Document filename:	**Annex A - Citizen Identity (NHS login) Technical Definition**		
Project / Programme	**NHS login Programme**		
Document Reference			
Project Manager	**[REDACTED]**	Status	**Final**
Owner	**[REDACTED]**	Version	**2.0**
Author	**[REDACTED]**	Version issue date	**05/08/2024**

Citizen Identity (NHS login) Technical Definition

Document management

Revision History

Version	Date	Summary of Changes
2.0	16 July 2024	Approved uplifted version.
2.0	5 July 2024	Taken to final and published

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
[REDACTED]	Product and Platforms Lead Technical Architect	16/07/24	2.0
[REDACTED]	NHS login Technical Architect	16/07/24	2.0

Approved by

This document must be approved by the following people:

Name	Title	Date	Version
[REDACTED]	IAO	16/07/24	2.0

Document Control:

The controlled copy of this document is maintained in the NHS England corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

1. Introduction

1.1. Purpose of Document

This document summarises the Architecture for the NHS login (previously known as Citizen Identity) service. NHS login services support the following scenarios:

- Providing access to digital health and social care services which have been commissioned by the NHS in England and have been approved by the PIB;
- Providing access to other digital health and social care services where the services are considered to be in the interests of the health service in England or the recipients or providers of adult social care in England;[1]
- Providing access to digital health and social care services which have been commissioned within Wales and have been approved by the PIB.
- Delivery of an NHS login ID verification and authentication service which can be used as a 'federated' capability to provide access across multiple digital services within England;
- Providing NHS login ID verification and authentication service to digital services which have been approved for use outside of England;
- Providing personal data about NHS login users to health and care professionals for direct care purposes;
- Supporting commissioners and policy teams by providing statistical data to achieve positive health outcomes;
- Providing data about NHS login users to NHS England data and management information services for the purpose of improving user experience, to determine future digital investments and strategy and to support internal and external reporting on the use of NHS England services, such as the NHS website and NHS App;
- Supporting those digital services that are assessed as beneficial to the health services, to social care services and to the recipients of health and adult social care services in England.

This document highlights the key requirements for NHS login, which have been gathered through stakeholder engagement and articulates where these requirements impact the architecture.

This document will be refreshed as the solutions and architecture evolves.

1.2. Audience

The primary audiences for this document are:

- NHS login Programme team
- NHS England
- Health and Social Care organisations

[1] Applications will be considered by the DHSC and NHS England, dependent on the policy area concerned. Such considerations will also take into account any recommendations of the Partner Integration Board.

1.3. Definitions

Where used in this document set, the keywords MUST, SHOULD and MAY are to be interpreted as follows:

- **MUST**: This word, or the terms "**REQUIRED**" or "**SHALL**", means that the definition is an absolute` requirement of the specification.
- **SHOULD**: This word, or the adjective "**RECOMMENDED**", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications **MUST** be understood and carefully weighed before choosing a different course.
- **MAY**: This word, or the adjective “**OPTIONAL**”, means that an item is truly optional. One implementer may choose to include the item because a particular implementation requires it or because the implementer feels that it enhances the implementation while another implementer may omit the same item. An implementation which does not include a particular option **MUST** be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option **MUST** be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

2. Problem Description

The COVID-19 pandemic accelerated a channel shift and an increased appetite to access health and care services digitally. To capitalise on the scale, we now see through NHS login, the need to optimise the experience, expand the offer, and extend our capability in order to ensure continued use and secure access to digital services.

We know that today, the NHS digital offer lags other sectors (for example banking and retail). Digital options are not well understood and are not always considered or able to be the first point of call for people when engaging with the health and care system.

The Department of Health and Social Care and NHS England want to encourage adoption of digital to protect our front-line services by providing users with the best possible experience and making more services available. Enabling digital services for people will improve their engagement with their health, drive greater uptake of self-service and self-care and improve people’s experience of the NHS.

NHS login is pivotal to enabling digital services, building on the existing NHS login platform we will continue to develop and focus on the following:

- Continue to improve the NHS login registration, verification, and authentication journeys to enhance the experience of our users and to maximise the number of users creating and continuing to use NHS login and its connected services.
- Continue to introduce new methods of authentication as they become available to ensure we protect data and enhance the experience of our users.
- Develop new APIs (the Provisioning API) which will enable the direct creation/provisioning of NHS login accounts, where identity verification has been

conducted offline. This will enhance accessibility and inclusion and open the door to fast tracked access to connected services.

- Support the National Proxy Service, by enabling validated proxy relationships to be shared through NHS login and consumed by connected services. This will allow more people to act on behalf of and care for others through digital services,
- Continue to enhance and scale the NHS login platform, to ensure the availability, security, and protection of the service.
- Explore opportunities for enhanced connections to central government identity sources such as HMPO, to enhance and create new journeys for people to verify their identity successfully.

