Science & Technology
Facilities Council

The ICAT permissions and authorisation rules system

Tom Griffin, STFC ISIS Facility

NOBUGS 2012 ICAT Workshop

tom.griffin@stfc.ac.uk

Overview

- Why rules
- Data policy
- Open tables
- Administration and Data Ingestion
- Facility staff
- Experiment Team (Investigators)
- Principal Investigator
- Embargo

Why Rules

- ICAT 3.3
- Explicit authorisation table + triggers
- >5,000,000 million entries for 150,000 investigations
- Limited in scope – Investigation & Dataset
- No mechanism for delegation
- Hard to change when staff move

- Addition of ‘Groups’

- Default deny

Science & Technology Facilities Council

Data Policy

- http://www.isis.stfc.ac.uk/user-office/data-policy11204.html

- tiny.cc/isisdp

Science & Technology Facilities Council

Data Policy

Data Policy

ISIS data management policy

1. General principles

1.1 This data management policy pertains to the curation of and access to experimental raw data and metadata collected and / or stored at the ISIS facility.

1.2 Acceptance of this policy is a condition of the award of beamtime at ISIS.

1.3 Users must not attempt to access, exploit or distribute raw data or metadata unless they are entitled to do so under the terms of this policy.

1.4 Deliberate infringements of the policy may lead to denial of access to ISIS raw data or metadata.

2. Definitions

For the purposes of this policy:

2.1 'raw data' are data collected from experiments performed on ISIS instruments. This definition includes data that are created automatically or manually by Facility-specific software and/or ISIS staff expertise in order to facilitate subsequent analysis of the experimental data, unless otherwise agreed.

2.2 'metadata' is information pertaining to data collected from experiments performed on ISIS instruments, including (but not limited to) the context of the experiment, the experimental team (in accordance with the Data Protection Act), experimental conditions and other logistical information.

2.3 the term 'principal investigator' (PI) pertains to the PI identified on the ISIS experiment proposal.

2.4 the term 'experimental team' includes the PI and any other person to whom the PI designates the right to access resultant raw data and associated metadata.

2.5 the term 'on-line catalogue' pertains to a computer database of metadata containing links to raw data files, that can be accessed by a variety of methods, including (but not limited to) www-based browsers.

2.6 the term 'results' pertains to data, intellectual property, and outcomes arising from the analysis of raw data.

2.7 the term 'long-term' means a minimum of ten years.

2.8. the term 'public domain' means belonging to the community at large, unprotected by copyright or patent and subject to appropriation by anyone.

3. Raw data and associated metadata

3.1 Free and commercial access to ISIS

3.1.1 All raw data and the associated metadata obtained as a result of free (non-commercial) access to ISIS, reside in the public domain, with ISIS acting as the custodian.

3.1.2 All raw data and the associated metadata obtained as a result of 'commercial-in-confidence' access to ISIS will be owned exclusively by the commercial user. Commercial users must agree with their relevant instruments scientists how they wish their raw data and metadata to be managed before the start of any experiment.

3.2 Curation of raw data and associated metadata

3.2.1 All raw data will be curated in well-defined formats, for which the means of reading the data will be made available by the Facility.

3.2.2 Metadata that is automatically captured by instruments will be curated either within the raw data files, within an associated on-line catalogue, or within both.

3.2.3 Data will be stored initially on instrument-related computers, and will be migrated or copied to archival facilities for long-term curation.

3.3 Access to raw data and metadata

3.3.1 Access to raw data and metadata beyond the period that it is stored on instrument-related computers will be via a searchable on-line catalogue.

3.3.2 Access to the on-line catalogue will be restricted to those who register with STFC/ISIS as users of the on-line catalogue.

3.3.3 Access to raw data and the associated metadata obtained from an experiment is restricted to the experimental team for a period of three years after the end of the experiment. Thereafter, it will become publicly accessible. Any PI that wishes their data to remain 'restricted access' for a longer period will be required to make a special case to the Director of ISIS.

3.3.4 It is the responsibility of the PI to ensure that the experiment number (RB number) is correctly entered into the metadata for each raw data set, in order to correctly associate each data set with the PI. If this is not done, the experimental team will not be able to access the data via the on-line catalogue and other users may inadvertently be given access rights to the data.

3.3.5 Appropriate STFC staff (e.g. instrument scientists, computing group members) may be given access to any Facility-curated data or metadata for Facility-related purposes. ISIS undertakes that they will preserve the confidentiality of such data.

3.3.6 The on-line catalogue will enable the linking of experimental data to experimental proposals. Access to proposals will only ever be provided to the experimental team and appropriate STFC staff, unless otherwise authorized by the PI.

4. Results

4.1 Ownership of results

4.1.1 Ownership of all results derived from the analysis of the raw data is determined by the contractual obligations of the person(s) performing the analysis.

4.2 Curation of results

4.2.1 ISIS will provide a facility for users to upload results and associated metadata to the facility and enable them to associate these results with raw data collected from the Facility.

4.2.2 The upload of results and metadata are subject to volume restrictions.

4.2.3 These results will be stored long-term by the Facility. It will not be the responsibility of the Facility to fully curate this data e.g. to ensure that software to read / manipulate this data is available.

4.3 Access to results

4.3.1 Access to the results of analyses performed on raw data and metadata is restricted to the person or persons performing the analyses, unless otherwise requested by those persons.

5. Good practice for metadata capture and results storage

5.1 The experimental team is encouraged to ensure that experimental metadata are as complete as possible, as this will enhance the possibilities for them to search for, retrieve and interpret their own data in the future.

5.2 ISIS undertakes to provide facilities for the capture of such metadata items that are not automatically captured by an instrument, in order to facilitate recording the fullest possible description of the raw data.

5.3 Researchers who aim to carry out analyses of raw data and metadata which are publicly accessible should, where possible, contact the original PI to inform them and suggest a collaboration if appropriate.

5.4 PIs and researchers who carry out analyses of raw data and metadata are encouraged to link the results of these analyses with the raw data / metadata using the facilities provided by the on-line catalogue. Furthermore, they are encouraged to make such results publicly accessible.

6. Publication information

6.1 References for publications related to experiments carried out at ISIS must be deposited in the STFC e-Pubs system http://epubs.cclrc.ac.uk/ within six months of the publication date, or during any new application for beamtime, whichever is the earlier.

Science & Technology Facilities Council

Data Policy

3. Raw data and associated metadata

3.1 Free and commercial access to ISIS

3.1.1 All raw data and the associated metadata obtained as a result of free (non-commercial) access to ISIS, reside in the public domain, with ISIS acting as the custodian.

3.1.2 All raw data and the associated metadata obtained as a result of 'commercial-in-confidence' access to ISIS will be owned exclusively by the commercial user. Commercial users must agree with their relevant instruments scientists how they wish their raw data and metadata to be managed before the start of any experiment.

3.2 Curation of raw data and associated metadata

3.2.1 All raw data will be curated in well-defined formats, for which the means of reading the data will be made available by the Facility.

3.2.2 Metadata that is automatically captured by instruments will be curated either within the raw data files, within an associated on-line catalogue, or within both.

3.2.3 Data will be stored initially on instrument-related computers, and will be migrated or copied to archival facilities for long-term curation.

3.3 Access to raw data and metadata

3.3.1 Access to raw data and metadata beyond the period that it is stored on instrument-related computers will be via a searchable on-line catalogue.

3.3.2 Access to the on-line catalogue will be restricted to those who register with STFC/ISIS as users of the on-line catalogue.

3.3.3 Access to raw data and the associated metadata obtained from an experiment is restricted to the experimental team for a period of three years after the end of the experiment. Thereafter, it will become publicly accessible. Any PI that wishes their data to remain 'restricted access' for a longer period will be required to make a special case to the Director of ISIS.

3.3.4 It is the responsibility of the PI to ensure that the experiment number (RB number) is correctly entered into the metadata for each raw data set, in order to correctly associate each data set with the PI. If this is not done, the experimental team will not be able to access the data via the on-line catalogue and other users may inadvertently be given access rights to the data.

