Digital Prescribing & Dispensing Pathways Programme

Deployment and Infrastructure Architecture Description

DOCUMENT CONTROL SHEET

Title:	
Date Published/Issued:	
Date Effective From:	
Version/Issue Number:	
Document Type:	
Document Status:	
Author:	
Approver:	
Approved by and Date:	
Contact:	
File Location:	

Approvals*:*

This document requires the following signed approvals:

Name	**Title**	**Date**	**Version**

Distribution:

This document has been distributed to:

Name:	**Title/Board:**	**Date of Issue:**	**Version:**

Revision History:

Version	**Date**	**Sharepoint Version**	**Summary of Changes**	**Name**

Contents

Approvals:.....2
This document requires the following signed approvals:.....2
Distribution:.....2
This document has been distributed to:.....2
Revision History:.....2
Introduction.....5
Purpose.....5
Audience.....5
Scope.....5
Structure of Architecture Documents.....6
References.....7
Deployment and Infrastructure Architecture.....9
Overall Solution Architecture.....9
Overall Solution Architecture Diagram.....10
Overall Physical Architecture.....11
Detailed Physical Reference Architecture.....12
Simplified Physical Architecture of DPDP Service.....13
Physical Architecture Dependencies.....14
Overall deployment Architecture.....15
Contextual Scope View of the Deployment and Infrastructure Architecture.....15
Overall View of Deployment and Infrastructure Architecture.....16
Detailed Views of Deployment and Infrastructure Architecture.....17
Build and Deploy Process.....21
Deployment Environments.....21
Pipeline.....23
Non-Functional Requirements and Failure Scenarios.....25
Non-Functional Requirements.....25
Criticality and Failure scenarios.....25
Deployment Configuration Considerations for NDP Authentication and MS Entra.....26
Appendices.....27
Appendix A –.....27

DPDP Deployment and Infrastructure Architecture Introduction

Introduction

Purpose

The purpose of this document is to describe the deployment and infrastructure architecture of the digital prescribing and dispensing pathways (DPDP) service, referencing overviews of the business and solution architectures that the deployment must support and realise in order to successfully deliver the DPDP programme objectives.

The deployment and infrastructure are both presented as a series of perspectives, each containing a number of views. Each perspective broadly groups together related views that describe particular areas of architectural concern.

Audience

The primary audience of this document are those stakeholders and other parties who have interests related to the overall technical solution. These stakeholders include internal NSS and NES teams, potential and incumbent suppliers, technical team members from organisations with system dependencies on DPDP or ePharmacy, and Scottish Govt technical strategists.

The secondary audience of this document are those stakeholders with an interest in the overall delivery of DPDP or services with a cross-dependency on the programme. This includes programme leads, business stakeholders, healthcare leads, sponsors, external agencies, suppliers and Scottish Govt healthcare strategists.

Scope

The scope of this document covers the technical solution, including how it realises the business capabilities. It does not include the business capabilities or processes with the context of the DPDP programme; these are described in a separate document. Other services outwith the DPDP domain may be referenced within the context of the solution if there is a dependency between the process/service/system in question and digital prescribing.

In scope for the DPDP solution architecture are:

- Advanced Electronic Signature (AES) signing of prescriptions.
- Public Key Infrastructure (PKI).
- API-centric integration of services and components within DPDP, including orchestration and choreography of underlying services, data transformation, service resilience.
- Notifications service for alerting patients of prescription events.
- API access control and management.
- New integration routes (“pipelines”) into existing systems as part of intermediate transition architectures.
- User registration and authentication for AES.
- Public access via a portal (possibly as a mobile app) for prescription-related information.
- Direct messaging between prescribers and dispensers.

Out of scope

- Network or domain authentication
- Changes to 3rd party systems, such as PMR’s, GP IT, beyond identifying the API operations needed to support those services
- Changes to downstream systems other than to provide pipelines to feed data into those systems.

- Identity and access management (IAM) beyond the core requirements to authenticate prescribers for AES.
- Analysis of the incumbent ePharmacy (aka ePMS) messaging-based prescription service from Atos. This analysis is available in the document DPDP - Analysis of ePMS.docx [1].
- Design of the business architecture required for the successful delivery of the DPDP programme. The business architecture is available in the document DPDP Business Architecture.docx [2].

Structure of Architecture Documents

The architecture documents are broken down as follows:

Section	Purpose
Introduction	This section contains the purpose, audience and scope of the document.
Business Architecture	Contained within a separate document [2]. That document contains the capability, actor and process views of the business architecture, including a breakdown into activities and value streams.
Solution Architecture	Contained within a separate document [9]. That document contains the logical views of the solution architecture, including overall vision and contextual views, the more detailed description of each subdomain and its services, and dynamic views showing collaborative behaviour between services where appropriate, within the solution domain.
Physical Solution Architecture	Contained within a separate document [10]. That document contains the physical views of the solution architecture, including the reference architecture that all new services within the DPDP will be expected to adhere to. The implementation technologies and platforms are described within the physical domain.
Solution Architecture Mapping to Business Architecture	Contained within a separate document [9]. That document maps the logical solution architecture to the capabilities, value streams, functions and processes within the business architecture [2].
Data Architecture	Contained within a separate document [11]. That document contains the logical and physical views of the data architecture, including data flows, state models, data schema and data-tier integration platforms.
Integration Architecture	Contained within a separate document [9]. That document contains views of the integration architecture where additional information is required beyond the descriptions in the preceding sections.
Deployment and Infrastructure Architecture	This section contains the deployment views, including availability and service continuity aspects, as well as the environment chain to be used within the DevOps delivery pipeline.
Delivery Phases	Contained within a separate document [9]. That document contains views of the logical architecture for the known delivery releases from MVP to target end-state architecture.

Section	Purpose
Appendices	This section contains supporting information and further detailed breakdowns.

References

[1] Analysis of the incumbent ePMS service: DPDP - Analysis of ePMS.docx (Sharepoint permissions required), current version

[2] DPDP Business Architecture design: DPDP Business Architecture.docx, (Sharepoint permissions required), current version

[3] DPDP Architecture Decision Log: DPDP Architecture Decision Log.xlsx, (Sharepoint permissions required), current version

[4] DPDP Proposal to use Public Internet rather than SWAN for Secured Connectivity: DPDP - SBAR Use of Public Internet for Secured Connectivity v2.2.docx, (Sharepoint permissions required), current version

[5] DPDP NFR Requirements Log (draft): DPDP NFR requirements.xlsx, (Sharepoint permissions required), current version

[6] DPDP Test Strategy: DPDP test strategy.docx, (Sharepoint permissions required), current version

[7] DPDP Architecture Principles: DPDP Architecture Principles v1.0.docx, (Sharepoint permissions required), version 1.0

[8] DPDP Business Glossary: Business Glossary.xlsx, (Sharepoint permissions required), current version

[9] DPDP Solution Architecture Description: DPDP Solution Architecture Description.docx (Sharepoint permissions required), current version

[10] DPDP Physical Architecture Description: DPDP Physical Architecture Description.docx (Sharepoint permissions required), current version

[11] DPDP Data Architecture Description: DPDP Data Architecture Description.docx (Sharepoint permissions required), current version

[12] DPDP Subdomain Criticality, Failure Scenarios, Impacts and Mitigations (draft): DPDP Subdomain criticality and failure scenarios v0.1.xlsx (Sharepoint permissions required), current version

[13] DPDP Roles, Actors and Service Permissions Matrix: DPDP Roles, Actors, Permissions, BUIs.xlsx (Sharepoint permissions required), current version

Deployment and Infrastructure Architecture

Deployment and Infrastructure Architecture

The deployment and infrastructure architecture of the solution for the DPDP service is broken down into the architecture of the deployment platforms (primarily within AWS cloud), related dependencies, and the matrix of linked environments necessary for the build pipeline for building and deploying the service. This last point includes both deployment as a live production service and as a set of integration environments for suppliers to use for integration testing. Refer to the Overall Logical Solution Architecture section of [9] for logical views of the entire DPDP service and the physical architecture descriptions [10] for views showing the built services, supporting technology platforms and physical dependencies.

