# UK Location Programme

## Access Control and Rights Management Position Statement

V1.0

# CONTENTS

1 Executive Summary ..... 3

2 Introduction ..... 4

3 Purpose of document ..... 5

4 Drivers for action ..... 5

5 Scope of the problem ..... 6

6 State of Play in Access Control and Rights Management ..... 6

7 Key findings from May 2012 survey ..... 7

8 Use Cases ..... 8

9 High level requirements ..... 8

10 Options for the future ..... 11

11 Recommendation ..... 13

12 Next steps ..... 14

Annex A. State of Play ..... 16

Annex B: Summary of online survey ..... 23

Annex C: Use cases ..... 30

Annex D. Advantages and disadvantages of the options ..... 44

# 1 EXECUTIVE SUMMARY

This paper is the result of work by the UK Location Architecture Interoperability Board - Business Interoperability Working Group (BIWG), a group that has wide cross-government membership.

UK Location had previously identified that it is not practical to develop applications which consume protected resources across administrative domains that have multiple different access control mechanisms. This is because when a variety of rights management systems are in place there are significant downstream impacts on other data providers and data users, placing additional burdens on both to register with multiple data providers, manage multiple passwords and understand incompatible licensing terms as defined by each data provider. A solution to these problems is essential to avoid adverse and significant impact on the achievement of benefits of both the INSPIRE Directive and the UK Location Strategy.

Hence BIWG has been tasked to study how digital rights management could be used with location data and services to improve the interoperability in these situations.

The study by BIWG gathered information from a number of sources including a stakeholder survey, use cases, state of play study and workshops to assess approaches to managing access controls. This included the use of location and non-location data. The scope of the study was then limited to make the problem with a more extensive roadmap to follow.

Options considered were:

Option 1. Do nothing.

Option 2. Centralised access control.

Option 3. Federated access management.

BIWG recommends that UK Location pursues Option 3.

BIWG further recommends that to achieve this the next steps involve further design work, engagement with stakeholders, and consideration of how to integrate with other cross government initiatives, in particular the ID Assurance Programme.

The first task will be to develop a roadmap which focuses on government to government[1] authentication first for OGC web services, followed by other relationships and authorisation.

UK Location will need to assess how to resource further work.

The UK Location Programme Board agreed on 28th November 2012 to take the recommendations of the BIWG forward.

[1] See Section 5 for definition of ‘government’.

# 2 INTRODUCTION

This paper draws together the work of the BIWG, which is a sub group of the UK Location Architecture and Interoperability Board (AIB). Between March and November 2012 BIWG has considered how to develop an approach to best tackle the problem of the lack of interoperability in the digital rights management of services providing location data to users. Assistance has been provided by Bloxstore Ltd.

Some of our government policies promote free and open access to public data where possible. However, in other instances access to data may be restricted as data may be sensitive, private or only available under licence (further details are set out in the UKLP Data Sharing Operational Guidance on Licensing and Charging[2]).

The work of the BIWG has determined that it is necessary to control and manage access to this data. Current practices of digital rights management are inconsistent and lack interoperability making it difficult and burdensome to the user as well as publisher of data to gain and manage access to, and use of, data.

To help frame this paper and to distinguish the different functions related to access and use, the following definitions, taken from the OGC GeoDRM Reference Model[3], are used:

> **Access control**: a combination of authentication and authorisation.
>
> Authentication – verification that a potential partner in a conversation is capable of representing a person or organisation (Ref: W3C).
>
> Authorisation – determination whether a subject is allowed to have the specified type of access to a particular resource.
>
> Usually, authorisation is in the context of authentication. Once a subject is authenticated, it may be authorised to perform different types of access.

> **Rights management**: tracking and controlling the use of content, rights, licences and associated information

Access control and rights management are inter-related in many ways, but should be considered separately when a technical solution is concerned. In this paper they are kept separate for two reasons:

- so as to make the issue more manageable; and
- because there are existing access control solutions available, whereas rights management has a less mature technology.

[2] http://location.defra.gov.uk/resources/data-sharing-operational-guidance/

[3] http://www.opengeospatial.org/standards/as/geodrmrm

The study by BIWG focused on access control but returned frequently to rights management to ensure developments were known and understood, and to check that any access control would be compatible with future requirements for rights management.

# 3 PURPOSE OF DOCUMENT

The purpose of this document is:

(i) to give the UK Location Programme Board a better understanding of rights management issues;

(ii) to report on the current state of play and discuss examples of current practice;

(iii) to set out potential solutions for digital rights management to make UK Location services interoperable.

# 4 DRIVERS FOR ACTION

The following are identified as the key drivers:

- Maximising the benefits achieved from delivery of INSPIRE conformant interoperability.
- Improving controlled access to sensitive and protected data. Content security may be necessary to support a commercial business model, or to comply with agreements with other providers, or to respect privacy rights or other confidentialities, or to restrict access to sensitive data. This will also help tracking access and use of data resources.
- Protection of intellectual property - geospatial content and services are becoming increasingly available in digital form and it is now easier to copy, modify and re-use that content, and to access the services. Organisations involved in the capture and sharing of geospatial content now find that they need to protect their IP whenever it is shared through a digital network.
- Government policy areas such as open government, open data, digital by default and transparency. Improved access control will offer the ability to allow some access to services which are currently ‘closed’.
- Consumer expectation – consistent, immediate and unhindered access to (geospatial) content at the point of use. Reduced burden – removing the need to manage multiple usernames and passwords for many websites or databases.
- Stronger management of licensing – given the scale and volume of data sets that will be accessible it is no longer practical or feasible to rely on legal and contractual measures alone to manage and enforce licensing terms.
- Standardisation – movement in the public sector is towards greater levels of licence simplification and more standardised and harmonised ways to control access and use of

location information.

# 5 SCOPE OF THE PROBLEM

The potential scope of the problem is all services providing location data. This would include transfers between all levels of the public sector, private sector, academia, the third sector and the citizen.

| To: / From: | Government | Business | Education | Voluntary | Citizen |
|---|---|---|---|---|---|
| Government | G2G | G2B | G2E | G2V | G2C |
| Business | B2G | B2B | B2E | B2V | B2C |
| Education | E2G | E2B | E2E | E2V | E2C |
| Voluntary | V2G | V2B | V2E | V2V | V2C |
| Citizen | C2G | C2B | C2E | C2V | C2C |

Government means all levels of government, public administrations and their contractors.
Business means all aspects of the private sector
Education means all levels of education and academic research
Voluntary means the third sector
Citizen is an individual acting in their capacity as a citizen and not as an employee or other role.

However, in order to approach the problem in a manageable way, priority has been given to initially focusing on a solution for services provided by government to government, (G2G in the diagram above). The intention, however, is that when developed any solution should be designed so as to be easily extendable to other sectors. G2G exchanges formed a major part of the concerns of UK Location due, in part, to the need to comply with INSPIRE legislation.

The next priorities, based on what we know now, are government to citizen (G2C) and government to business (G2B).

# 6 STATE OF PLAY IN ACCESS CONTROL AND RIGHTS MANAGEMENT

Within the wider geospatial community there is the growing realisation that while issues of access control and rights management remain unresolved there is a negative impact on the value we are able to collectively deliver to our stakeholders. An extensive range of different approaches are documented in some detail at Annex A, giving a view of current trends, though it must be noted that it is not an exhaustive survey.

Across Europe there is a mixed implementation of access control and rights management. Some implementations are bespoke to meet a specific need while others have chosen more open

standards solutions. For example, the European Union Location Framework (EULF) as part of the EU-funded ISA (Interoperability Solutions for European Public Administrations) programme is taking forward work done previously by ESDIN (**E**uropean **S**patial **D**ata **I**nfrastructure with a Best Practice **N**etwork). However, there does not appear to be any access control and rights management policy or strategy in place as yet.

The UK Government's Digital Strategy contains actions to enable services to be 'digital by default', including plans for cross government identity assurance, common platform component and improved departmental digital leadership. It is widely reported that new business models will evolve from the cloud; these will offer more fine grained services across a wide business spectrum with potential in the geospatial community. There may, therefore, be developments we can benefit from coming along in the near future.

With a lack of central policy, implementations will continue to be a mix of standard and non-standard approaches. Any UK implementation would require taking the best practice from a variety of solutions to deliver the benefits required.

# 7 KEY FINDINGS FROM MAY 2012 SURVEY

An online survey was conducted of the main stakeholders of UK Location. The aim was to gather a cross section of views on how access control and rights management is currently implemented, and views on how it can be improved and made more interoperable in the future. The survey was put on the UK Location website and emails sent to invite all those who have registered for updates on UK Location to respond, along with members of all UK Location groups and boards. IT was also announced on the UK Location twitter account. The questions asked and responses are in Annex B.

The four key findings of the survey were:

- **UK Location is highly dependent on public sector data**

  The vast majority of respondents wish to access and use public sector data. Much of the funding and initiative behind UK Location is from the public sector, and in this phase of development a natural emphasis has been placed on the use and re-use of public sector data by public sector organisations.

- **Moderate use of access control measures and point solutions are common**

  About half of respondents employ technical measures to protect access and use of their data services. These measures include encryption and password access. None use the Government Gateway. This indicates that data providers do not see a common government ICT approach to access control and are turning to ad-hoc and point solutions to satisfy their immediate business needs. A major consequence of this is a lack of interoperability.

- **There is a confusing mix of different approaches to licensing the use of data sets and services**

  There were a total of 18 different licensing approaches from a survey where there were 17 respondents. This illustrates part of the rights management problem.

- **Services with non-open data licences incur cost and resource**

  At the heart of many of the licensing issues raised was the fact that public sector data encompasses both open data and data with other, more restrictive, licences. The latter often requires more stringent access control and rights management which can incur cost.

# 8 USE CASES

Use Cases on the current state of the art for access to location information services and resources were collected during the study and are provided in detail in Annex C. These are presented in 3 categories:

- enabling access to open data;
- accessing data restricted in some way;
- enabling commercial use of data.

At first interpretation, the Use Cases illustrate the variety of ways in which organisations are making their data and resources available, and the variation in the type of controls that are applied. It is possible however to abstract from these varied examples, a degree of commonality in terms of the intended relationship between user and provider/publisher, and these were discussed at length by the Working Group. It was clear to the group that independent of the underlying business driver (protection of IP, revenue collection, data sensitivities) there was significant evidence of the need for publisher/providers to be able to control access to resources based on the identity of their users. These publisher/provider needs inform the first set of the high-level requirements identified below.

What the Use Cases also provide evidence for, however, is the perspective of the user. It is clear that the diversity of the current approaches illustrated is not the ideal situation from this perspective. Building on this, the Working Group also established a set of requirements from this perspective.

Although the Use Cases are presented to a certain extent in a formal notation form that represents a pre-cursor to the definition of functional requirements, the Working Group also used these examples to discuss the user experience and other non-functional requirements. Thus the presentation below is a blend of both the functional and non-functional.

# 9 HIGH LEVEL REQUIREMENTS

UK Location requires an operational framework that enables the management of access control under harmonised licensing terms. The framework will be flexible and enable providers[4] data and services to be licensed under specific licensing models and accessed by common technologies, making it easier for the user to access appropriate and authorised data.

[4] Data Provider – The organisation that creates the data and supplies the data for web publication, along with its metadata.

