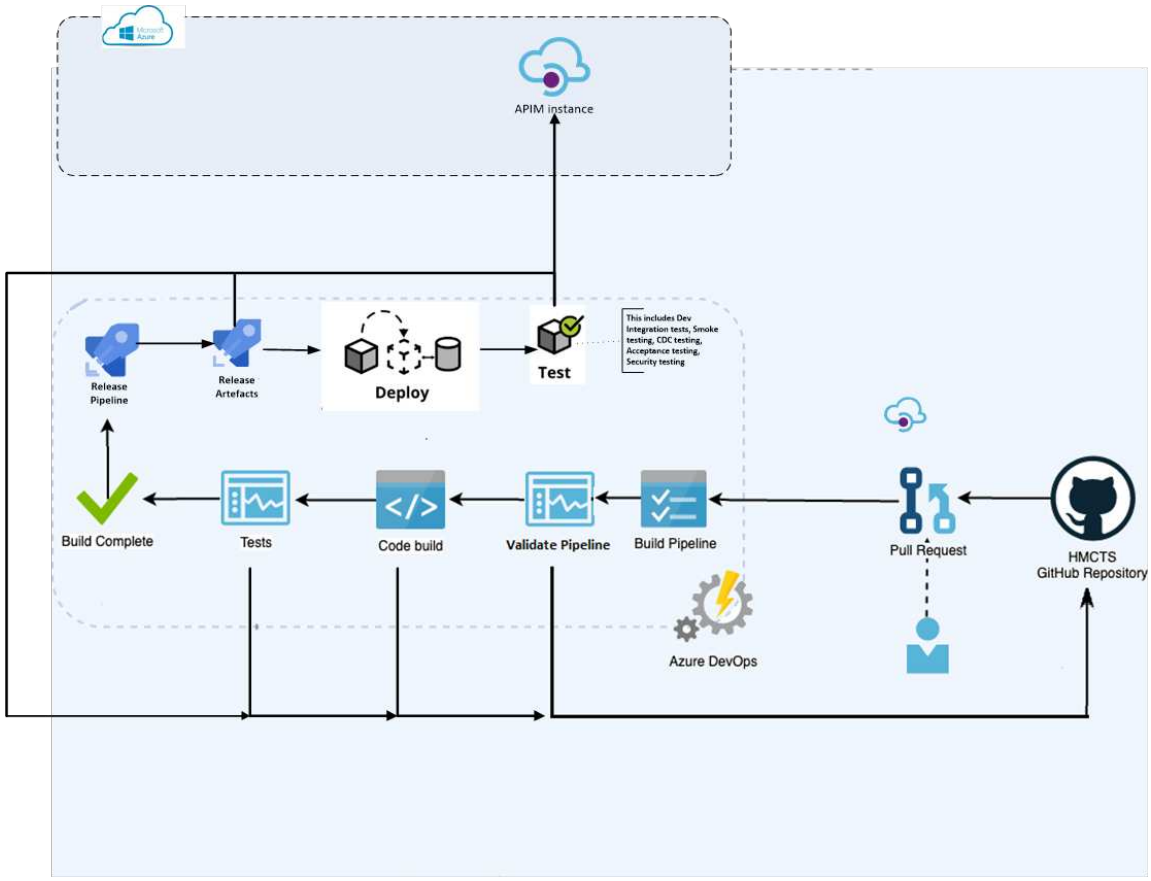
Terraform scripts will be written to manage the build and deployment of the Azure API Gateway and the respective API Endpoints needed.

API Gateway automated tests will be run using Azure DevOps and when satisfied we will promote the release to the next Subscription in the pipeline.

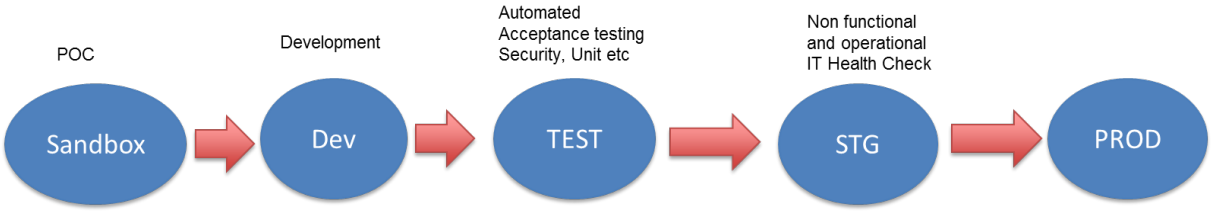
Similarly, for the remainder of the P&I microservices, they will run using SDS Jenkins before being promoted. The code will be linked to a Github repository which will be used for version control.