Note that there are a number of critical architectural decisions within the overall DPDP solution architecture. Where they have been made the physical and deployment architecture will reflect any impact of that decision and references made to the decision log [3] that contains a record of that decision and the relevant options paper that supports it if one exists.

As the architecture of each domain evolves, the physical architecture and logical deployment architecture will be updated. The overall physical architecture is provided within [10]. The solution architecture is aligned to the programme architectural principles [7]. Business terms are defined in a central business glossary [8].

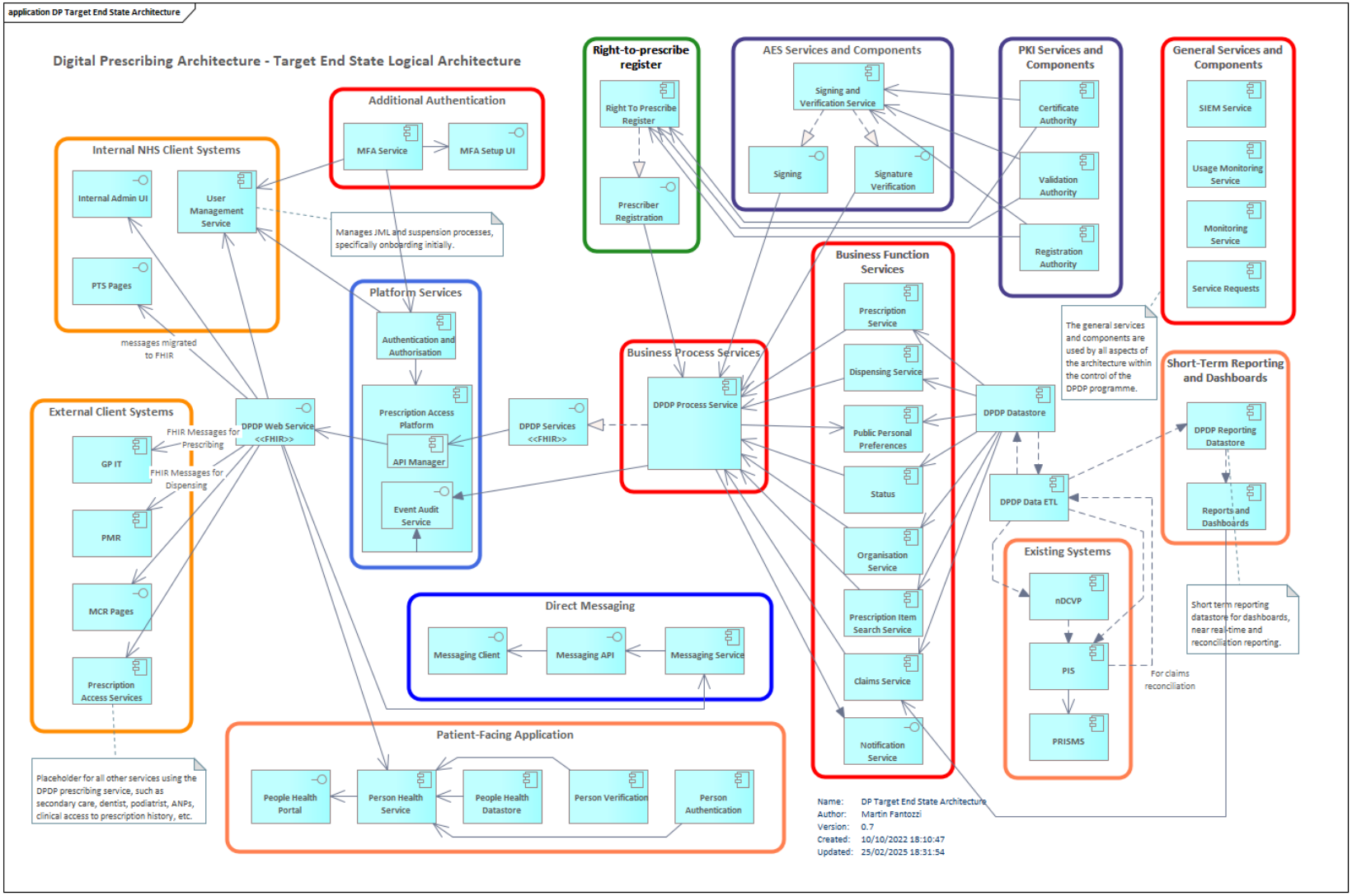
Overall Solution Architecture

The solution is API-centric and structured as an n-tier, micro-service architecture. It is cloud-deployed and uses a mix of synchronous and event-driven services. The architecture is stateless and designed to be highly scalable, resilient, flexible and extensible. The significant NFR constraints are the need for 99.99% availability, an RPO that stipulates loss of inflight transactions only, and security considerations typical of a healthcare-related critical national service. Significant technology constraints are that the majority of deployment platforms should be those provided by AWS.

The following diagram shows the overall solution architecture, using coloured boundaries to separate the whole into subdomains.

Overall Solution Architecture Diagram

The following diagram provides the overall logical solution architecture for DPDP, refer to [9] for further details

