



Federated Architecture Blueprint - Part 4 (Components)

DARE UK Delivery Team


Version 2.2 final

November 2024



FOR CONSULTATION & COMMENT

Licence

This work © 2024 by HDR UK and other members of the DARE UK consortium is licensed under CC BY-NC-SA 4.0 The Creative Commons license icons for CC BY-NC-SA 4.0, showing the CC logo, a person icon (BY), a crossed-out dollar sign (NC), and a circular arrow (SA).

FOR CONSULTATION & COMMENT

Document control

Version	Date	Authors/Reviewers	Notes
0.6	22/03/2023	Rob Baxter	First complete draft.
0.7	31/03/2023	Fergus McDonald, Hans-Erik Aronson	DARE UK internal review.
1.0 initial	13/04/2023	Rob Baxter	For publication and public comment.
1.1	03/08/2023	Rob Baxter	Updated. Feedback until end June 2023 incorporated.
1.2	11/08/2023	Rob Baxter	Version for internal review.
1.3	15/08/2023	Fergus McDonald, Emily Jefferson	DARE UK & HDR-UK internal review.
1.4	25/08/2023	Rob Baxter	Updated. Greatly expanded Executive Summary. Version for internal review.
1.5	04/10/2023	Fergus McDonald, Emily Jefferson	DARE UK & HDR-UK internal review.
1.6 interim	18/10/2023	Rob Baxter	For broader circulation and comment.
2.0 draft	11/12/2023	Rob Baxter	Incorporated revisions and lessons learned from Driver Projects and wider engagements.
2.0A draft	12/12/2023	Rob Baxter	Incorporated review feedback from SACRO project PI.
2.0B draft	08/01/2024	Rob Baxter	Incorporated review feedback from TRE-FX project PIs.
2.0C draft	29/02/2024	Fergus McDonald, Emily Jefferson	DARE UK & HDR-UK internal review.
2.0D draft	28/03/2024	Rob Baxter	Final tidy-up, incorporating research use-cases from February 2024 workshop.
2.0E draft	13/06/2024	Fergus McDonald, Emily Jefferson, Caole Goble, Phil Quinlan, Simon Thompson	Partner review.
2.0F draft	05/08/2024	Rob Baxter, Heikki Lehväslaiho	Fixed error in Chapter 8, prototype descriptions.
2.1 draft	30/08/2024	Rob Baxter	Restructuring across Chapters 2-4; realignment and rationalisation of user roles.
2.1 Part 1..5	19/09/2024	Rob Baxter	Separation into multiple parts for release.
2.2	31/10 2024	Emily Jefferson	DARE UK & HDR UK internal review.
2.2 final	11/11 2024	DARE UK	For release.

FOR CONSULTATION & COMMENT

Contents

Document control	3
Contents.....	4
About document versions	7
1. Federated architecture: infrastructure layer	8
1.1. Notation	8
1.1.1. Symbols	8
1.1.2. Colours	8
1.2. Actors and roles	10
1.2.1. Researcher (actor)	10
1.2.2. Information Governance (actor)	10
1.2.3. Data Controller (actor)	11
1.2.4. TRE Operator (actor)	11
1.3. Participants	11
1.3.1. Trusted research environment (TRE)	11
1.3.2. Index Service	15
1.3.3. Discovery Service	15
1.3.4. Job Submission Service	16
1.3.5. Software Service	17
1.4. Interface Types	18
1.4.1. Query (Direct)	18
1.4.2. Query (Indirect)	18
1.4.3. Response	18
1.4.4. Data Ingress and Data Egress	19
1.4.5. Index	19
1.4.6. Software	19
1.4.7. Sync	20
1.5. Structured data objects	20
1.5.1. Data Extract Object	20
1.5.2. Index Object	21
1.5.3. Query Object	21

FOR CONSULTATION & COMMENT

1.5.4.	Job Request Object	22
1.5.5.	Job Payload Artifact	22
1.5.6.	Response Object	23
1.5.7.	Environment Software Artifact	23
1.5.8.	Project Sync Object	23
1.6.	SDRI core services.....	23
1.6.1.	Federation Services	24
1.6.2.	Security Server.....	25
1.7.	Related concepts	25
1.7.1.	Projects.....	25
1.7.2.	Federation identities.....	26
1.7.3.	Authentication and authorisation	26
2.	Federated architecture: data layer	28
2.1.	Classifying sensitive data	28
2.1.1.	A seven-point scale.....	28
2.2.	Federation metadata.....	29
2.2.1.	Infrastructure metadata	30
2.2.2.	Content metadata	31
2.2.3.	Governance metadata	32
2.2.4.	Structured data packaging formats	34
2.2.5.	Other considerations.....	35
2.3.	Data findability.....	35
2.3.1.	Discovery metadata.....	35
2.4.	Data accessibility	37
2.5.	Data interoperability	38
2.5.1.	Syntactic interoperability.....	38
2.5.2.	Terminological interoperability	38
2.5.3.	Semantic interoperability.....	39
2.5.4.	Data linkage.....	39
2.6.	Data reusability.....	39
3.	Federated architecture: organisational layer.....	41

FOR CONSULTATION & COMMENT

3.1. Centralised vs distributed vs decentralised.....	42
4. Summary and further work.....	45
5. References.....	46
A Usage patterns	48
A.1 “Classic” TRE inter-operation.....	48
A.2 Francis Crick Institute federation model	50
A.3 OpenSAFELY	52
A.4 TELEPORT federation with pop-up TREs.....	54
A.5 TRE-FX federation with stand-alone job submission.....	56
A.6 TRE-FX federation with TRE-hosted job submission.....	58

FOR CONSULTATION & COMMENT

About document versions

This document is Part 4 (Components) of the *Federated Architecture Blueprint* for DARE UK. It defines a potential approach for an overall architecture for a network of sensitive data sources and secure analytical services in terms which are broadly—and deliberately—**technology neutral**. Choices of implementation technology are not dealt with here, nor are details of costs, benefits and delivery plan.

This document covers architecture version 2. It refines the model of a federated network infrastructure from the “initial” and “interim” versions, builds further on the “data layer” and most significantly draws in lessons and learnings from the 2023 DARE UK Driver Project programme.

FOR CONSULTATION & COMMENT

1. Federated architecture: infrastructure layer

This blueprint draws on current best practice in secure data exchange environments but also reflects the design principle of “start from where you are”. This architecture proposes the minimum necessary new infrastructure to create the required trustworthy federation while causing the least disruption to TREs and data services already in use. It is also explicitly a “back end” architecture that connects TREs to other TREs. Adherence to the principle that all research with sensitive data take place within a TRE means that Researchers will interact only with TREs and never with the Federation infrastructure directly.

Figure 1 depicts the high-level architecture of the SDRI Federation. It shows a number of Federation Participants—TREs and supporting services—and indicates the principal information flows between them. For illustrative purposes we show two TREs and single versions of other services. In practice there will be more of each. A single set of Federation Services hold a record of all Federation Participants and provide a set of trust services that together create the required trustworthy environment.

1.1. Notation

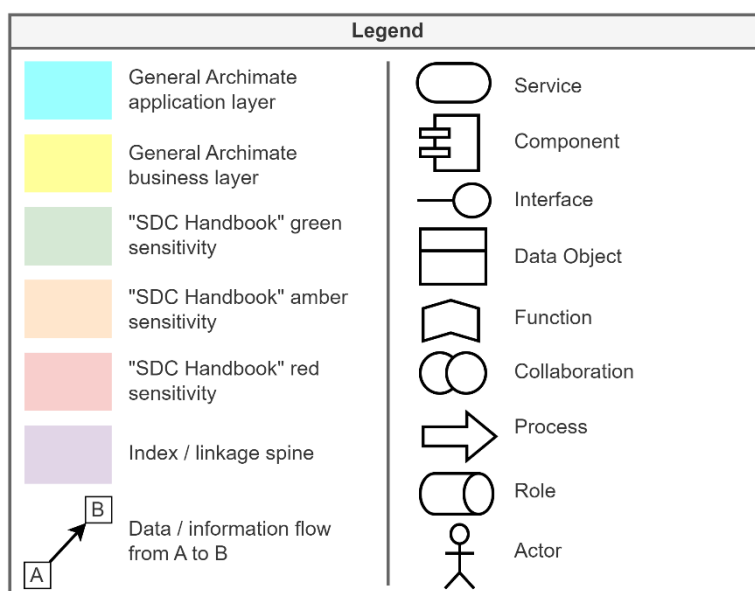
The diagrams follow the ArchiMate standard (version 3.1) [10] according to the following legend.

1.1.1. Symbols

The diagram elements have their usual ArchiMate meanings (right-hand column) with the exception of connecting lines.

Solid connecting lines indicate channels of data or information flow, with arrows indicating direction. Importantly, the absence of an arrow indicates that there is no data flow in that direction.

Dotted lines indicate an (unspecified) relationship between the connected elements.



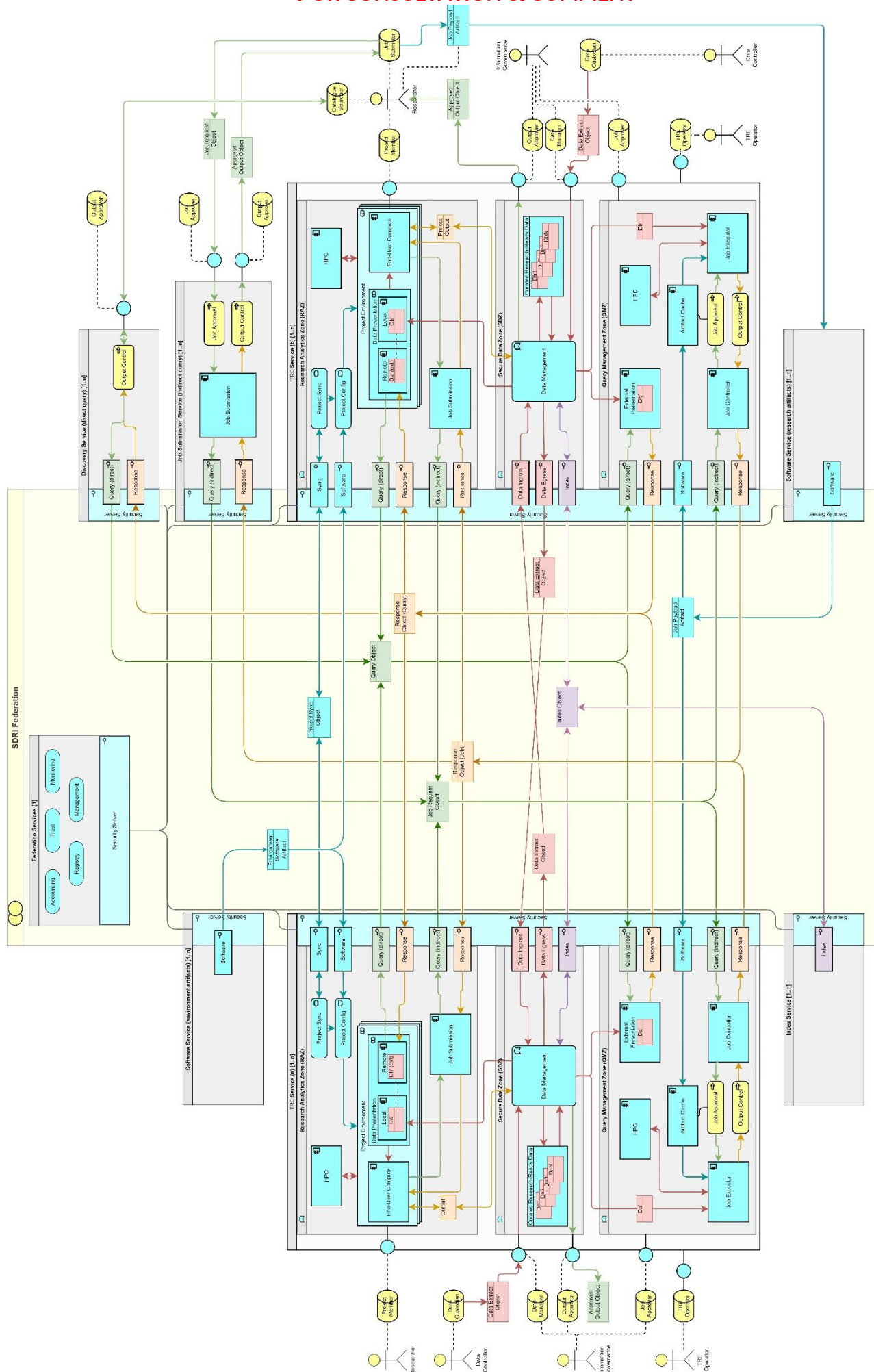
1.1.2. Colours

Yellow and cyan colours indicate elements in default ArchiMate architectural layers – the higher business layer and lower application layer respectively.

We use green, amber and red colours to indicate “data sensitivity” in the sense of potentially disclosive, aligning with the terminology used in the Statistical Disclosure Control Handbook [11].

Purple indicates indexing or linkage spine data, what might be termed “sensitive metadata”.

FOR CONSULTATION & COMMENT



FOR CONSULTATION & COMMENT

Figure 1 (previous page). Architectural diagram of the infrastructure layer of the SDRI Federation network. The notation broadly follows the ArchiMate v3.1 standard [10], although we use colour in a different way (see above). Note that the scope of the core federation is captured in the central “yellow collaboration” element and associated “blue box” security servers. Please refer to the key in Section 1.1 for definitions of the diagram elements.

1.2. Actors and roles

We resolve the federation users identified in Part 3 (Use Cases) into *actors* and *roles* in the infrastructure picture. *Actors* are actual individuals or small teams. *Roles* capture specific activities or responsibilities taken on by actors.

1.2.1. Researcher (actor)

Researchers take on a number of roles within the overall federated system. We use these roles to model their interactions with TREs and other services.

1.2.1.1. Project Member (role)

A Researcher may become an approved and authorised member of one or more Projects (see below), and in that role (and in the context of these Projects) will interact with specially provided project environments within one or more TREs. Access to data within a TRE is granted to a Researcher in their role as a Project Member, on the basis of their individual project authorisations.

1.2.1.2. Job Submitter (role)

(Possibly a sub-role of Project Member.)

In contrast to the direct interaction of a Project Member, the Job Submitter role interacts indirectly with TREs through externally accessible Job Submission and Software services.

1.2.1.3. Catalogue Searcher (role)

The Catalogue Searcher role interacts with externally accessible data discovery and catalogue services. In this role the Researcher need not be a member of an existing project, and thus may not have approvals to access sensitive data of any sort.

1.2.2. Information Governance (actor)

Information Governance is a shorthand for the team of people charged with overseeing a TRE and the research that happens within it. The Information Governance actor takes a number of data-related roles. They may also take the role of TRE Operator, or may delegate it (see below).

1.2.2.1. Data Manager (role)

This role covers a wide range of data management tasks within a TRE, from curating and maintaining long-term copies of research-ready data, to receiving data extracts from other Data Managers in other TREs, linking them and providing them onwards to research Project Members within the TRE. The Data Manager role will typically work closely with the Data Custodian role (see below).