The requirements below have been drawn from a number of sources including the Online Survey (see Annex B), the use cases (See Annex C), BIWG members experience and views expressed at meetings and Workshops and the input from Bloxstore Ltd.

| ACCESS CONTROL<br>HIGH LEVEL REQUIREMENTS | |
|---|---|
| **The data publisher[5] shall be provided with the ability to:** | |
| 1 | Protect its Intellectual Property and the rights of third parties by making access and/or use dependent on agreement of licences and acknowledgement of any 'information warnings' (such as caveats, inappropriate use, and so on.). |
| 2 | Monitor compliance of licence terms through ability to monitor and report on usage. |
| 3 | Make use dependent on payment of any charge that may be dependent on dataset, usage or other factor set by the data publisher. |
| 4 | Allow access and/or use of certain datasets only to defined users and/or user categories. |
| **The user[6] shall be provided with:** | |
| 5 | A service that allows them to view and download data certain datasets through their agreement to licences prescribed by data publishers and payment of any relevant charges. |
| 6 | The ability to consume multiple data sources through a single sign on. |

[5] Data Publisher - The organisation that publishes the data on the web and supplies data services to data users.
[6] Data User – Anyone who uses the location information published through the UK Location Information Infrastructure

| ACCESS CONTROL<br><br>HIGH LEVEL REQUIREMENTS | |
|---|---|
| **The solution will:** | |
| 7 | Comply with the design principles of the UKL Infrastructure Blueprint where appropriate. |
| 8 | Meet security requirements for protecting sensitive and/or restricted data. |
| 9 | Be based as far as possible on Open Standards. |
| 10 | Adhere to relevant rights management standards, for example basing on OGC reference Model for Geospatial Digital Rights Management (GeoDRM). |
| 11 | Meet customer's needs in terms of ease of use and response times, for example Rights Management functionality must not degrade a data publisher’s existing service. |
| 12 | Allow for use of machine readable licences where a Data Publisher has capability. |
| 13 | Have a governance and management structure which enables devolved administrations and thematic communities to maintain responsibility and control of their parts. |
| 14 | Comply with any standards set at a UK, European or international level. |
| 15 | Capable of being implemented/ deployed relatively quickly to meet initial requirements. |

| RIGHTS MANAGEMENT<br><br>HIGH LEVEL REQUIREMENTS<br><br>(Rights Management High Level Requirements are not being considered at this stage.) | |
|---|---|
| **The data publisher[7] shall be provided with the ability to:** | |
| 16 | Use a simplified, harmonised and automated licensing process. |
| **The user[8] shall be provided with:** | |
| 17 | Details of release conditions and caveats. |
| **The solution will:** | |
| 18 | Be based on a common licensing model which encompasses harmonised and standardised terms. |

# 10 OPTIONS FOR THE FUTURE

As noted in sections 2 and 5 we have focused, in the first instance, on access control for Government to Government transfers. These options apply only to that scenario.

There are many options we could consider in taking this forward with different shades of implementation. However they coalesce into three main types of approach:

- Option 1. Do nothing.
- Option 2. Centralised access control.
- Option 3. Federated access management.

These are detailed below. The advantages and disadvantages of each option are at Annex D.

[7] Data Publisher - The organisation that publishes the data on the web and supplies data services to data users.
[8] Data User – Anyone who uses the location information published through the UK Location Information Infrastructure

## 10.1 Option 1. Do nothing

In this option organisations would administer their own access controls. There would be:

- No guidance.
- No standards.
- No coordination.
- No technical infrastructure from UK Location programme.
- No immediate cost for UKLP.

It is possible that some guidance may come from Europe in due course, which could be considered by UK Location and adopted for UK if considered appropriate.

## 10.2 Option 2. Centralised access control

Under this option one organisation would be responsible for storing data on a central data store and setting up authentication and authorisation to the store (potentially for a group of data providers across a number of organisations). Access would be enabled by enforcing mandatory licences on users accessing the web-based services, according to their allocated authorisation which would be managed on a central system. Various bespoke licence models would be defined. This option would require:

- Central upload, storage and publishing of public sector location data.
- Standardised authentication and authorisation of data.
- Lead organisation to implement.
- Supported by public sector organisations.
- Agreed identifier.
- Clear operating model.
- Rules based licensing framework

## 10.3 Option 3. Federated access control

This option would involve establishing, or using a pre-existing access management federation. This is a collection of organisations that have agreed to build a trust relationship and which interoperate under an agreed set of rules.

The objective would be to make online resources securely available to users who have properly authenticated and which are authorised to access that resource. Member organisations participating in a federation operate Identity Providers (IdP) for their users and any number of Service Providers (SP) to expose their protected resources.

Responsibility for authorisation would generally be devolved to users' home organisations. Authorisation would be established through the secure exchange of information (known as attributes) between the two parties.

A central use case for access management federations is **Single Sign On**[9]. Once a user has successfully provided their credentials with their home organisation, they are authenticated, and thereby gain access to a protected resource within the federation. If a user then wants to access subsequent resources, they are not required to re-authenticate.

It is important to note that it is not uncommon for organisations to outsource installation and running of IdP's, and that larger organisations may provide IdP services for clusters of smaller organisations. If a similar approach was adopted, the federation would consist of individual service providers and centralised hubs which would provide services on behalf of a number of other providers.

# 11 RECOMMENDATION

This position paper considered access control and rights management issues facing UK Location, the state of play in this field within and outside the GI sector both in UK and further afield. Three main options for a solution have been set out, but these are broad generalisations – there are many variations on these options. BIWG has considered how the options meet the high level requirements, the time and resources required to implement them, and their own experience in BIWG members' own organisations.

**Option 1**

Option 1 does not meet the high level requirements. Individual data publishers can implement access control methods, but these will be point solutions and not necessarily interoperable.

- **BIWG recommends that Option 1 should be excluded from further consideration.**

**Options 2 and 3 compared**

Both Options have the potential to meet most if not all the high level requirements. There are, however, some significant differences between them.

The key differences between Options 2 and 3 lie in requirements for quick implementation and a governance structure agreed which will accommodate distributed responsibility and control (Requirements 13 and 15). This reflects the difficulty in gaining political support across the whole UK for a centralised solution and the likelihood that a quick implementation may not be possible. The level of overall governance required for Option 3 need only be for management of the access federation, which is a considerably smaller challenge than Option 2.

The resources required to implement Options 2 and 3 have not been quantified, but there are two points to note. First, the burden of cost for Option 2 is likely to fall on one organisation. Second, for Option 3 costs are likely to be spread more widely among members of the federation, with a smaller cost for the coordination of the federation falling to one organisation.

[9] See Annex A.

In an architectural sense, Option 2 is inflexible – all must use the same centralised system. Option 3 by contrast allows service providers to join the federation in their own right or through a data publisher (as in the case, for example, of the Scottish SDI portal, Spatial NI™ or the MEDIN portal). This arrangement might also extend to centralised publishing of local authority services in due course.

However, there would be greater resource challenges to individual organisations to meet the requirements of option 3.

- **The considered opinion of the BIWG, taking all the above into account, is the recommendation that UK Location progresses further with Option 3 and works towards a federated approach to access control.**

# 12 NEXT STEPS

If the Board agrees that a federated approach to access control should be the general direction of travel, then BIWG proposes the following approach. .

Further scoping work will be required. In terms of priority, authentication will be considered before authorisation, followed by consideration of rights management. As noted earlier, priority will be given to G2G access. A possible longer term roadmap is as follows, although the steps will not necessarily be discrete and sequential:

| Steps | Scope |
|---|---|
| A | Authentication, primarily for G2G. PSMA and other groupings may be used. |
| B | Possible inter-federation authentication with the education sector |
| C | Authorisation infrastructure |
| D | Electronic licence negotiation, machine readable licencing, delegation of authority down service chains |
| E | Full rights management |

As progress is made additional sectors will be brought in but there are dependencies which need to be further researched.

To move forward on A,B and C the next work packages involve:

- further scoping and design work, ,
- engagement with stakeholders, and
- consideration of how to integrate with other cross government initiatives,,

In order to accurately determine the feasibility of the option. Tasks will include:

- Development of an outline architecture to form the basis for further communication with stakeholder groups. It is crucial that key stakeholders and the location user group are involved early on in testing any design principles and proposals.

- Make a strong link in particular to GDS to maintain consistency and avoid duplication of work. Work must also be consistent with European initiatives both location-based and non-location-based.

- Assess the mechanisms and responsibilities for authentication and authorisation and align with ID assurance programme where feasible. A working assumption is that authentication will align with the ID Assurance Programme which introduces a dependency.

- Assess the level and hierarchy of a federated structure to include known and planned 'nodes'

- Development and testing of a more detailed architecture. The working assumption is that we will need to build a SAML-based access federation but consideration needs to be given to how this will work with OGC web services, whether it is sufficient for government IT security levels and how it could interoperate with other ID assurance networks. These assumptions need to be tested.

- Assess technical readiness across the public sector initially to meeting the requirements of a federated structure and implement authorisation. Explore options for authorisation.

- Design of governance and administrative structure.

- Costing for implementing a federated solution and possible funding models.

- Testing of the ability of the private sector to support such a solution.

UK Location will need to determine how this work can be taken forward and resourced.

## 12.1 Is an interim solution required?

It is likely that development of a federated access solution will take time to design, get approved and funded, and developed. One of the high level requirements was for a solution which can be implemented relatively quickly.

It may, therefore, be necessary to consider interim tactical measures, possibly for a small subset of cases and record feasibility against emerging design principles. A solution for the issue of access to services through data.gov.uk Preview might, for example be solved through the use of proxies. On a larger scale, extension of the UKAMF[10] might provide a short term solution for some groups of data providers. Limited scope pilots may also provide a tactical measure and inform the wider developments.

- **BIWG further recommends that consideration is given to tactical measures to meet short term requirements.**

[10] See Annex A.

# ANNEX A. STATE OF PLAY

## Introduction

The UK Location rights management study bridges the gap between current data sharing and business interoperability best practice and the current technical infrastructure. Its purpose was to conduct a “state-of-play” review of current best practice, understand the existing licensing frameworks in place and to provide example use cases to illustrate how these might be practically implemented in a more streamlined and automated way within the current technical infrastructure.

Rights management cuts across political, legal, social and technical aspects and aligning these aspects to arrive at a suitable implementation poses a significant challenge. Our existing political, legal and social frameworks were built for a different world based on managing and trading physical property. Adapting and modifying these frameworks to support managing and sharing intellectual property represents a dramatic cultural change.

The following paragraphs outline some of the current implementations and emerging trends in the field of access control and rights management with reference to some of the standards which support interoperability. The list of standards, implementations and emerging trends are by no means exhaustive in this vast complex technical field.

## Standards and Interoperability.

Authentication and Authorisation. There are a number of standards already in use in the wider IT industry that could be used for authentication and authorisation of geospatial services. Some of these have been implemented already within the use cases detailed in Annex C. The two key authentication protocols in use today are SAML (Security Assertion Markup Language) and Open ID. SAML is XML-based open standard data format for exchanging authentication and authorisation data between parties using single sign on (SSO). OpenID is an open standard that describes how users can be authenticated in a decentralised manner also with a single sign on. There are a number of security issues with OpenID such as phishing, interception attacks, privacy, and a centralised risk to hackers as it opens up access to multiple sites but many of these can be overcome with mandatory security implementation by the developers. SAML has robust security provisions but they must also be mandated consistently at the development stage.

Access Control . At the web service level access control has been successfully trialled by OGC in the Open Web Services 4 initiative. This initiative used GeoXACML (Geospatial eXtensible Access Control Markup Language) which defines a geo-specific extension to the OASIS standard XACML (eXtensible Access Control Markup Language). This standard provides a method for access control which protects access to distributed geographic information. More information can be found on the Open Geospatial consortium (OGC)[11] website and also that of on the Andreas Mattheus[12].