3.3.5 Appropriate STFC staff (e.g. instrument scientists, computing group members) may be given access to any Facility-curated data or metadata for Facility-related purposes. ISIS undertakes that they will preserve the confidentiality of such data.

3.3.6 The on-line catalogue will enable the linking of experimental data to experimental proposals. Access to proposals will only ever be provided to the experimental team and appropriate STFC staff, unless otherwise authorized by the PI.

Science & Technology Facilities Council

Data Policy

4. Results

4.1 Ownership of results

4.1.1 Ownership of all results derived from the analysis of the raw data is determined by the contractual obligations of the person(s) performing the analysis.

4.2 Curation of results

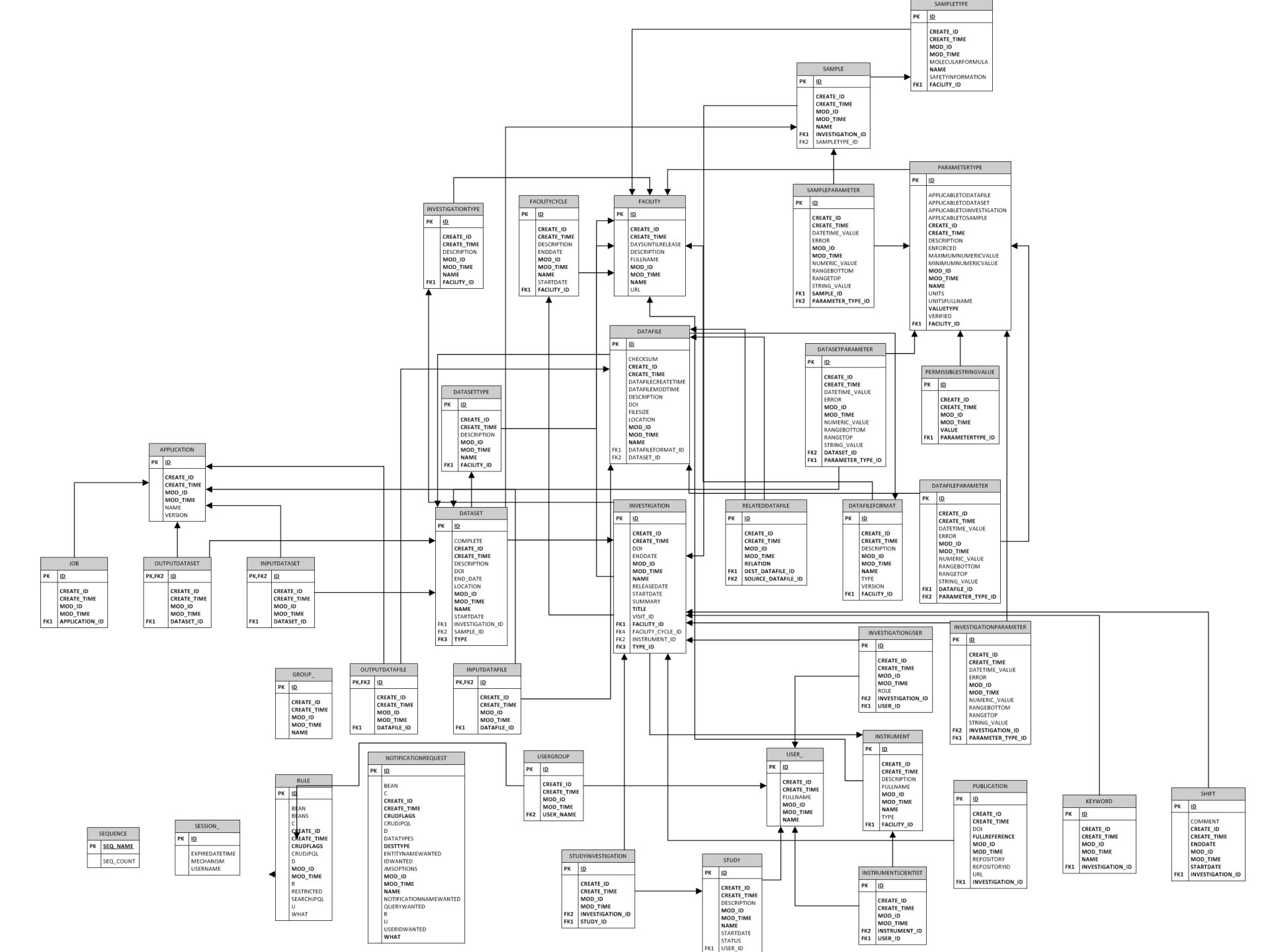
4.2.1 ISIS will provide a facility for users to upload results and associated metadata to the facility and enable them to associate these results with raw data collected from the Facility.

4.2.2 The upload of results and metadata are subject to volume restrictions.

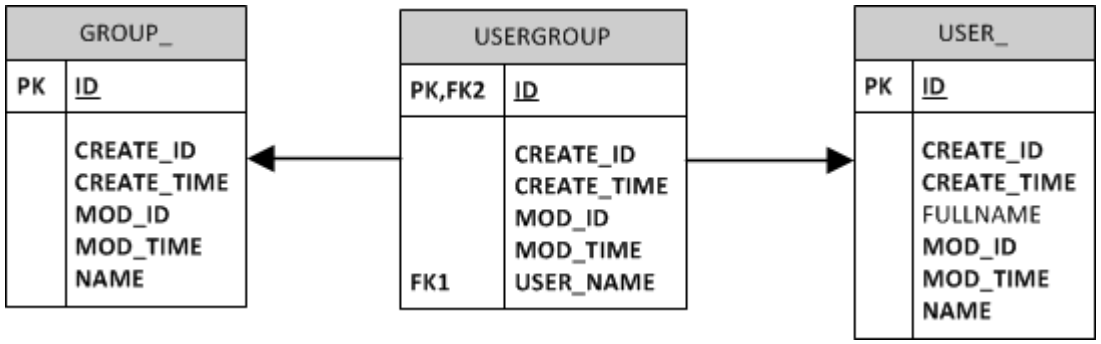
4.2.3 These results will be stored long-term by the Facility. It will not be the responsibility of the Facility to fully curate this data e.g. to ensure that software to read / manipulate this data is available.

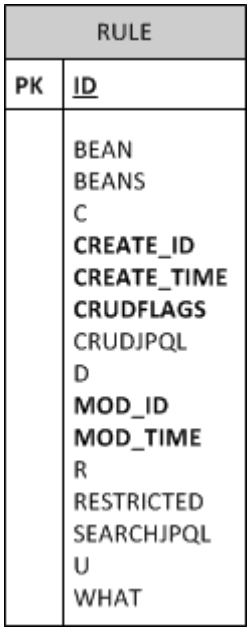
4.3 Access to results

4.3.1 Access to the results of analyses performed on raw data and metadata is restricted to the person or persons performing the analyses, unless otherwise requested by those persons.