This role could be further broken down into finer-grained sub-roles.

FOR CONSULTATION & COMMENT

1.2.2.2. *Output Approver (role)*

Output Approvers are responsible for checking any and all research outputs to be released from the TRE to the “outside world” (rather than sent to another TRE).

1.2.2.3. *Job Approver (role)*

Job Approvers review computational jobs submitted by Researchers (in their roles as Job Submitters) for their safety and suitability to run inside the Job Approver’s TRE.

1.2.3. Data Controller (actor)

1.2.3.1. *Data Custodian (role)*

In the TRE domain, Data Controllers take the role of Data Custodians, releasing data approved for research to projects via TRE Data Managers.

1.2.4. TRE Operator (actor)

1.2.4.1. *TRE Operator (role)*

The TRE Operator runs the TRE technical service day-to-day. This role may be taken by the Information Governance actor, or it may be delegated by them to a different actor (the TRE Operator actor) under their direction.

1.3. Participants

Participants is the general name for the services connected together to form the SDRI Federation.

In this document we focus on securing the connections **between** Participants within a federated network. We must be aware that **any** Participant judged (by Federation governance processes) “good enough” to join the Federation must have an appropriate level of security around all participating service elements. This may mean that all Federation Participants must demonstrate a certain level of secure hosting and management, not merely deploy a Federation Security Server. This will form one aspect of the governing rules for the Federation.

1.3.1. Trusted research environment (TRE)

TREs are the main vehicles for delivering sensitive data to Researchers in secure, controlled and approved ways.

In developing this architecture we have tried to avoid specifying in too much detail what a TRE “is” and what it “isn’t”. Nevertheless, the linking of TREs into cooperating services capable of supporting federated analytics imposes certain requirements on the internal structures of TREs. We model this using a number of “zones” within a TRE (see Figure 2).

Different TREs can offer different capabilities, and so not every TRE needs to support the functions of every zone. Figure 2 illustrates the *maximal* TRE, which includes every zone.

The zones are illustrated with gaps between them. This is deliberate: the zones require different levels of governance and approval for the roles accessing them, and in particular, movement of data between them

FOR CONSULTATION & COMMENT

should be subject to appropriate controls and potential “air-gapping” to manage the related disclosure risks.

1.3.1.1. Research Analytics Zone (RAZ)

This zone provides the means for a Project Member to gain direct access to the data their project is approved to use, in an environment suitable for the analyses their research requires. This is often realised as a virtual desktop environment, a computational notebook or similar. There is often a strict requirement that project environments be completely isolated from one another.

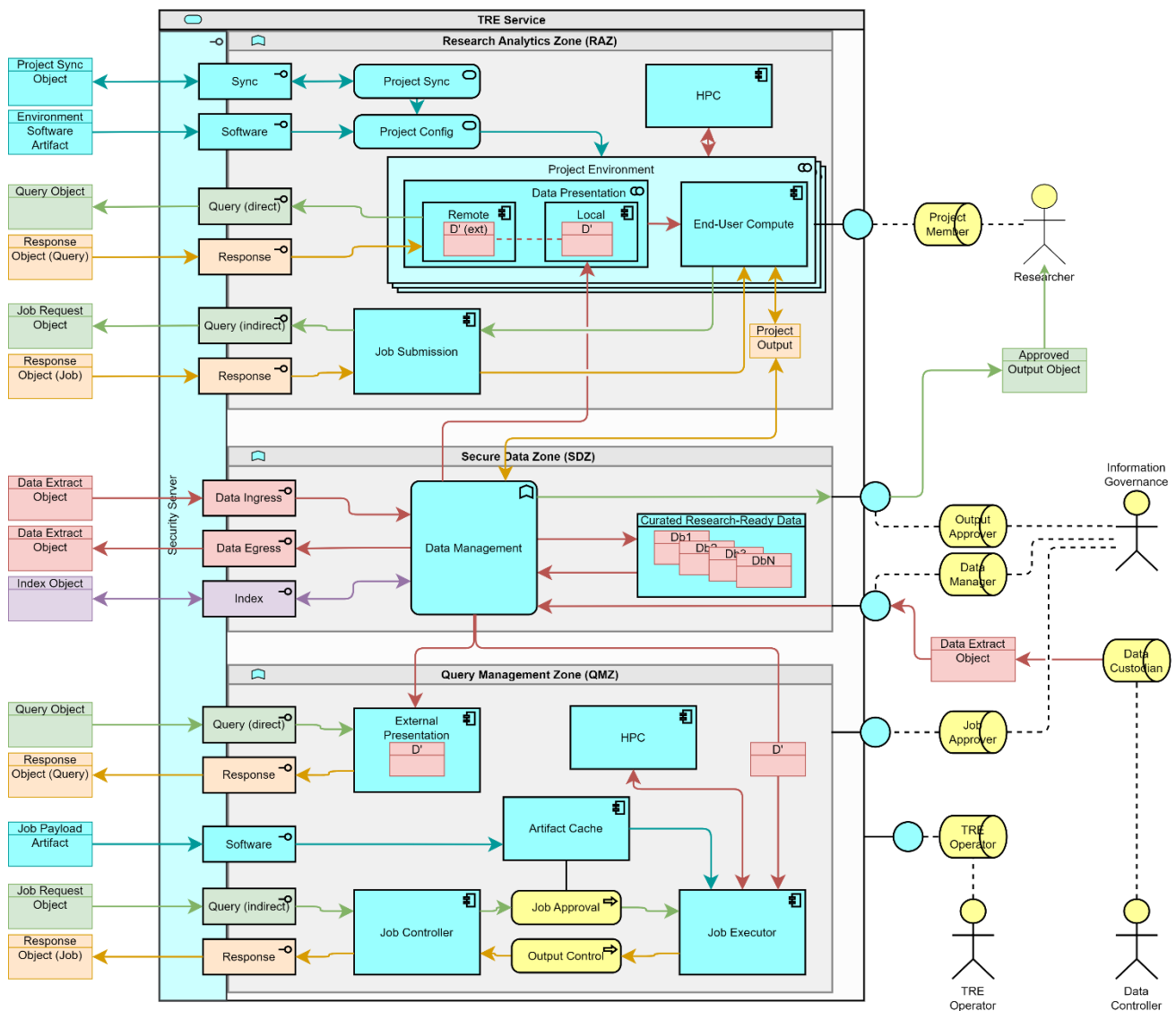


Figure 2. An expanded view of the TRE service from Figure 1.

FOR CONSULTATION & COMMENT

NB: A TRE need not have an RAZ. Instead it may operate as a pure data provider (with just a Secure Data Zone), or as a “headless” TRE able to run queries against data it hosts (with both a Secure Data Zone and a Query Management Zone).

An RAZ has a number of elements, not all of which need be present.

An RAZ **MUST** have one or more **Project Environments**. Project Environments **MUST** be suitable for the kinds of research the TRE supports and **SHOULD** be configured in standard and repeatable ways, modelled here by a relationship with a **Project Config** service. The Project Config service **MAY** connect to approved external software repositories, in which case the RAZ **SHOULD** support the **Software** interface type.

A Project Environment **MAY** be provisioned and managed dynamically and kept in sync with an agreed and approved project state (the “pop-up TRE” model). This project state may be shared between a number of participating TREs (strictly, between the participating TRE Governance actors) and synchronisation may require continually maintained connections between the participating TREs, modelled as a control relationship between a **Project Sync** service and the Project Config service. In this case the RAZ **MUST** also support the **Sync** interface type.

Each Project Environment is a combination (modelled as a collaboration) of an **End-User Compute** component and a **Data Presentation** component. The Data Presentation component **MAY** be composed of a **Local** data view (e.g., a file), **OR** a **Remote** data view (e.g., a representation of a remote resource in a web browser), **OR** a combination of the two (e.g., a polystore representation of two or more databases).

If the RAZ supports Remote data views then it **MUST** support the outgoing **Query (direct)** and incoming **Response** interface types (q.v.).

An RAZ **MAY** support indirect queries against remote TREs by providing a **Job Submission** component accessible directly from Project Environments. In this case the RAZ **MUST** support the outgoing **Query (indirect)** and incoming **Response** interface types (q.v.).

An RAZ **MAY** provide high-performance or other advanced computing capabilities (e.g., GPU clusters), modelled as an **HPC** component. This component **SHOULD** be accessible from the Project Environments and **MAY** be provisioned as a shared service, in which case special care must be taken in maintaining the strict isolation between projects.

The underpinning hardware for this component may overlap with – or indeed be the same as – the HPC component provided within a query management zone (cf. below). Its double inclusion in the diagram reflects the possibility of different modes of user access – interactive access directly from a Project Environment, or batch access via a job queue and potentially an internal Job Submission component.

1.3.1.2. Secure Data Zone (SDZ)

This zone supports the ingress, egress, management, linkage, curation and provision of research-ready sensitive datasets. TRE Governance actors with roles Data Manager and Output Approver **SHALL** be granted access to the SDZ; all other roles **SHALL NOT** be granted access.

FOR CONSULTATION & COMMENT

NB: A TRE need not have an SDZ. Instead it may operate as a pure analytics environment, with an RAZ supporting Project Environments with purely Remote data views, or with access solely to a Job Submission layer.

An SDZ has a number of elements, not all of which need be present.

An SDZ **MUST** have a **Data Management** function. The details of this function are largely out of scope, but its presence defines the core of an SDZ. All movement of data from the SDZ to other parts of the TRE, to other TREs or Index services, or to the outside world via an Output Approver **SHALL** pass through the Data Management function.

An SDZ **MAY** host and curate one or more datasets as **Curated Research-Ready Data**. Via its Data Management function it may provide these to local Project Members within Project Environments, to remote Project Members via external queries managed through the Query Management Zone, or to other Data Managers in remote TREs and Index services.

An SDZ **SHOULD** support the **Data Egress** and **Data Ingress** interface types for sending and receiving Data Extract Objects to and from remote TREs and Index services. (In practice, data ingress and egress may be managed through less formalised interfaces available to TRE Governance Data Managers.)

An SDZ that supports data linkage **SHOULD** support the **Index** interface type.

In this version of the blueprint a TRE with only an SDZ is equivalent to the Data Provider service in versions 1.x.

1.3.1.3. Query Management Zone (QMZ)

This zone handles queries sent to the TRE from other, remote TREs or external Job Submission services. Typically it sits alongside an SDZ and provides different methods of access to approved research-ready datasets stored within the SDZ.

NB: A TRE need not have a QMZ. Instead it may operate as a “classic” TRE, with an RAZ supporting Project Environments and an SDZ supporting data hosting, ingress and linkage, or as a pure analytics environment, with an RAZ supporting Project Environments with purely Remote data views.

A QMZ **MAY** support direct queries, where the received query object contains the actual runnable analytical artifact as a payload (e.g., an SQL query); or it **MAY** support indirect queries, where the received query object contains a reference to a runnable artifact held within an external repository of some kind; or it **MAY** support both.

A QMZ supporting direct queries **MUST** have an **External Presentation** component which can provide the approved dataset for the querying Project Member in a way that matches the query payload (e.g., as a project-specific database view for an SQL query). It **MUST** also support the incoming **Query (direct)** and outgoing **Response** interface types.

A QMZ supporting indirect queries **MUST** have a **Job Controller** component which can receive the incoming Job Request object. The Job Request **MUST** pass through a **Job Approval** process which **SHOULD** import the matching Job Payload Artifact from its remote repository, or take it from an internal **Artifact Cache**.

FOR CONSULTATION & COMMENT

Approved Job Payload Artifacts shall be passed to a **Job Executor** component which is able to execute them against the project dataset approved for access by the querying Project Member. Any results from the job's execution shall be returned to the Job Controller via an **Output Control** process.

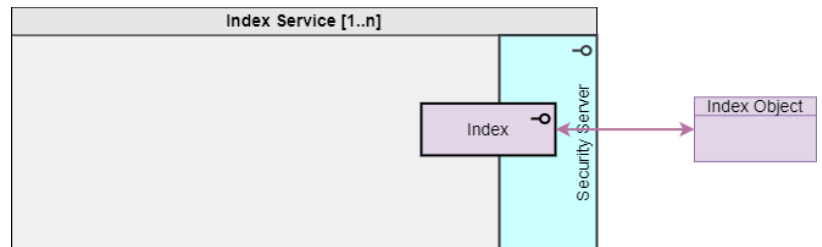
Note that either or both of the Job Approval and Output Control processes may involve manual inspection and assessment by TRE Governance Job Approver or Output Approver roles – hence their modelling as business processes rather than components or services.

A QMZ supporting indirect queries **MUST** also support the incoming **Query (indirect)** and outgoing **Response** interface types.

A QMZ **MAY** provide high-performance or advanced computing capabilities, modelled as an **HPC** component, in particular to support the execution of indirect query jobs. This component **SHOULD** be accessible from the Job Executor component and **MAY** be provisioned as a shared service, in which case special care must be taken in maintaining strict isolation between running jobs.

1.3.2. Index Service

An Index Service creates linkage spines for different Datasets. How a given service does this will depend first and foremost on the principal index key in question. For personal data, for example, the Index service will create depersonalised linkage spines by converting between “bare” personal identifiers and project-specific linkage keys.

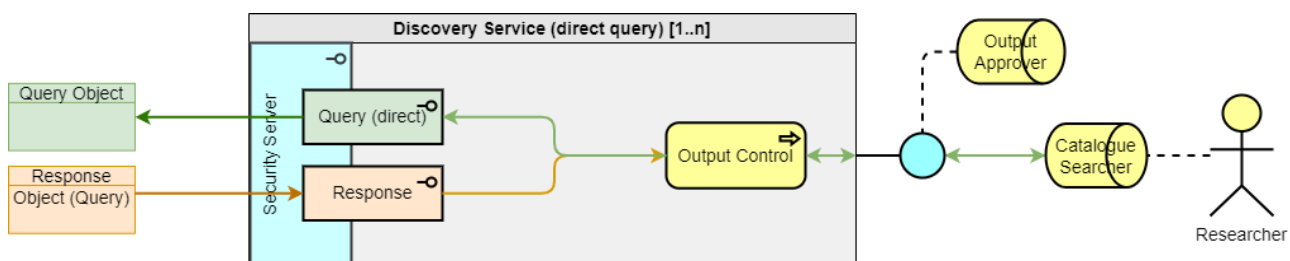


The Federation may include many Indexing Services, each perhaps specialising in a different kind of index.

Index Services **MUST** be trustworthy enough potentially to handle personal identifiers by which vertically partitioned datasets might be linked together. How indexes for such identifiers might be constructed is out of scope for this architecture. For a fuller treatment on how the *exchange* of indexes or linkage spines could be realised within the architecture see Chapter 2 *Federated Architecture: Data Layer*.

Indexing Services **SHALL** interact with other Federation participants solely through Indexing interface service calls.

1.3.3. Discovery Service



A Discovery Service provides information (metadata) about features of the Federation to users outside the Federation. It may achieve this by querying the Registry or other services within the Federation.