2.1. What we do know?

The NHS login service has been operational since Sep 2018 and has supported the creation of over 40 million NHS login user accounts. The NHS login programme has delivered a service to address the following:

- Improving the process for patients and carers to verify who they are so that they can receive care;
- Reduction in the amount of ‘face to face’ in person ID verifications;
- Providing an ID and verification service which can be accessed from a user’s environment, e.g. home, at a time which is convenient to their schedules and availabilities;
- Providing consistency to the ID verification process, irrespective of the practice the user is registered with or the care setting;
- Re-use of a verified ID for connected services who have onboarded with NHS login.

Key deliveries by the NHS login programme to date include:

- A cloud based (UK hosted) resilient, dynamic, scalable, and secure NHS login platform and infrastructure.
- An industry leading, trusted and first of type way for individuals to prove their identity online and be securely matched to their NHS record.
- Industry standard security and web application firewall controls to prevent cyber-attacks and bad actors.
- A real-time and automated identity verification journey using the best and latest technologies such as facial scan. Automated identity verification enables the NHS login service to dynamically scale.
- Re-use of existing GP Online identity verifications within the NHS to create an NHS login, removing burden from users.
- Identity verification and authentication standards for health and care, supporting identity consistency and interoperability across health and social care.
- A progressive and self-service integration process for the integration of partner services to NHS login, to date there are 85 integrated services.
- Adaptive risk-based authentication based on device and/or passkeys, removing the need for one-time passwords (OTP).

- Multi-tiered identity verification and trust escalation which supports services which require a low/medium level of identity verification and enables users to transition between differing identity assurances.
- Users can manage, maintain, and delete their NHS login via the NHS login account settings.
- Ability for users to update their contact details, where a mismatch is detected between NHS login authenticated and those held by Personal Demographics Service (PDS), to date ~15 million contact details have been updated.
- National scaling of infrastructure and capabilities to support national coverage of integrated services, such as the NHS App.

2.2. Stakeholders and their Concerns

The key stakeholder defined future requirements for the Architecture are outlined below:

Category	Stakeholder Needs Identified
Programme Benefits Realisation	• NHS England – Meet the defined objectives for the programme and drive reusable benefit across Programmes • GPs and practice staff – Reduce burden of managing patients' identities • Citizens/Members of the Public – Access digital services via a convenient, secure, consistent and singular sign-in process • NHS Bodies – Provide access to or commission digital services, enabling the vision of digital first • Third Parties – Provide quickly access to digital services in alignment with *Identity Verification and Authentication Standard for Health and Care*
Reuse (operational)	• Other NHS Organisations – A Platform to support the reuse of Identity Verification • Third-party Suppliers – A Platform of reusable identity capabilities for the purposes of providing authorisation between connected systems
Operational	• NHS England - Minimise the cost and effort in managing the NHS login Platform • NHS England – Extensible, portable and flexible platform to accommodate future change and use across programmes
IG and Security	• NHS England - Secure and consistent Identity Management service for individuals provided in line with GDPR requirements • NHS Bodies (identity providers and authentication hubs) – Assurance of compliance with Identity Verification and Authentication Standard for Health and Care prior to on-boarding to the national service • Third Parties (identity providers and authentication hubs) – Assurance of compliance with *Identity Verification and*

	Authentication Standard for Health and Care prior to on-boarding to the national service
Privacy	• NHS England – Service provisioned in accordance with Legal Directions, Specification and ICO requirements • NHS England - Reduce the data which users must share across bodies. • PCAG – Data collected from citizens is proportionate and managed appropriately

From the Citizen Identity Programme Strategic Outline Case, a useful summary of the needs is set out below:

The NHS login service has addressed the following:

- **Consistency in how patients prove their identity** or how people enable others to act on their behalf when accessing digital services today
- **Improved the process and mechanism for patients** to access services which require ID verification prior to access
- Provided an online mechanism for Identity Verification available to the NHS and approved digital services
- **Reduced the amount of ID verification activities** previously conducted by the NHS front-line staff
- **Provided a common set of authentication credentials** which can be used across digital services who have onboarded to NHS login, ensuring economies of scale from using a one-time verified ID**.**

2.3. List of Scenarios to be Addressed

The key scenarios for the NHS login Platform, which the Architecture must support, are outlined below:

High-Level Scenario	Architecture Implications
User proves who they are, so that they may access a digital health and care service which has been commissioned by the NHS in England and has been approved by the Partner Integration Board (PIB)	Drives many of the functions available within the platform including registration, identity verification and federation with the digital service Data must be stored within the platform, including identifiers, credentials and contact information, but flexible enough to empower the user, via consent, to allow NHS login to share data items with the Digital service they are using.
User manages their account	Further functions within the platform around self-service.
Identity solution changes over time	Flexibility and evolution of the platform itself. Capabilities to draw in new providers of identity functions, including third parties.