SAMPLETYPE
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
MOLECULARFORMULA
NAME
SAFETYINFORMATION
FK1 FACILITY_ID
SAMPLE
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
NAME
FK1 INVESTIGATION_ID
FK2 SAMPLETYPE_ID
PARAMETERTYPE
PK ID
APPLICABLETODATAFILE
APPLICABLETODATASET
APPLICABLETOINVESTIGATION
APPLICABLETOSAMPLE
CREATE_ID
CREATE_TIME
DESCRIPTION
ENFORCED
MAXIMUMNUMERICVALUE
MINIMUMNUMERICVALUE
MOD_ID
MOD_TIME
NAME
UNITS
UNITSFULLNAME
VALUETYPE
VERIFIED
FK1 FACILITY_ID
SAMPLEPARAMETER
PK ID
CREATE_ID
CREATE_TIME
DATETIME_VALUE
ERROR
MOD_ID
MOD_TIME
NUMERIC_VALUE
RANGEBOTTOM
RANGETOP
STRING_VALUE
FK1 SAMPLE_ID
FK2 PARAMETER_TYPE_ID
INVESTIGATIONTYPE
PK ID
CREATE_ID
CREATE_TIME
DESCRIPTION
MOD_ID
MOD_TIME
NAME
FK1 FACILITY_ID
FACILITYCYCLE
PK ID
CREATE_ID
CREATE_TIME
DESCRIPTION
ENDDATE
MOD_ID
MOD_TIME
NAME
STARTDATE
FK1 FACILITY_ID
FACILITY
PK ID
CREATE_ID
CREATE_TIME
DAYSUNTILRELEASE
DESCRIPTION
FULLNAME
MOD_ID
MOD_TIME
NAME
URL
DATAFILE
PK ID
CHECKSUM
CREATE_ID
CREATE_TIME
DATAFILECREATETIME
DATAFILEMODTIME
DESCRIPTION
DOI
FILESIZE
LOCATION
MOD_ID
MOD_TIME
NAME
FK1 DATAFILEFORMAT_ID
FK2 DATASET_ID
DATASETPARAMETER
PK ID
CREATE_ID
CREATE_TIME
DATETIME_VALUE
ERROR
MOD_ID
MOD_TIME
NUMERIC_VALUE
RANGEBOTTOM
RANGETOP
STRING_VALUE
FK2 DATASET_ID
FK1 PARAMETER_TYPE_ID
PERMISSIBLESTRINGVALUE
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
VALUE
FK1 PARAMETERTYPE_ID
DATASETTYPE
PK ID
CREATE_ID
CREATE_TIME
DESCRIPTION
MOD_ID
MOD_TIME
NAME
FK1 FACILITY_ID
APPLICATION
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
NAME
VERSION
DATASET
PK ID
COMPLETE
CREATE_ID
CREATE_TIME
DESCRIPTION
DOI
END_DATE
LOCATION
MOD_ID
MOD_TIME
NAME
STARTDATE
SUMMARY
TITLE
VISIT_ID
FK1 INVESTIGATION_ID
FK2 SAMPLE_ID
FK3 TYPE
INVESTIGATION
PK ID
CREATE_ID
CREATE_TIME
DOI
ENDDATE
MOD_ID
MOD_TIME
NAME
RELEASEDATE
STARTDATE
SUMMARY
TITLE
VISIT_ID
FK1 FACILITY_ID
FK4 FACILITY_CYCLE_ID
FK2 INSTRUMENT_ID
FK3 TYPE_ID
RELATEDDATAFILE
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
RELATION
FK1 DEST_DATAFILE_ID
FK2 SOURCE_DATAFILE_ID
DATAFILEFORMAT
PK ID
CREATE_ID
CREATE_TIME
DESCRIPTION
MOD_ID
MOD_TIME
NAME
TYPE
VERSION
FK1 FACILITY_ID
DATAFILEPARAMETER
PK ID
CREATE_ID
CREATE_TIME
DATETIME_VALUE
ERROR
MOD_ID
MOD_TIME
NUMERIC_VALUE
RANGEBOTTOM
RANGETOP
STRING_VALUE
FK1 DATAFILE_ID
FK2 PARAMETER_TYPE_ID
JOB
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
FK1 APPLICATION_ID
OUTPUTDATASET
PK,FK2 ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
FK1 DATASET_ID
INPUTDATASET
PK,FK2 ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
FK1 DATASET_ID
GROUP_
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
NAME
OUTPUTDATAFILE
PK,FK2 ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
FK1 DATAFILE_ID
INPUTDATAFILE
PK,FK2 ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
FK1 DATAFILE_ID
INVESTIGATIONUSER
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
ROLE
FK2 INVESTIGATION_ID
FK1 USER_ID
INVESTIGATIONPARAMETER
PK ID
CREATE_ID
CREATE_TIME
DATETIME_VALUE
ERROR
MOD_ID
MOD_TIME
NUMERIC_VALUE
RANGEBOTTOM
RANGETOP
STRING_VALUE
FK2 INVESTIGATION_ID
FK1 PARAMETER_TYPE_ID
NOTIFICATIONREQUEST
PK ID
BEAN
C
CREATE_ID
CREATE_TIME
CRUDFLAGS
CRUDJPQL
D
DATATYPES
DESTTYPE
ENTITYNAMEWANTED
IDWANTED
JMSOPTIONS
MOD_ID
MOD_TIME
NAME
NOTIFICATIONNAMEWANTED
QUERYWANTED
R
U
USERIDWANTED
WHAT
USERGROUP
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
FK2 USER_NAME
USER_
PK ID
CREATE_ID
CREATE_TIME
FULLNAME
MOD_ID
MOD_TIME
NAME
INSTRUMENT
PK ID
CREATE_ID
CREATE_TIME
DESCRIPTION
FULLNAME
MOD_ID
MOD_TIME
NAME
TYPE
FK1 FACILITY_ID
PUBLICATION
PK ID
CREATE_ID
CREATE_TIME
DOI
FULLREFERENCE
MOD_ID
MOD_TIME
NAME
REPOSITORY
REPOSITORYID
URL
FK1 INVESTIGATION_ID
KEYWORD
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
NAME
FK1 INVESTIGATION_ID
SHIFT
PK ID
COMMENT
CREATE_ID
CREATE_TIME
ENDDATE
MOD_ID
MOD_TIME
STARTDATE
FK1 INVESTIGATION_ID
RULE
PK ID
BEAN
BEANS
C
CREATE_ID
CREATE_TIME
CRUDFLAGS
CRUDJPQL
D
MOD_ID
MOD_TIME
R
RESTRICTED
SEARCHJPQL
U
WHAT
SEQUENCE
PK SEQ_NAME
SEQ_COUNT
SESSION_
PK ID
EXPIREDATETIME
MECHANISM
USERNAME
STUDYINVESTIGATION
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
FK2 INVESTIGATION_ID
FK1 STUDY_ID
STUDY
PK ID
CREATE_ID
CREATE_TIME
DESCRIPTION
MOD_ID
MOD_TIME
NAME
STARTDATE
STATUS
FK1 USER_ID
INSTRUMENTSCIENTIST
PK ID
CREATE_ID
CREATE_TIME
MOD_ID
MOD_TIME
FK2 INSTRUMENT_ID
FK1 USER_ID

Special Tables





"root" group

Science & Technology Facilities Council

Very Special Tables

NOTIFICATIONREQUEST	
PK	ID
	BEAN
	C
	CREATE_ID
	CREATE_TIME
	CRUDFLAGS
	CRUDJPQL
	D
	DATATYPES
	DESTTYPE
	ENTITYNAMEWANTED
	IDWANTED
	JMSOPTIONS
	MOD_ID
	MOD_TIME
	NAME
	NOTIFICATIONNAMEWANTED
	QUERYWANTED
	R
	U
	USERIDWANTED
	WHAT