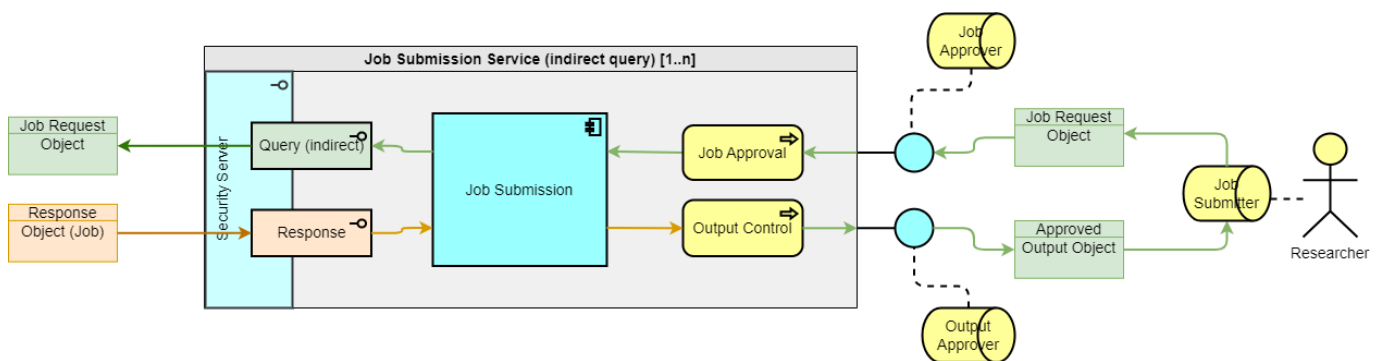
FOR CONSULTATION & COMMENT

The Federation may include many Discovery Services, perhaps specialising in different kinds of data.

A Discovery Service which enables dynamic discovery of metadata by querying other Federation services **MUST** support the outgoing **Query (direct)** and incoming **Response** interface types. Because Query interface services encompass a range of capabilities, Discovery Services are not restricted to static lists of metadata. They can range from simple high-level data or service discoverability to dynamic cohort discovery and “Beacon-like” services [21].

This dual “inward-outward” facing role will need careful security design; any outward-facing catalogue, for instance, **MUST** be air gapped or otherwise isolated from any other zone within the service. We model this with an **Output Control** process on the outward-facing interfaces.

1.3.4. Job Submission Service



A Job Submission Service combines the inward-outward facing nature of a Discovery Service with the indirect query capability of an RAZ. Job Submission Services are Federation Participants in their own rights, independent of any one TRE.

A Job Submission Service receives job requests from Job Submitters. These requests may need to be approved before being executed and so **MUST** pass through a **Job Approval** process overseen by a Job Approver role.

Approved job requests shall be passed to a **Job Submission** component which shall package them into standard Job Request Objects, forward them to the requested TREs and handle the Job Response Objects as they are returned. Handling the responses may involve composing or assembling them into a unified output object (e.g., aggregating the partial results from a federated query).

NB: how the requested TREs are made aware of job requests is undefined at this stage. They might choose to poll Job Submission Services that support a (currently undefined) polling interface, meaning that every TRE in the Federation might need to poll every Job Submission Service regularly. Or they might “listen” on their QMZ’s incoming Query (indirect) interface, requiring this interface to be open to incoming traffic from other Federation services.

Any unified output object **MUST** pass through an **Output Control** process overseen by an Output Approver role before it can be returned to the originating Job Submitter.

A Job Submission Service **MUST** support the outgoing **Query (indirect)** and incoming **Response** interface types.

FOR CONSULTATION & COMMENT

1.3.5. Software Service

A Software Service provides access for Federation participants to sources of software from outside the Federation.

A Software Service may:

- act as a direct network proxy for Internet-based third-party software services (e.g., CRAN¹);
- act as an independently curated, high-assurance mirror service for popular software packages (e.g., Anaconda Python Enterprise²);
- act as a proxy for defined and approved user accounts on a public open-source software repository (e.g., GitHub³);
- act as a proxy for Researcher workflows or analytical scripts stored in external repositories (e.g., WorkflowHub⁴) to be used as payloads for indirect queries;

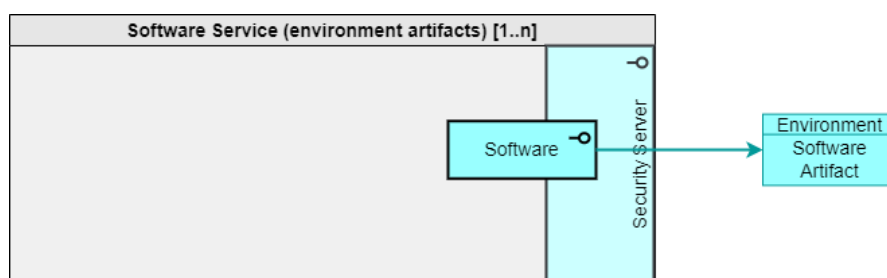
and so on.

Software Services **MUST** support the **Software** interface type.

As suggested, the Federation may have many Software Services, some specialising in particular kinds of software, language packages and so on. Two kinds are described here.

1.3.5.1. Environment Artifacts

To provision and configure Project Environments a Project Config service within a TRE's Research Analytics Zone should connect to a Software Service (environment artifacts). This service shall act as a proxy to approved sources of "environmental software" from which to build Project Environments – a Harbour repository of assured Docker containers; an approved source of Python packages, etc.



A Software Service (environment artifacts) supplies Environment Software Artifacts to requesting TREs.

1.3.5.2. Research Artifacts

Indirect queries sent as Job Request Objects from Job Submission components within TREs or Job Submission Services include "pointers" to external analytics objects held in repositories, rather than actual query payloads. A Software Service (research artifacts) acts as a proxy for such external repositories, handling requests from components within TRE Query Management Zones and returning the requested research artifact (workflow, container or script, as examples) as a Job Payload Artifact.

¹ The Comprehensive R Archive Network. See <https://cran.r-project.org/>

² Anaconda Python Enterprise DS Platform. See <https://www.anaconda.com/products/enterprise>

³ GitHub. See <https://github.com/>

⁴ WorkflowHub. See <https://workflowhub.eu/>

FOR CONSULTATION & COMMENT



1.4. Interface Types

Interface services expose various capabilities for use by other members of the Federation. Note that traffic to and from all interface services route first through the Security Servers of the host Participant (q.v.).

At this level of the architecture we do not specify the details of individual interface calls but instead classify interface services into a small number of types, each of which will have a defined security context. We leave open the definitions of particular interfaces to promote innovation and expansion within the Federation, while providing an overall framework within which services can be placed. For example, an interface service that moves datasets between TREs **MUST NOT** be usable by Researcher system actors.

Note also that we use the terms “incoming” and “outgoing” to mean “incoming *from* another Federation Participant” and “outgoing *to* another Federation Participant”. Interface services do not connect Federation Participants to the wider Internet.

1.4.1. Query (Direct)

The Query (Direct) interface type supports queries between TREs and other Federation services. These interfaces produce and consume Query Objects, where the executable part of the query is fully contained in the object payload.

Query (Direct) interface services **MUST** connect solely to other Query (Direct) interface services.

1.4.2. Query (Indirect)

The Query (Indirect) interface type supports queries between TREs and other Federation services. These interfaces produce and consume Job Request Objects, where the executable part of the query is not contained in the object payload itself but is instead hosted in an external repository and only referred to by the Job Request Object.

Query (Indirect) interface services **MUST** connect solely to other Query (Indirect) interface services.

1.4.3. Response

Responses are data generated by the execution of a query across several Federation services, whether direct or indirect. The model of federated queries assumed in the SDRI is entirely asynchronous and so

FOR CONSULTATION & COMMENT

we make a clear distinction between query and response interface types and do not assume a synchronous interaction between them. In practice, implementations of direct queries are very likely to require tight coupling between query and response interfaces (e.g., the coherent representation of remote datasets in a “single pane of glass” within a TRE Project Environment).

Response interface types produce and consume Response Objects.

The invocation of a Response interface service is triggered indirectly by the prior invocation of a Query service. Our working assumption is that, within the network of trust created by the SDRI Federation, responses can be returned safely to a querying entity without the need for IG intervention.

Response interface services **MUST** connect solely to other Response interface services.

1.4.4. Data Ingress and Data Egress

In contrast to returning query results, Data Ingress and Egress services move complete sensitive Datasets (or large extracts of Datasets) between Federation Participants. This places them in a different security context to query/response interfaces. Data Ingress and Egress services must only be accessible to TRE Governance actors in Data Manager roles.

Data Egress services produce Data Extract Objects, which Data Ingress services can consume.

Data Egress services **MUST** connect solely to Data Ingress services.

Conversely, Data Ingress services **MUST** connect solely to Data Egress services.

System actors with Data Manager roles **SHALL** be able to invoke Data Ingress/Egress services.

System actors without Data Manager roles **SHALL NOT** be able to invoke Data Ingress/Egress services.

1.4.5. Index

Index interface services provide a mechanism for TRE Governance roles and Index Services to exchange lists of personal identifiers, corresponding lists of depersonalised identifiers and master linkage spines for different Datasets. For more information see Section 1.3.2 *Index Service*.

Index interface services **MUST** connect solely to Index interface services.

As with Data Ingress/Egress services, system actors in Data Manager roles **SHALL** be able to invoke Index services.

System actors not in Data Manager roles **SHALL NOT** be able to invoke Index services.

1.4.6. Software

Software interface services provide a mechanism for TRE Operator roles to download and import approved software from a Federation Software Service. As described under Software Service, this may include environment software such as system components, standard analytics runtimes and packages, or research artifacts developed by Researchers and invoked via indirect queries.

Software interfaces produce and consume objects which encapsulate the approved software artifact.

Software interface services **MUST** connect solely to Software interface services.

FOR CONSULTATION & COMMENT

System actors in TRE Operator roles SHALL be able to invoke Software interface services.

System actors not in TRE Operator roles SHALL NOT be able to invoke Software interface services.

1.4.7. Sync

Sync interface services provide a mechanism to maintain synchronisation of configuration state for Project Environments between multiple TREs. Details will be quite implementation specific but it is possible to model some general features.

Sync interfaces produce and consume Project Sync Objects which encapsulate the required configuration state.

Sync interface services MUST connect solely to Sync interface services.

System actors in TRE Operator roles SHALL be able to invoke Sync services.

System actors not in TRE Operator roles SHALL NOT be able to invoke Sync services.

1.5. Structured data objects

Participants in the Federation communicate by exchanging structured data objects over a common data exchange layer. The common data exchange layer provides the required technical security controls for exchange between Participants (see Section 1.6.2 *Security Server*) but additional security controls may be applied to certain types of objects.

Certain object types are closely associated with certain interface service types (see Section 1.4 *Interface Types*) and are produced and consumed by those interface services. Others are associated with Federation security control and are produced and consumed by underpinning security services.

The contents of structured data objects will depend on the particular interface services that produce or consume them.

The Federation requires that all objects to be exchanged between Participants MUST be packaged in a standard way. In this regard, we suggest the use of the “Five Safes” RO-Crate standard as the packaging format for all structured data objects in the Federation (cf. Section 2.2.4 and footnote 9).

1.5.1. Data Extract Object

Data Extract Objects are datasets or subsets of datasets that have been approved by a Data Controller for specific uses within the Federation. Data Extract Objects will typically contain sensitive data, often de-identified but individual-level personal data. Data Extract Objects are exchanged by TREs via Data Egress and Data Ingress interface services. Use of Data Ingress and Egress interface services must be restricted to TRE Governance actors in roles of Data Manager.

Data Extract Objects are designated “SDC Red” in the architecture, meaning that, were they to be offered as candidates for release to the outside world, they would attract the most stringent statistical disclosure checks and would likely fail them. We reiterate, however, that the SDRI Federation is, by design, a closed environment and Data Extract Objects are only ever exchanged between TREs. Nevertheless, exchange of Data Extract Objects will require approvals from Data Controllers (in their roles as Data Custodians) to be in place, and MUST be overseen by TRE Governance Data Managers.

FOR CONSULTATION & COMMENT

1.5.2. Index Object

Index Objects are exchanged by TRE Data Managers and Index Services via Index interface services. Index Objects do not contain sensitive data but could be said to contain “sensitive metadata”. Indexing individuals means that Index Objects will contain lists of personal identifiers and their exchange must be governed accordingly.

Index Objects are needed for certain kinds of data linkage. See Section 2.5.4 *Data Linkage* for a fuller treatment.

1.5.3. Query Object

Query Objects encapsulate direct queries and are produced and consumed by the Query (direct) interface type.

Direct queries can originate from Project Members working in Project Environments within a TRE, or from Discovery Services external to any TRE. In both cases they are targeted at one or more data resources remote from the calling service (i.e., hosted by another TRE).

Where a query originates from a Project Member the Query Object **MUST** contain enough information for the receiving TRE to be able to make the necessary authorisation decisions. This information includes, but is not limited to:

- Project Identity, in a form recognisable by the receiving TRE, indicating the project context this query is in;
- Project Member Identity, in a form recognisable by the receiving TRE, indicating who submitted the query;
- The target Dataset or Data Extract, in a form recognisable by the receiving TRE.

Where a query originates from a Discovery Service without an obvious Project context, how it is handled becomes a governance question to be codified in the Federation rulebook.

Query Objects are exchanged by Query (direct) interface services. Query Objects contain the full executable query for the remote data resource (e.g., as an SQL statement) and are not expected to contain sensitive data. In the architecture they are designated “SDC green”, meaning no form of output control is necessary before they can leave their originating environment.

A significant caveat to this last point arises where Query Objects might encapsulate partially trained deep neural networks in a federated machine learning setting, in which case they would be extremely likely to be sensitive at certain stages.

Again, though, we reiterate that Query Objects are exchanged between Federation Participants and not with the “outside world”. Thus, like all other structured data objects described here, their confidentiality, integrity and traceability are guaranteed by the secure data exchange layer common to all Federation Participants.

Note that we use “query” in a broad sense to encompass both the trivial (a microservice API call) and the complex (an encapsulated SQL script). **In all cases, though, everything the receiving TRE needs to execute the query and create an appropriate response is encapsulated in the Query Object.**

FOR CONSULTATION & COMMENT

1.5.4. Job Request Object

Job Request Objects encapsulate indirect queries and are produced and consumed by the Query (indirect) interface type.

Indirect queries originate from Job Submission components, originated either by Project Members working in Project Environments within a TRE, or from Job Submission Services external to any TRE. In both cases they are targeted at one or more data resources remote from the calling service (i.e., hosted by another TRE).

As with direct queries, where the job request originates from a Project Member the Job Request Object **MUST** contain enough information for the receiving TRE to be able to make the necessary authorisation decisions. This information includes, but is not limited to:

- Project Identity, in a form recognisable by the receiving TRE, indicating the project context this query is in;
- Project Member Identity, in a form recognisable by the receiving TRE, indicating who submitted the query;
- The target Dataset or Data Extract, in a form recognisable by the receiving TRE.

Where a job request originates from a Discovery Service without an obvious Project context, how it is handled becomes a governance question to be codified in the Federation rulebook.