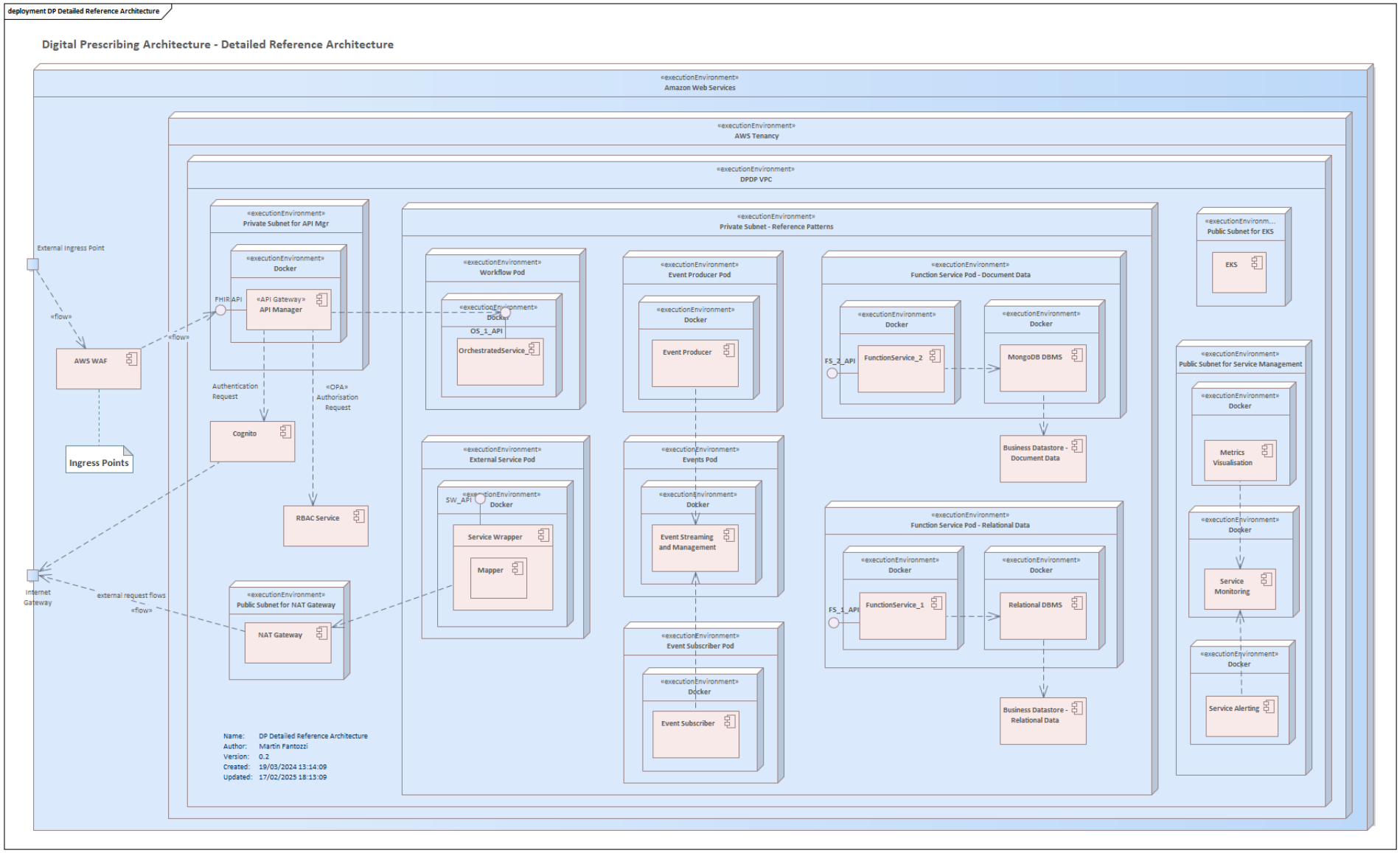


Overall Physical Architecture

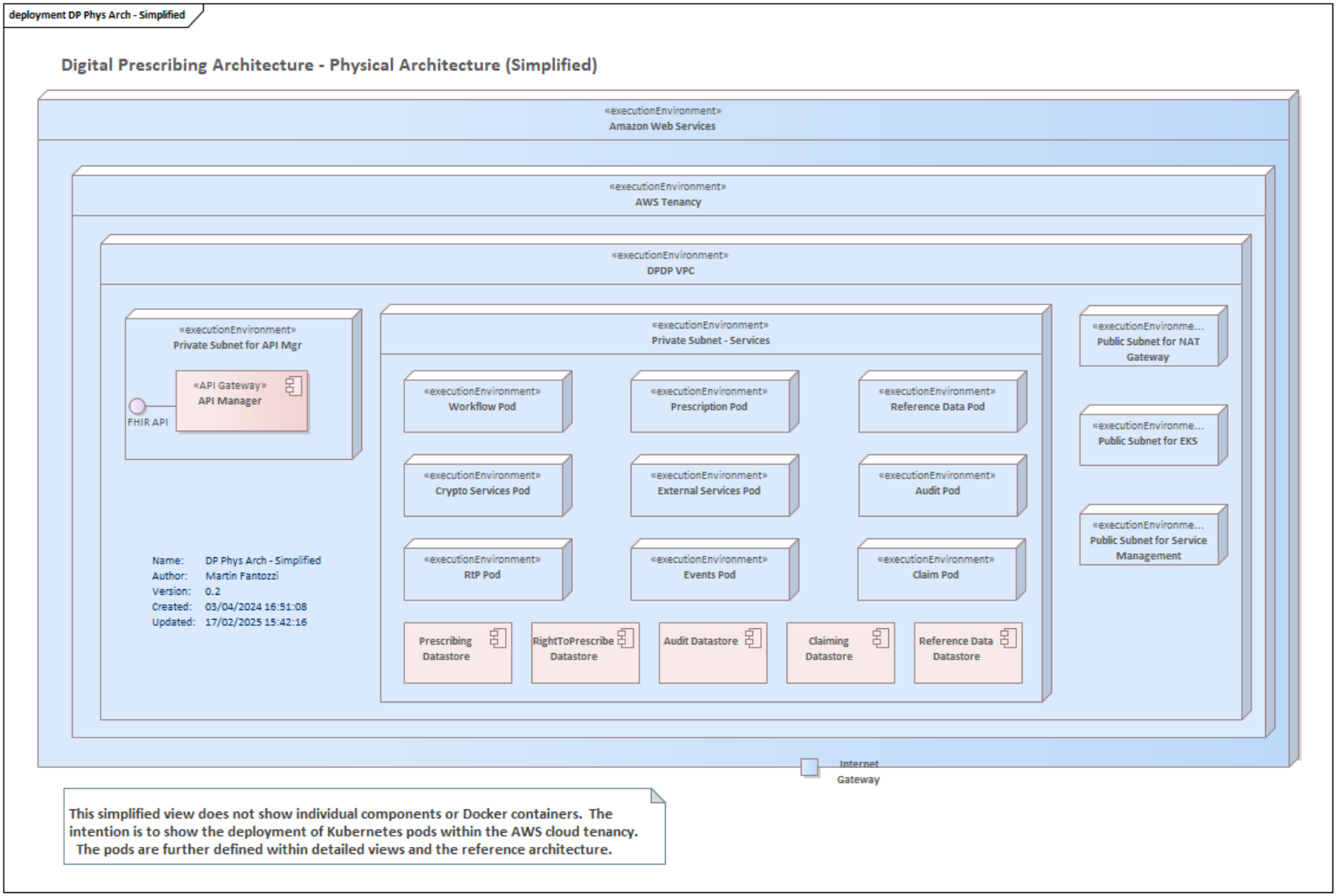
The physical architecture diagrams, extracted from the physical architecture [10], show the major artefacts and dependencies that must be deployed as part of the DPDP implementation. The physical architecture diagrams are:

- The reference architecture for the DPDP services, including managed execution environments. These provide a pattern-driven basis for the build and deployment approach for DPDP, including the management platforms and dependencies with AWS software infrastructure, such as WAF, NAT gateways, etc.
- A simplified physical architecture showing the managed pods that must be deployed within the context of the overall DPDP service
- External physical architectural dependencies that the DPDP service has on services deployed within other environments.