[11] http://www.opengeospatial.org/

[12] http://www.andreas-matheus.de/index.html.en

Snowflake Software[13] has been doing some work on securing web services in the aviation community around location based services and has also carried out a short trial with the GeoXACML Policy engine/decision point extension to XACML, as well as using Kerberos (authentication) and LDAP (authorisation).

Geospatial Digital Rights Management. (GeoDRM). A significant amount of work has been done in the area of data ownership and rights management. This work is of particular interest to the geospatial community as many providers need to control or track access and use of their geospatial resources. The absence of a rights management capability for geospatial resources was identified as a major barrier to the broader adoption of web-based geospatial technologies[14]. In 2004, the OGC Geospatial Digital Rights Management Working Group was established[15] which by 2007 resulted in the development of the OGC abstract specification Geospatial Digital Rights Management Reference Model (GeoDRM RM)[16]. It defines a reference model for Digital Rights Management (DRM) functionality for geospatial resources. Essentially, the reference model provides a framework to automate the transfer of rights to a given user based on the terms specified in an electronic licence.

The GeoDRM Reference Model was implemented as part of the European Commission sponsored ORCHESTRA Project (Open Architecture and Spatial Data Infrastructure for Risk Management)[17]. An overview of the project including the implementation of the DRM capability is provided in the ORCHESTRA Book[18].

Rights expression. One area of interest in terms of rights management is that of MPEG (Moving Picture Experts Group) which provides a multimedia framework which encompasses the rights management issues, referred to as Intellectual Property Management and Protection. MPEG-21 took this further through use of a rights expression language (REL) which has been used by the OGC community under the Geo rights Management Digital Rights Management WG to put forward geoREL (geospatial rights expression language) which was subsequently published as ISO standard 19149. To date there has been no implementation of this standard; it has often been seen as too complex and faces many of the problems that the media industry face with attempting to restrict access to resources.

---

[13] http://www.snowflakesoftware.com/2012/08/secure-location-based-services/

[14] Geo-Digital Rights Management Working Group Charter - https://portal.opengeospatial.org/modules/files/details.php?m=projects&a=view&project_id=82&tab=0&artifact_id=399

[15] The working group has been renamed as the Geo Rights Management (GeoRM) Domain Working Group - http://www.opengeospatial.org/projects/groups/geormdwg

[16] Geospatial Digital Rights Management Reference Model (GeoDRM RM) - http://portal.opengeospatial.org/files/?artifact_id=17802

[17] ORCHESTRA Website - http://www.eu-orchestra.org/

[18] ORCHESTRA Book - http://www.eu-orchestra.org/docs/ORCHESTRA-Book.pdf

Licensing. Within the United Kingdom a practical guide for licensing open data[19] has been developed for organisations that are considering the issues associated with licensing open data.

Creative Commons[20] (CC) licences are becoming one the most used and recognized ways for providers to allow access to data and other resources. They were used extensively as part of the Orchestra Project. The standardised licences selectively release certain rights to the content and permit the copying, reuse, distribution and potentially modification to the original work. Many of the existing licenses such as the Open Government Licence could extend the Creative Commons model to simplify the licences and terms used.

Licence conditions have to meet a provider's business model rather than round the other way so any licensing software would need to be flexible enough to cover all eventualities.

### Implementations – Use cases

A key part of the Rights Management study was the analysis of representative use cases which were selected by the BIWG to document and discuss aspects of data access and use, primarily with the sharing of spatial data sets from the public sector, both within the public sector and more widely within academic, voluntary and private sectors and citizens at large. A summary of these can be found at Annex C.

### Other Implementations

**UK Access Management Federation** (UKAMF) is a Shibboleth-based authentication system used by the academic sector. It may be possible to use this as an interim solution. It must be made clear that no discussion of any sort has taken place between BIWG and JISC and there is no indication that JISC welcome an approach by UK Location. However, there would appear to be some potential benefit in this approach, not least as a means of gaining experience in the public sector of access federations.

**France – IGN** have written their own GeoDRM software which sits above the services on the GeoPortail. The present GeoDRM uses tokens to identify users. In 2012 they will have a new solution without tokens. It should be easier to use with GIS software. It still won't be a standard solution available on the market.

**Germany –** A pilot for access control, based on Shibboleth open source software, has been implemented. Two use cases have been implemented and further use cases, for example access based on machine readable ID cards, are being evaluated. The result of the pilot has shown that access control is technically feasible and they are now looking to roll it out more widely.

[19] Licensing Open Data: A Practical Guide - http://discovery.ac.uk/files/pdf/Licensing_Open_Data_A_Practical_Guide.pdf

[20] Creative Commons – www.creativecommons.org

**Kadaster (NL) –** have implemented an access control solution using Layer7 http://www.layer7tech.com/ – a proprietary software solution apparently from the security sector.

**con terra's software -** Many ESRI customers are using con terra's software, for example Centre for Ecology and Hydrology in the UK[21]. A similar approach is being used in Northern Ireland and the Republic of Ireland. Netherlands and part of Italy are pursing this[22].

**Mapbender –** is open source developed mainly in Germany. It provides a framework for managing spatial data services including authentication and authorisation. It is used by, amongst others, three of the German states and many cities. It allows the service provider to manage the metadata relating to those authorised to use their service on a central hub[23].

**Community Image Data Portal**[24]. This portal is a European Commission Joint Research Project which provides satellite remote sensing data whilst respecting the applicable Intellectual Property Rights (IPR).

A discovery service is available to the public with view and download services available to staff of the Institutions and bodies of the European Union, national administrations and their contractors depending on individual licensing terms and conditions of the respective dataset also for a number of other specific uses under separate licences e.g. development, research and general public. Details of these can be found at the link above.

The portal provides an authentication system which appears to be via a manual registration process which checks the users' rights to access from their credentials sent as part of the registration. There is also a catalogue with a CSW (Catalogue service for the web), a web-based interface for various dissemination services, file-based access (from within the JRC, web mapping interface, ECWPS (Image compression protocol?), WMS and WCS services and a data upload module (from within the JRC).

**Managing Data Licencing**[25]**.** From a presentation given at the FIG Congress 2010 Facing the Challenges – Building the Capacity Sydney, Australia, 11-16 April 2010.

This commercial, proprietary system built by Innogistic in collaboration with Mouchel serves only permitted data extracts as OGC services to authorised users under centrally-defined managed permission levels. There is no detail on how this is done but it states that it "cuts out time consuming administration, significantly reduces the risk of IPR infringement and automatically

[21] See Peter Vodden's paper at INSPIRE Conference 2011 http://inspire.jrc.ec.europa.eu/events/conferences/inspire_2011/presentations/72.pdf

[22] See Bastiaan van Loenenat paper INSPIRE Conference 2010 http://inspire.jrc.ec.europa.eu/events/conferences/inspire_2010/presentations/118_pdf_presentation.pdf

[23] http://www.mapbender.org/What_is_Mapbender

[24] http://cidportal.jrc.ec.europa.eu/home/idp

[25] http://www.fig.net/pub/fig2010/papers/ts04b/ts04b_james_richardson_4746.pdf

provides an audit trail showing which user accessed any given data, when it was accessed, and for which project it was used". They didn't solve the problem of licence variations and complexity as the project appears to have been based on OS data with only one licence. Having said that there is obviously scope to restrict use, monitor usage and protect IPR across a business enterprise.

## Other areas of Interest

ESDIN[26] (**E**uropean **S**patial **D**ata **I**nfrastructure with a Best Practice **N**etwork). This project was concluded in March 2011; the reports can be found at http://www.esdin.eu/project/summary-esdin-project-public-deliverables.

The ESDIN project has initially planned to create and implement a role based rights management model. In the course of the project it became apparent that the desired results form a GeoRM approach would not be achievable. WP 4 covered Data Access and Licensing Policy and there may be some best practice and lessons identified to be taken on board as part of UK Rights Management and compliance with INSPIRE.

EULF (the European Location Framework[27]) as part of the EU funded ISA (Interoperability Solutions for European Public Administrations) programme is taking forward some of this work but there doesn't appear to be any rights management policy or strategy based on the findings of the ESDIN research, although there is agreement within the community that there is a definite requirement for a rights management layer.

## Emerging Trends

Government Digital Strategy[28]

The Government Digital Strategy published in November 2012 contains 14 actions the government will take to become digital by default, including plans for cross government identity assurance, common platform component and improved departmental digital leadership.

Scotland has recently published their Digital Strategy - Scotland's Digital Future: Delivery of Public Services which includes geospatial data in its data sharing objective.

ID Assurance Programme

The Cabinet Office's Government Digital Service has within it the ID Assurance Programme (IDAP) which is putting in place a framework for ID Assurance. The IDAP is seeking to put in place a framework for ID assurance which can be used initially for government services accessed by citizens, but potentially wider. They seem themselves as:

[26] http://www.esdin.eu/

[27] http://ec.europa.eu/isa/actions/02-interoperability-architecture/2-13action_en.htm

[28] http://publications.cabinetoffice.gov.uk/digital/strategy/

- setting standards,
- assuring the ID Providers (IDPs) who will come from the private sector,
- encouraging government depts providing services to use the framework
- and probably running a hub for a few years until a critical mass has been achieved and other pricing models are viable.

GDS recently announced that it will be joining the Open Identity Exchange (OIX). OIX is based on an Open Identity Trust Framework model. It utilises the technologies of OpenID and Information cards (SAML implementation?). These are described briefly under Standards and Interoperability above. IDAP will use OIX to enable organisations to participate in the development of the initiative and enable engagement with partners on projects that experiment with solutions to real world problems.

Trends in Cloud Computing

Cloud computing is a potential area for the future in terms of Data as a Service (DaaS) where the product or data can be provided on demand but there are still real concerns with security. 'Consider that 27% of respondents to the *InformationWeek* 2012 Cloud Security and Risk Survey say they have no plans to use public cloud services. And 48% of those respondents say their primary reason for not doing so is related to security, including fears of leaks of customer and proprietary data"[29] Some security solutions can also be costly negating one of the benefits. Currently the focus for new business models appears to be on the financial aspects with changes to corporate pricing models bringing together volume based and data type charging policies which provide a fine grained model that meets the needs of provider and user.

New business models

One of the business models that appear to have had some success over the past year or so is 'cheap and easy'. Make product easy to download at a low price in opposition to the complexity of pirated copies (conversion and application download issues) quality and search issue. This model identifies with the media industry which is rife with piracy. Some believe that high levels of piracy are due to the cost and complexity of the product. This doesn't relate closely to the issues within the geospatial community as the protection of IPR is required even when data is freely available. Media DRM was introduced to restrict reuse whereas the geospatial information community encourages reuse.

Another model is that of a cloud based system where all the required data is held centrally and then accessed on a pay monthly or annual basis (This could be translated to permission based access based on licenses). In the geospatial environment this would mean that the applications would need to be remotely hosted in the cloud also to stop download of data to system applications which could then be copied and transferred any number of times disregarding the license. Accessing and processing on the cloud would allow any derived data to be made available through the same permission based system as original access depending on user privileges. Geospatial data processing/caching is already managed in this way by several geospatial companies.