SEQUENCE	
PK	SEQ_NAME
	SEQ_COUNT

SESSION_	
PK	ID
	EXPIREDATETIME
	MECHANISM
	USERNAME

Science & Technology Facilities Council

Rules Syntax

Group

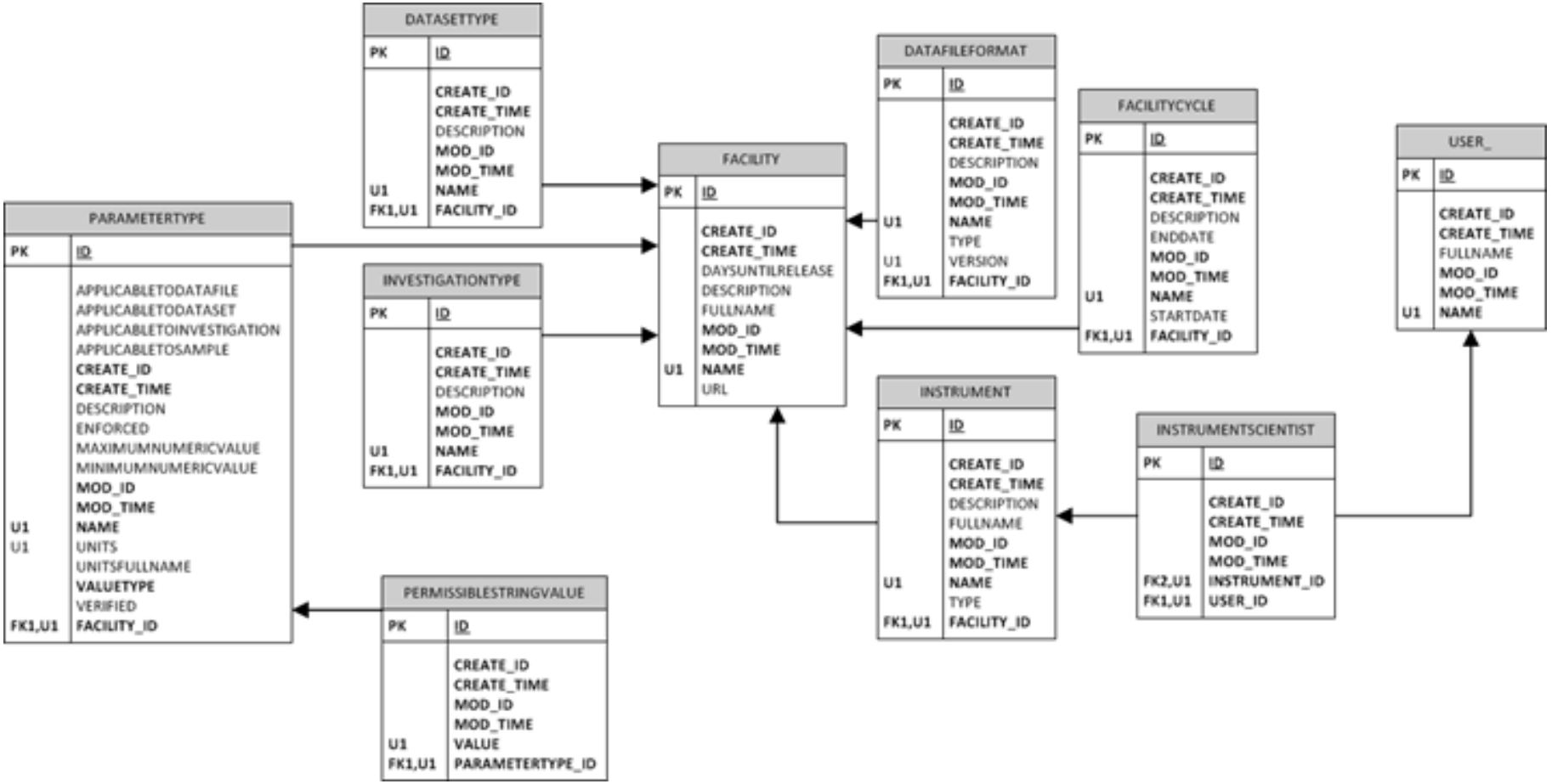
CRUD Flags

‘What’

```
Rule myRule = new  Rule();
myRule.group = facilityAdmins;
myRule.crudFlags = "CRUD";
myRule.what = “Facility”;
```

Open Tables

- Allow any authenticated reader to read all values



Open Tables

```
Rule rule = new  Rule();
rule.crudFlags = "R";
rule.what = table;
rule.setGroup(null);
port.create(sessionId, rule);
```

Open Tables

```
List<String> publicTables = new ArrayList<>();
publicTables.add("Application");
publicTables.add("DatafileFormat");
publicTables.add("DatasetType");
publicTables.add("Facility");
publicTables.add("FacilityCycle");
publicTables.add("Instrument");
publicTables.add("InstrumentScientist");
publicTables.add("InvestigationType");
publicTables.add("ParameterType");
publicTables.add("PermissibleStringValue");
publicTables.add("Publication");
publicTables.add("Shift");

for(String table : publicTables)
{
    Rule rule = new  Rule();
    rule.crudFlags = "R";
    rule.what = table;
    rule.setGroup(null);
    port.create(sessionId, rule);
}
```

Science & Technology Facilities Council

Facility Admin Access

```
Group facilityAdmins = (Group)port.search(sessionId, "Group[name='FacilityAdmins']" ).get(0);

List<String> adminTables = new ArrayList<String>();
adminTables.add("Application");
adminTables.add("Datafile");
...
...
adminTables.add("DatafileFormat");
adminTables.add("User");
adminTables.add("UserGroup");

for(String table : adminTables)
{
    Rule rule = new  Rule();
    rule.group = facilityAdmins;
    rule.crudFlags = "CRUD";
    rule.what = table;
    port.create(sessionId, rule);
}
```

Data Ingest Account

- Assume a group – “DataIngestors”
- Very similar to admin rules – just no delete

Application	InputDatafile	Publication
	InputDataset	RelatedDatafile
Datafile		
DatafileFormat	Investigation	Sample
DatafileParameter	InvestigationParameter	SampleParameter
	InvestigationUser	SampleType
Dataset		
DatasetParameter	Job	Study
DatasetType	Keyword	StudyInvestigation
	ParameterType	User

Science & Technology Facilities Council

Data Ingest Account

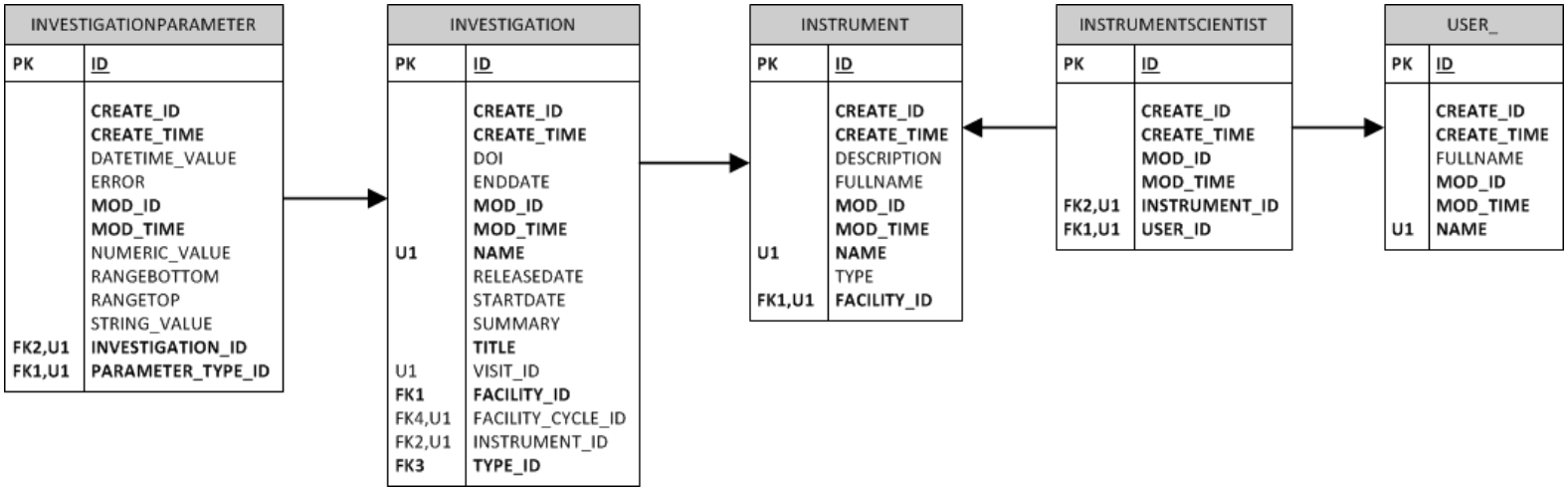
```
Group dataIngestors = (Group)port.search(sessionId, "Group[name='DataIngestors']" ).get(0);
List<String> ingestorTables = new ArrayList<String>();

ingestorTables.add("Application");
...
...
ingestorTables.add("User");

for(String table : ingestorTables)
{
    Rule rule = new  Rule();
    rule.group = dataIngestors;
    rule.crudFlags = "CRU"; //no delete permission for ingestors
    rule.what = table;
    port.create(sessionId, rule);
}
```