All environment management such as restarting or making large changes will be entirely controlled by the Platform Operations team. The P&I service team will manage the code that is on the environments and some basic configuration.

The diagram below illustrates the core tasks undertaken during the CI/CD pipeline process for our API Gateway.



The following diagram shows the SDS subscriptions that P&I will use the following:



There will be no exceptions to the programme standard approach, and our pipelines will follow the same extensive tests seen elsewhere through the programme.

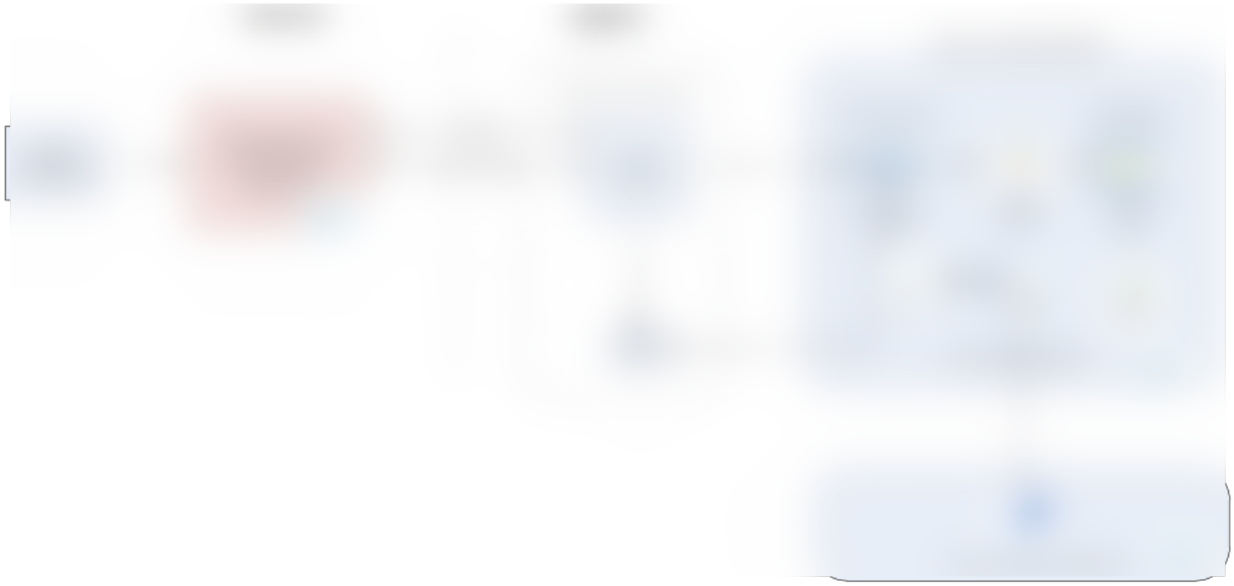
Environment	Activities	Connectivity needed	Rationale
SANDBOX	POCs, Development, unit testing changes, building tests (needs connectivity to S&L)	Connectivity to S&L stubs, Connectivity to AKS for running automated testing tools	Allows parallel dev activities if Dev is unavailable. Is a test bed for testers to build tests before TEST environment deployment
DEV	Development and unit testing, acceptance testing of tests before merge to master (ensures integrity of PR merge to master)	HUB access to Active Directory, connectivity to S&L stubs, Connectivity to AKS for running automated testing tools	No need to connect to S&L
TEST	Dev integration testing, smoke, acceptance(whitebox, blackbox, boundary, value partition,static against LLD), CDCs (contract testing),Functional testing (connectivity of S&L, lifecycle behaviour -create, list, amend hearings), Security (pipeline jobs), Performance(pipeline jobs)	HUB access to Activity Directory, Connectivity to S&L UAT/Test environments, connectivity to PACT broker (where is this?), S&L need access to PACT broker	Full complement of tests
STAGING	Performance testing and ITHC	HUB access to Active Directory, Connectivity to S&L UAT/TEST environments, Connectivity to CFT and CRIME, Connectivity to AKS, ITHC connectivity, SPLUNK and Dynatrace connectivity	All connectivity as its replicating PROD
PROD	Deployment of production ready code from master	Connectivity to S&L prod end points, Connectivity to CFT and CRIME prod end points	Production connectivity to CFT, CRIME and S&L endpoints

6.6.2 Logging and Auditing

No deviation from TGL standards. The following activities and events will be logged in logs generated by APIM which can be viewed within Azure Monitor and Dynatrace. These are taken from the recommendations from the DACS policy for applications on Logging and Monitoring for further information (Logging and Monitoring Policy).