[29] http://reports.informationweek.com/abstract/5/8978/Cloud-Computing/research-cloud-security-verify-don-t-trust.html?cid=pub_analyt_iwk_20120820

The banking industry has experienced the growth of mobile web usage focused on simple straightforward transactions, and there appears no reason why this shouldn't spread to the geospatial community if access to data becomes more straightforward and the rights management and licensing less complex.

Web based services have become ubiquitous with users expecting to be able to access the same information on their mobiles and tablets as they do on their desktops. Access to geospatial resources is sure to follow suit as mobile GIS applications are developed to make use of geospatial web services. The introduction of any access control and rights management solutions should be cognisant of this so as the Government Digital Strategy takes shape transition to mobile computing is possible.

## Conclusion

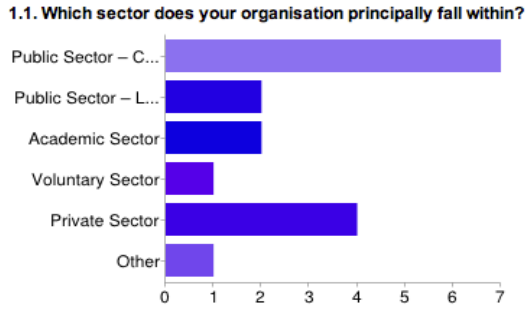
The study shows that there is a highly complex landscape of different approaches and technologies currently in use within the UK Location community and beyond into Europe. This is fragmenting and limiting the value that can be delivered to stakeholders. Not all the answers are in the geospatial community as many implementations of access control and rights management in the commercial world of banking, entertainment and communications offer solutions to many of the geospatial issues. Any solution would need to extract best practice from a number of different implementations in order to provide the necessary strategy and policy to the UK Location Community.

# ANNEX B: SUMMARY OF ONLINE SURVEY

## 12.1.1 B1 Overall

- 17 Responses
- Mix of public, private and academic sector with one voluntary
- Senior level representation.

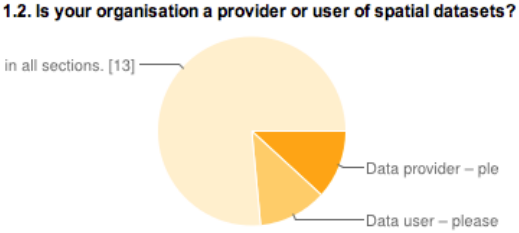
### *B1.1. Which sector does your organisation principally fall within?*




| | | |
|---|---|---|
| Public Sector – Central Government | 7 | 41% |
| Public Sector – Local Government | 2 | 12% |
| Academic Sector | 2 | 12% |
| Voluntary Sector | 1 | 6% |
| Private Sector | 4 | 24% |
| Other | 1 | 6% |

- Majority of respondents are public sector, with representation from the private, academic and voluntary sectors

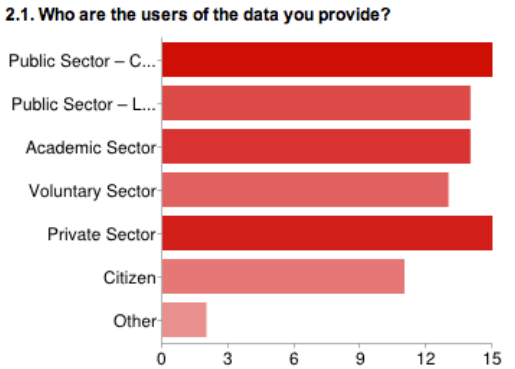
### *B1.2. Is your organisation a provider or user of spatial datasets?*




| | | |
|---|---|---|
| Data provider – please fill in sections 2 and 4 | 2 | 12% |
| Data user – please fill in sections 3 and 4 | 2 | 12% |
| Both – please fill in all sections. | 13 | 76% |

- Three quarters of respondents are both providers and users of spatial datasets.
- Remaining respondents have provided input from a data provider or data user perspective.

### *B2.1. Who are the users of the data you provide?*

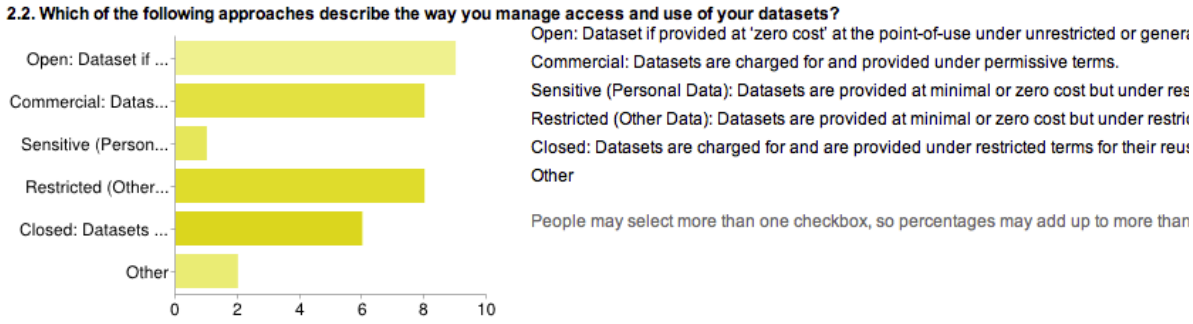



| | | |
|---|---|---|
| Public Sector – Central Government | 15 | 100% |
| Public Sector – Local Government | 14 | 93% |
| Academic Sector | 14 | 93% |
| Voluntary Sector | 13 | 87% |
| Private Sector | 15 | 100% |
| Citizen | 11 | 73% |
| Other | 2 | 13% |

People may select more than one checkbox, so percentages may add up to more than 100%.

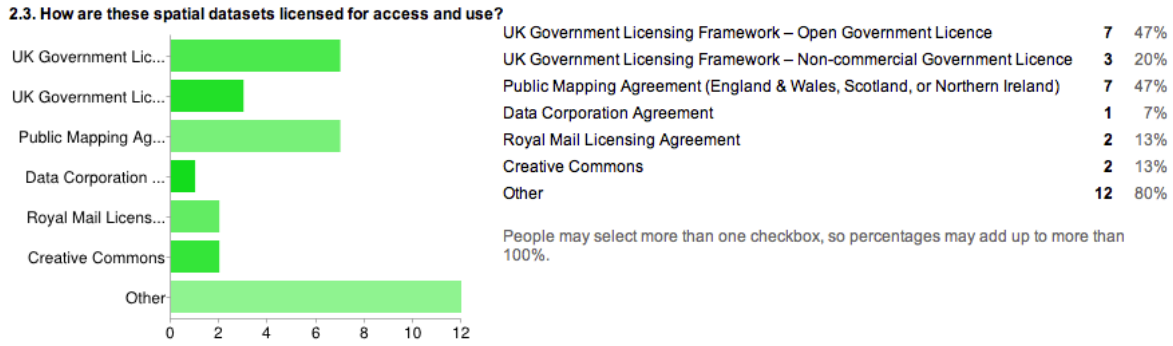
- Data providers' data is used broadly across the different sectors.
- Others are “Commercial Sector” and “European Research Partners”

### *B2.2. Which of the following approaches describe the way you manage access and use of your datasets?*




- The majority of datasets in the survey are not open.

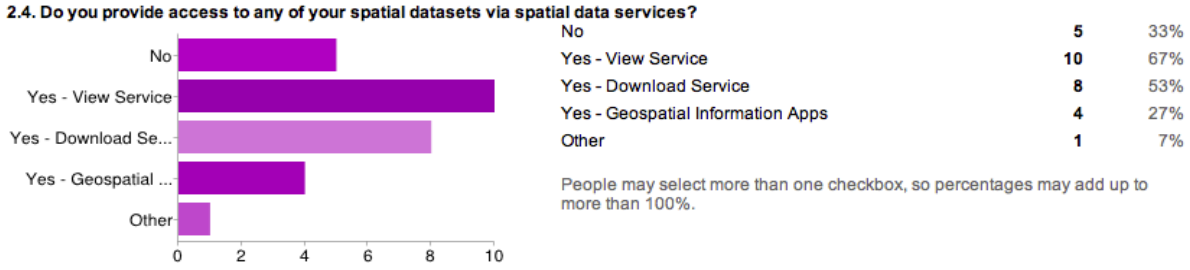
### *B2.3. How are these spatial datasets licensed for access and use?*




Others included:

- Our own licence terms – 3 respondents
- Local Government owned license (see Worcestershire)
- Data agreements between RSPB and end user
- Occasionally we use OS sub-contracts for sub-contractors
- SeaZone drafted EULA
- Northern Ireland
- Various other OS licenses.

### *B2.4. Do you provide access to any of your spatial datasets via spatial data services?*




- Of the 15 data providers, 10 provide at least a View Service

### *B2.5. What technical measures do you use to protect access and use of your datasets and services?*

- None – 7 respondents
- Data protected via licence only – 2 respondents
- Password protected web services - 5 respondents

Other approaches:

- Restrict access to certain functionality, only provide subsets of data, some data not made available.
- Encryption, role-based access and individual access controls.
- OS web mapping license turning off get feature service, GI app which only allows the graphic display of data with watermark, request for data and download after permission for data is given.

### *B2.6. Do you make use of government initiatives in this area such as the Government Gateway and Government ICT Strategy to provide your spatial datasets?*

- No/no response – 13 respondents.
- Data.gov.uk – 3 respondents.
- Integration into GeoPlace for address and street gazetteers.

### *B2.7. As a provider of spatial datasets what changes to access and use would make your life easier?*

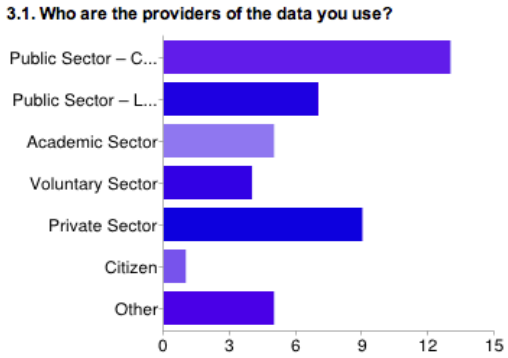
- Being easily able to share derived data, particularly those derived from Ordnance Survey datasets – 6 respondents.
- It would be easier if we were able to publish some data more openly – 4 respondents.
- Consistency of approach to access of public data across all Departments, agencies and trading funds – 3 respondents

“If as a nation we are serious about making data open then organisations should be paid from central government to create the data and then it can be freely available to all. This would need to be a full payment and not a token amount”.

“We do all have issues with those derived datasets we have created using non - PSMA OS data (i.e. OS MasterMap) being subject to such high OS royalties that we are in effect prevented from licensing for commercial use”.

“Simplified PSMA licensing terms. True streamlining of exemption to derived data categories instead of applying for individual datasets per authority. Initial estimates suggests that local authorities would have to seek exemption for over 12000 individual datasets under INSPIRE themes if a more streamlined approach is not taken”.

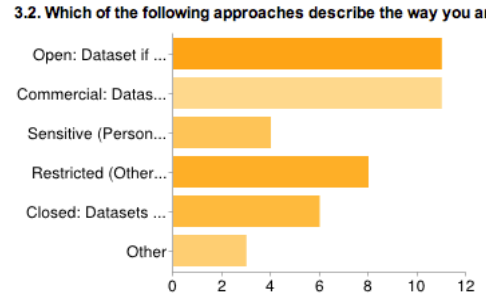
### *B3.1. Who are the providers of the data you use?*




| | | |
|---|---|---|
| Public Sector – Central Government | 13 | 76% |
| Public Sector – Local Government | 7 | 41% |
| Academic Sector | 5 | 29% |
| Voluntary Sector | 4 | 24% |
| Private Sector | 9 | 53% |
| Citizen | 1 | 6% |
| Other | 5 | 29% |

People may select more than one checkbox, so percentages may add up to more than 100%.