User proves who they are, so that they can access a health or care service without a Commissioned body, but meets criteria set out by the Citizen Identity Platform onboarding process	Drives many of the functions available within the platform including registration, identity verification and federation with the digital service Data must be stored within the platform, including identifiers, credentials and contact information, but flexible enough to empower the user, via consent, to allow NHS login to share data items with the Digital service they are using.
Users proves who they are once, and this verification is used to provide a federated authentication and authorisation to other connected digital services via a single sign on method.	Drives many of the functions available within the platform including registration, identity verification and federation with the digital service Data must be stored within the platform, including identifiers, credentials and contact information, but flexible enough to empower the user, via consent, to allow NHS login to share data items with the Digital service they are using.

2.4. Compliance with PCAG Principles

The Privacy and Consumer Advisory Group (PCAG) is an independent forum that advises the government on how to provide trusted and secure means of accessing public services. PCAG has published Identity Assurance Principles to support identity assurance services and to ensure that users have control over access to their identifying information when interacting with Government online services. The focus is on control and consent.

As these principles are published by a nationally recognised body that advises the Government, there is a clear benefit for the NHS login processes to overtly respond to and comply with them. The programme will ensure that these principles are met, through assuring compliance with the *Identity Verification and Authentication Standard for Health and Care.*

Principle	Met/Comments
USER CONTROL "I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them."	Met. Privacy Notice, Terms and Conditions and Cookie Policy provide the controls and limitation around this principle
TRANSPARENCY "Identity assurance can only take place in ways I understand and when I am fully informed."	Met. Privacy Notice, Terms and Conditions and Cookie Policy provide the transparency
MULTIPLICITY "I can use and choose as many different identifiers or identity providers as I want to."	The NHS login service allows the user to verify their identity using multiple journeys (GP/Patient Online credentials, offline, online, automated).

DATA MINIMISATION "My interactions only use the minimum data necessary to meet my needs."	Met. Identity information only held in accordance with retention periods stated in the Privacy notice.
DATA QUALITY "I choose when to update my records."	Met. Within the context of the identity element of the record – rather than the health record itself.
SERVICE USER ACCESS AND PORTABILITY "I have to be provided with copies of all of my data on request; I can move / remove my data whenever I want."	Partially met. Data portability is not supported by the service, data will be removed unless required for legal purposes.
CERTIFICATION "I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements."	Met. Common governance requirements delivered by the Connection Agreements, End User Declaration and SCAL process.
DISPUTE RESOLUTION "If I have a dispute, I can go to an independent Third Party for a resolution."	Met. Existing NHS dispute resolution mechanisms are already in place and will be used.
EXCEPTIONAL CIRCUMSTANCES "Any exception has to be approved by Parliament and is subject to independent scrutiny."	Met. Existing healthcare and data protection laws are deemed sufficient and further parliamentary scrutiny is deemed unnecessary for access to health records.

3. High-Level Objectives

NHS login was created in direct response to the demands and requirements of the NHS eco-system and to support the enablement of digital first, control and self-care for our users of the NHS and Social Care.

The NHS login service directly supports the strategic building blocks of the health and social care digital architecture and leverages the best use of available technology. The NHS login service has six key objectives:

1. **Improve patient uptake and adoption of online health and care services** - by making service adoption for individuals simple by providing a consistent way of accessing multiple digital health and care service, e.g. creating a single account and providing a common log on experience and providing a way of proving who you are online.
2. **Ensure patient information is protected to a consistent level** - through provision of a trusted process and supporting technical services for verifying identity to a consistent level that meets defined standards.
3. **Improve efficiency and reduce costs, and time to market of online health and care services** - by providing an identification/verification service that can be re-used so that service providers do not have to deliver identity services themselves**.**
4. **Reduce burden on health and care front line** - by providing capabilities that enable patients to self-manage their health and access online health and care services without having to present themselves physically at a health service location.

5. **Enable improved decision making, and ability to self-care** – by providing the facility for a patient to enable another individual to access digital services on their behalf, and therefore actively participate in managing their health conditions.
6. **Enable effectiveness and efficiency of future service implementation** - standards and guidance on identity assurance, including technical standards for identity proofing and how health and care service providers delivering digital services to patients and citizens can make use of strategic.

4. Environment and Process Models

4.1. Current Process Description

NHS login provides identity verification and authentication services. In addition to providing a patient with the ability to reuse GP/Patient Online details for verifying their identity, NHS login also provides a standalone Prove Your Identity (PYI) verification service – this is delivered using a blend of automation and manual ID verification processes.

4.2. Future Process Description

There are a number of outline areas where the introduction of NHS login will introduce new processes and business capabilities, as well as impact various existing processes and capabilities.