Science & Technology Facilities Council

Instrument Scientists

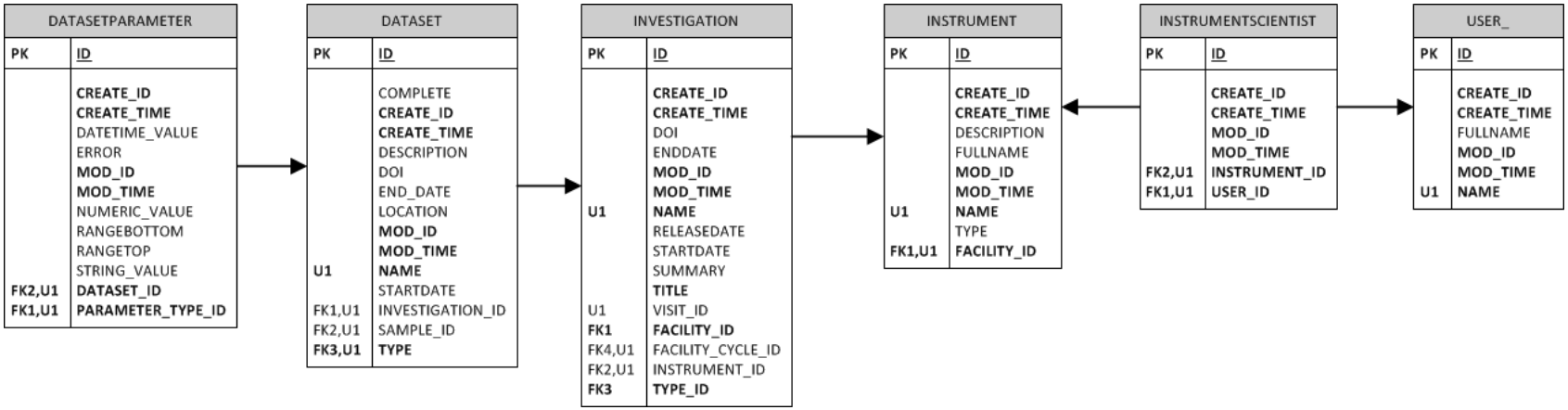



```
Rule isInv = new Rule();
isInv.crudFlags = "CRU";
isInv.what = "Investigation <-> Instrument <-> InstrumentScientist <-> User [name = :user]";
isInv.group = null; //rules applies regardless of group membership (not explicitly needed)
port.create(sessionId, isInv);
```

```
Rule isInvParam = new Rule();
isInvParam.crudFlags = "CRU";
isInvParam.what = "InvestigationParameter <-> Investigation <-> Instrument <-> InstrumentScientist <->
User [name = :user]";
port.create(sessionId, isInvParam);
```

Science & Technology Facilities Council

Instrument Scientists

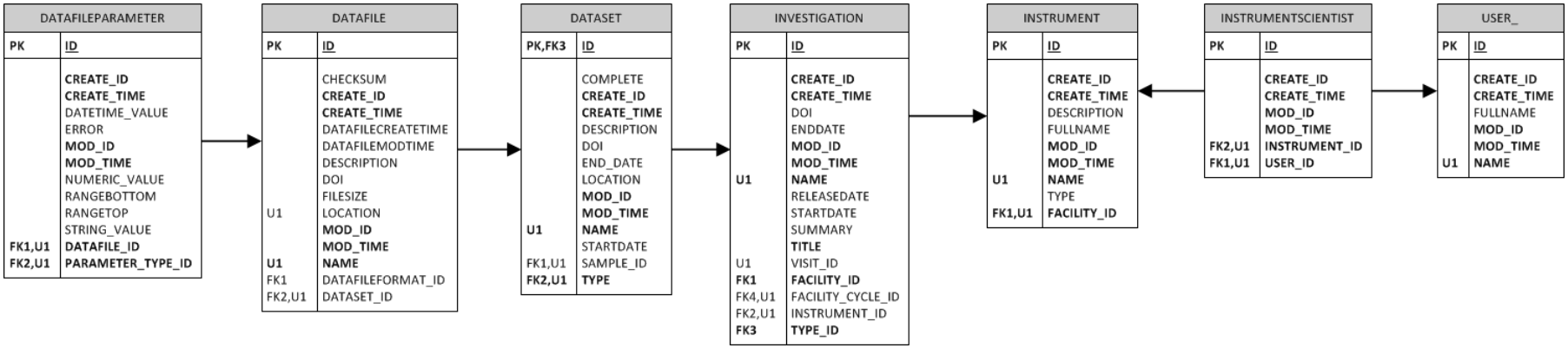



```
Rule isDs = new Rule();
isDsParam.crudFlags = "CRU";
isDsParam.what = "DatasetParameter <-> Dataset <-> Investigation <-> Instrument <-> InstrumentScientist
<-> User [name = :user]";
port.create(sessionId, isDsParam);

Rule isDsParam = new Rule();
isDsParam.crudFlags = "CRU";
isDsParam.what = "DatasetParameter <-> Dataset <-> Investigation <-> Instrument <-> InstrumentScientist
<-> User [name = :user]";
port.create(sessionId, isDsParam);
```

Science & Technology Facilities Council

Instrument Scientists

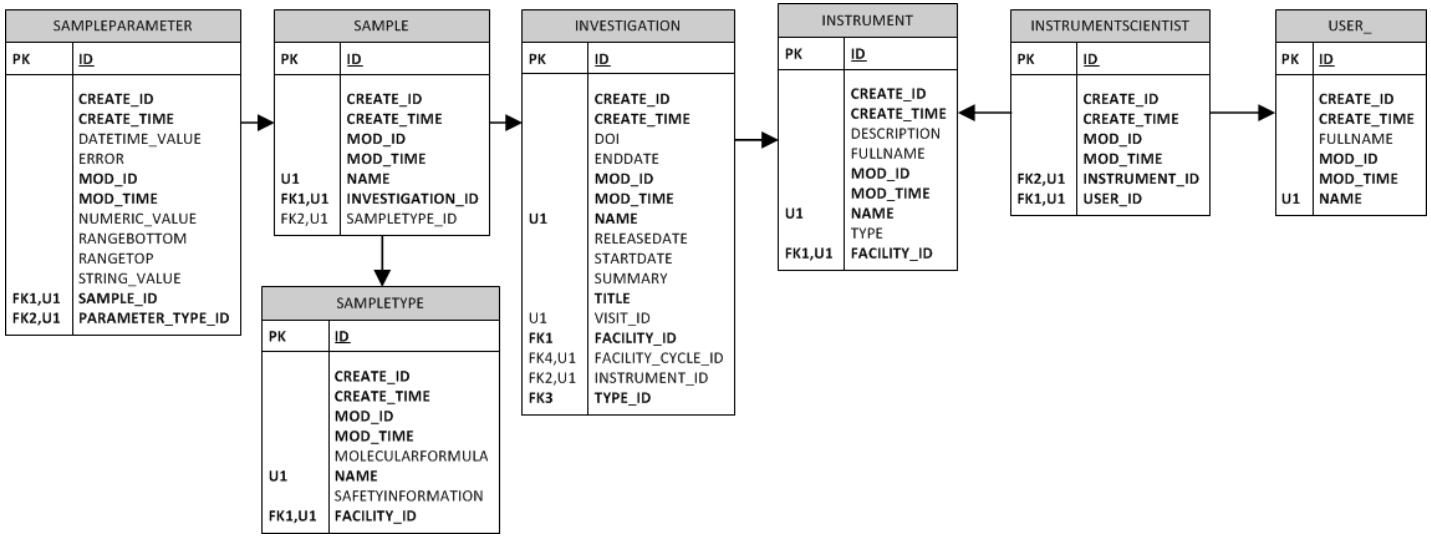



```
Rule isDf = new Rule();
isDf.crudFlags = "CRU";
isDf.what = "Datafile <-> Dataset <-> Investigation <-> Instrument <-> InstrumentScientist <-> User
[name = :user]";
port.create(sessionId, isDf);
```

```
Rule isDfParam = new Rule();
isDfParam.crudFlags = "CRU";
isDfParam.what = "DatafileParameter <-> Datafile <-> Dataset <-> Investigation <-> Instrument <->
InstrumentScientist <-> User [name = :user]";
port.create(sessionId, isDfParam);
```