Job Request Objects are exchanged by Query (indirect) interface services. Job Request Objects do not contain executable payloads but instead contain “pointers” to executable artifacts held in external repositories (e.g., the URL of a CWL workflow)⁵.

As with Query Objects, Job Request Objects are not expected to contain sensitive data and are designated “SDC green”, meaning no form of output control is necessary before they can leave their originating environment.

1.5.5. Job Payload Artifact

Job Payload Artifacts encapsulate the executable artifacts referenced in Job Request Objects – the workflows, containerised applications or scripts prepared by Researchers in their role as Job Submitters and deposited in Internet-hosted repositories of some kind.

The artifacts themselves are retrieved from their repositories by Software Services which then package them into Job Payload Artifacts and return them to the requesting TREs via the Software interface.

Job Payload Artifacts **MUST** be subject to a receiving TRE’s Job Approval process and **MUST** encapsulate sufficient information to enable the receiving TRE to assess their safety, in terms of the acceptability of their risk of execution. Because of these requirements it is possible, if not likely, that Job Payload Artifacts will be retrieved by TRE operations ahead of time, subjected to Job Approval and, if approved, cached locally within the TRE’s Artifact Cache in readiness for matching indirect queries. It is thus not

⁵ It is not necessary that the TREs receiving a Job Request Object be able to resolve these payload URLs. Instead, TREs will request the payload artifact from a known, trusted Software Service (research artifacts) (or an internally cached version of same), and will receive in return a Job Payload Artifact object.

FOR CONSULTATION & COMMENT

safe to assume there is a synchronous connection between receipt of a Job Request and retrieval of a Job Payload.

1.5.6. Response Object

Response Objects encapsulate the “answers” to queries submitted to TREs and are produced and consumed by the Response interface type.

Response Objects SHOULD have the same encapsulation structure for direct queries and indirect queries.

Response Objects may well contain data of high sensitivity: a direct query equivalent to “`SELECT * FROM Person_table`” will result in a Response Object equivalent to a Data Extract Object, for instance. In the architecture they are designated “SDC amber” but what level of oversight would be needed before a Response Object can leave its environment will depend on the context in which it was created. There are two scenarios we should consider.

1. Response Objects created in response to queries from an approved Project cannot, by definition, include data not already authorised for use by the Project Members. In this case Response Objects will either be returned to a Project Environment within a TRE, or to a secure Job Submission Service with an Output Control process in place. In neither sub-case is onward dissemination to the “outside world” possible without passing the Project’s approved disclosure control.
2. Response Objects created in response to queries from a Discovery Service do not have an equivalent Project context, and are destined, by construction, to be disseminated to the “outside world” (this is a *Discovery Service*, after all). They must be handled differently, almost certainly handed directly to the Discovery Service’s Output Control process.

1.5.7. Environment Software Artifact

Environment Software Artifacts encapsulate software artifacts used to construct Project Environments and are exchanged by Software interfaces.

In constructing and configuring Project Environments, TREs, rather than “downloading from source”, SHOULD request software artifacts from a Software Service. Not only does this provide an audit trail (the Software Service is a Federation Participant with a Security Server) but it also enables the Software Service to augment the software artifact with additional metadata and encapsulate everything in the Environment Software Artifact object.

1.5.8. Project Sync Object

Project Sync Objects encapsulate information about required Project-Environment configuration state and are produced and consumed by Sync interface types.

1.6. SDRI core services

Core Services are a number of common services that together define the SDRI Federation. They include a set of Federation Services and a number of distributed Security Servers, one per Federation Participant.

All Core Service MUST be connected in a secure network which is independent of the Federation data exchange network.

FOR CONSULTATION & COMMENT

1.6.1. Federation Services

The SDRI's Federation Services provide the coordinating functions and gatekeeping, registration and discovery services which, taken together, define the SDRI Federation. The lowest level of the Federation layer is agnostic towards both the nature of any exchanged objects and the purposes for which they are exchanged (see *Structured Data Objects* above).

There is only one set of Federation Services.

Federation Services **MUST** be highly available.

1.6.1.1. Accounting

Accounting services provide the means to track and record resource use across the Federation. In scenarios where remotely-executed queries may become complex, long-running workflows, a view of what costs are incurred where will become important.

1.6.1.2. Management

Management services provide the necessary tools for the operators of the Federation to maintain and run it to its agreed levels of service.

Management services **MUST** support mechanisms to ensure Security Servers across the Federation are up-to-date and synchronised with the currently agreed and approved global configuration.

1.6.1.3. Monitoring

Monitoring services include infrastructure monitoring for service availability and general system health and operational monitoring of the data exchange layer to ensure the necessary levels of confidentiality, integrity and auditability are being met.

1.6.1.4. Registry

Registry services record information about the different pieces of the Federation. There are a number of key records that **MUST** be recorded in the Registry:

- Federation Participants. Which Participants, defined by their security servers (qv), are part of the Federation. There are five kinds:
 - TREs;
 - Job Submission Services;
 - Software Services;
 - Discovery Services;
 - Index Services.
- Datasets. Datasets are provided by Data Custodians and made available for use in TREs.
 - See Data topics later.
- Projects. In Federation terms Projects provide contexts which encapsulate Researcher users and Datasets into approved pieces of work.
- Users. Each and every user of the federation must be registered.

FOR CONSULTATION & COMMENT

1.6.1.5. Trust

Trust services provide the necessary services for securing the foundational data exchange layer of the Federation. These services support the key security requirements of confidentiality, integrity, non-repudiation and availability. Trust services may include timestamping, encryption key management, security certificate management and so on.

In any implementation, trust services may be provided by trusted third-party suppliers⁶.

1.6.2. Security Server

Security servers act as the gateways of every Federation Participant and are the only components of the Federation that interact directly with each other and with the other Federation Services. The security features required of a Federation Participant are as far as possible abstracted into the Security Server. In particular the Security Servers provide the agency for the secure data exchange layer and hence are the guarantors of the confidentiality, integrity and auditability of inter-Participant exchanges within the Federation.

Every Federation Participant **MUST** run a Security Server.

Security Servers **MUST** operate to an agreed and approved global configuration.

Security Servers **MUST** support a mechanism to synchronise their configuration with the agreed global configuration.

If control-plane connectivity to Federation Management Services is interrupted, Security Servers **MUST** be able to continue operating independently.

1.7. Related concepts

1.7.1. Projects

The Project is a key concept in the use of the SDRI Federation. A Project defines a context for an approved research activity, including the Project Members involved, information about the data they are authorised to use, the TRE that hosts it, its duration and so on. A Project defines an authorisation context which provides a key piece of information for overall SDRI governance (cf. Chapter 3).

All Projects **MUST** be registered with the Federation's Registry services. An example of the kind of metadata required in a Project's Registry entry is offered in Section 2.2.3.1 *Project metadata*.

Simple Projects, typical of most current projects across the UK TRE landscape, will follow the data pooling pattern of access. They involve one TRE with a Research Analytics Zone (the host), a number of TREs acting as data providers and, potentially, a trusted third-party Index Service.

More complex Projects will follow the federated analytics pattern and involve direct and indirect queries across multiple TREs with Query Management Zones capable of processing incoming query objects. For

⁶ For a good discussion of trust services in the context of the UK eIDAS regulation, see the relevant pages at the UK Information Commissioner's Office, <https://ico.org.uk/for-organisations/guide-to-eidas/>.

FOR CONSULTATION & COMMENT

the purposes of governance and authorisation context, one TRE MUST be designated as the “host” or “instigator” of the Project.

The most complex Projects will potentially require a mix of data pooling—perhaps in an initial exploratory or development phase—and federated analytics—a “full production run” across remote data. For such Projects, one TRE should be designated as the host for the data pooling phases and, by construction, the “host” for the Project overall. This complex pattern anticipates large-scale federated machine learning across complex datasets (such as medical image stores).

1.7.2. Federation identities

Many elements of the SDRI Federation will have an *identity* and a number of *attributes* that can be used by system components and other system actors to reason about them. For example, a research user could have an identity and an associated list of active projects of which they were a member. Taken together, this information could be used by a remote data provider to decide whether or not to allow a query from that user to run in a particular project context.

These “Federation identities” must be unique within the Federation but do not necessarily need to have meaning outside the Federation. For the user example, the user’s Federation identity could be implemented as an SSO Token, for instance. This is further discussed in Section 1.7.3 below.

Implementation details are not dealt with here, but the table illustrates some of the required identities and some possible attributes for them. Attributes like this should be captured and recorded in metadata (cf. Section 2.2).

Identity type	Example attributes
Participant	Name; List of interfaces supported; List of capabilities accessible to the Federation; etc.
Researcher / Project Member	Name; Home institution (organisation vouching for their bona fides); Home TRE (TRE vouching for their access to the Federation); List of projects they are currently associated with (“currently” requires each membership be time-bound); etc.
Project	Name; List of current members (using their Federation identities; again, “current” requires these be time-bound); List of datasets associated with the project; Agreed disclosure control strategy; etc.
Dataset	Name; Data controller; Home service (Federation identity of the service regarded as the canonical source for this dataset); etc.
Data Extract	Name; Data controller; creation criteria (e.g., cohort definition); etc.
Linkage Spine	Identity of associated project; List of identities of associated datasets; etc.

1.7.3. Authentication and authorisation

The authentication of Researchers’ identities and their subsequent authorisation to access Projects, Datasets and other Federation resources are split into two stages. This two-tier approach is not uncommon in large-scale federated environments (cf., for example, Appendix III of the *Architecture Vision*

FOR CONSULTATION & COMMENT

of the proposed EU Smart Middleware Platform [2]). To support a rich ecosystem of participants deploying different technology stacks, it is also necessary.

The sequence of events runs like this.

1. Two TREs establish a trust relationship, brokered by the Federation Services and using the Federation's foundational trust services. This "server to server" trust relationship is a standard approach to securing services across the Internet and is typically implemented using X.509 certificates and a public key encryption infrastructure. (We do not cover the details here.) At a foundational level, this is what joining the Federation as a Participant means.
2. A Researcher then authenticates themselves to "their" TRE using the TRE's locally preferred authentication mechanism. This may be Microsoft Active Directory, Linux LDAP/X509, OpenID Connect or a number of other technologies. The TRE may support more than one authentication mechanism for different kinds of user identity (federated identity management).
3. The authenticated Researcher's local identity is mapped onto an internal Federation identity using a common format which all participants in the Federation agree to support. Attributes associated with this identity can then be used by other Federation participants to reason about the Researcher, to make, for instance, authorisation decisions about granting the Researcher access to Projects, Datasets or other resources (single sign-on).

This division also helps enforce the principle of "no TRE, no data": Researchers access Datasets only through TREs, never directly. It also follows from "start from where we are" and "a standards-based ecosystem", allowing TREs to continue to serve their user communities in the best way while providing common back-office connections to federated resources.

FOR CONSULTATION & COMMENT

2. Federated architecture: data layer

In this chapter we discuss the data layer of the Federation from the angles of metadata and the FAIR principles of findability, accessibility, interoperability and reusability.

2.1. Classifying sensitive data

There is no generally agreed definition of “sensitive data”. Most working classifications are built around three considerations: the subject of a given dataset; the organisation responsible for custody of a given dataset; and the potential harm, to either subject or custodian organisation (or both), from unauthorised disclosure of the dataset.

The nature of a dataset’s subject often requires a particular legal or regulatory approach to classification. In the UK, for example, data about living natural persons is covered extensively in the UK GDPR [6]. A firm’s intellectual property may fall under the Copyright Designs and Patents Act [12]. Where the data subject is an endangered species, its treatment may be covered by international treaty such as CITES [13]. Still other subjects may require certain approaches because of cultural sensitivity⁷.

Organisations responsible for collecting or holding potentially sensitive data typically apply their own classification criteria. As responsible custodians, the impact of unauthorised disclosure will likely fall on them, making good data classification part of good corporate risk management practice.

In the interests of manageability, organisational risk management approaches tend to aim for a handful of sensitive data classes only. UK Government (and the US Government) apply three [14] (OFFICIAL, SECRET and TOP SECRET), or four if the UK’s OFFICIAL-SENSITIVE is counted separately. The International Information System Security Certification Consortium (ISC)² defines five in its standard commercial scale [15]. Work at the Alan Turing Institute has developed a five-tier classification model [16]. The NHS in England has an extensive example-driven list of over a dozen but these map onto just two on the UK Government scale [17].

The principal reason for an organisation to classify sensitive data is to help it decide how to manage them. This makes it possible to divorce the “why” from the “how”: why a particular dataset has been classified as “sensitive” doesn’t matter when it comes to storing and protecting it as a sensitive dataset. This is the approach taken in the Harvard Datatags system [18].

2.1.1. A seven-point scale

DARE UK aims to facilitate the combination and linkage of datasets from any and all possible sources. Linked data typically carry higher disclosure risk than their individual constituents, so some comparative scale will be useful. We recommend that datasets used within the SDRI Federation be recorded with two key pieces of information and a number from 1-6 on a “scale of harm”.

In assessing risk of harm, we assume that any unauthorised disclosure of data brings the chance of the data falling into the hands of someone in a position to cause harm to either the data subject or data

⁷ For example certain world cultures have, over the years, expanded traditional taboos on naming the recently deceased in speech to include electronic recordings, including digital photographs. See https://en.wikipedia.org/wiki/Taboo_on_the_dead and references within.

FOR CONSULTATION & COMMENT

custodian. Thus, we do not distinguish between data release to a small group and data release to everyone.

Datasets should be classified by:

- Data subject (what it's about): individuals; firms; locations; intellectual property; ...
- Data custodian (who's responsible for sharing it);
- "Harm", which can mean physical, mental, emotional, economic or reputational, depending on the context.

Category	Harm	UK Gov	GDPR	(ISC) ²	Turing
	None	Public	Public	Public	Tier 0
1	Inconvenience	-	-	Proprietary	Tier 1
2	Distress, embarrassment, some reputational damage	OFFICIAL	Personal	Private	Tier 2
3	Actual harm	OFFICIAL-SENSITIVE	Personal	Confidential	-
4	Serious harm	OFFICIAL-SENSITIVE	Special Category	Sensitive	Tier 3
5	Loss of life	SECRET	-	-	Tier 4
6	Widespread loss of life	TOP SECRET	-	-	-

NB: It must be emphasised that data classification in this manner is not a simple badge-it-and-forget affair. The sensitivity of a given dataset (whether Dataset or Data Extract) can and will change depending on the context it is in. The classifications themselves are also something of a blunt instrument: "John has asthma" and "John has HIV" are both personal health data (GDPR Special Category), but one could cause far more harm than the other if disclosed. It is far better to use this kind of classification only as a starting point and always consider the use of sensitive data within a "Five Safes" context, managing risk holistically across a number of dimensions.

2.2. Federation metadata

Our concept of Federation metadata covers high-level descriptions of all the elements of the SDRI Federation, from the services that comprise its infrastructure to the data, users and projects that make it useful. It is descriptive of the Federation and its activities, and provides a very high-level view of data assets within the Federation, but does not include rich, detailed descriptions of these data assets. How best the technical infrastructure could support rich discovery and exploration of datasets from many different disciplines is a challenging question; we offer some thoughts in Sections 2.3, 2.4 and 2.5 below.