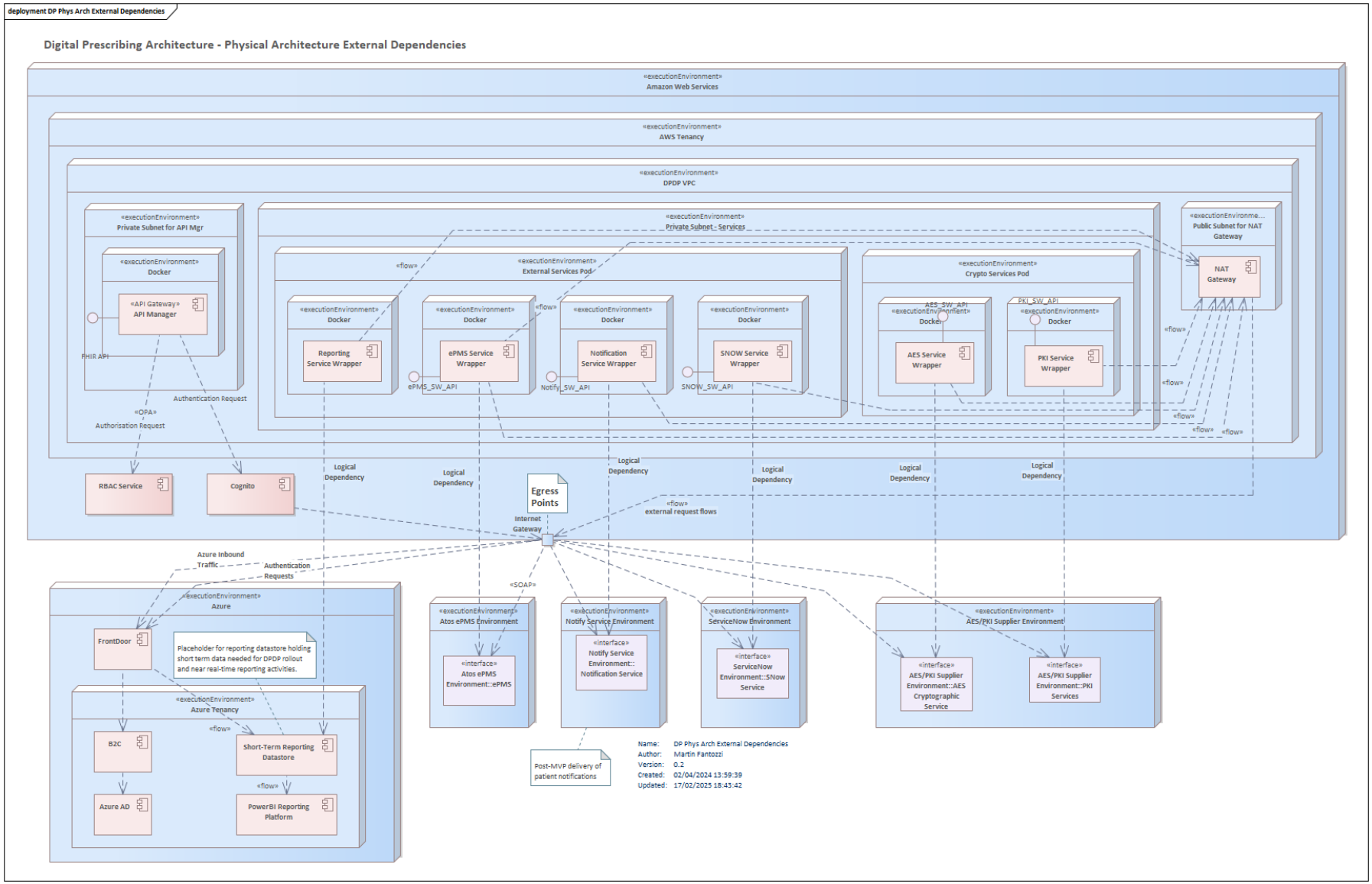
Detailed Physical Reference Architecture