1. Client requests and server response
2. Authentication attempts for privileged accounts (failed or successful)
3. Authentication attempts for API consumers (failed or successful)
4. Account changes
5. Number and size of transactions
6. Operational events
    a. Start-up and shutdown
    b. Errors
7. Configuration changes
8. Application-specific events such as:
    a. Service request
    b. System-level transactions
    c. The function performed (such as read, write, modify, delete)

The following diagram shows the architecture components that will be used for logging and monitoring events. Dynatrace also makes use of calling API health endpoints in the Azure stack. Security events will be sent to the appropriate Log Analytics Workspace which is the interim SIEM tool until SPLUNK is available in production in the future.



6.6.3 Monitoring and Alerting

The solution will be supported by the HMCTS PlatOps team in the first instance, and will require monitoring, logging and alerting in accordance with Reform operational standards. Any issues that cannot be resolved directly by DevOps will be escalated to the P&I Service delivery team for support. (Logging and Monitoring Policy can be found here:

Logging and Monitoring Policy

The Dynatrace application will be used to monitor System events and activities listed in section 6.6.2 which the Dynatrace agent and API will monitor and Log. Within the P&I Service stack the Azure Monitor component will be used to monitor from a system administrator perspective such as End point statuses.

6.6.4 Failover and Disaster Recovery

The P&I Service follows the following HMCTS standard approach, as defined by PlatOps:

Availability is described here:
Availability Standards

DR here:
Disaster Recovery

6.6.5 Backup and Restore

Backups and restoration will be performed as follows:

1. The P&I project will back up the list of registered media subscribers whenever a new user is added onto the system.
2. No backups of the published information will be performed by the P&I project as we are not the source of information.
3. Backups of logs will be managed by the Platform Operations team as per programme standard.
4. Any restoration will have to be carried out with consultation from the Platform Operations team.

6.6.6 Archiving

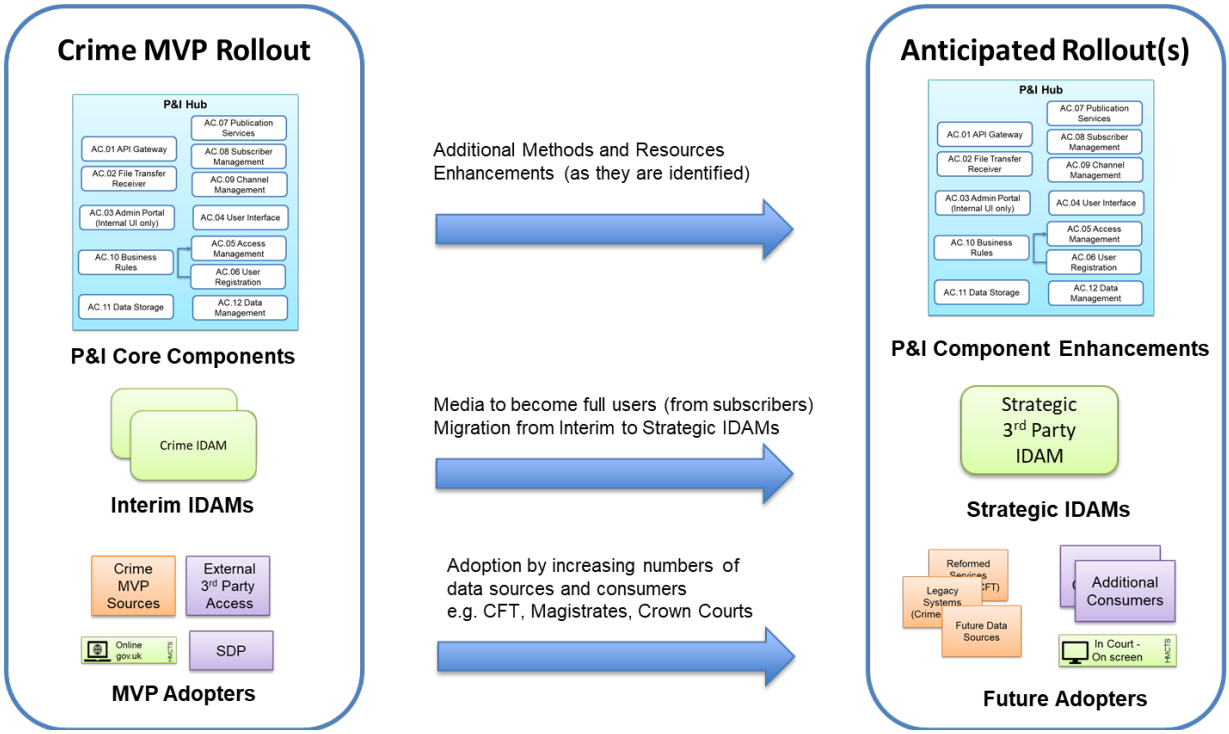
No archiving requirements and no exceptions from the programme standard approach. It is up to the source systems providing data to the P&I Service, to ensure that the data is accurate and up-to-date.