For now, we divide Federation metadata into three groups: metadata that capture information about the Federation itself (infrastructure metadata); metadata that capture information about the datasets accessible within the Federation (content metadata); and metadata that capture information about what purposes the Federation is being used for (we can call this governance metadata). By construction, these map to the three layers of the SDRI Federation.

FOR CONSULTATION & COMMENT

In general, the visibility of metadata—private to a Participant, private to the Federation as a whole, or public—should be determined and agreed by Federation governance rules, perhaps following a “need to know” approach. Some examples:

- Public: names of Participants in the Federation; names of Datasets available within the Federation; counts and names of active Projects; counts of active Researchers; ...
- Federation-private: Federation identities of Participants and other entities and artifacts; service capabilities; Project risk-management information; ...
- Participant-private: Researchers’ and other users’ contact details; ...

2.2.1. Infrastructure metadata

Our definition of infrastructure metadata is best captured by the answer to the question: if the Federation had no users at all, what metadata would we still need to describe it? We divide this further into static descriptive metadata that describe the Federation “at rest” and dynamic operational metadata that describe it “in motion”.

2.2.1.1. Descriptive metadata (Federation at rest)

The Participants – the services described in Chapter 1 – require machine-readable descriptions which shall be recorded in the Registry Services, and which provide enough information to be reasoned about (e.g., for the purposes of automation).

Examples of descriptive metadata are:

- Basic metadata: name, Federation identity, ...
- Capabilities: available computation; available software; ...
- Datasets hosted (persistently available not project-specific): count; list of Federation identities; ...
- Indexes hosted (types of linkage available): list of Federation identities; ...

Most descriptive metadata should be visible within the Federation.

Some may be visible publicly (meaning able to be published rather than exposed directly from within the Federation to the public Internet!).

2.2.1.2. Operational metadata (Federation in motion)

Operational metadata are metadata captured and recorded through the operation of the Federation and its Participants. Operational metadata notably include information on data exchange logged by the Participant Security Servers and by the Federation Services.

Clear governance rules must be established around the use of operational metadata. It must be clear, for instance, which metadata logged within a Participant’s Security Server are private to the Participant, which may be shared with Federation Services, and which might be visible to other Federation Participants.

No operational metadata should ever be visible to the public.

FOR CONSULTATION & COMMENT

2.2.2. Content metadata

Content metadata describe, at a high level, the Datasets the Federation supports. When structuring metadata to describe such concepts steps should be taken to eliminate or reduce any duplication of information that would risk drift, divergence or fragmentation.

2.2.2.1. Dataset metadata

Datasets, while treated as dynamic, are potentially persistent and long-lived. Dataset metadata should record information about the data themselves, including the Data Controllers accountable for their use, but not things like where they can be accessed. The latter information should be left to the hosting Participant to advertise, and to the Federation Registry and Discovery Services to collate for search and discovery purposes. For example:

- Dataset record:
 - Name: Covid-19 self-reported symptoms in London, 2020
 - Federation identity: ee6574ac-8ad7-440c-8200-ca86dd556bbf
 - Data controller: ...
- TRE record:
 - Name: SAIL Databank
 - Federation identity: 5756f2c9-c6f3-4fcf-8d81-c4647e2a12bb
 - Datasets hosted: {ee6574ac-8ad7-440c-8200-ca86dd556bbf; ...}
 - ...

The dynamic nature of datasets arises not from their ephemerality or their movement around the Federation but from their changeability. Datasets are updated (new entries made, old entries pruned) and their schemas or formats change (more slowly). How different versions of a dataset should be managed and recorded is out of scope, but we would recommend that its Federation identity remain unchanged, just as its name would.

Summary metadata for a Dataset will be public, perhaps conforming to a common high-level catalogue schema. As a current starting point for defining the required fields in these high-level metadata records we would recommend Appendix A of the UK Statistics Authority DEA Data Capability Guidance [19]. We use this to derive the example metadata records below, our goal being to design defensively and align Federation metadata as closely as possible with anticipated governance or accreditation requirements⁸. Particular data domains may, of course, introduce their own standards, and commonality will need to be distilled and agreed accordingly. (In the health domain, for example, the HDR Alliance have defined a useful standard for data use registers [20].)

Some detailed Dataset metadata will be Federation-private.

⁸ The UK Statistics Authority Digital Economy Act scheme for UK-based processors of statistical data is a rigorous approach to accreditation but does not cover health-related data. However it has been announced (June 2023; see <https://transform.england.nhs.uk/key-tools-and-info/data-saves-lives/data-saves-lives-implementation-update/>) that the UK NHS and Statistics Authority will work together to co-design an updated version of the DEA scheme suitable for both statistical and health data.

FOR CONSULTATION & COMMENT

Example metadata record: Dataset	
Id	A unique Federation identity number for the Dataset.
Data name	A unique name provided to identify the Dataset.
Data description	A short description.
Data classification	The type of data (perhaps using a controlled terminology such as Dublin Core, eg, household survey data, administrative data, open data).
Data keywords	A set of related keywords.
Data supplier	The owner or supplier of the data. For personal data this should be the data controller.
Time coverage – start	The first point in time the data covers.
Time coverage – end	The latest point in time the data covers.
Data frequency	Where the data have a temporal frequency.
Update frequency	Where data are updated in their hosting provider environment.
Geography	The levels of geography included in the data.

2.2.3. Governance metadata

What we term governance metadata covers the users of the Federation and the activities they carry out. Central to this idea is the concept of the Project: any and all research activities across the Federation are conducted within the contexts of Projects.

Governance metadata should be viewed as a machine-readable form of the record-keeping required of TREs, data providers and researchers under research approval and accreditation regimes. As with Dataset metadata above, we recommend making use of prevailing information governance requirements to drive the metadata standards within the Federation. Where multiple accreditation regimes exist a degree of harmonisation or duplication will be required in metadata records (cf. footnote 8 on previous page). As before, we use the current DEA standard to derive the example metadata records below.

2.2.3.1. Project metadata

As discussed in Chapter 1 the Project is a strong concept within the Federation. Projects are conceived outside the Federation and, once approvals are in place, are instantiated in a hosting TRE. At the point of Project instantiation, the hosting TRE should register the Project's existence with the Federation Registry Service.

A Project's metadata should encapsulate its scope including its hosting TRE, the Datasets or Data Extracts it has permissions to work with, the Researchers permitted to work on it, its start and end dates and so on. It should be detailed enough that authorisation or disclosure decisions can be taken by Federation Participants, for example upon receipt of a remote query.

Most metadata for a Project will be public.

Some detailed Project metadata may be Federation-private, and some may be Participant-private (e.g., held by the instantiating TRE).

FOR CONSULTATION & COMMENT

Example metadata record: Project	
Id	A unique Federation identity number for the Project.
Project title	The official Project title as approved .
Project abstract	A short paragraph summarising the purpose of the Project.
Expected public benefits	A short paragraph summarising the expected public benefits.
Project keywords	A set of keywords describing the Project.
Project start date	The date this Project started in the hosting TRE. A Project is considered to start in a TRE when Researchers have access to the TRE and all data as approved in the Project application.
Project end date	The expected end date of the Project.
Host research environment	The name of the hosting TRE where research will take place. In the case of a Project involving federated analytics this should be the TRE which instantiates the Project.
Research environments	A list of any and all other TREs involved in the research—for instance in the case of a Project involving federated analytics.
Research sponsor	The name(s) of the organisations sponsoring this research.
Project approval on	The date this Project was approved by its governing authority.
Ethical approval on	The date ethical consideration/approval was given to this Project.
Ethical approval by	Who provided ethical approval for the Project.
Ethical restrictions	Any restrictions identified as part of the ethical approval.
Research Lead	The Federation identity for the lead Researcher (often termed "principal investigator" in academic projects).
Researchers	A list of Federation identities for all other Researchers on the Project.
People restrictions	Any restrictions on the people involved in this project identified as part of the Project accreditation.
Data used	A list of Federation identities for all Data Extracts used in this Project.
Data restrictions	Any restrictions on the data available to the project identified as part of the Project accreditation.
Dissemination restrictions	Any restrictions on the dissemination of research outputs identified as part of the Project accreditation.

2.2.3.2. User metadata

Researchers within the Federation may be, and indeed should be able to be, involved in multiple Projects concurrently. Not all of these Projects need be hosted by the same participating TRE; thus Researchers will need a registered Federation identity which is common across all Participants. This echoes current best practice in DEA-accredited TREs where a researcher's "identity number" is provided centrally by the UK Statistics Authority (the accreditation authority for DEA standards).

The primary reason we classify metadata for Researchers (and other users such as TRE Operators or Data Service Operators) under "governance" is that best practice captured in the Five Safes phrase "Safe People" requires all users or handlers of sensitive data to be trained or accredited to an acceptable level.

FOR CONSULTATION & COMMENT

“Acceptable” here typically means acceptable to the governance authority concerned with the data in question. The DEA record required for a researcher places a strong emphasis on this aspect, suggesting the example metadata record below.

Example metadata record: Researcher	
Id	A unique Federation identity number for the Researcher.
Full name	This should include any middle names as recorded in official documents.
Research affiliation(s)	Where the Researcher has affiliation to an organisation or organisations all these affiliations should be recorded.
Type of accreditation	Provisional/Full accreditation.
Training course	The name of the training course attended as part of the accreditation.
Course provider	The organisation responsible for delivering this course.
Trained on	The date the researcher attended the training course.
Assessed on	The date the researcher completed the assessment.
Accredited on	The date the researcher was accredited.

2.2.3.3. Data Extract metadata

We define Data Extracts as snapshots created from Datasets according to some query—a cohort definition, for instance.

Data Extracts are one kind of structured data exchanged between Participants.

Metadata for Data Extracts will be logged by the secure data exchange layer and so must prove useful in that context (e.g., for audit purposes). Attributes could include: Data Controller; “parent” Dataset; version or timestamp of parent Dataset at extract creation; etc.

2.2.4. Structured data packaging formats

While the contents of metadata records will be driven by governance requirements, the format into which they are packaged for exchange between TREs or other services is an entirely technical decision.

The 2023 DARE UK Driver Projects pioneered the development and use of a “Five Safes” profile of the international RO-Crate standard for structured data packaging⁹. RO-Crate (“Research Objects + DataCrates”) extends the BagIt file packaging format¹⁰ to include standard representation for machine-actionable metadata. The “Five Safes” RO-Crate profile adds additional metadata structure useful in the TRE context.

The “Five Safes” RO-Crate profile has been demonstrated as fit for purpose in prototype implementations of this architectural blueprint and so we suggest that “Five Safes” RO-Crate be adopted as the packaging format for all structured data objects in the Federation.

⁹ See <https://trefx.uk/5s-crate/0.4/> and <https://www.researchobject.org/ro-crate/1.2-DRAFT/>

¹⁰ See <https://datatracker.ietf.org/doc/html/rfc8493>

FOR CONSULTATION & COMMENT

2.2.5. Other considerations

Many exchanges of structured data within the Federation will occur in a Project context: an initial Data Extract sent at Project instantiation (see above); a Linkage Spine created to connect extracts to create a Project's working dataset; a query, sent from a TRE to one or more remote data providers.

We RECOMMEND that all such exchanges of structured data objects be tagged with a metadata record indicating this Project context.

2.3. Data findability

The Federation "content metadata" records introduced in the previous section are examples of the types of information that need to be captured and recorded in the Registry services of the Federation, but are largely useless in helping researchers find what data might actually be available to support their research within the Federation. As described in *Rachel's Journey* in Part 3 (Use Cases) this data discovery needs to happen outside the Federation, before a researcher has even defined the project they might ultimately propose.

A consequence of this is that data findability, or discovery, is not a core use-case for the SDRI Federation. The Federation does, however, have a role to play in supporting data discovery where it can—maintaining a record of what datasets from which providers are available in which TRE with what linkages available—and ensuring that such information can be accessed usefully in standard ways from outside the Federation without compromising its secure perimeter.

The Federation architecture as proposed does permit the exposure, via query interfaces, of metadata from the Federation to the public Internet. By this statement we mean there is nothing proposed in the architecture that renders this impossible. Whether and in what form it might be realised is currently left as a question of governance and of implementation. Possible approaches to exposing public metadata from controlled environments can be found in the GA4GH Beacon work [21] and in the HDR-UK CO-CONNECT work [22].

2.3.1. Discovery metadata

The ELIXIR Ontology Lookup Service hosts 280 life-science ontologies¹¹. The NHS list of approved national information standards¹² counts 90 standards and twice as many collections, while the NHS Data Model and Dictionary describes over 2,750 data elements¹³. The INSPIRE Technical Guidelines on metadata implementation for geospatial data run to 99 pages¹⁴.

Harmonising data discovery in such a landscape is simply intractable. The best we can hope for across a federation of data resources and analysis environments is to adopt common basic discovery metadata

¹¹ See <https://www.ebi.ac.uk/ols/ontologies>

¹² See <https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections>

¹³ See https://www.datadictionary.nhs.uk/data_elements/overview.html

¹⁴ See <https://inspire.ec.europa.eu/documents/inspire-metadata-implementing-rules-technical-guidelines-based-en-iso-19115-and-en-iso-1>

FOR CONSULTATION & COMMENT

which is aligned with metadata standards used by the likely largest sensitive data providers. In our terms this means looking at catalogue-level standards mandated within UK Government and health services.

From an architectural perspective the SDRI Federation is an “overlay” on top of Web standards, notably HTTPS, XML and JSON. Hence we favour “Web facing” formats for metadata over internally-oriented standards.

2.3.1.1. Recommended standards

Our three key reference sites for metadata standards are:

- Central Digital and Data Office: *Open standards for government data and technology*.
 - <https://www.gov.uk/government/collections/open-standards-for-government-data-and-technology>
- Department of Health and Social Care: *A guide to good practice for digital and data-driven health technologies* (particularly section 10).
 - <https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology#section-10>
- Office for National Statistics: *Data Standards*,
 - <https://www.ons.gov.uk/aboutus/transparencyandgovernance/datastrategy/datastandards>

There are a number of common themes across these sources. For interoperability and easier linkage we recommend that new, born-digital data aim for compatibility with the standards below—with the caveat that these may change or evolve over time.

- General discovery metadata:
 - W3C DCAT data catalogue standard¹⁵ and extended application profiles;
 - schema.org¹⁶;
 - schema.org includes definitions for data catalogue and dataset drawn directly from DCAT;
 - the serialisation of schema.org markup into JSON-LD format provides a compact, machine-readable version ideal for data exchange and query results.
 - CSVW¹⁷ for CSV files published on the Web;
 - DCMI Dublin core metadata¹⁸ where there is no current match in schema.org.
- Place metadata:
 - UPRN¹⁹ unique property reference number for addressable locations in the UK;
 - ETRS89²⁰ European terrestrial reference system for locations in Europe;

¹⁵ See <https://www.w3.org/TR/vocab-dcat-3/> for the current version 3 working draft.

¹⁶ See <https://schema.org> and <https://www.w3.org/wiki/WebSchemas/Datasets> for its extensions from DCAT.