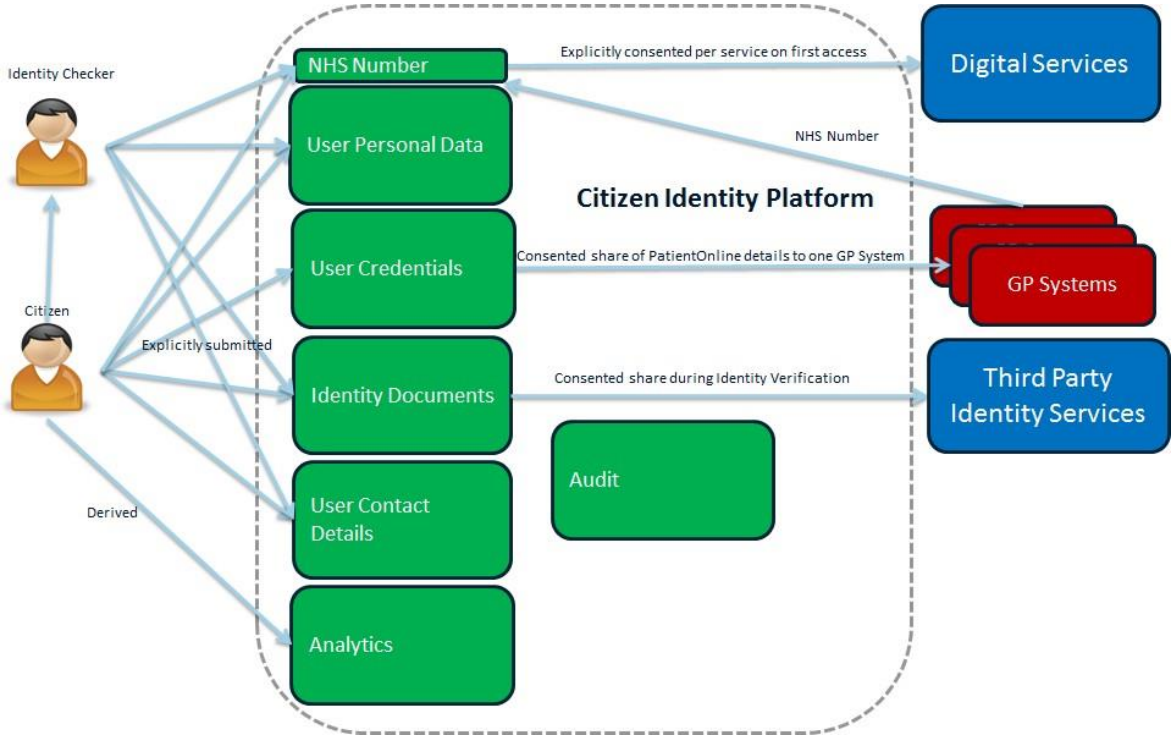
These changes are:

- Increase the roll out of the medium level of ID verification service
- Provide the ability for users to update contact details within PDS with data they have provided to NHS login
- Leverage existing ID verification processes conducted at the GP practices to improve the user journey for the registration of NHS login
- Provide a Single Sign On feature which will federate an identity across different services which use NHS login
- Provide a Provisioning API capability
- Identity verification – offline user journey
- Identity verification – online-to-offline user journey

Development of the NHS login to support these new processes will be undertaken using an Agile methodology and hence is envisaged to occur in phases.

4.3. Information Flow

The diagram below shows the key information flows to be supported by NHS login.



The Platform captures a range of data types:

- NHS Number
- User Personal Data such as:
- First name
- Middle name
- Family name
- Date of Birth
- Biometrics
- User Credentials – password hash, device identifiers
- Identity Documents – as images and/or document identifiers
- User Contact Details – email address, postcode and mobile phone number
- Analytics – which pages within the Identity Platform all users visited and when
- Audit – who made changes to data items, when and under what context

The above shows the main flows, the key points being:

- The above data items are provided by the individual, in the majority of cases.
- In other cases, the data is provided by an authorised user for example a care worker who is able to vouch for the identity of an individual etc.
- Identity Documents and/or identifiers may be cross referenced against external third-parties and other government departments, as part of Identity Proofing and document validation.
- If the user provides their GP System ‘linkage’ and/or other GP System credentials, then these will be sent to the relevant GP System for validation and verification

- The NHS Number and other data items requested by the connected service will be provided to the connected service once the user provides the consent for NHS login to share this with them.

4.4. Participating Organisations

Data items will be processed by NHS login for:

- Individuals applying for their Identity to be verified or authenticated
- Any NHS or non-NHS provider, organisation, company, or authority that provides identity services for individuals accessing online health or Adult social care services

NHS login will use its established partner Onboarding process to evaluate, assess and integrate a supplier's product with NHS login. As part of the Onboarding process, the supplier's product will be presented to the Partner Integration Board (PIB) for approval to proceed – this process is in line with the statement within the NHS login Legal Direction. On completion of the testing, the service will be subject to a release approval process prior to going live.