Simplified Physical Architecture of DPDP Service



Physical Architecture Dependencies

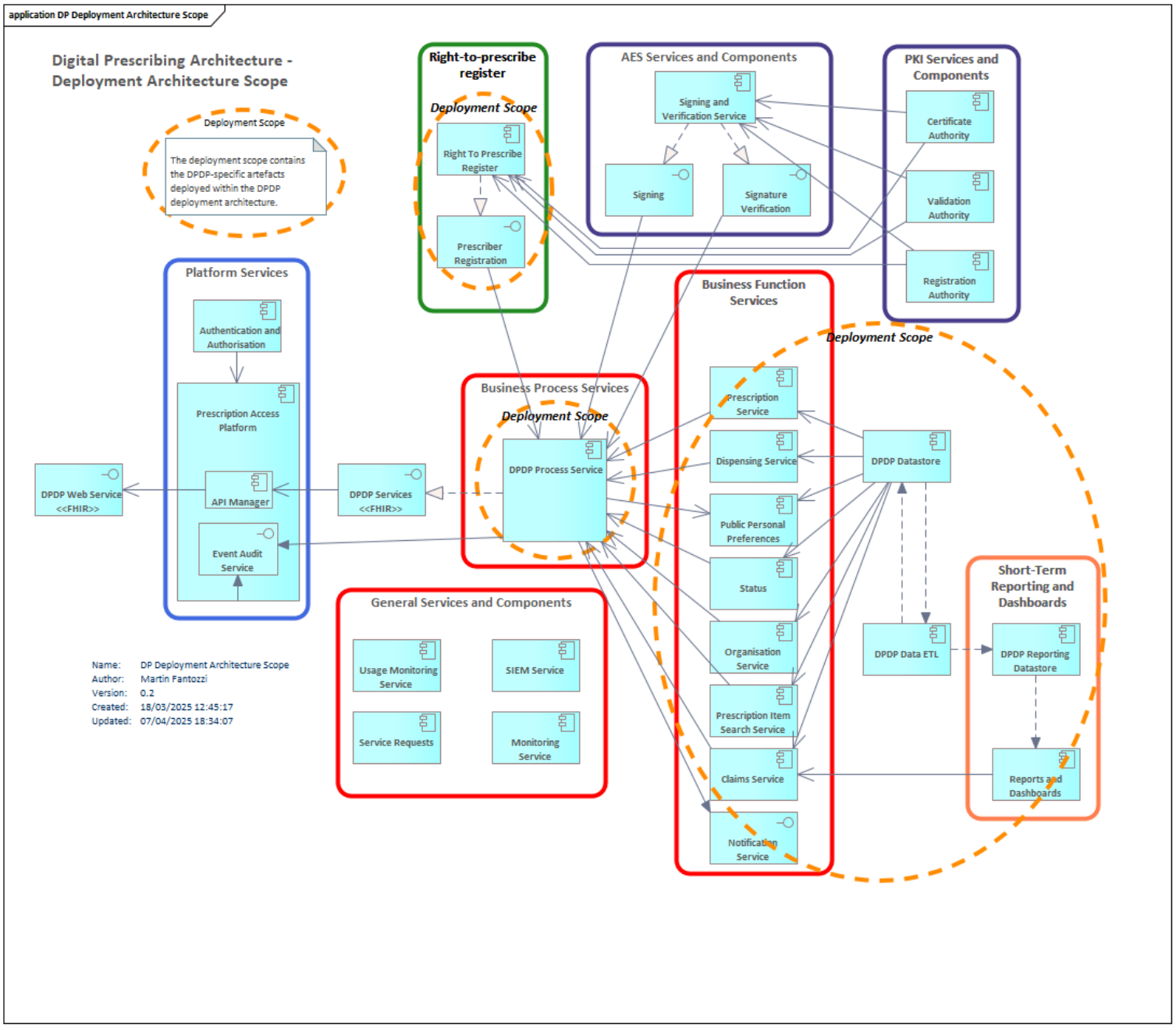


Overall deployment Architecture

Contextual Scope View of the Deployment and Infrastructure Architecture

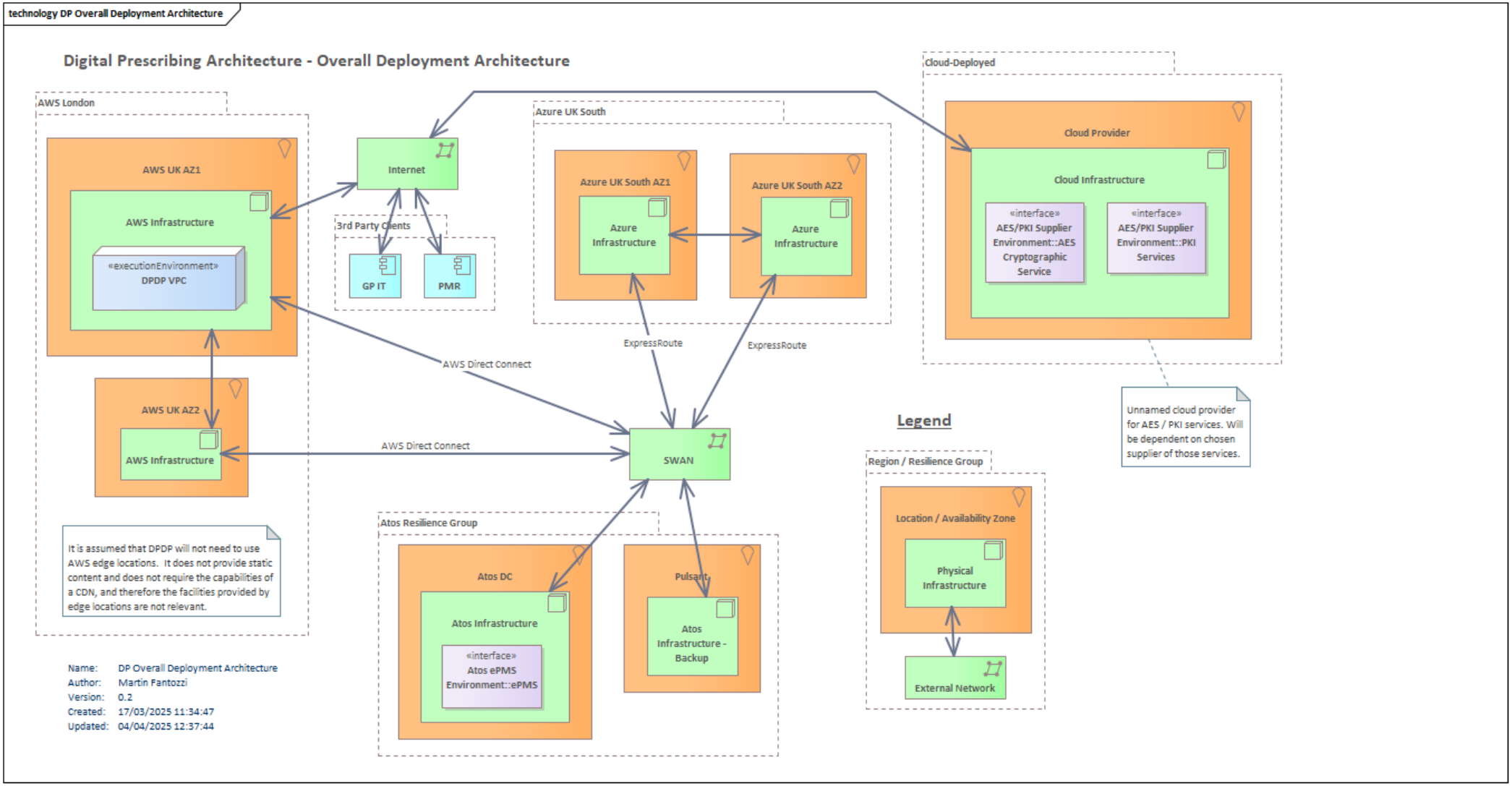
The deployment and infrastructure architecture covers internally deployed DPDP subdomains defined within the solution architecture [9], other NHS Scotland domains, such as those provided within the NHS National Services Scotland Azure tenancy, connectivity between those domains, and some aspects of the connectivity between those subdomains and external dependencies, such as Atos' ePMS system or the AES / PKI services that will be provided by an as yet undecided external supplier.

The overall scope of the deployment architecture in terms of DPDP subdomains is shown in the summary scope diagram below. Existing production subdomains within NHS Scotland are not described further. Subdomains outwith NHS Scotland are referred to as external dependencies.



Overall View of Deployment and Infrastructure Architecture

The overall view shows the primary regions and zones for the deployed DPDP services and the overall connectivity between those locations.



Regions and Zones

The DPDP service is defined as critical national infrastructure and must be available on a 24*7 basis with 99.99% availability and loss of in-flight transactions only during failover [5]. To meet those requirements it will be deployed across two availability zones in the AWS London region within the NHS NTS AWS tenancy.

DPDP will use the current national instance of Microsoft Entra managed by NSS DAS to provide the authentication service, and it is assumed that the NHS NSS Azure tenancy is currently deployed across multiple availability zones in the Azure UK South region.

The incumbent ePMS (aka ePharmacy) service is deployed within an Atos data centre, with an additional instance deployed to a Pulsant data centre to meet availability requirements. Whilst DPDP must send prescription and claims data to ePMS, failure of ePMS or the communications link to it will not prevent DPDP from processing prescriptions.

The AES / PKI services will be hosted within a cloud environment owned by the service vendor. As part of the ITT and subsequent SLA that service must adhere to the same requirements for availability and recoverability. The cloud provider will be dependent on chosen supplier of those services.

Static Content Delivery for User Interfaces

DPDP primarily provides APIs for client systems to consume, however there are a limited number of UI requirements for basic reference data and simple data access needs, which will only be accessible to production users within NSS and territorial health boards. These will not contain significant static data and will not require CDN capabilities nor the use of AWS Edge locations.

Communications

DPDP will not mandate the use of the Scottish Wide Area Network (SWAN) for connectivity between client systems and the NDP platform hosting the DPDP APIs [4]. Those inward connections will use public internet connectivity with appropriately secured endpoints, however individual deployments can use existing SWAN connections if desired. Connections outward from DPDP to other services where there is no existing SWAN connectivity and where SWAN is not mandated will also use public internet connectivity.

For communications where SWAN is mandated, such as any connection to the ePMS service hosted by Atos, this will continue to be used. DPDP is hosted exclusively within AWS at the time of drafting this specification, so this will require use of AWS Direct Connect. It is assumed that all AWS-to-Azure connections for NTS and DAS tenancies will be via SWAN at this point.