Science & Technology Facilities Council

Instrument Scientists

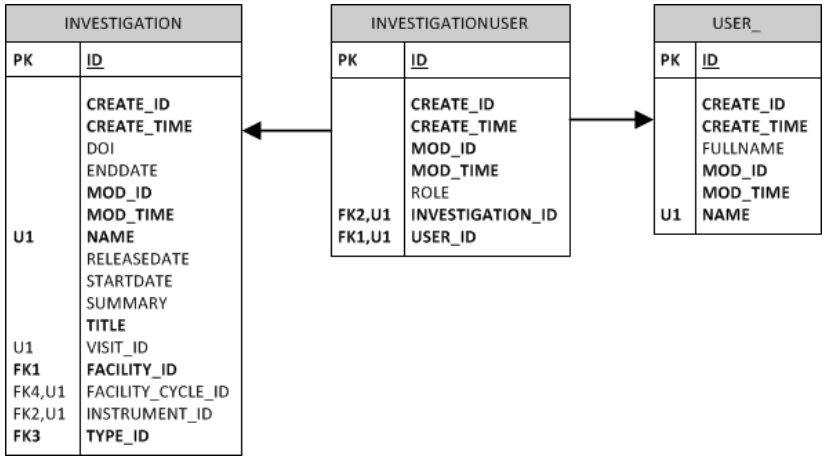



```
Rule isSampleInv = new Rule();
isSampleInv.crudFlags = "CRU";
isSampleInv.what = "SampleType <-> Sample <-> Investigation <-> Instrument <-> InstrumentScientist <->
User [name = :user]";
port.create(sessionId, isSampleInv);
```

```
Rule isSampleParamInv = new Rule();
isSampleParamInv.crudFlags = "CRU";
isSampleParamInv.what = "SampleParameter <-> Sample <-> Investigation <-> Instrument <->
InstrumentScientist <-> User [name = :user]";
port.create(sessionId, isSampleParamInv);
```

Science & Technology Facilities Council

Experiment Team

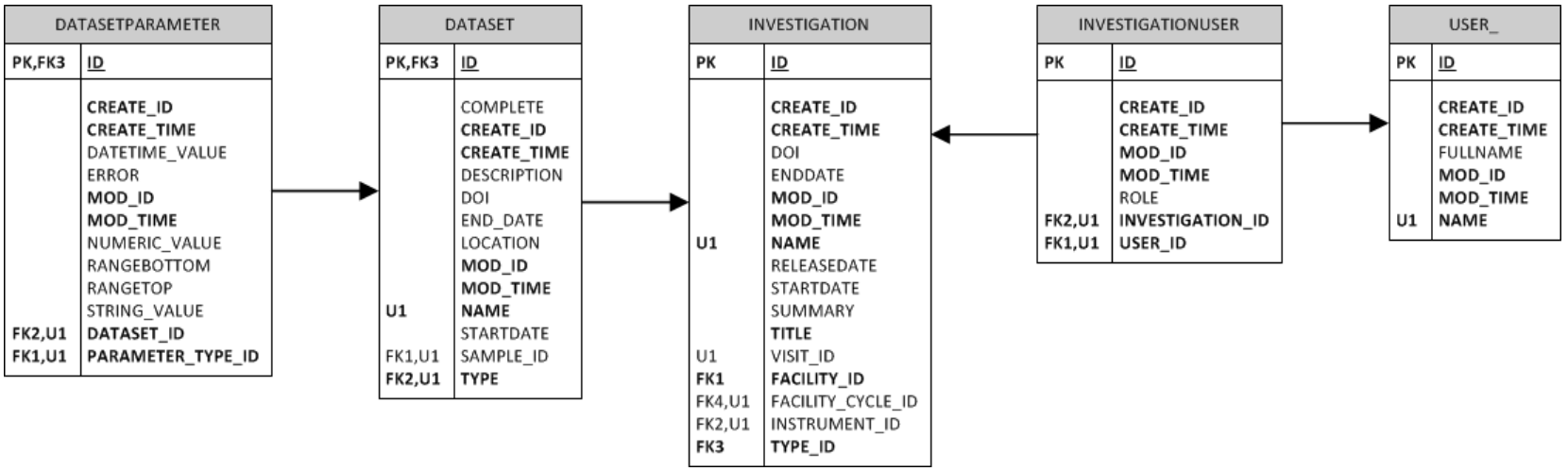



```
Rule coiInv = new Rule();
coiInv.crudFlags = "R";
coiInv.what = "Investigation <-> InvestigationUser  <-> User [name = :user]";
port.create(sessionId, coiInv);

Rule coiInvParam = new Rule();
coiInvParam.crudFlags = "R";
coiInvParam.what = "InvestigationParameter <-> Investigation <-> InvestigationUser
<-> User [name = :user]";
port.create(sessionId, coiInvParam);
```

Science & Technology Facilities Council

Experiment Team

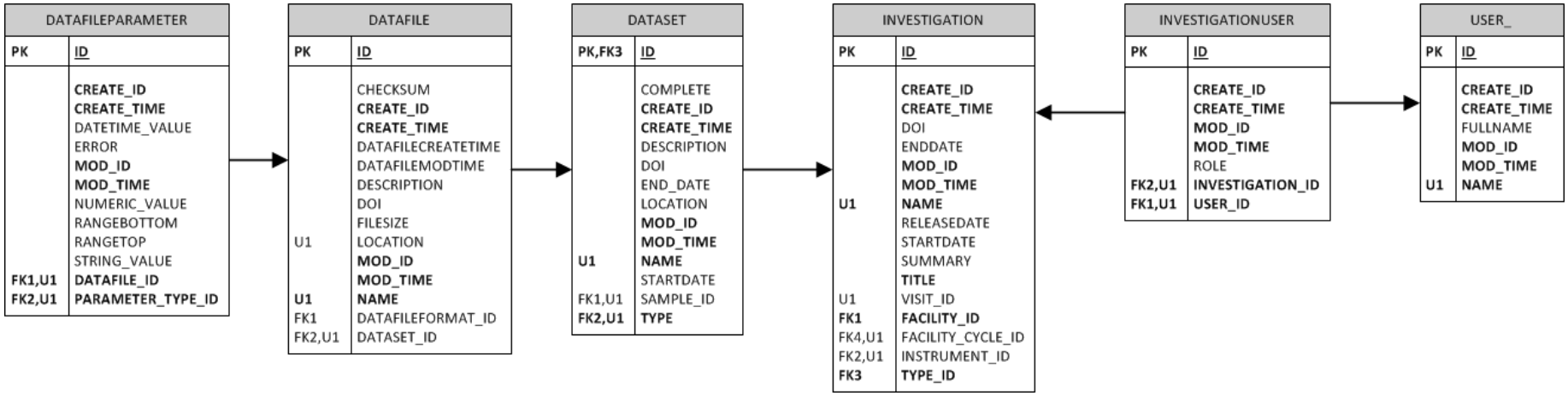



```
Rule coiDs = new Rule();
coiDs.crudFlags = "R";
coiDs.what = "Dataset <-> Investigation <-> InvestigationUser  <-> User [name = :user]";
port.create(sessionId, coiDs);

Rule coiDsParam = new Rule();
coiDsParam.crudFlags = "R";
coiDsParam.what = "DatasetParameter <-> Dataset <-> Investigation <-> InvestigationUser
<-> User [name = :user]";
port.create(sessionId, coiDsParam);
```