### *B3.2. Which of the following approaches describe the way you are required to access and use data?*



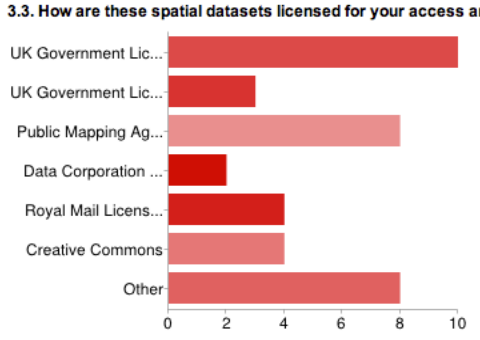

Open: Dataset if provided at 'zero cost' at the point-of-use under unrestricted or generally permis
Commercial: Datasets are charged for and provided under permissive terms.
Sensitive (Personal Data): Datasets are provided at minimal or zero cost but under restricted terr
Restricted (Other Data): Datasets are provided at minimal or zero cost but under restricted terms
Closed: Datasets are charged for and are provided under restricted terms for their reuse.
Other

People may select more than one checkbox, so percentages may add up to more than 100%.

Others include:

- Individual bilateral arrangements.
- LA data through GeoPlace.

### *B3.3. How are these spatial datasets licensed for your access and use?*




| | | |
|---|---|---|
| UK Government Licensing Framework – Open Government Licence | 10 | 59% |
| UK Government Licensing Framework – Non-commercial Government Licence | 3 | 18% |
| Public Mapping Agreement (England & Wales, Scotland, or Northern Ireland) | 8 | 47% |
| Data Corporation Agreement | 2 | 12% |
| Royal Mail Licensing Agreement | 4 | 24% |
| Creative Commons | 4 | 24% |
| Other | 8 | 47% |

People may select more than one checkbox, so percentages may add up to more than 100%.

Others includes:

- Google Maps
- Individual bilateral arrangements
- Re-use of Public Sector Information – 2 respondents
- Chest for Academic use

### *B3.4. As a user of spatial datasets what changes to access and use would make your life easier?*

- Consistency across trading funds re. their licensing models – 3 respondent.
- Standard (and straightforward) guidance on the onward use of 3rd party data in commercial products – 3 respondents.
- Ability to use Royal Mail field within products (e.g. Addressing) without limitations – 2 respondents.
- None – 2 respondent.

“Simplified licensing terms applied by organisations, Central rights management software especially for PSMA licensing to manage licensing centrally”.

“Most of the changes are beginning to happen - increased availability of data via download from web services and more open licensing”.

“There have been changes recently that have improved access to spatial data. OK for now”.

### *B4.1. Do you have specific lessons learned from managing access and use of datasets, which would be of benefit to others?*

- We have found that the main challenge is not in approach to data licensing, but more in actually getting organisations to deploy resources to manage their data properly and make their data available.
- It is not really practical to extend the methods we used for managing and protecting rights in the last century to the service---based environment we now find ourselves in. We need a paradigm shift and to use new methods.
- Many people don't read the terms and conditions and the 'non-commercial' restriction is being ignored.
- It can still be frustrating gaining permissions to use public sector data in a way that meets the requirements of customers who see electronic transmission as the only way forward in 2012
- Dealing with warranties and limitations of liabilities is a fundamental part of any licensing arrangements that cannot be dealt with using standard "off the shelf" licence templates, such as OGL or Creative Commons.
- Natural England Licensing terms are useful as the responsibility of using the right licensing term is with the user rather than the organisation having to administer it.

### *B4.2. What recommendations can you make for building an integrated and interoperable solution for rights management within UK Location?*

- More harmonised licensing terms - keep it simple to understand and implement.

- We need to start with the low hanging fruit - simple access management and the move on to use management. Government needs to involve itself with standards not implementation, and let the market take care of the implementation.

- A new expensive rights management system is likely to become a white elephant before it recovers its costs. The costs of the RMS MUST be born only by the organisations which insist on charging and /or restricting use of their data. Investment in development of open source products such as Geoserver would enable better rights management.

### *B4.3. Would you be willing to contribute a use case to the UKL Rights Management Study – where we might benefit from improved rights management?*

- The main area we find rights management can be a problem is not in the access to raw or source data, but in how to deal with higher level products that have been compiled from a number of sources - where there may be a number of different use licences to pull together

- For us, it is all about access to key OS products (OS vector map local and aerial imagery) on a national scale which help us do our day to day business. It means we can act fast and early, helping developers and Government ensure development is sustainable and rapid.

- Often our site managers work together with the emergency services to deal with outbreaks of fire (eg on moorland), avian flu or other emergencies. We need the same mapping as the emergency services to work to best effect together.

### *B4.4. Do you have an example best practice or technical implementation on access and use that would be of wider interest to the UK Location community?*

- We use the National Biodiversity Network which may provide a suitable example?

- Possibly something on delivering data via Smartphone devices. BGS has an iPhone app ('iGeology'), and is developing a second ('MySoil') app with the Centre of Ecology and Hydrology. The first has been very popular, and we're hoping the Mysoil app will follow on these lines.

- "The SeaZone EULA is an example of making best use of UK Government data, and integrating the terms of use into a single end user agreement.

- The seaZone HydroSpatial One product comprises data from various UK Public Sector agencies including: UKHO, BGS, Conservation Agencies etc, integrated by the private sector (SeaZone) and supplied back to both UK Public and Private Sector."

- Indicator Portal

### *B4.5 If you are able to provide a use case, how would you classify it on the following grid?*

| From: / To: | Public Sector (Central) | Public Sector (Local) | Academic Sector | Voluntary Sector | Private Sector | Citizen |
|---|---|---|---|---|---|---|
| Citizen | | 1 | | 1 | | |
| Private Sector | 1 | 1 | | | 1 | |
| Voluntary Sector | 1 | 1 | 1 | | 1 | 1 |
| Academic Sector | | | | 1 | | |
| Public Sector | 5 | 1 | 2 | | | |

Note: Numbers indicate number of respondents who offered use cases in each area

### *B4.6. Any other comments or suggestions, which might help us with our work?*

- I am pleased that UK Location is looking for ways to improve access and use of location data.
- At the moment I know of nobody and no organisation that would come through UKLP when looking for spatial data. It is just possible that we are beginning to see people using the data.gov.uk site for this purpose but I will need convincing. So, if UKLP is to set up a RMS it will need to have users directed to it by the data providers themselves (where users currently go for their data direct) and those same providers will need to be constrained from offering a similar service (or forced to use UKLP themselves).

# ANNEX C: USE CASES

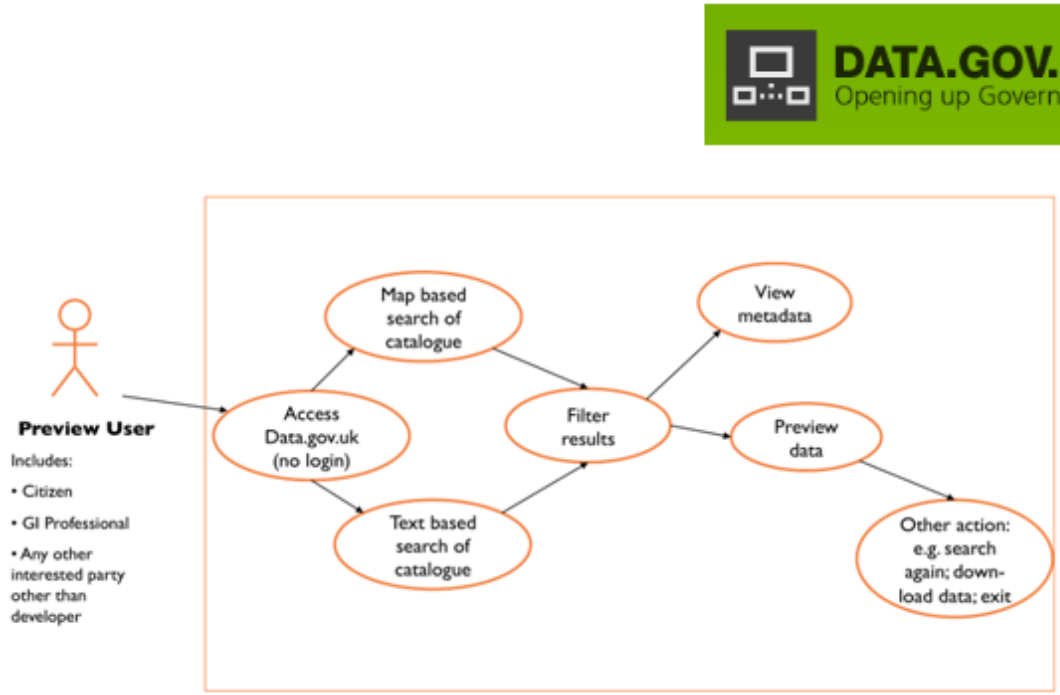
This Annex is sets out a number of use cases gathered during the study by Bloxstore. They are divided into three sets; those relating to enabling access to open data, those relating to access to data restricted in some way, and those enabling commercial use of the data.

## Set 1. Enabling access to open data

This set of use cases are about improving access to open data or making other data accessible in a more open way.

### *C1.1 Preview function of data.gov.uk*

Enables a user to visually inspect, and evaluate against background mapping (and other datasets), those spatial data sets that they are interested as a result of searching the data.gov.uk catalogue.

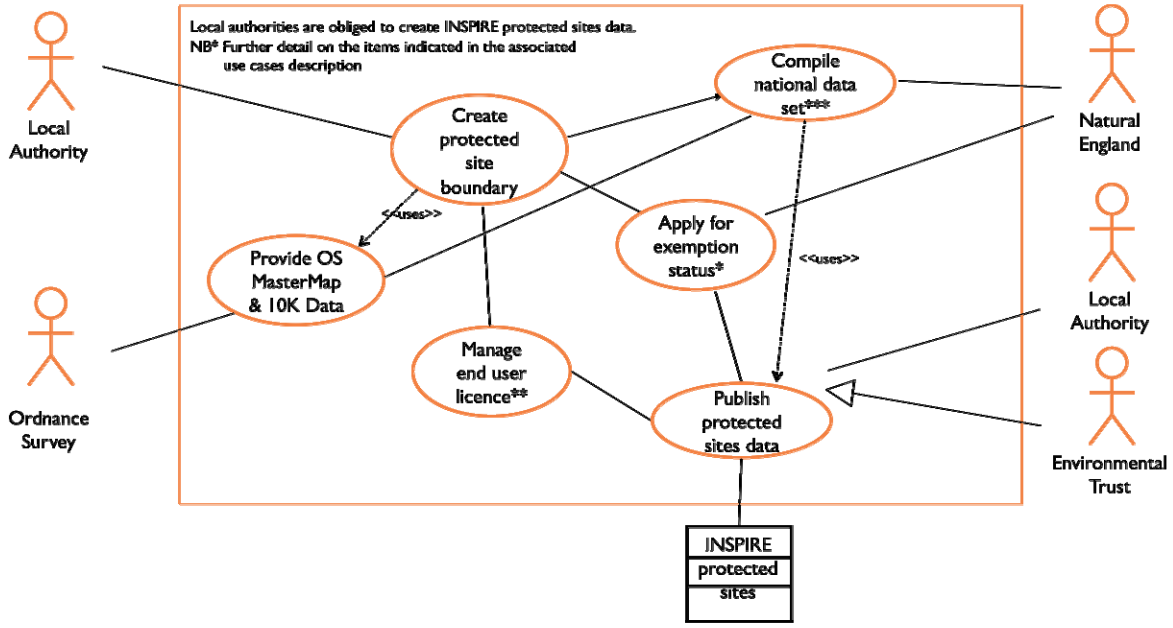



There is no login to data.gov.uk for searching the catalogue or previewing UKL datasets. Data Publishers datasets displayed in Preview must conform to UK Location Operational Guidance in particular the URL must be directly accessible.