7 Architecture Roadmap

7.1 Roadmap

The initial delivery of the P&I Service will be in support of the Crime MVP rollout. In terms of capability the majority of the P&I Core Components will be delivered together, however, the following areas are anticipated to be enhanced as part of future rollouts:

1. Users – The initial verified user base will relate to Legal Professionals, however, it is expected that the Media will move from being subscribers to having verified access rights (i.e. enhanced access to information via the UI as well as via email subscriptions)
2. IDAMs – It is understood that as part of a wider HMCTS initiative the current Interim IDAMs are being reviewed and may potentially move to strategic 3rd Party IDAMs. If/when this happens it is anticipated that the P&I Service will follow this business change
3. Adopters – Whilst the P&I service will provide methods & resources to support the Crime MVP as future data sources and consumers wish to adopt the service, additional methods and resources may be introduced



The Delivery Roadmap for the P&I Service is:

7.2 Transitions

The initial roll out, as part of project scope, will be for the P&I Service to be provided to meet the Crime MVP. From this point, it will be handed over to the DTS team.

Note: The DTS team are being incorporated within the core delivery team to aid this transition process.

The MVP requirements for the P&I Service can be found here:

P&I MVP Requirements

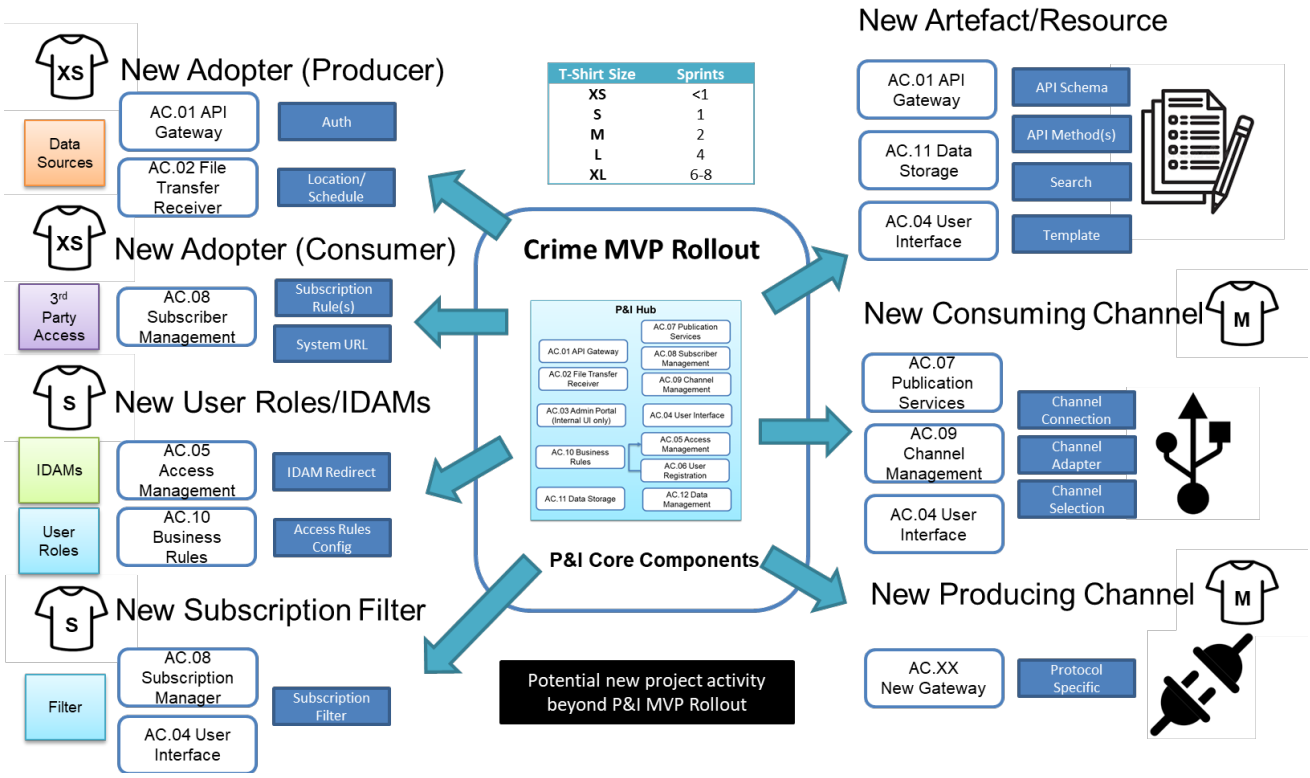
Beyond this roll out it is anticipated the CFT, Magistrates, Crown Courts and other Data Sources will follow on as further services are on-boarded on a service-by-service basis by DTS and not a reform delivery team.