¹⁷ See <https://csvw.org/>.

¹⁸ See <https://www.dublincore.org/>.

¹⁹ See <https://www.geoplace.co.uk/addresses/uprn/>.

²⁰ See <http://etrs89.ensg.ign.fr/>.

FOR CONSULTATION & COMMENT

- WGS84²¹ world geodetic system for global locations.
- Date/time metadata:
 - ISO-8601²² for dates and times.
- Health-related metadata:
 - OMOP observational medical observations partnership standard²³ for electronic health records and similar;
 - **NB:** while the DHSC guidelines cited above recommend NHS use of the HL7 FHIR standard²⁴ for data interchange, the HDRA White Paper of 2021 [23] considers both and leans towards OMOP as a more appropriate data model for research use. Further, at time of writing, the NHS Data for Research and Development programme is settling on use of OMOP as a common standard for research-ready versions of health records and hospital observation data across its planned network of secure data environments (SDE, an NHS term synonymous with TRE)²⁵.
 - DICOM²⁶ image storage format for medical images.

2.4. Data accessibility

Easier and more streamlined access to sensitive data is the *raison d'être* of the DARE UK programme and of the Federation described here. We adhere strongly to the principle of “no TRE, no data”—data access in a secure environment over data distribution to researchers’ local systems—which offers a far greater degree of data security but does place some new restrictions on data access.

One particular consideration is “data understanding”. Most models of analysis for any datasets bar the very smallest introduce an “understanding” or “exploratory” step between discovery and full-blown production analysis. A good illustration of this is the CRISP-DM process²⁷, a widely-used industry standard dating back to the 1990s. It introduces both “business [domain] understanding” and “data understanding” as steps before “data preparation” and “modelling” but crucially emphasises the iterative nature of the process. These steps are cyclic, not serial.

The data access model of TREs introduces a hard serialisation into the end-to-end data research process, especially where information governance requires a researcher to request in advance of their project being approved only the data elements they will need to answer their particular research question. Without an initial exploratory phase that request can be difficult to get right.

A proper understanding of the “linkability” of two or more datasets can also be difficult to achieve without some level of access to both datasets in advance (see also Section 2.5 *Data interoperability* below). Full data harmonisation of this nature (especially across our broadest possible definitions of sensitive data) is out of scope for this architecture. However, the restrictions introduced by the “no TRE,

²¹ See <http://earth-info.nga.mil/GandG/update/index.php?action=home> .

²² See https://en.wikipedia.org/wiki/ISO_8601 for a good discussion.

²³ See <https://ohdsi.github.io/CommonDataModel/> and <https://www.ohdsi.org/> .

²⁴ See <https://www.hl7.org/fhir/summary.html> .

²⁵ NHS Data for Research and Development Technology and Data Working Group, *working documents*.

²⁶ See <https://www.dicomstandard.org/> .

²⁷ See <https://www.datascience-pm.com/crisp-dm-2/> .

FOR CONSULTATION & COMMENT

no data” principle are worthy of consideration: are there changes at architectural level that could facilitate a data harmonisation step?

OpenSAFELY [4] have shown that, for certain kinds of well-structured data, the majority of the algorithmic development and data exploration work can be done outside a TRE, on “fake data” that match the sensitive data schema and terminology sets but which contain random values. OpenSAFELY couples this development stage with an indirect query job submission model to deploy a researcher’s analysis code into the TRE without needing to grant them as an individual any kind of secure access. The “fake data” development model could be extended to other data sources even if the actual analysis step were to follow the “traditional” TRE model of secure access over remote desktop.

Enabling this degree of data exploration (or at least schema exploration) could be supported by additional Discovery Services sitting on the edge of the Federation.

2.5. Data interoperability

So far within the architecture we have recognised the fundamental importance of data interoperability in the form of data linkage but our treatment has been deliberately naïve. There are multiple levels on which to consider data interoperability and most of these are out of the scope of a federated architecture. Nevertheless we note them here and may expand on them in future iterations.

2.5.1. Syntactic interoperability

The most straightforward level of interoperability is syntactic or schema-level: are the datasets to be connected the same shape in at least one of their dimensions? In the horizontally and vertically partitioned dataspace we introduced in Part 2 (Strategic Case) there are two strong assumptions:

- EITHER the datasets have the same set of data subjects in the same order (e.g., different sets of attributes about the same group of people, ordered the same way);
- OR the datasets have the same set of attributes in the same order (e.g., the same set of attributes about two different groups of people).

Connecting datasets by these criteria is reasonably straightforward; relational databases are very good at exactly this kind of thing. Even differences in the ordering are easy to manage, by sorting, for example. We may need to define rules to handle gaps in the resulting dataset (either common rules or context-specific ones) but again, this is a well-understood area.

It is feasible to imagine an Index Service which could automate the linkage of two datasets under these conditions.

2.5.2. Terminological interoperability

Simple syntactic joining becomes harder when two datasets are probably interoperable but have been put together with slightly different terms. For example:

- Surname; Christian Name; Age;
- Given Name; Family Name; Age;
- Nom; Prénom; Age.

FOR CONSULTATION & COMMENT

Human experience tells us that these three datasets most likely record the same information (even with the transposition of name parts and dual languages in play). An equivalent level of experience for an automated service could be created using terminology bases, in much the same way that computer-assisted translation tools work today. (The proposed EU Smart Middleware Platform architecture includes just such a vocabulary service [2].)

By introducing one or more terminology services, it is feasible to imagine an Index Service which could automate the linkage of two datasets under these conditions.

2.5.3. Semantic interoperability

By far the most complex level of interoperability is semantic: two data items may have the same name but the way they were recorded might be very different. Different people, in different contexts, under different time pressures, might record nominally identical data items in subtly different ways which make them non-interoperable in ways almost impossible for an automated system to identify.

Another semantic variant arises in linkage between two or more datasets which each contain a number of data elements that, either alone or combined, mean *nearly* the same thing. Here, human intervention can harmonise the datasets, perhaps by introducing a new, common element, constructed differently in different datasets but which is nevertheless equivalent between them. Whether this kind of harmonisation could be achieved outside the TRE, working purely with dataset schemas and terminology sets (cf. Section 2.4), is likely to be highly case dependent.

It is difficult to imagine a scenario in which an Index Service could automate the linkage of two datasets under these conditions.

2.5.4. Data linkage

With the caveats noted above we have introduced a model of data linkage within the federated architecture which can, in principle, be automated (at least to some extent). Our model makes three design assumptions:

- Linkage between Data Extracts for a Project is done using a common linkage spine, which may be created explicitly for the Project or may be persistent.
- Linkage spines are created and maintained by Indexing Services which are trusted third-parties ("TTPs") independent of TREs or a Project's information governance.
- Identifiers used in the linkage spines are transformed as part of the linkage process into Project-specific identifiers. Such identifiers have no meaning outside the Project and thus cannot be used, by themselves, to link to anything else.

Linkage spines are exchanged between Federation Participants as structured documents.

2.6. Data reusability

Reusability in a sensitive data environment has to be balanced against governance principles which restrict use of data to pre-approved purposes only. We can draw two broad categories of reusability:

1. Reuse under original approvals. Assembled datasets and analyses derived from them (including computer programs) may result in a model for which evidence must be preserved for many years (for example clinical trials or medical devices). The datasets and analyses must be preserved in a

FOR CONSULTATION & COMMENT

way that could be checked and re-validated in the future, but all within the same purpose for which approvals were originally granted (and all within the same, or an equivalent, TRE). This then becomes the challenge of preserving long-term a digital object that is quite possibly encrypted. Specialised archive services could be developed that would do this (many already exist).

2. Reuse for new research. Whether a new research project—perhaps under a new team, perhaps linking in additional data—could be authorised to build on the full results of another is clearly a governance question. (By “full results” we mean the full linked data and analysis environment that remains within the TRE, not the summary results approved for egress.)

In technical terms, a service which preserved the TRE environment for the purposes in (1) would serve equally to support those in (2). We do not expand on the details of such a service here.

FOR CONSULTATION & COMMENT

3. Federated architecture: organisational layer

Chapters 1 and 2 have attempted to distil and write down the technical specifics of a federated architecture for TRE services – the “what” of the SDRI Federation. This chapter is much more open. Reaching agreement on an organisational model to manage the required new elements of standards and core services – the “how” – must be done through wider community processes.

The functionality required of a federated architecture implies a certain logical organisational structure, as captured in the preceding chapters. However, there is flexibility in how that logical structure could be realised in practice, depending on how the community of potential Participants might agree on its setup and operation.

To meet the public need for a more standardised, more trustworthy environment, the Federation needs to be real, in the sense of some kind of membership organisation with rules and standards. For the Federation to be real it will need a Federation Authority (FA) to act at least as gatekeeper and maintainer of standards.

The rules of participation for the Federation need to be agreed by all relevant stakeholders, and captured in a “Federation Rulebook”. The role of the FA then becomes one of maintaining the Rulebook and overseeing its implementation. The Rulebook should cover the “how to” for at least the following:

- Agree baseline technical standards for the Federation (as described in Chapters 1 and 2). This may involve defining or approving invitations to tender for technology suppliers of Federation services.
- Agree baseline procedures for key events: onboarding a new Participant; offloading a departing Participant; etc.
- Agree baseline maturity or accreditation standards for Federation Participants. This could involve setting minimum capabilities for new Participants accompanied by continual improvement plans towards nationally-agreed standards.
- Agree the setup and operation of trust services, trust anchors and frameworks – essentially who is able to vouch for and sign identity assertions made by Participants, and how.
- Agree the setup and operation of registry services.
- Agree baseline training or accreditation standards for Federation users, including service operators, Researcher PIs and other researchers.
- Approve new Participants joining the Federation.
- Approve Participants leaving the Federation. (This may be trumped by contractual arrangements arising from the joining process.)
- Approve technical changes with implications for, or impact on, part or the whole of the Federation, including:
 - changes to Federation standard software, for instance changes to Federation Services software;
 - changes to data exchange protocols or formats;
 - changes to metadata standards.
- Oversee regular audit and accreditation for the Federation as a whole.

Note that the governance focus of the FA is emphatically on what here is *new*: interoperability standards, service onboarding, coordinated change management and incident response. The existing stakeholders already have governance arrangements in place to enable research with sensitive data within TREs. The

FOR CONSULTATION & COMMENT

FA *should not* disrupt existing data governance arrangements for participants wanting to join, but should instead complement them.

3.1. Centralised vs distributed vs decentralised

How could the Federation Authority be realised?

Chapter 3 of the “IDSA Rulebook” [24] on the creation and operation of data spaces, published by the International Data Spaces Association, offers a good discussion of the pros and cons of centralised vs de-centralised models of federated governance for Data Spaces. We adapt that discussion here for the SDRI Federation.

One way to group the key services required of an FA is as follows:

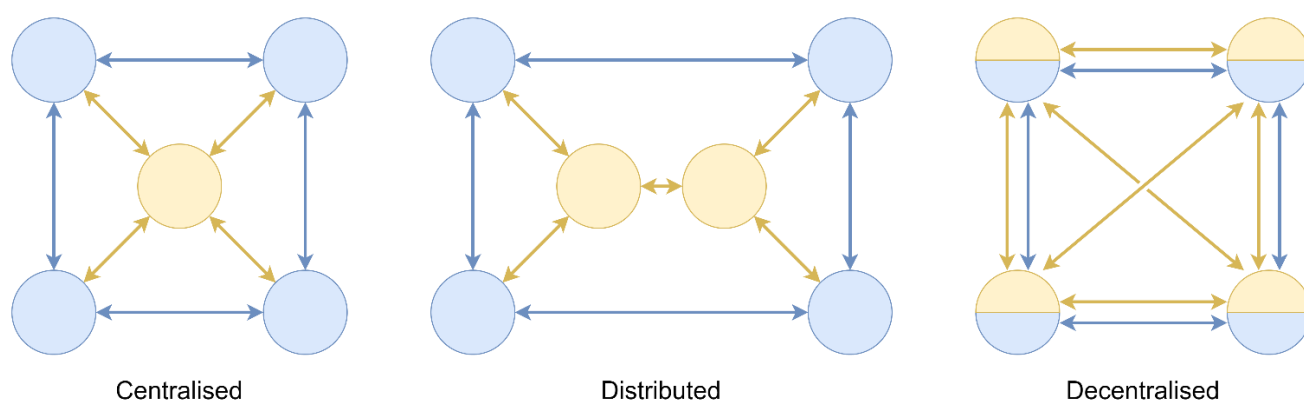
- Rules & Policies – underpinning agreements about what joining the Federation means, and technical implementations of them that enable digital handling.
- Trust, Identity & Certification – agents and methods for vouching for digital identities.
- Registry (Participants) – queryable records of who is a member of the Federation.

We could also add:

- Catalogue (data) – queryable records of what data assets could be accessible within the Federation, and how to go about applying for access.
- Observability – records of datasets exchanged by Participants, in which Project contexts, with what authorisation.

Each of these functions of the FA could be provided using different models of centralisation. Some functions fit certain models better than others.

The diagram below shows idealised models of centralisation, from fully centralised to fully decentralised.



Federation Participants and data exchanges between them are shown in blue (the Federation “data plane”), while services provided by the FA are indicated in yellow (the “control plane”). We illustrate three organisational models – centralised, distributed and decentralised – that could be used to provide FA services.

FOR CONSULTATION & COMMENT

Centralised. With a centralised FA, a central node runs all required Federation Services, including services to identify, verify, onboard and register Participants. In a maximally centralised model it could also run a single data discovery catalogue for the whole Federation.

Every Participant requires one control-plane connection to the central FA node.

Pros: Simplicity, familiarity and maturity of implementation and operation; advantages for observability and discovery; minimal attack surface for key FA security services.

Cons: Single point of failure and single point of attack; may be viewed as ceding too much sovereignty to a single entity; a single bad-faith operator could disrupt the activities of Participants arbitrarily.

Distributed. The distributed model retains some degree of centralised control but addresses the single point of failure challenges. Functional roles are distributed among a few synchronised nodes, enabling multiple entities to share responsibility for providing FA services.

Every Participant requires one control-plane connection to their “nearest” FA node. “Nearest” can be interpreted in flexible ways.

Pros: Greater flexibility in service deployment over centralised; more resilient to single-node failure; more resistant to bad-faith FA actors; small attack surface for key FA security services

Cons: Technically more complex to implement and run, requiring synchronisation protocols between FA nodes; observability and discovery become more complex; only partially addresses the sovereignty issue.

Decentralised. A decentralised design creates the highest levels of autonomy and sovereignty, notably around identity. A decentralised identity system requires that each Participant maintain identity information that can be verified by other Participants in ways that meet the agreed FA rules and policies. The operation of other required FA services – notably registry – also falls to the Participants.

Every Participant requires one control-plane connection to every other Participant.

Pros: Maximises individual Participant sovereignty; highly resilient to single-node failure; highly resistant to bad-faith FA actors.

Cons: Technically very complex to implement and run, requiring synchronisation protocols between all Participant nodes; observability and discovery become challenging; maximal attack surface for key FA security services.