Detailed Views of Deployment and Infrastructure Architecture

The detailed views of the deployment architecture are split into the NES NTS tenancy and the DAS Azure tenancy.

AWS Deployment Architecture

Within the AWS deployment the overall deployment of three example Kubernetes pods are shown, highlighting the Prescription, Right-to-Prescribe and External Services pod deployments. It is expected that deployment will use an IaC approach, with pod definitions contained within Kubernetes deployment templates. Some of the critical additional configuration aspects are also shown, specifically around WAF policies, API management, NAT routing, and the use of an Atos-supplied x.509 certificate for signing HTTP requests sent to the Atos ePMS messaging platform.

See the Communications subsection immediately above for information about scenarios mandating the use of SWAN from AWS.

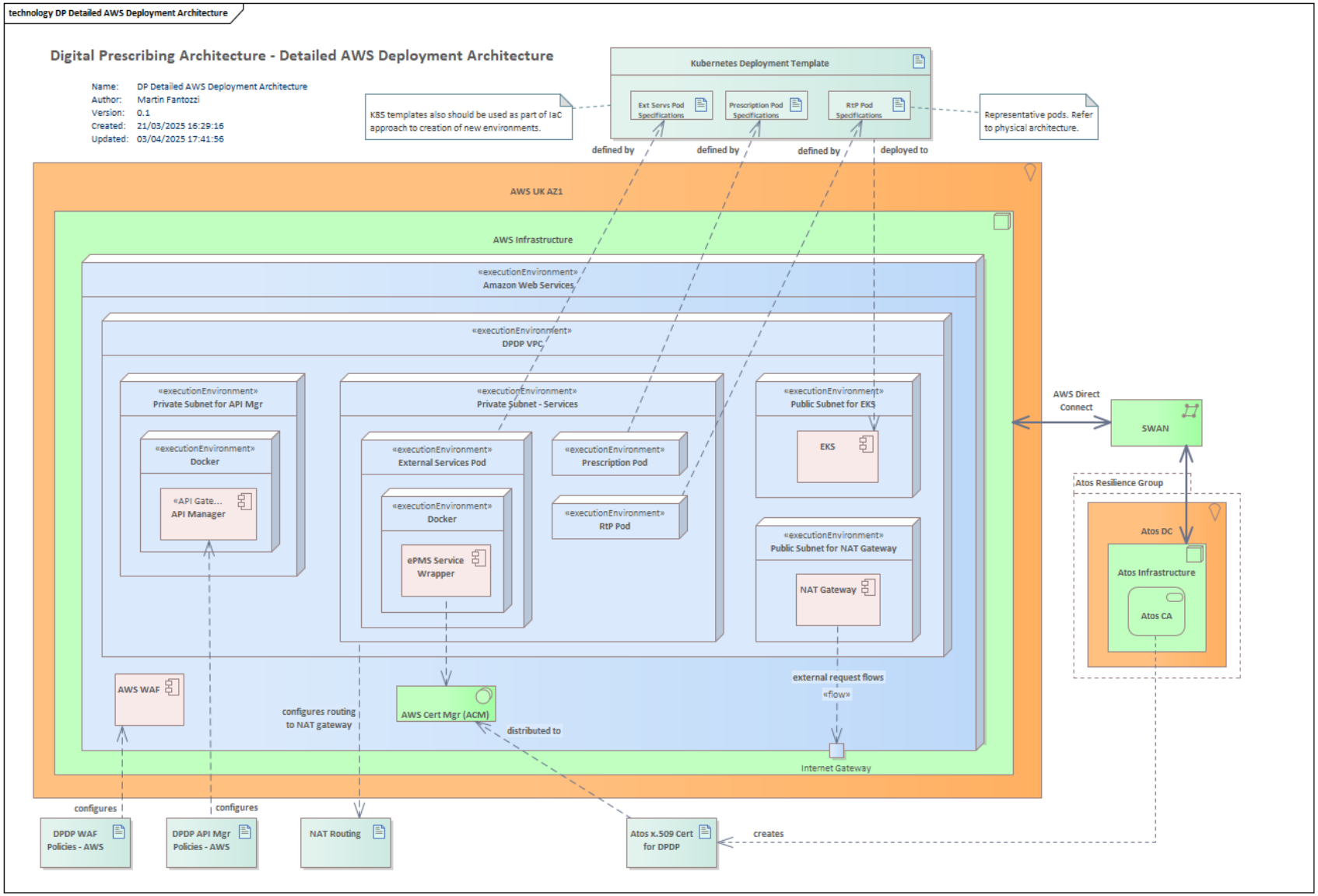
Azure Deployment Architecture

The Azure tenancy holds the central Microsoft Entra authentication service and the Seer analytics and reporting platform.

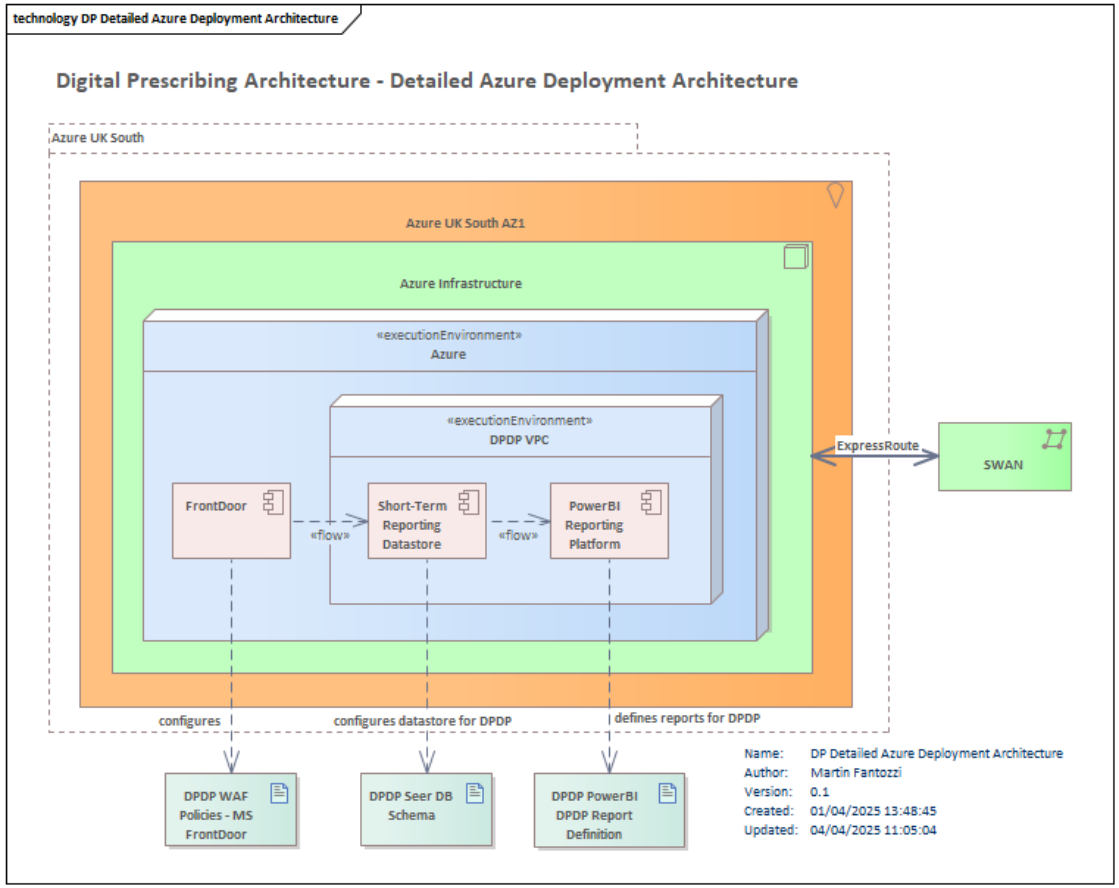
The former is not shown nor described within this document: it is an existing service that will be used directly or indirectly by the AWS-deployed API manager and with the exception of policy changes for DPDP requirements is outside the scope of the programme deliverables. This will be described in more detail elsewhere.