5. Data to be Collected

The NHS login service has a registered DPIA, IAR0000610. The DPIA has been reviewed as part of the approval by TRG and Platform and Infrastructure Board. The data processed by the NHS login service has been assessed as Class V in accordance with the NHS England data classification process. The NHS login has a registered System Level Security Policy (SLSP) to manage updates to the service architecture, the following data is collected and processed by the Platform:

Data Categories	Yes/No	Explanation
Personal Data		
Name	Yes	First names and surnames will be collected for all users so the user can be accurately matched to their record. This field is one of the 'mandatory fields' on which the Personal Demographic Service (PDS) look up is based in order to find an NHS record for a data subject. The middle name may be processed if it's included within the ID document or provided by the data subject.
Address	Yes	The address is processed during the ID document check if provided within documents such as a UK drivers licence.
Postcode	Yes	The postcode is collected as part of one of the verification journeys available to the data subject. This data set is needed to match

		against the postcode within the data subject's record.
DOB	Yes	DOB will be collected for all users, so the user can be accurately matched to their record.
Age	Yes	This can be derived from the form of evidence provided by the user/delegated individual.
Sex	Yes	This can be derived from the subset of information contained in the passport and when the user submits a photo/video selfie.
Gender	Yes	This can be derived from the subset of information contained in the passport and when the user submits a photo/video selfie.
Email Address	Yes	An email address will be used as a part of the authentication credentials the user has to access the NHS login service.
Physical Description	Yes	This is derived from the video selfie, driving licence and passport photos.
General Identifier e.g. NHS No	Yes	The NHS number will be utilised to match against the PDS data set to authenticate and match the individual to a record. NHS Number may also be sent to Connected Services which the data subject uses once explicit consent has been received from the data subject.
Mobile/Landline Phone Number	Yes	A code could be sent to the individual's mobile and or landline phone number for 2 Factor Authentication, as a security measure for their NHS Account. Where an individual's mobile and/or landline phone number has been authenticated, NHS login may use this phone number, alongside GP Online Credentials, to enable a match of the individual to a record.
Online Identifier e.g. IP Address/Event Logs	Yes	Audit/event logs will be generated and will contain IP addresses. These will be stored within the Platform Protective Monitoring function securely; these logs may be utilised for investigative and legal requests.
Website Cookies	Yes	These will be for non-essential and essential cookies. Data subjects are made aware of the cookies used as this is stated within our Cookie Policy.
Mobile Phone / Landline Phone/ Device No / IMEI No	Yes	This could be derived.

		The IMEI and IMSI numbers will not be directly requested but may be accessible by a determined threat actor who exploits the knowledge of the user's mobile phone number.
GP/Patient Online Credentials	Yes	GP Online Credentials may be utilised to verify and match the data subject to a record. GP Online Credentials may be entered by the data subject or retrieved by the NHS login service.
Authentication	Yes	For the purposes of multi-factor authentication, NHS login will process passwords and receive secure public keys through device based biometric or passkey authentication*. *Biometric and passkey data will not be processed directly by NHS login.
Proxy	Yes	The details of Proxy relationships and corresponding proxy subject details, including NHS Number(s), may be sent to Connected services, once explicit consent has been received from the data subject. Proxy relationships and associated access permissions will be established by the National Proxy Service.
Audit Data	Yes	Audit is essential to record events conducted on the system and service. This supports investigations, accountability, and access control to the NHS login service.
Analytics	Yes	Analytics provides data that can be used to measure the performance and success of the of the service and is used to improve performance and user experience. Cookies used for analytics are non-essential cookies - the data subject can opt out of non-essential cookies. This is made clear in the Cookie Policy.
Special Category Data		
Racial / Ethnic Origin	Yes	This may be derived from personal information provided from the selfie or identity document.
Biometric Data (Fingerprints / Facial Recognition)	Yes	NHS login conduct a Liveness and Likeness check of a data subject in line with the elements of the NHS ID and Verification Standard. This is done via: • a video selfie, with a comparison of the photo(s) within the driving licence and passport;

		• contracted supplier’s facial recognition software to support a solution to support ID verification at scale.

Subsequent phases of delivery will further impact the logical information flow, and potentially the data collected. This document (and DPIA) will be updated accordingly.

6. Actors and their Roles and Responsibilities

6.1. Human Actors and Roles

The existing human roles described in the table below will interact with the NHS login Platform.

Role	Actor
People	Any member of the general public within England (Wales and Isle of Man) who is using a digital service accessed via NHS login.
Identity Checker	A specific individual part of the NHS login identity checking team trained to verify individuals identities.
NHS login operational and platform staff.	NHS England staff operating, developing, supporting and managing the platform

6.1.1. System Actors and Roles

The table below summarises the computer actors and roles.