### *C1.2 Local Nature Reserves*

To meet INSPIRE obligations there are three options for local authorities to publish this data:

1. LAs apply for exemption of the datasets to provide it as open data under OGL.
2. They license the data under an OS End User license (EUL).
3. They pass the dataset to Natural England or Environmental Trust for publishing.



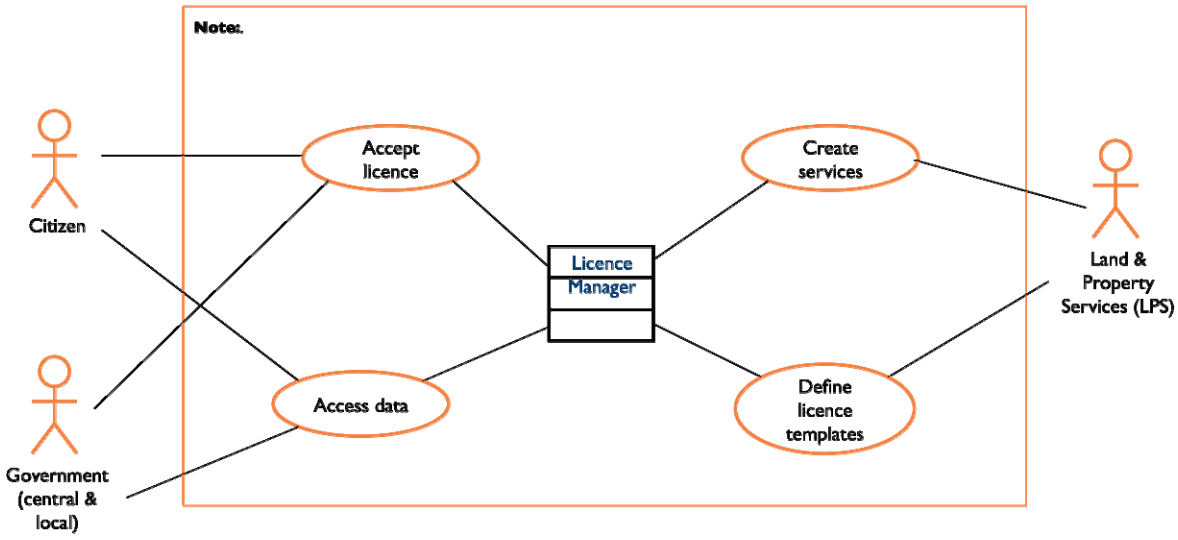

If local authorities wish to publish protected sites as open data they have to individually apply to OS for exemption status for data derived from OS MasterMap or 1:10K Topographic data. However, a number of authorities publish the data as open data regardless while others charge for the data to cover minimal cost.

LAs issue OS EUL to individual applicants which have to be tailored to the specific purpose of use. A generic EUL covering all protected site data is not sufficient

To meet INSPIRE compliance LA publish local nature reserves through Natural England. Natural England publish the data free for non-commercial use but has been granted open data use for the data, However, it needs to seek permission from local authority to make the data openly available. Some LAs refer to the Environmental Trust for access to the data. Under EIR a local authority has to grant access to the data on site for inspection.

### *C1.3 Non Commercial INSPIRE licence*

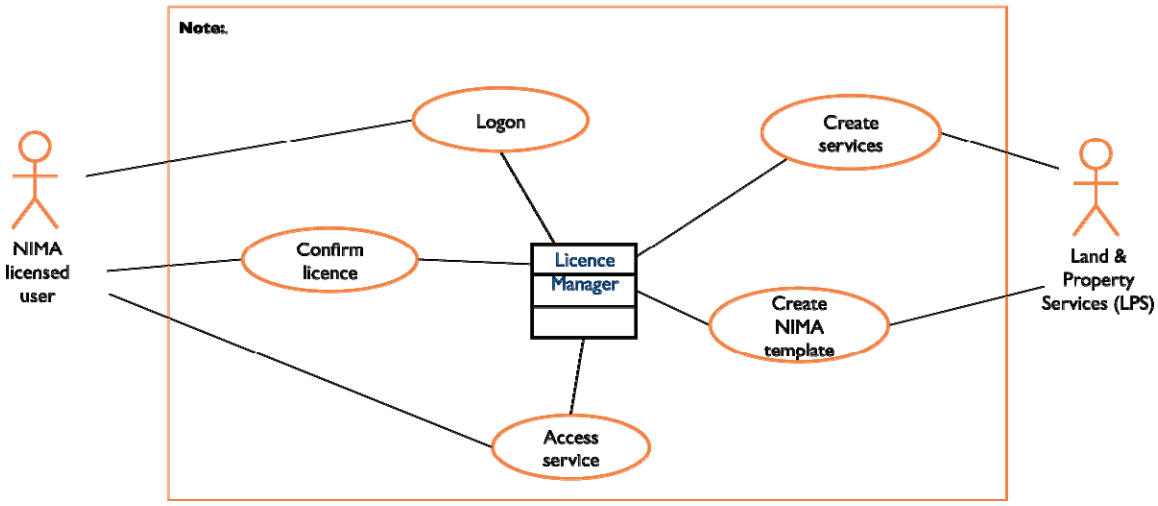
In order to facilitate access to Northern Ireland's INSPIRE datasets, Land & Property Services IPR team developed a click acceptance Non Commercial INSPIRE licence for the use of all NI INSPIRE data (apart from LPS data as they have delegated authority to charge for their data and operate a commercial business model). The click acceptance licence, created through the use of con terra licence manager software facilitates access to INSPIRE view and download data services via Spatial NI™




Prior to the implementation of the Non Commercial INSPIRE licence in many cases access was via a number of hard copy individual licences created by each of the different government suppliers which had to be signed. Following the creation of the new licence in hand with the technology to enable click licensing access is both widening and opening up web access and it's simpler to use.

### *C1.4 Facilitating upstream agreements*

Land & Property Services have a framework agreement in place for access to a suite of core underlying mapping data for Northern Ireland. All departments are signed up to this agreement which gives free use at the point of access through top level financing from each department. In order to give access through web services to this data a licensing system was necessary which authenticated users to determine they are government and the allows them access following a click reminder of the constraints of their NI Mapping Agreement licence.

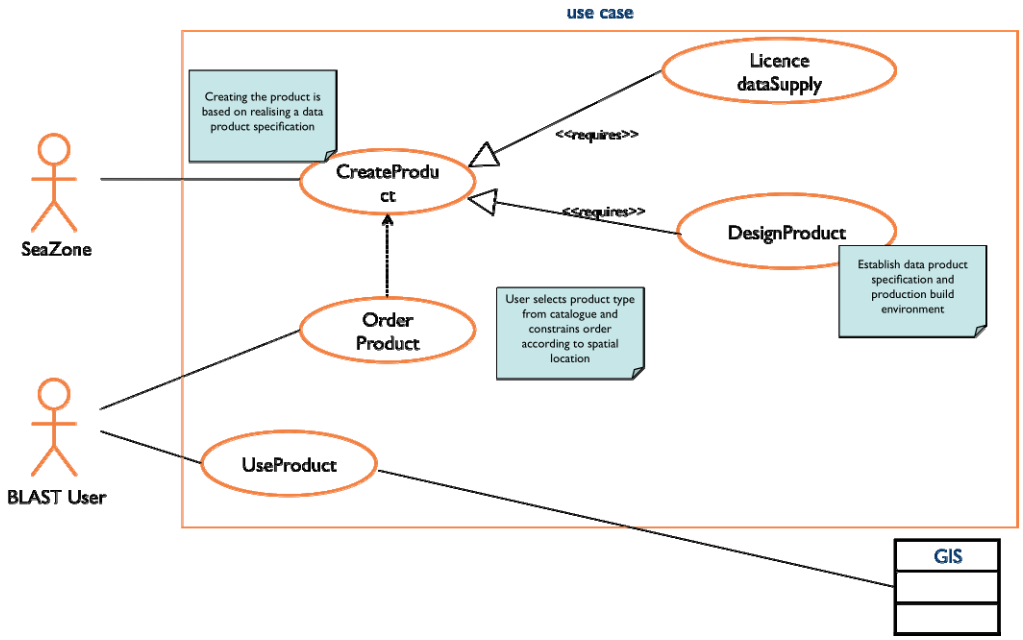



Access is currently via a licence which is physically signed at departmental level which prompts the delivery of an encrypted hard drive of data. Delivery of this data via web services shall lessen the burden of both LPS supplying the data and the user hosting and serving the data within their organisation.

## *C1.5 Seazone - Blast Project*

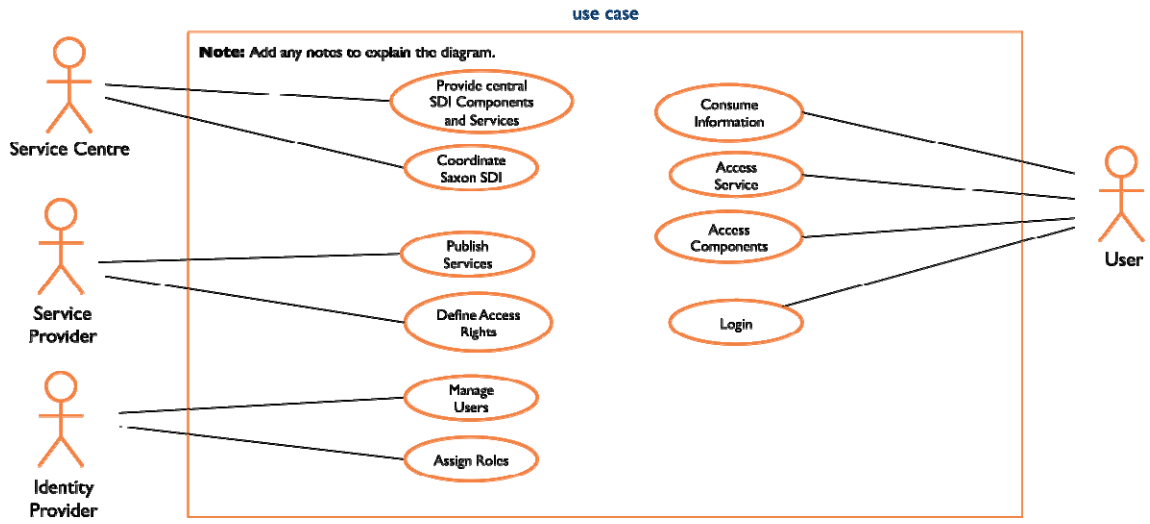
SeaZone has previously established license terms with all the data providers, based on the re-use licence terms adopted by national hydrographic offices. These are broadly consistent. In addition as this was a research project, a research agreement allowed the data to be exchanged for use on the project.

At this time there is no mechanism to re-licence the specific project deliverables post project.