The Seer analytics and reporting platform will be sent DPDP business event information for short-term reporting purposes. This will require the deployment of an appropriate database schema and also report specifications for the PowerBI reporting tool in use.

Detailed View of AWS Deployment Architecture



Detailed View of Azure Deployment Architecture



Build and Deploy Process

The development of DPDP will be based on DevOps principles, with automated building, testing and deployment of components and the overall service. The testing regime is described in the DPDP test strategy [6].

There are exceptions to the auto-deployment of successfully tested services. It is not appropriate to auto-deploy critical healthcare services to pre-prod / production; such decisions must be part of a governance process that takes into account the risks associated with deploying to those environments. In addition, deployment to suppliers' integration test environments must be based on the defined sub-release schedule to enable them to follow controlled build and QA processes.

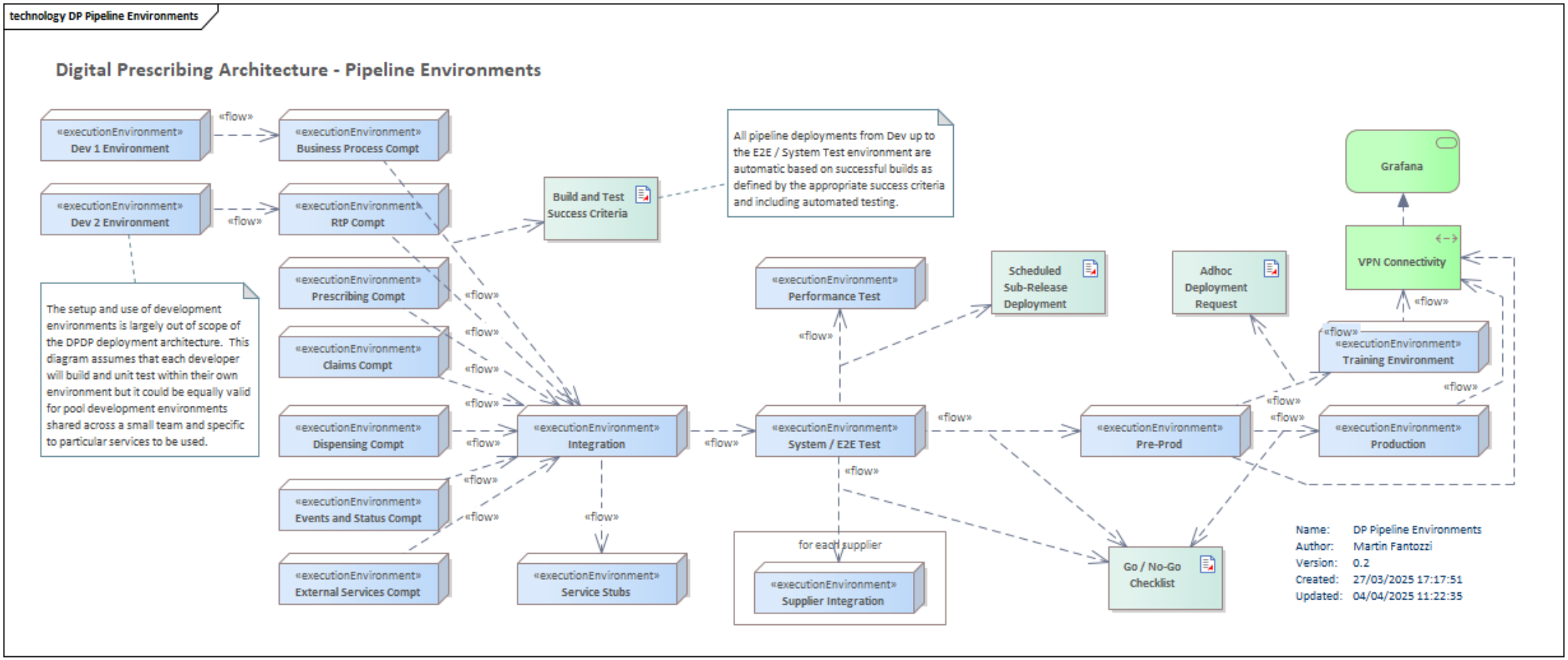
Deployment Environments

The following diagram shows the environment setup needed for the build and successful deployment of DPDP as a production service. Promotion and lateral deployment is controlled by a mix of automated and manual controls, with the specific mechanism dependent on the target environment:

- Deployment from Dev environments to component environments is controlled by check-in to the source repository and is at the discretion of the developer;
- Promotion from the Component environments through to the System / End-to-end test environment is based on automated deployment rules;
- Linear promotion to Pre-Prod and Production is at the discretion of the team, based primarily on a Go / No-go checklist of criteria;
- Lateral promotion to the Supplier Integration and Performance test environments is again discretionary but should occur for each sub-release during the build process, however this should not preclude ad-hoc updates of the supplier integration environments or ad-hoc performance testing of new capabilities if required.