Science & Technology Facilities Council

Experiment Team

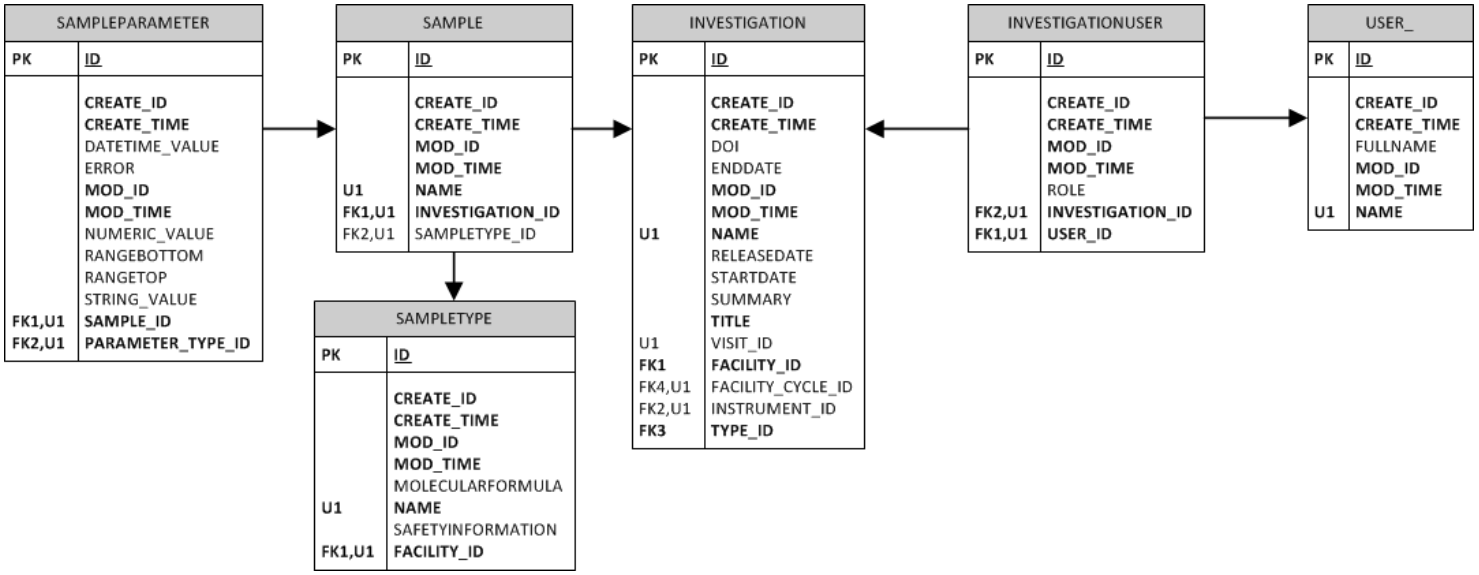



```
Rule coiDf = new Rule();
coiDf.crudFlags = "R";
coiDf.what = "Datafile <-> Dataset <-> Investigation <-> InvestigationUser  <-> User [name = :user]";
port.create(sessionId, coiDf);

Rule coiDfParam = new Rule();
coiDfParam.crudFlags = "R";
coiDfParam.what = "DatafileParameter <-> Datafile <-> Dataset <-> Investigation
<-> InvestigationUser  <-> User [name = :user]";
port.create(sessionId, coiDfParam);
```

Science & Technology Facilities Council

Experiment Team

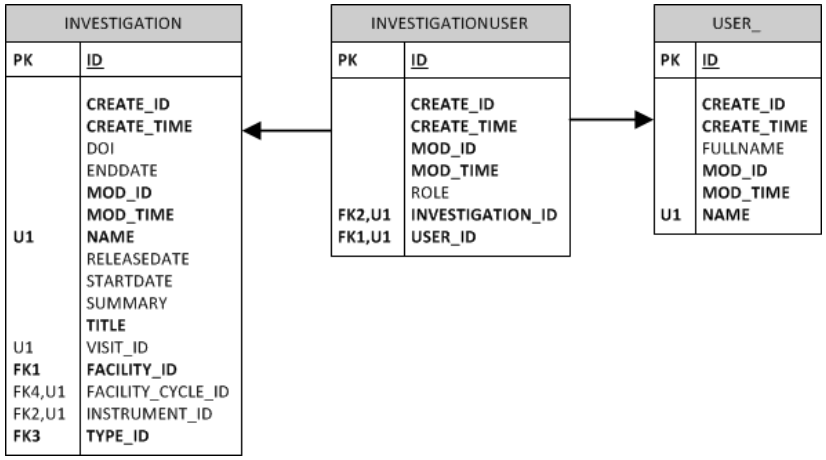



```
Rule coiSampleInv = new Rule();
coiSampleInv.crudFlags = "R";
coiSampleInv.what = "Sample <-> Investigation <-> InvestigationUser  <-> User [name = :user]";
port.create(sessionId, coiSampleInv);

Rule coiSampleParamInv = new Rule();
coiSampleParamInv.crudFlags = "R";
coiSampleParamInv.what = "SampleParameter <-> Sample <-> Investigation <-> InvestigationUser
<-> User [name = :user]";
port.create(sessionId, coiSampleParamInv);
```

Science & Technology Facilities Council

Principal Investigator

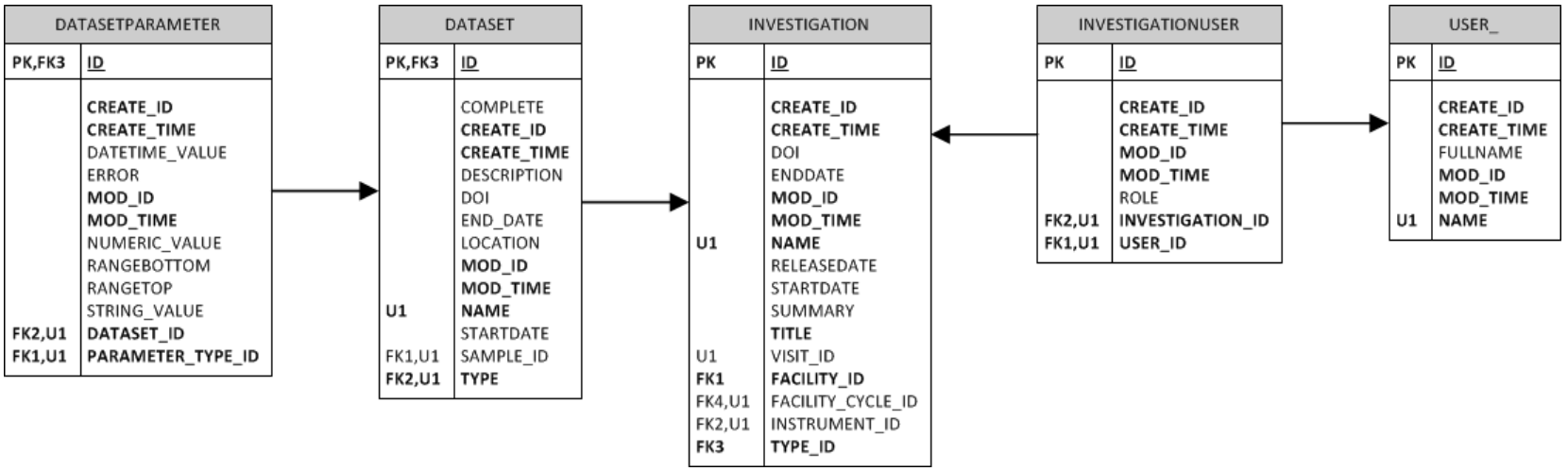



```
Rule coiInv = new Rule();
coiInv.crudFlags = "R";
coiInv.what = "Investigation <-> InvestigationUser [role = 'Principal Investigator']
<-> User [name = :user]";
port.create(sessionId, coiInv);

Rule coiInvParam = new Rule();
coiInvParam.crudFlags = "R";
coiInvParam.what = "InvestigationParameter <-> Investigation <-> InvestigationUser [role = 'Principal
Investigator']
<-> User [name = :user]";
port.create(sessionId, coiInvParam);
```