These models are not exclusive. Different models can be used for the different service functions required of the Federation and Federation Authority. Trust and identity services, for instance, could be realised centrally, while data discovery through catalogues may be much easier to realise as a distributed service or set of services.

It's worth highlighting that the choice of model here impacts only the *control plane* of the Federation. Data exchange connections between Participants are the same in each case – direct and point-to-point. The functions of the control plane determine only *how* the connection is made, not where it goes.

FOR CONSULTATION & COMMENT

Following [24], the figure below shows the three organisational models on a single radar diagram against axes representing six desirable properties.

Sovereignty. The first goal of the Federation is to improve data sharing for research while maintaining, or even enhancing, sovereignty for data providers. Sovereignty is partly a function of autonomy, trust and transparency: is the decision to share this dataset mine? Do I trust the recipient I'm sharing with? Do I retain sight of where and how my dataset is being used? In our use of the term, sovereignty sits with Federation Participants, particularly data providers, in contrast to "control" below.

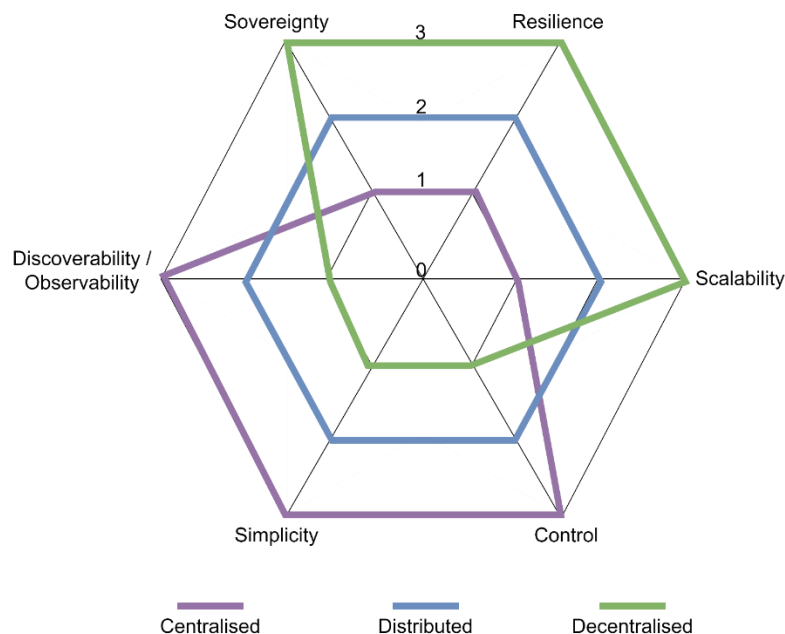
Resilience. Resilience is the ability of the overall Federation ecosystem to continue functioning in the event of unforeseen problems, such as the failure of a service node.

Scalability. In Federation terms scalability is not about the volume of data exchanged but about the number of Participants and number of concurrent Projects. These factors determine the potential load upon FA services.

Control. In Federation terms, control sits in contrast to sovereignty: what level of control does the FA have over the core federation services, not only in terms of their content but also in terms of who is allowed to access them? How much "say" does the FA have over day-to-day operations within the ecosystem?

Simplicity. In terms of both building the Federation and running it, mature, well-established technologies and architecture models are easier to deploy and operate.

Discoverability / Observability. This describes the overall transparency of the Federation, in terms of its content (essentially, the discoverability of data) and its operation (can everyone see what they need to see to retain overall trust?).



FOR CONSULTATION & COMMENT

4. Summary and further work

This blueprint addresses the challenge of connecting researchers and resources within the UK's existing landscape of digital research infrastructure by proposing a secure, managed federation of data and service providers. By proposing a foundational layer of secure data exchange and broad classes of interface services we seek to create the necessary trustworthy environment while imposing as few operational restrictions on service providers as possible.

This technical architecture supports current models of data linkage through the indexing and assembly of disparate datasets into one secure setting, and also newer models of remote and federated analytics where complex “query objects” can be submitted securely to remote data services (directly or indirectly).

We describe the architecture in three layers: infrastructure, data and governance. This version 2.1 covers significant refinements to the infrastructure layer set out in detail in the “initial” version (April 2023), expands on discussion of the data layer but covers the governance layers in less detail. We invite comment from the broader UK research community on the ideas and approaches presented here.

FOR CONSULTATION & COMMENT

5. References

- [1] DARE UK (2023); *UK Sensitive Data Research Infrastructure: A Landscape Review*; Zenodo; <https://doi.org/10.5281/zenodo.10082545>.
- [2] European Commission; *Simpl: cloud-to-edge federations and data spaces made simple*; news article, 24/02/2023; <https://digital-strategy.ec.europa.eu/en/news/simpl-cloud-edge-federations-and-data-spaces-made-simple> (accessed 02/03/2023).
- [3] T. Giles, et al. *TRE-FX: Delivering a Federated Network of Trusted Research Environments to Enable Safe Data Analytics*. Zenodo, 30 Oct. 2023, doi:10.5281/zenodo.10055354.
- [4] OpenSAFELY; *The OpenSAFELY Secure Analytics Platform*; <https://www.opensafely.org/> (accessed 23/03/2023)
- [5] C. Orton, et al. *TELEPORT: Connecting Researchers to Big Data at Light Speed*. Zenodo, 30 Oct. 2023, doi:10.5281/zenodo.10055358.
- [6] UK Government; *The UK General Data Protection Regulation*; <https://www.legislation.gov.uk/eur/2016/679/contents> (accessed 09/03/2023).
- [7] M. Wilkinson, M. Dumontier, I. Aalbersberg et al; *The FAIR Guiding Principles for scientific data management and stewardship*; *Sci Data* 3, 160018 (2016); <https://doi.org/10.1038/sdata.2016.18>.
- [8] IETF; *The Internet Engineering Taskforce*; <https://www.ietf.org/> (accessed 20/03/2023).
- [9] S. Bradner, B. Leiba; *BCP14; The Internet Engineering Taskforce Best Current Practice*; <https://www.ietf.org/rfc/bcp/bcp14.html> (accessed 01/12/2023).
- [10] The Open Group; *ArchiMate 3.1 Specification*; <https://pubs.opengroup.org/architecture/archimate3-doc/toc.html> (accessed 20/03/2023).
- [11] Welpton, Richard (2019). *SDC Handbook*. Figshare. Book. <https://doi.org/10.6084/m9.figshare.9958520.v1> (accessed 29/11/2023).
- [12] UK Government; *Copyright, Designs and Patents Act 1988*; <https://www.gov.uk/government/publications/copyright-acts-and-related-laws> (accessed 20/03/2023).
- [13] CITES; *Convention on International Trade in Endangered Species of Wild Fauna and Flora*; <https://cites.org/eng> (accessed 20/03/2023).
- [14] UK Government; *Government Security Classifications*; May 2018; https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf (accessed 20/03/2023).
- [15] (ISC)²; *Certified Information Systems Security Professional*; <https://www.isc2.org/Certifications/CISSP> (accessed 20/03/2023).
- [16] D. Arenas, J. Atkins et al; *Design choices for productive, secure, data-intensive research at scale in the cloud*; arXiv:1908.08737v2 [cs.CR] 15 Sep 2019; <https://arxiv.org/pdf/1908.08737.pdf> (accessed 25/04/2023).
- [17] NHS Digital; *Health and Social Care Cloud Risk Framework*, Chapter Dimensions that affect risk; 14 October 2021; <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services/cloud-risk-framework> (accessed 20/03/2023).
- [18] L. Sweeney, M. Crosas, M. Bar-Sinai; *Sharing Sensitive Data with Confidence: The Datatags System*; Technology Science, 2015101601. October 15, 2015; <https://techscience.org/a/2015101601/> (accessed 20/03/2023).

FOR CONSULTATION & COMMENT

- [19] UK Statistics Authority; *Data Capability Guidance*, v1.0; September 2022; available via <https://uksa.statisticsauthority.gov.uk/digitaleconomyact-research-statistics/better-access-to-data-for-research-information-for-processors/> (accessed 12/07/2023).
- [20] N. Karrar, S.K. Khan, S. Manohar, P. Quattroni, D. Seymour, S. Varma, & The UK Health Data Research Alliance. (2022). *Improving transparency in the use of health data for research: Recommendations for a data use register standard*. Zenodo. <https://doi.org/10.5281/zenodo.5902743>
- [21] GA4GH Beacon Group; *Beacon v2 standard*; <https://docs.genomebeacons.org/> (accessed 23/03/2023).
- [22] HDR-UK; *The CO-CONNECT Project*; <https://www.hdruk.ac.uk/projects/co-connect/> (accessed 23/03/2023).
- [23] UK Health Data Research Alliance; *Recommendations for Data Standards in Health Data Research*; November 2021; <https://ukhealthdata.org/wp-content/uploads/2021/12/211124-White-Paper-Recommendations-of-Data-Standards-v2-1.pdf> (accessed 13/07/2023).
- [24] International Data Spaces Association, *IDSA Rulebook*, https://docs.internationaldataspaces.org/ids-knowledgebase/v/idsa-rulebook/idsa-rulebook/3_functional_requirements (accessed 30/01/2024)
- [25] P. Barnsley, J. Fleming; (2023). *Trusted Research Environments – federating data to complete research*. The Francis Crick Institute. Report. <https://doi.org/10.25418/crick.23626653.v1>

FOR CONSULTATION & COMMENT

A Usage patterns

How well does this architecture model existing patterns of inter-TRE communication and federation?

This second version has been guided by work ongoing through 2023 and by interactions with key stakeholders and service operators through the UK TRE community²⁸.

Below we map published information about other patterns of TRE federation against the architecture picture in Chapter 1.

A.1 “Classic” TRE inter-operation

This model is an amalgamation of many current TREs which feature virtual desktop access to project environments and access to approved datasets.

Features:

- Data pooling model.
- Isolated research projects.

Elements:

- TRE “a” (left), acting purely as a data provider.
- TRE “b” (right), acting as both a data provider and analytics service provider.
- Index service, providing linkage spines.
- Software service, providing packages and other software components for the analytical project environments.

Diagram: (next page)

²⁸ The UK Trusted Research Environment Community. See <https://www.uktre.org/>

FOR CONSULTATION & COMMENT



FOR CONSULTATION & COMMENT

A.2 Francis Crick Institute federation model

Reference:

- The Francis Crick Institute, *Trusted Research Environments – federating data to complete research* [25].

Features:

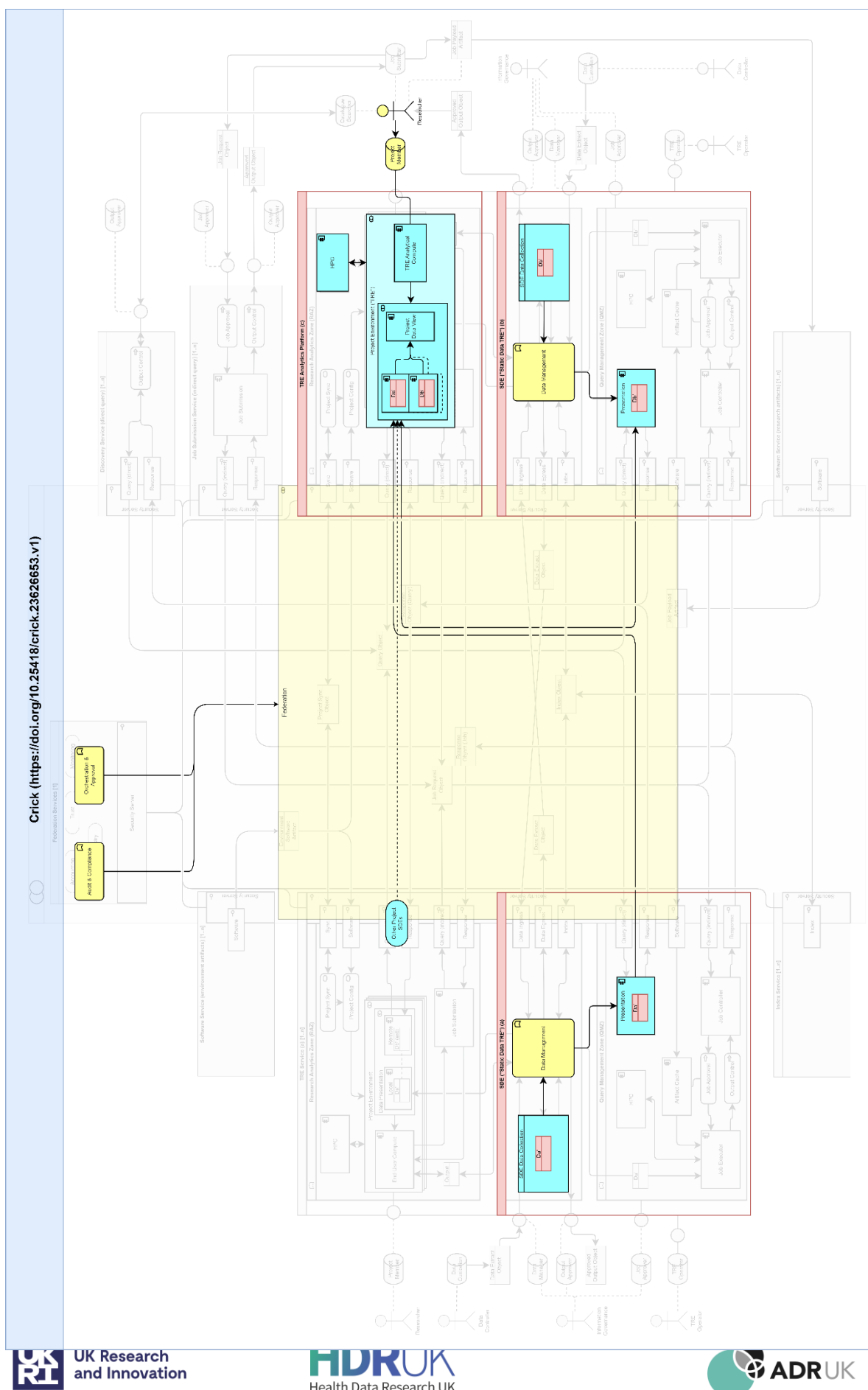
- TRE federation realised dynamically on a per-project basis.
- Separation of project analytics from data sources.
- Direct query model.

Elements:

- TRE “c” (upper right), acting purely as an analytical project environment, presenting a view of remote data to project members.
- SDE “b” (lower right) (“secure data environment”, a “static data TRE” in [1]), acting purely as a data provider with a remote presentation of data to TRE “c”.
- SDE “a” (left), acting purely as a data provider with a remote presentation of data to TRE “c”.
- Other project-specific SDEs (not illustrated in full).
- Federation between these elements on a per-project basis.