Role	Role Description	Actor
Connected Services	These are health and/or Adult Social care applications and tools – in this context, they require the individual to sign-in/login	Applications/tools provided by NHS England, other NHS organisations, and suppliers who have been commissioned to deliver a service in accordance with the NHS login Legal Direction and agreed at the PIB.
GP Systems	These are systems procured by GP Practices. They provide current Identity Verification and Management within Primary Care for GP/Patient facing services. The NHS login platform can re-use credentials issued by GP Practices, where identity verification has been conducted offline.	GP Systems provided by GP Systems of Choice framework (GPSoC), and GPITF

Identity Verification Services	These are Identity Services which can provide all, or part-aspects of Identity Verification capabilities	This could include services which have been contracted by NHS login (NHS England) to support NHS login in the delivery of its identity verification and authentication services.

7. Resulting Architecture Model

7.1. Constraints

The following have been identified as constraints on the Architecture Model for the NHS login Solution:

- Technology selection must reflect the operational capabilities of NHS England.
- The NHS login Programme, and to a certain extent, NHS England, has limited control over user uptake and usage of the NHS login Platform. The Architecture Model for the NHS login Platform must therefore be flexible and scalable to deal with rapid fluctuations in service utilisation with no impact to end users.

7.2. Requirements

Requirements captured here are relevant to the component architecture view of the NHS login Platform. Requirements relevant to other architecture views (such as technology architecture) are managed with the NHS login Architecture Repository:

- The architecture must support multiple Digital Services, providing a consistent user and technical interface.
- The architecture must support multiple solutions for Identity Verification as well as a number of Identity Providers for user authentication.
- The architecture should abstract from the Digital Service the detailed mechanism of Identity Verification which the user has been routed through – Information Hiding.
- The architecture must support the changing landscape of Identity types and approaches, such that the service can take advantage of new solutions and technologies.
- The architecture must adhere to existing standards for Identity Federation (sharing Identity within defined rules on trust and interoperability).
- The architecture must be capable of flexing to user and service volumes on a day-to-day basis – Scalability.
- The architecture should support the general move towards ‘thin technologies’ such as microservices and ‘serverless’ operations.

7.3. Design Principles

The key Architecture and Design principles based on experience from previous NHS England programmes are included in the table below:

Priority	Principle	Implications/What this means in the design
1	Design for security	Assurance that the Service and Platform complies with the Identity Verification and Authentication Standard for Health and Care. Assurance that the Service and Platform complies with the ICO recommendation of ‘Data Protection by Design and by Default’. Continued security improvement processes in place and maintained. This is to be supplemented by annual independent technical review of the service. Assurance that parties (for example other Government Departments) submitting verified identities to the service comply with the Identity Verification and Authentication Standard for Health and Care (on-boarding process).
2	Design for operational simplicity and efficiency	Automated testing at unit and acceptance level Automated build. 'Thin' technologies - serverless where possible and containerised if not.
3	Flexible functionality via simple designs and loose-coupling (without extra-engineering)	Interfaces between components should be standards-based wherever possible. Interfaces between components should be simple to implement and extend later. We don't code/implement for future unknowns and "maybe's".
4	Provide interfaces to the 'outside' using open standards	Stay within published standards - extend only where permitted by the standard.
5	Design for Scalability	Use technologies which are simple to scale and manage - serverless, or containerised. Scale horizontally where possible. Allow the underlying platform to manage scale rather than our own additional tooling. State needs to be carefully managed and designed out where possible.