Operability and implementation will be defined in more detail as progress is made through the transition steps.

Initially, the roll out plan will be to go location-by-location with risk and mitigation designed to work with the delivery partners (e.g. Courtel) to ensure no duplicate fed data is published on their service despite it coming from one source. Detailed communications will be made around what is coming and implementation plans will be developed that will stipulate the need for source services to stop sending to legacy and come to P&I instead. P&I will manage the communications backward or through the partner services and will ensure that there are no duplicated comms or publications.

7.3 Product Enhancements

The P&I service is designed to be extensible and common use cases that might be required by new projects are presented below, including a typical T-Shirt sizing delivery estimate:



These use cases may require additions to core P&I components which are indicated by the table below:

New Use Case	T-Shirt Size	AC.01	AC.02	AC.03	AC.04	AC.05	AC.06	AC.07	AC.08	AC.09	AC.10	AC.11	AC.12	AC.XX
Adopter (Producer)	XS	X	X											
Adopter (Consumer)	XS								X					
User Roles/ IDAM	S					X					X			
Subscription Filter	S				X				X					
Artefact/ Resource	M	X			X									
Consuming Channel	M				X			X		X				
Producing Channel	M													X

Key:

AC.01 API Gateway	AC.07 Publication Services
AC.02 File Transfer Receiver	AC.08 Subscriber Management
AC.03 Admin Portal	AC.09 Channel Management
AC.04 User Interface	AC.10 Business Rules
AC.05 Access Management	AC.11 Data Storage
AC.06 User Registration	AC.12 Data Management

7.4 Product Enhancements Use Case

Scenario (Illustrative):
Display P&I lists on Court Screens

Can existing artefacts be used?	Can the P&I UI be used via a web-redirect?	Can an API subscription to P&I data be used?	Can a new consuming channel be created?	Is a new subscription required?	Action	T-Shirt Estimate
YES					Use Existing Artefacts	None
	NO				Look for alternative access method	N/A
		NO			Raspberry PI is not able to ingest existing API methods	N/A
			YES		Create new consuming channel (HTML based)	M
				YES	Create new consuming adopter subscription	XS

In this use case there is a requirement for P&I to provide List information so that it may be displayed on Court Screens. Whilst the Lists information satisfies their data requirements they rely on HTML messages to be sent to a Raspberry PI.

To achieve this a new consuming channel would be required to send List information in the HTML format and an update to the consuming subscriptions would be required to ensure that this information is sent to the appropriate Raspberry PI addresses.

Whilst enhancements are required other core components around ingestion, storage, rules, audit and channel management remain unchanged and these enhancements do not impact existing features or operation.