Science & Technology Facilities Council

Principal Investigator

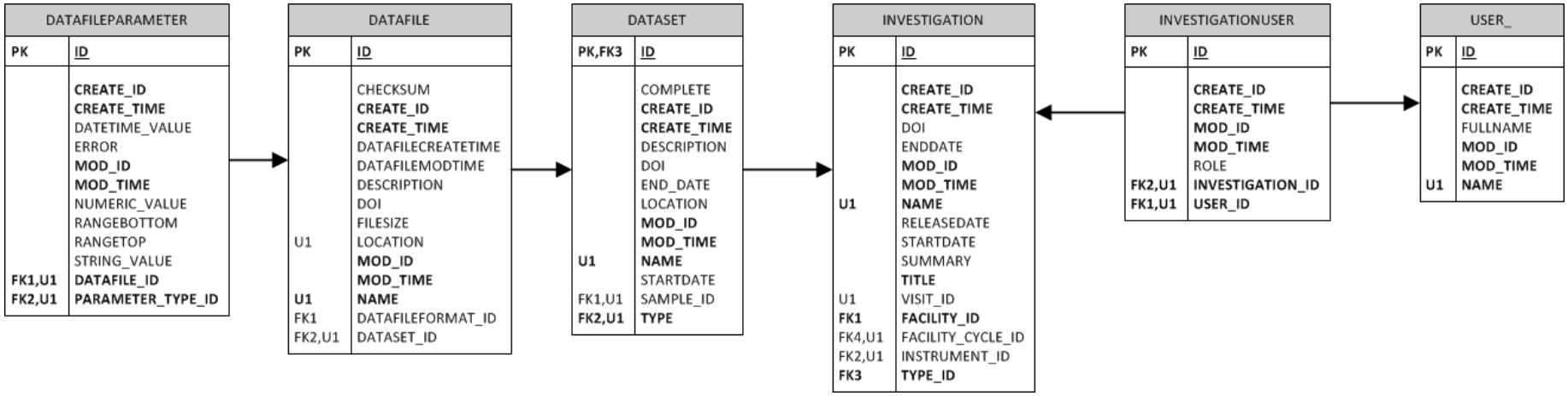



```
Rule coiDs = new Rule();
coiDs.crudFlags = "R";
coiDs.what = "Dataset <-> Investigation <-> InvestigationUser [role = 'Principal Investigator']
<-> User [name = :user]";
port.create(sessionId, coiDs);

Rule coiDsParam = new Rule();
coiDsParam.crudFlags = "R";
coiDsParam.what = "DatasetParameter <-> Dataset <-> Investigation
<-> InvestigationUser  [role = 'Principal Investigator'] <-> User [name = :user]";
port.create(sessionId, coiDsParam);
```

Science & Technology Facilities Council

Principal Investigator

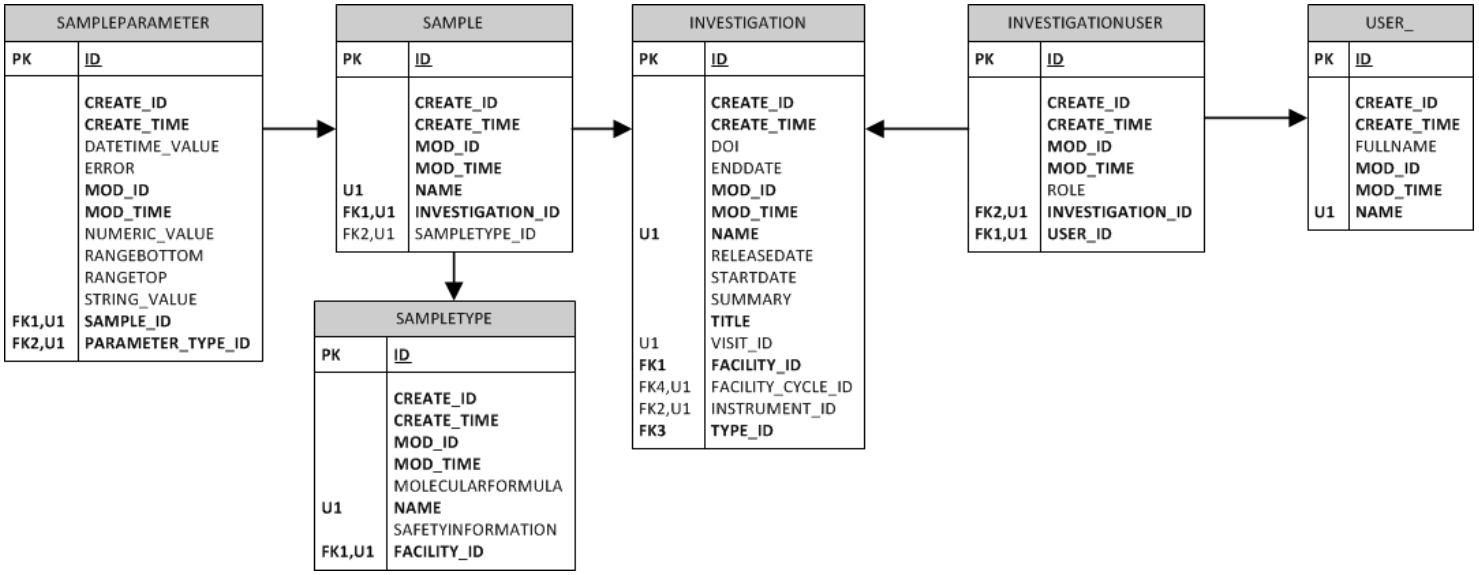



```
Rule coiDf = new Rule();
coiDf.crudFlags = "R";
coiDf.what = "Datafile <-> Dataset <-> Investigation
<-> InvestigationUser  [role = 'Principal Investigator'] <-> User [name = :user]";
port.create(sessionId, coiDf);

Rule coiDfParam = new Rule();
coiDfParam.crudFlags = "R";
coiDfParam.what = "DatafileParameter <-> Datafile <-> Dataset <-> Investigation
<-> InvestigationUser [role = 'Principal Investigator']  <-> User [name = :user]";
port.create(sessionId, coiDfParam);
```

Science & Technology Facilities Council

Principal Investigator




```
Rule coiSampleInv = new Rule();
coiSampleInv.crudFlags = "R";
coiSampleInv.what = "Sample <-> Investigation <-> InvestigationUser [role = 'Principal Investigator']
<-> User [name = :user]";
port.create(sessionId, coiSampleInv);

Rule coiSampleParamInv = new Rule();
coiSampleParamInv.crudFlags = "R";
coiSampleParamInv.what = "SampleParameter <-> Sample <-> Investigation
<-> InvestigationUser [role = 'Principal Investigator'] <-> User [name = :user]";
port.create(sessionId, coiSampleParamInv);
```

Science & Technology Facilities Council

Delegating Permission

- Allow a data owner to grant other users access to their data

4.3.1 Access to the results of analyses performed on raw data and metadata is restricted to the person or persons performing the analyses, unless otherwise requested by those persons.

Science & Technology Facilities Council

Delegating Permission

Not currently possible with a single rule

Create a group and a rule per investigation

```
rule.setCrudFlags("CRUD");
rule.setGroup(oneControllers);
rule.setWhat("InvestigationUser <->
Investigation [name = 'InvestigationOne']");
```

- Scalable?

Science & Technology Facilities Council

Embargo

```
rule.setCrudFlags("R");
rule.setWhat("Investigation [InvestigationType IN
('calibration', 'commissioning');
```

```
rule.setCrudFlags("R");
rule.setWhat("Dataset <->
Investigation [InvestigationType IN ('calibration',
'commissioning');
```

```
rule.setCrudFlags("R");
rule.setWhat("DataFile <-> Dataset <->
Investigation [InvestigationType IN ('calibration',
'commissioning');
```

+ parameters x3 + samples

Science & Technology Facilities Council

Embargo

```
rule.setCrudFlags("R");
rule.setWhat("Investigation [enddate +
Facility.daysuntilrelease] < Now ");
AND InvestigationType <> 'commercial'");
```

3.3.3 Access to raw data and the associated metadata obtained from an experiment is restricted to the experimental team for a period of three years after the end of the experiment. Thereafter, it will become publicly accessible.

Any PI that wishes their data to remain 'restricted access' for a longer period will be required to make a special case to the Director of ISIS.

Science & Technology Facilities Council

Embargo

```
rule.setCrudFlags("R");
rule.setWhat("Investigation [releasedate] < Now AND
InvestigationType <> 'commercial'");
```

Must set Investigation.releasedate as part of data ingest

Rules would need to consider non-facility owned data

dataset.type = 'raw'

Summary

- Rules syntax
- How to implement a PaNdata like policy in Rules

- All tables need to be considered

- Limitations and scalability

- Must be carefully thought out

Should ICAT ship with some rules/scripts?

Questions?

www.icatproject.org
code.google.com/p/icatproject

http://groups.google.com/group/icat-developers/
http://groups.google.com/group/icatgroup/

icat-developers@googlegroups.com
icatgroup@googlegroups.com