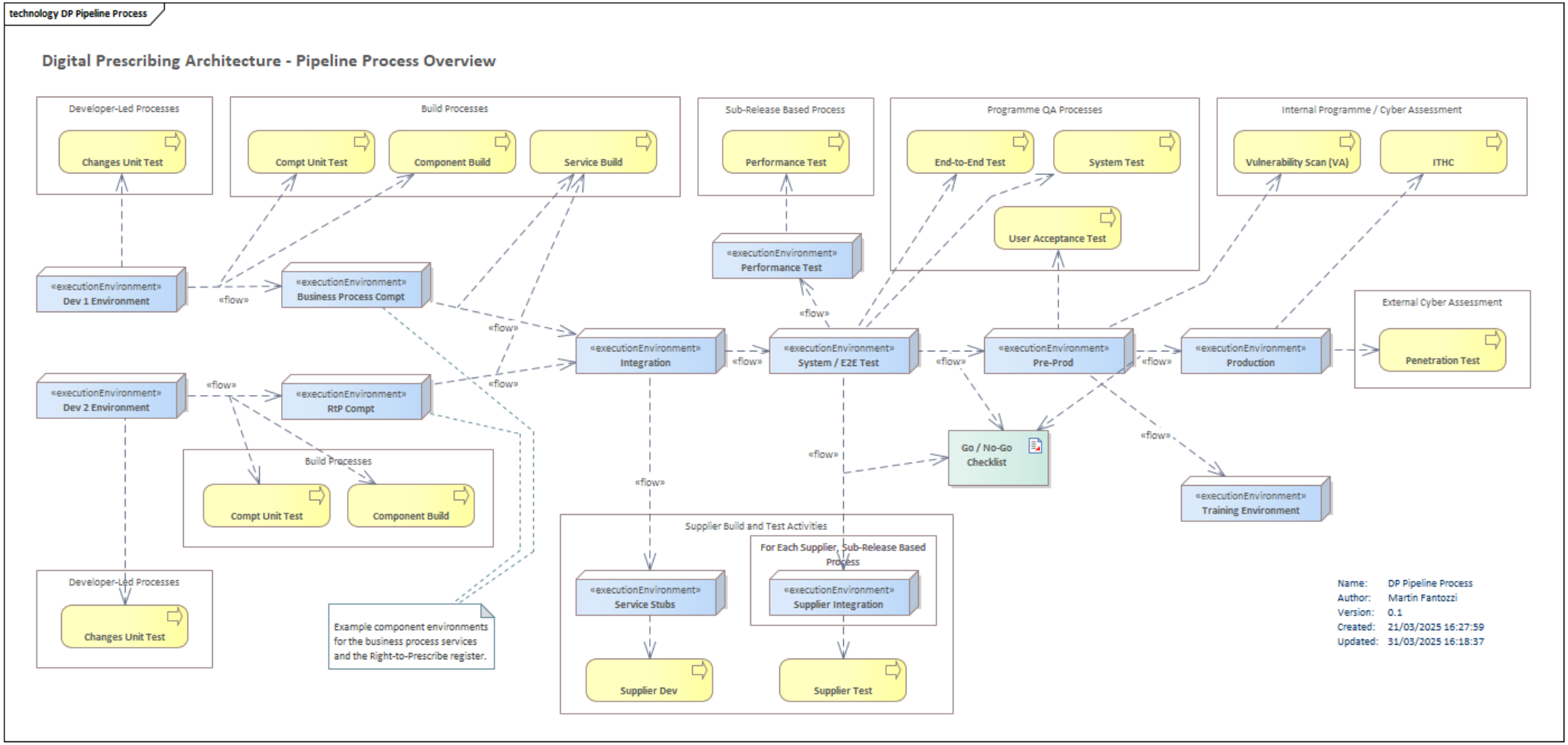
New environment builds should be created using IaC (Infrastructure-as-Code) configuration to ensure consistency of the environments created. Pod definitions should be contained within the Kubernetes deployment templates.

Deployment Environments Diagram



Pipeline

The activities that will occur within each environment are shown below. Note: (1) the Dev environments shown are not prescriptive; (2) there will be a number of component environments for the QA team to perform automated tests for each micro-service domain – see the environments diagram above.



Pipeline Activities

The internal QA activities shown above are described in detail in the DPDP test Strategy document [6]. It is expected that the vast majority of testing will be automated, repeatable and repeated frequently.

Unit testing is expected to be conducted both by developers and as part of the build process. There are no specific requirements set by DPDP on the exact setup of the development environments.

Promotion of DPDP to the performance and supplier integration environments is expected to be based on the sub-release cycle, whilst not precluding ad-hoc deployments to either as well.

Whilst VA scanning can occur on the pre-production environment, it is essential that ITHC and penetration (pen) testing is carried out on the production environment. Pen testing in particular is designed to discover the weaknesses within live systems, so must be carried out on those systems.

Supplier-based development and testing regimes are outwith the scope of the programme's activities, however it will be a requirement for a supplier wishing to access a DPDP API to register with the programme. That registration will enable the programme team to provide both access to a standard set of stub APIs (which will provide a simple, generic response) and a supplier-specific integration environment that will provide full prescribing and dispensing test harnesses. The former is available for low-level development and unit-testing workloads whilst the latter is intended to provide the ability to create and dispense prescriptions so that suppliers can undertake full end-to-end testing of their products' integration with DPDP.

Non-Functional Requirements and Failure Scenarios

The DPDP service is classed as critical national infrastructure, and therefore the solution, security, physical and deployment architectures have all been designed with that in mind. The following sections highlight a few key considerations that must be borne in mind for the deployment of the DPDP service to production and for appropriate performance and resilience testing.

Non-Functional Requirements

The current set of NFRs is described in [5]. Note: these are still in development and will require further discussion and governance approval. *In particular the overall volumes of transactions in the spreadsheet have been underestimated (as of 15/04/2025 the peak tps figure in [5] is 80 tps, whereas it is likely to be closer to 200 tps).*

Specifically the service must be available on a 24*7 basis and must provide at least 99.99% availability. To facilitate this the service will be deployed across two availability zones in the AWS London region. Furthermore the RPO objective is for the loss of inflight transactions only. Expected transactional volumes currently suggest a possible peak of around 200 tps for sustained peaks during exceptionally busy, seasonal periods, however normal daytime transactional volumes are likely to be an order of magnitude lower. Overnight volumes will be much lower however there is currently no indication of what those will be.

All configuration decisions around the deployment of AWS- and vendor-supplied platforms must take the performance, resilience and volume requirements into consideration.

Criticality and Failure scenarios

Within the enterprise context of DPDP a failure scenario is the loss of some aspect of the overall DPD service, upstream or downstream dependency that has the potential to prevent a patient receiving their medication in a timely, secure and clinically safe manner.

For the components and connections that are within the scope of this deployment architecture the emphasis is on prevention of failure, with the requirement to achieve 99.99% availability and an RPO for the loss of inflight transactions only. **This must be a key factor in all deployment decisions**.

There are several upstream dependencies, primarily the client prescribing and dispensing applications, that are outwith the scope of responsibility of the DPDP programme and NHS Scotland, and are therefore outside the scope of this document.

The failure scenarios are described in more (albeit still draft) details in [12], based on failures of different components within the overall enterprise context. Where a component or connection is outside the scope of the DPDP programme's direct responsibility, such as loss of physical connectivity between a pharmacy location and the public internet, this will be described within the failure scenarios but is not within the scope of this deployment architecture.

Deployment Configuration Considerations for NDP Authentication and MS Entra

The preferred multi-factor authentication platform is the MS Entra Authenticator app. This will need policies in place to ensure that the MFA is triggered based on the roles that are expected to require such authentication. It is essential that MFA must always be active for prescriber and prescriber registrar roles regardless of the origin point for activities involving the signing of prescription items and the creation or modification of entries on the prescriber register. Note: *This is understood to be not in line with current DAS policy whereby some originating points, such as IP addresses indicating origin point is within the SWAN network, do not trigger an MFA challenge*.

Whilst it is currently expected that the MFA challenge will be provided by the Entra Authenticator app, at least one of the enterprise-level suppliers of AES signature services requires that their authenticator app is used instead. If this supplier is chosen to provide the DPDP AES digital signatures then their MFA platform will be used rather than Entra to provide the additional MFA challenge. It is expected that prescriber registrars will still use the Entra app.

Refer to the actors / roles / service permissions matrix for a detailed breakdown of the RBAC roles and permissions assigned to those roles [13] within the context of DPDP.

Appendices

Appendix A –