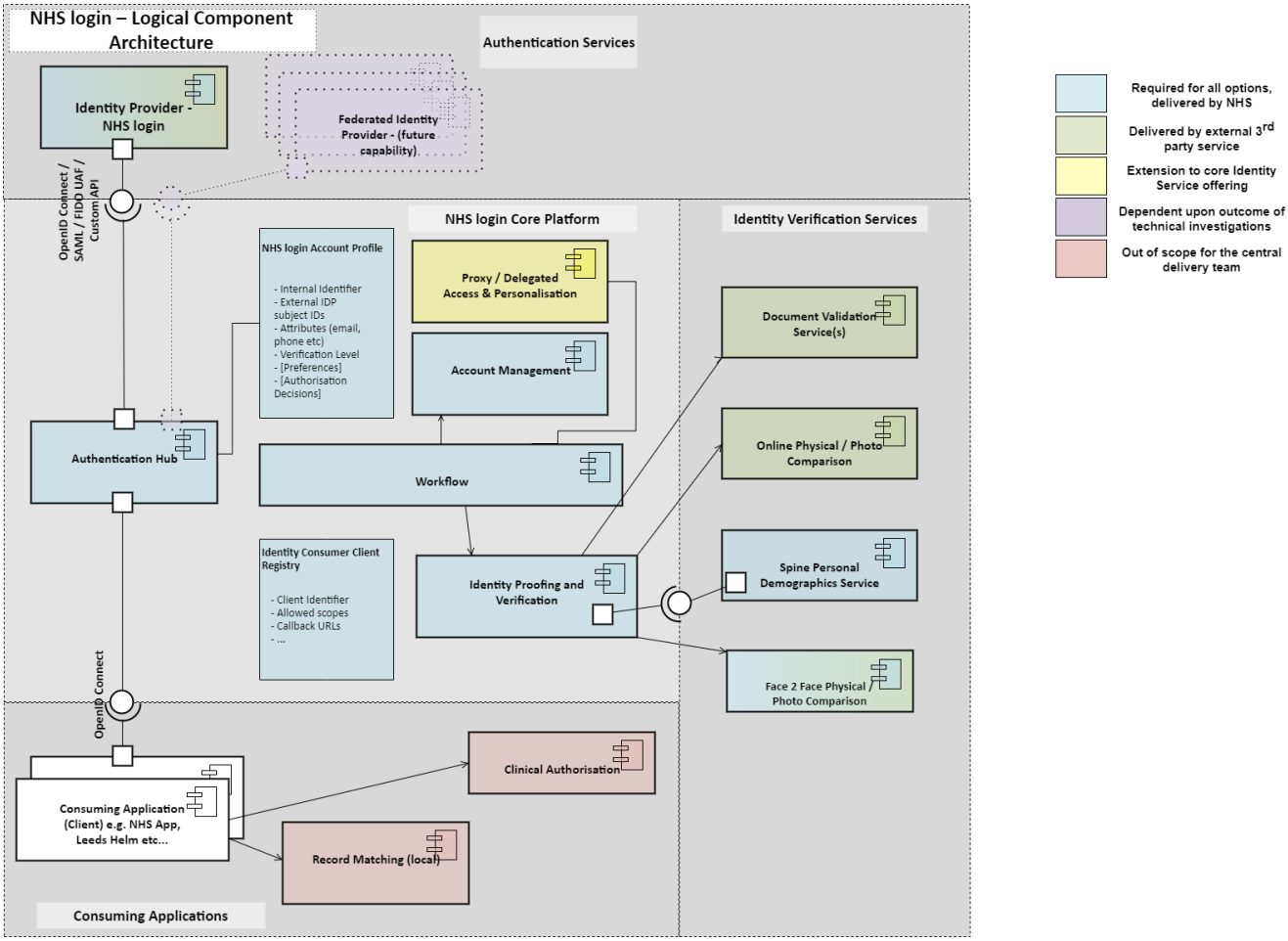
6	Choose technologies to support rapid delivery	Choose products and technologies that support rapid procurement (none if possible). Choose technologies which we have skills to deliver in.
7	Platform Portability	Avoid decisions which unnecessarily lock the architecture into specific platform providers.

Alignment with wider NHS England Principles, Policies and Standards will be ensured through the NHS England governance processes.

In addition, the principles included in the GOV.UK Service Manual and NHS Service Standard will be adopted for the NHS login Platform solution.

8. Component Architecture View

The diagram below shows the component architecture view for the Citizen Identity solution following the first phases of development.



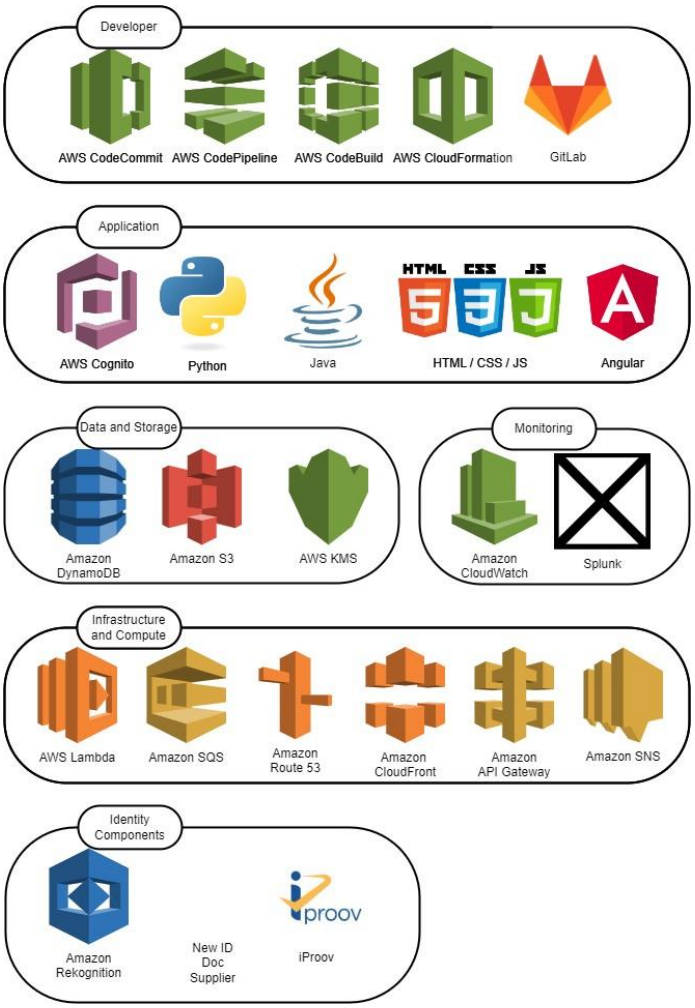
9. Technology Architecture View

The technology architecture view encompasses two main perspectives; the software platform on which the service will be developed and run, and the infrastructure platform on which the service will be delivered.