## *C1.6 Saxony Distributed and Federated Security and Licensing*

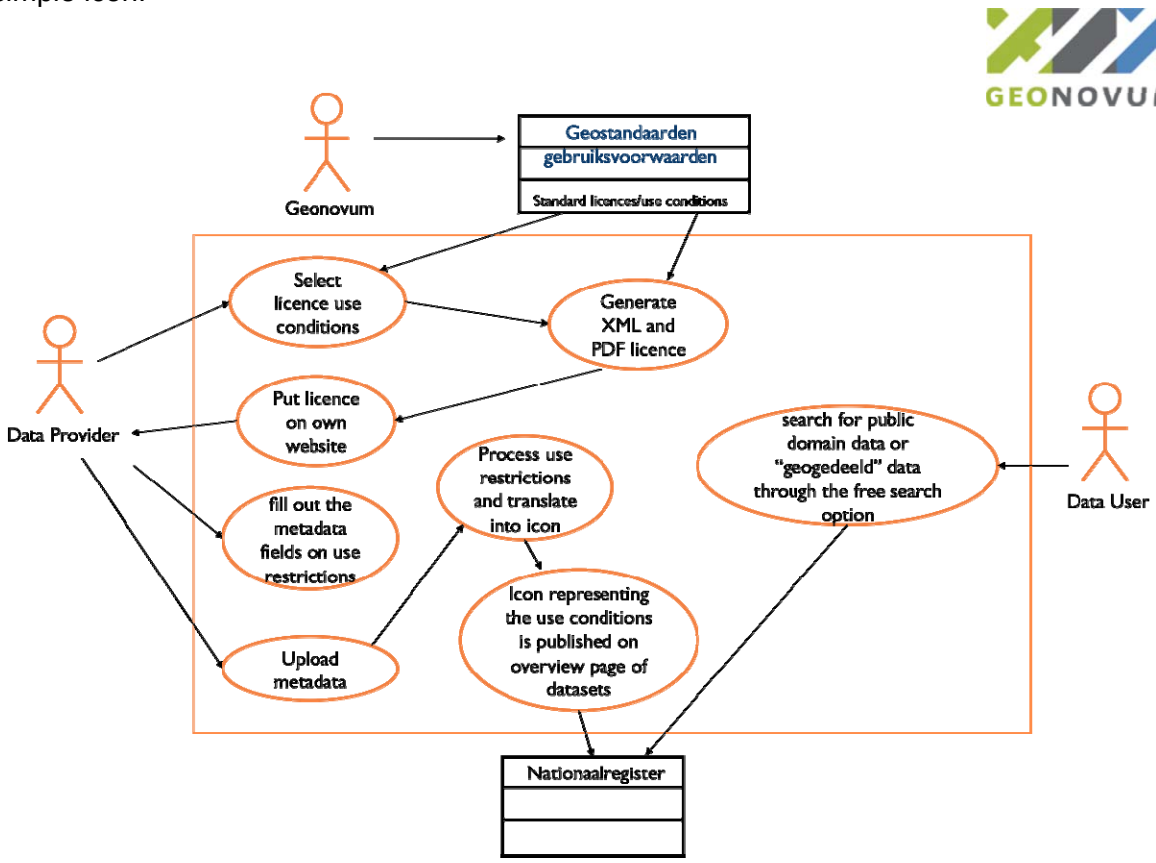
Saxony security and licensing allows restricted access to INSPIRE services, OGC services as well as portal components and functions based on user identity and support federated user management.




Con terra sdi.suite securityManager is used for access control. Currently, there is no explicit (electronic) agreement on terms of use but this is planned in the future. Access permissions are assigned based on user roles within a federated user management.

## *C1.7 Geonovum and GeoGedeeld*

As part of the INSPIRE implementation program, Geonovum facilitates the creation, transparency and consistency of licences and use conditions for public sector geographic data. A use condition generator with standard licences/use conditions has been developed, an implementation guideline is provided to data providers, and in the central register the use conditions are represented by a simple icon.



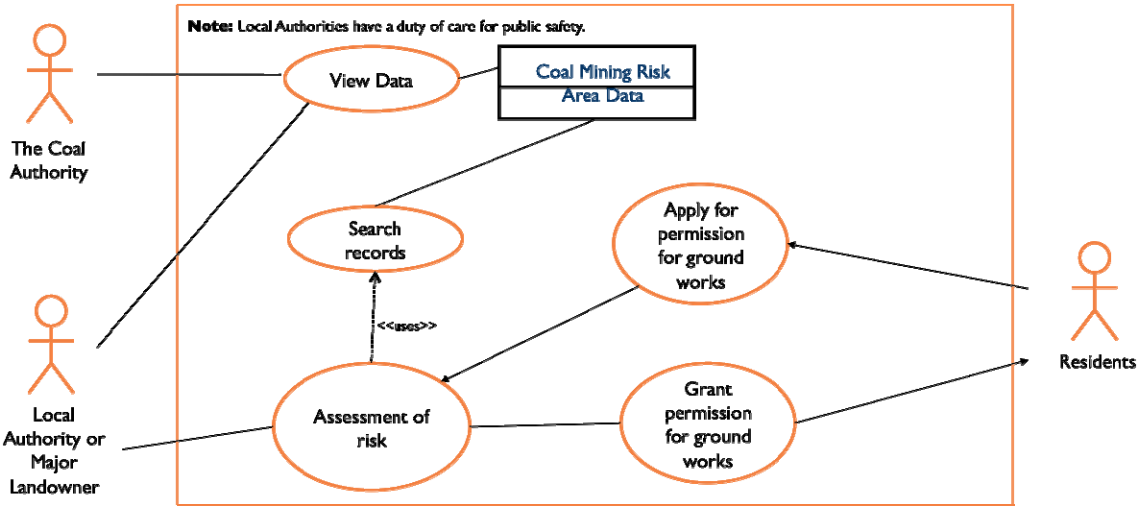

Geonovum does not control access/use but rather enables data providers to manage use based on standardised terms. Licensing terms for use are multi-fold standardised conditions. It is up to the data provider to select the conditions that apply to its datasets

## Set 2. Enabling access to restricted data=

### *C2.1 Coal Authority Case Study*

The Coal Authority is the government body tasked with protecting the public and the environment in coal mining areas; managing the effects of past coal mining in order to promote public safety and safeguard the landscape. This case study aimed to improve the public's understanding of the risks of legacy coal mining to help improve safety and to make it easier to live with the legacy by sharing information and discussing legacy risks with Local Authorities and other major landowners, engaging them in active risk management measures and embarking on an inspection programme of 170,000 mine entries across Great Britain.

The COAL AUTHORITY

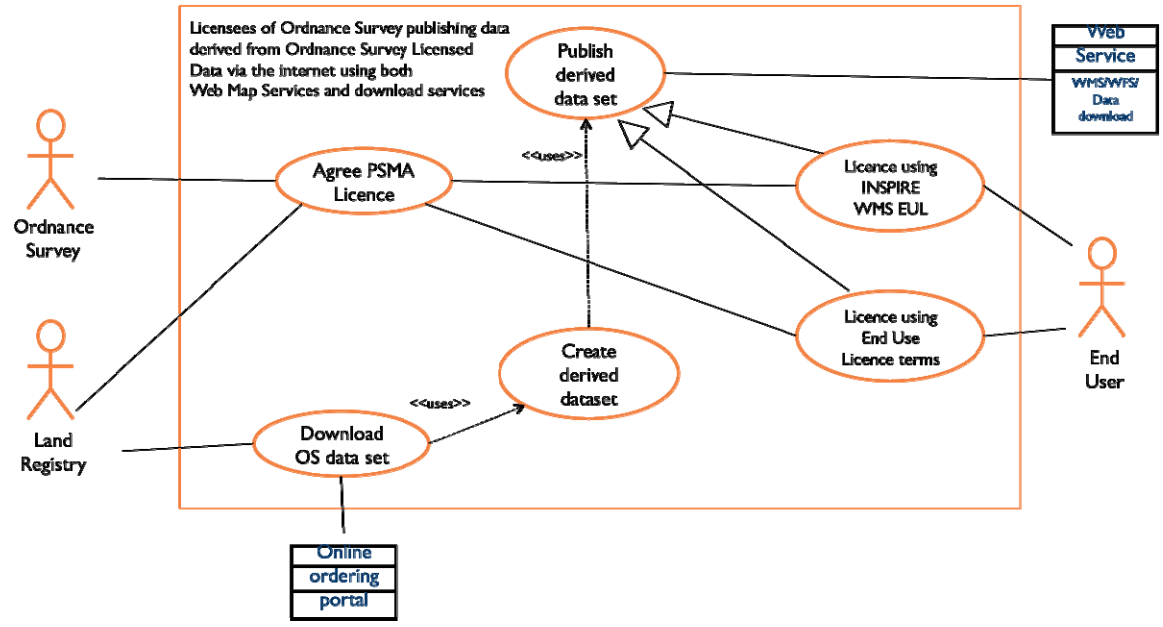



Access to coal mining data had been traditionally through the mining reports service or by viewing abandonment plans on site.

Data is now proactively shared with Local Authorities under a simple memorandum of understanding or made available through a WMS feed or viewed through an interactive GIS, free to use under the Open Government Non Commercial Use license. However, access is restricted due to the sensitivity of the data.

## *C2.2 User Derived Data publishing via web services*

Licensees of Ordnance Survey (within the Public Sector for example Land Registry) publishing data derived from Ordnance Survey Licensed Data via the internet using both Web Map Services and download services. (they may include Web Feature Services as well as more straightforward standard dataset download)

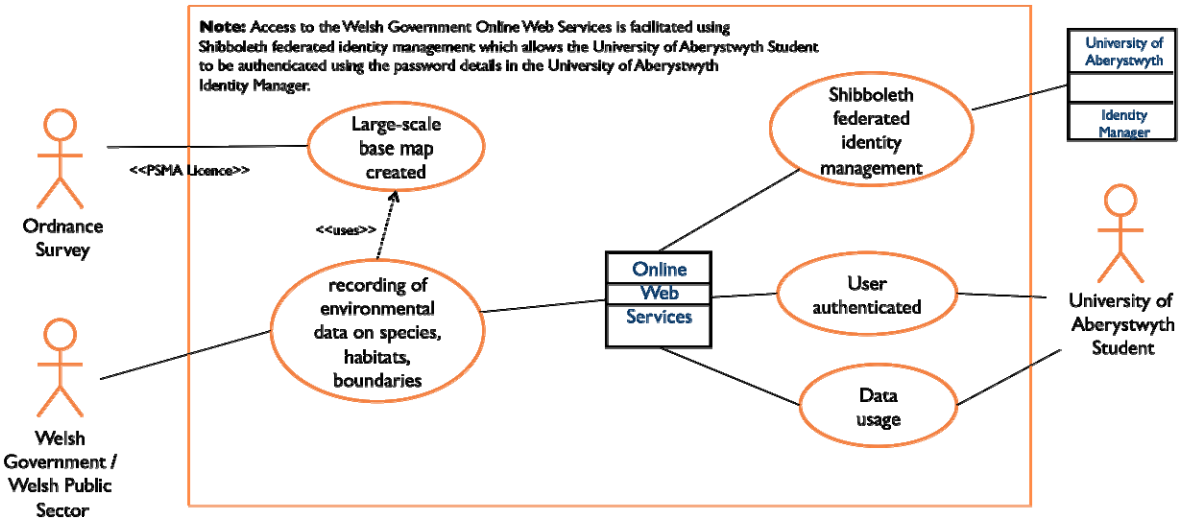



Access to data by licensees and end users is controlled by Licence terms only.
The PSMA member licence details the rights conveyed from Ordnance Survey to the Licensee including the right to publish and share data under End User Licence arrangements.