Diagram: (next page)

FOR CONSULTATION & COMMENT



FOR CONSULTATION & COMMENT

A.3 OpenSAFELY

Reference:

- OpenSAFELY, *The OpenSAFELY Secure Analytics Platform* [4] and particularly <https://docs.opensafely.org/images/c4-container.svg>

Features:

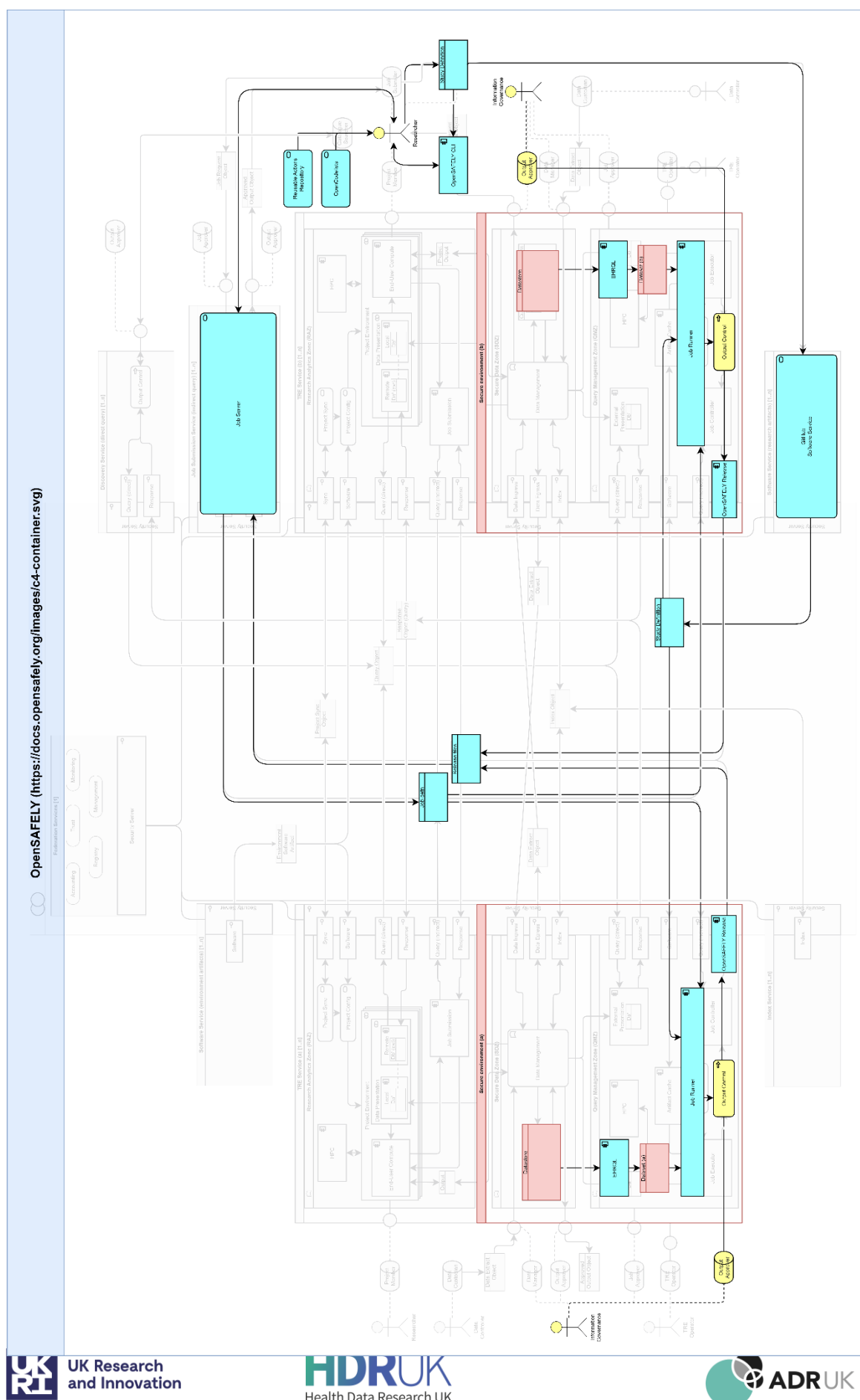
- Indirect query model.
- Researcher code and job development via local development tools (OpenSAFELY command line interface) and public repositories (notably GitHub, OpenCodelists).
- Job submission from outside TRE environments.

Elements:

- Job Server (upper right), acting as the point of interaction between researchers and TREs.
- Secure environment “a” (left), acting as a data provider and job handler.
- Secure environment “b” (right), acting as a data provider and job handler.
- GitHub (lower right), acting as a software service.

Diagram: (next page)

FOR CONSULTATION & COMMENT



FOR CONSULTATION & COMMENT

A.4 TELEPORT federation with pop-up TREs

Reference:

- C. Orton, et al. *TELEPORT: Connecting Researchers to Big Data at Light Speed* [5].

Features:

- Direct query model using polystore presentation.
- Dynamically-provisioned pop-up TREs with keep-alive sync to “mutually approved” state.
- GitOps synchronisation between participating TREs.

Elements:

- TRE “a” (left), acting as both data provider with remote data presentation, and potential provider of analytical project environments.
- TRE “b” (right), acting as both data provider with remote data presentation, and potential provider of analytical project environments.
- Package repo (upper left), providing software components for dynamic provisioning of project environments to mutually approved state.
- Continual policy sync between TREs “a” and “b”.

Diagram: (next page)

FOR CONSULTATION & COMMENT



FOR CONSULTATION & COMMENT

A.5 TRE-FX federation with stand-alone job submission

References:

- T. Giles, et al. *TRE-FX: Delivering a Federated Network of Trusted Research Environments to Enable Safe Data Analytics* [3].
- T. Giles, et al, TRE-FX primary implementation report
<https://docs.google.com/document/d/1FxrwXoYjx5aUI3MQyrnHs7xigvATJME/>

Features:

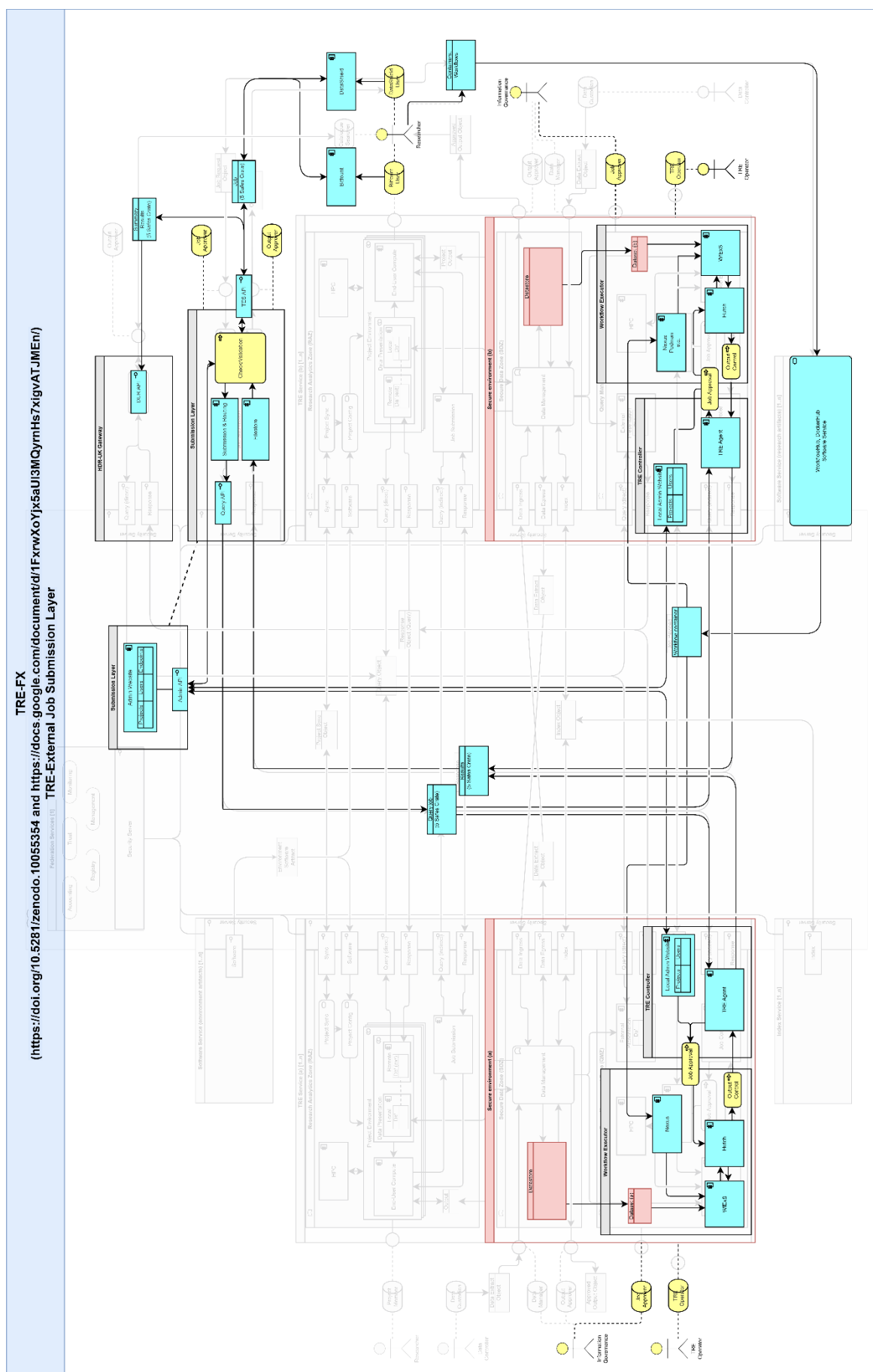
- Indirect query model.
- Researcher code and job development via local development tools (Bitfount, DataSHIELD) and public repositories (notably WorkflowHub and DockerHub).
- Standardised packaging methods for exchanged digital objects.
- Job submission from outside TRE environments.
- Single registry of projects and users.

Elements:

- Secure environment “a” (left), acting as both a data host and job handler.
- Secure environment “b” (right), acting as both a data host and job handler.
- Submission layer (upper right), acting as both a job submission service and a common lookup-registry for projects, users and data.
- WorkflowHub and DockerHub, acting as software services for researcher-developed artifacts.

Diagram: (next page)

<https://doi.org/10.5281/zenodo.10055354> and <https://docs.google.com/document/d/1FrxwXoYjx5aU3WQymHs7xigVATJME/n/>
 TRE-FX
 TRE-External Job Submission Layer
 Publication Series (1)



FOR CONSULTATION & COMMENT

A.6 TRE-FX federation with TRE-hosted job submission

References:

- T. Giles, et al. *TRE-FX: Delivering a Federated Network of Trusted Research Environments to Enable Safe Data Analytics* [3].
- T. Giles, et al, TRE-FX primary implementation report
<https://docs.google.com/document/d/1FxrwXoYjx5aUI3MQyrnHs7xigvATJME/>

Features:

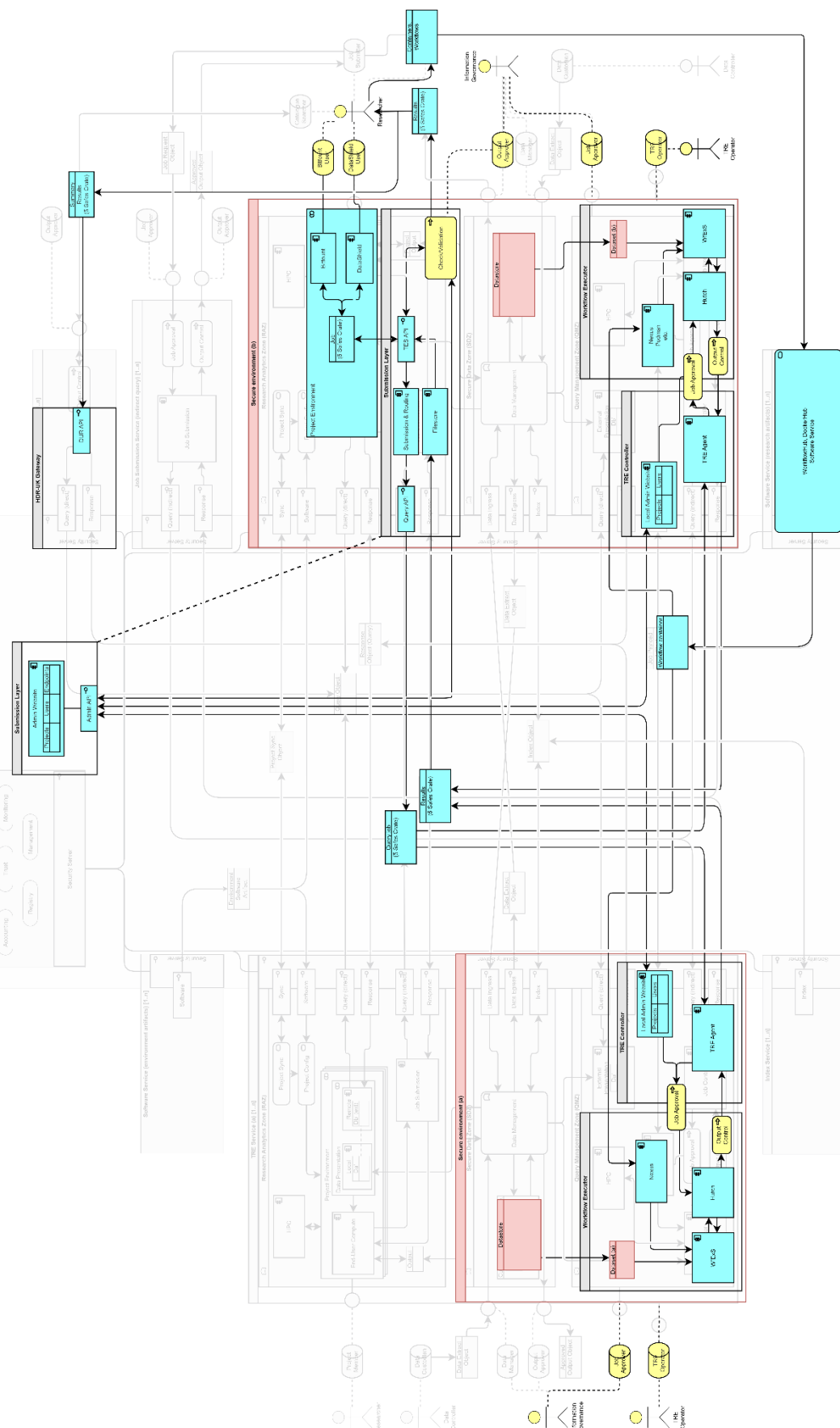
- Indirect query model.
- Researcher code and job development via local development tools (Bitfount, DataSHIELD) and public repositories (notably WorkflowHub and DockerHub).
- Standardised packaging methods for exchanged digital objects.
- Job submission from inside TRE project environments.
- Single registry of projects and users.

Elements:

- Secure environment “a” (left), acting as both a data host and job handler.
- Secure environment “b” (right), acting as an analytical project environment, a data host and job handler.
- Submission layer (upper right), acting as both a job submission service and a common lookup-registry for projects, users and data.
- WorkflowHub and DockerHub, acting as software services for researcher-developed artifacts.

Diagram: (next page)

<https://doi.org/10.5281/zenodo.10055354> and <https://docs.google.com/document/d/1FrxwXoYjx5aUI3WQymHs7xIgvATJMEh/>



FOR CONSULTATION & COMMENT