9.1. Software Architecture

At a high level the software architecture employed to deliver the service will broadly conform to a standard web-based tiered architecture, albeit implemented using serverless cloud computing technologies. This type of architecture layering is well understood and there are many individual software options available which have proven implementations meeting the non-functional performance, availability, and security requirements of the NHS login service.

The key technologies currently implemented within the service are shown below.

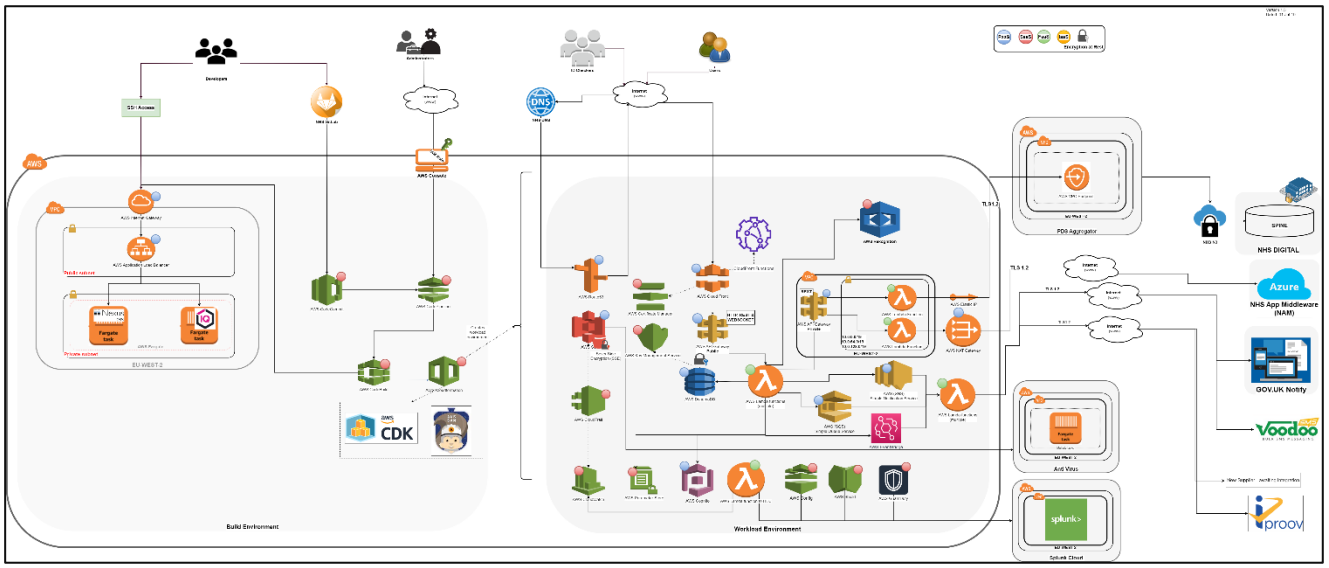


9.2. Infrastructure Architecture

A summary of the infrastructure is shown below – fundamentally, the design makes use of the ‘flat’ nature of the cloud. The NHS login Platform is effectively, given its own virtual network, private from other customers using the same cloud.

Access to the Platform is via the Internet – this aligns with the ‘Internet First’ principle across NHS England services.

Access to HSCN is minimised and used only where necessary for access to Spine Demographics



10. Enterprise Architecture Alignment

10.1. Architecture Governance

Key capabilities of the Architecture and technologies used by the platform are captured within the NHS England Enterprise Architecture Tooling.

NHS login Key Architecture Decisions are reviewed by the NHS England Technical Review and Governance (TRG) group against policies and standards set within the Enterprise Architecture tooling by the relevant Design Authorities. The TRG group can issue approvals, waivers for minor non-conformity or escalate up to Design Authorities for further guidance and discussion.

Further details of the NHS England Architecture Governance Model and Architecture Principles can be found on the NHS England Intranet

10.2. Architecture Re-Use

The NHS England Architecture Principles and NHS England's aim to support national NHS system live services through a common DevOps capability drive the need to ensure a level of consistency between national systems from a component perspective.

Component re-use is evaluated at multiple levels during the lifecycle of programme:

- Through the TRG and Platform Infrastructure Boards– these groups generally consider entire functional component re-use at a sub-system level.
- Through peer-review of design and architecture decisions – this identifies overlaps and consistencies across programmes.
- Through architect review meetings between programme architects – these meetings identify technical products and patterns which can be re-used across programmes. E.g. the pattern of connecting public cloud infrastructure to HSCN.

Within NHS login, a "Key Design Decision" document is produced to describe each key technical decision or product selected. These are captured within the NHS England Confluence. Part of the evaluation required in a Key Design Decision document is an evaluation of the re-use options within NHS England.