## *C2.3 Welsh Government - Shibboleth Implementation*

Access to spatial data services for a community of known users, using an established federated identity management service.

Llywodraeth Cymru
Welsh Government

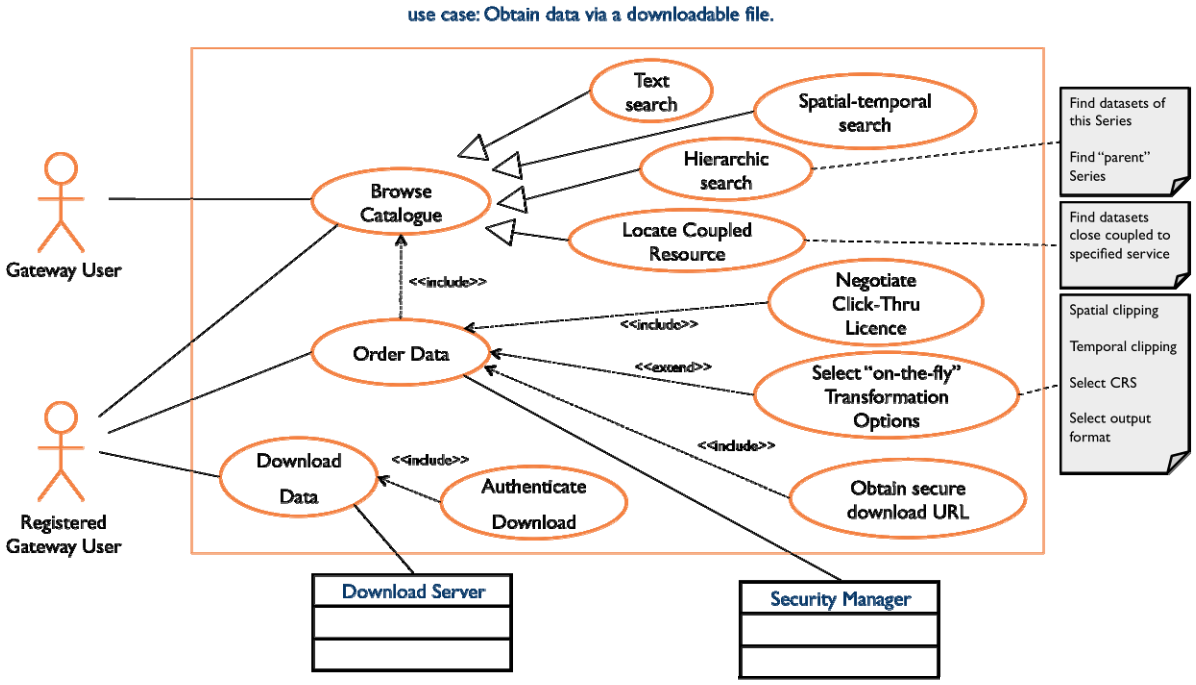



The input data for the services is derived from Ordnance Survey information provided under the terms of the Public Sector Mapping Agreement.

The PSMA licence sets out various licensing mechanisms for derived data, including potential exemption from the need for licences. A common condition of these licences is a known end-user, who is either a PSMA member, or otherwise affirms that they hold a licence for the same underlying Ordnance Survey datasets.

## C2.4 CEH Information Gateway – File Access

Access is managed by a security application using an aggregator (CROWD) to homogenise user credentials from various sources.



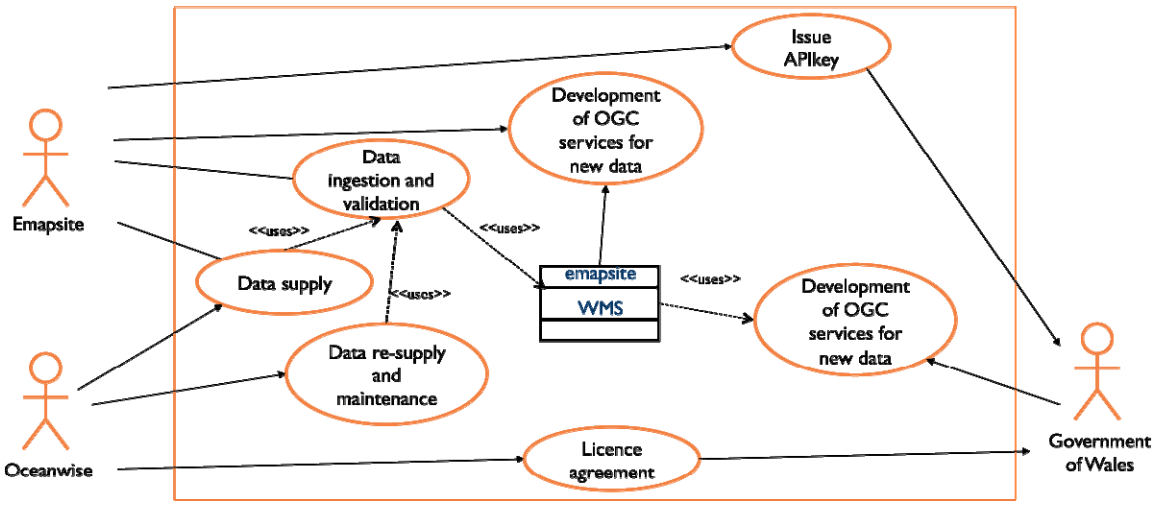

Licensing terms are offered and agreed per data resource (often an organisation default, but may be custom), and may be different for internal/external users.

The download URL is time-limited, and involves a key known only to the Registered User.

## Set 3. Enabling commercial use of data

### *C3.1 Contractor Licensing through Emapsite*

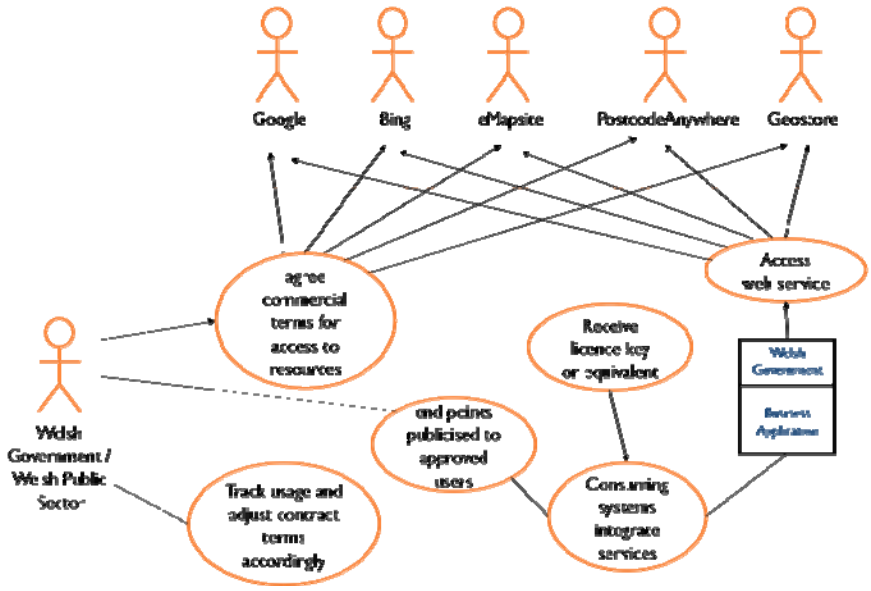
To provide a seamless service for data under licence to the public sector to citizens and internal business users alike ensuring currency of content, flexibility of visualisation, use of standards, licence compliance and appropriate access control.




Access is controlled through ISO9001 accredited processes, suppliers licensing terms are used and access is managed using APIkey, logging, log shipping, analytics and reporting.

## *C3.2 Access Control Regime (Welsh Government)*

It is increasingly the case that the spatial information resources needed to support systems and business processes in Welsh Government can be provided most cost-efficiently (i.e. outsourced) to commercial providers. These providers offer economies of scale, service breadth, quality and resilience that cannot be achieved through the use of Welsh Governments own internal resources. Primarily transactional in nature, these resources utilise a variety of web protocols and approaches (SOAP, REST). There is a similar diversity in the approaches adopted to control access to these resources.

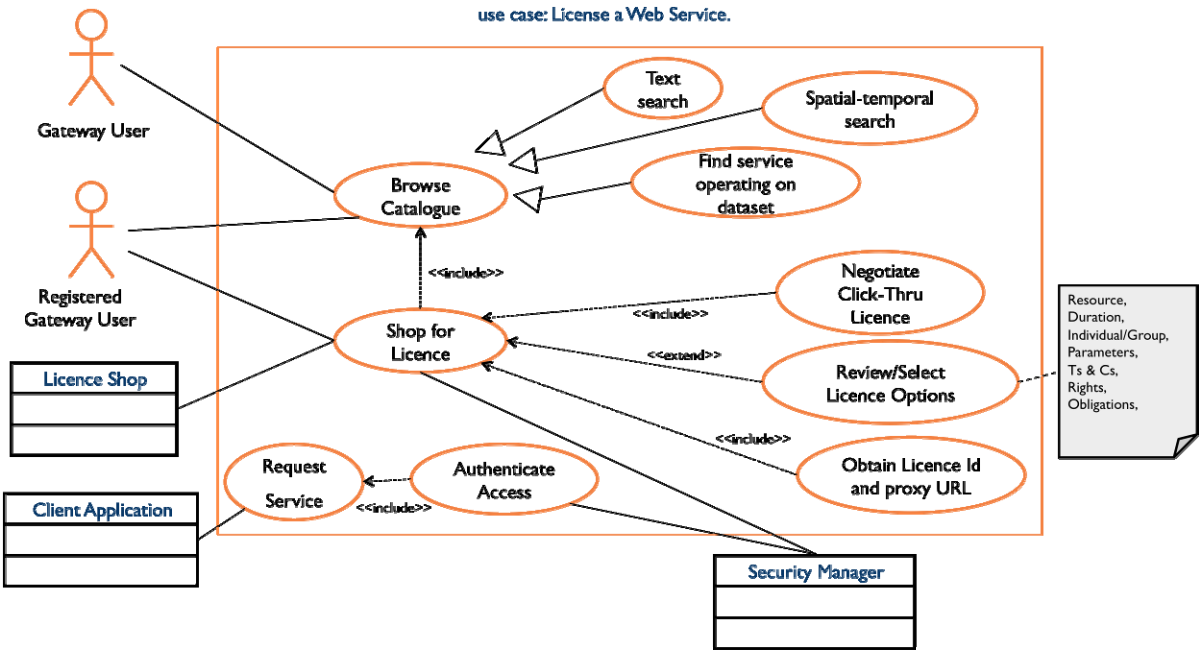



Access and use is managed using the following techniques:

- Service contract, with fee payment and commercial structure negotiated by Welsh Government.
- Service end points publicised to approved users within Welsh Government and the wider Welsh public sector.
- Consuming systems integrate services, including protection mechanisms. These include Welsh-Government bespoke service end-points, unprotected but obfuscated end-points and – most commonly – the inclusion of a long-string API-key in the service request.
- Ongoing monitoring of usage and uptake through online dashboards, commercial and contractual reporting arrangements.

### *C3.3 CEH Information Gateway – Licensed Services*

Obtain data via a downloadable file.




Access is managed by a security application linked to a License Shop.

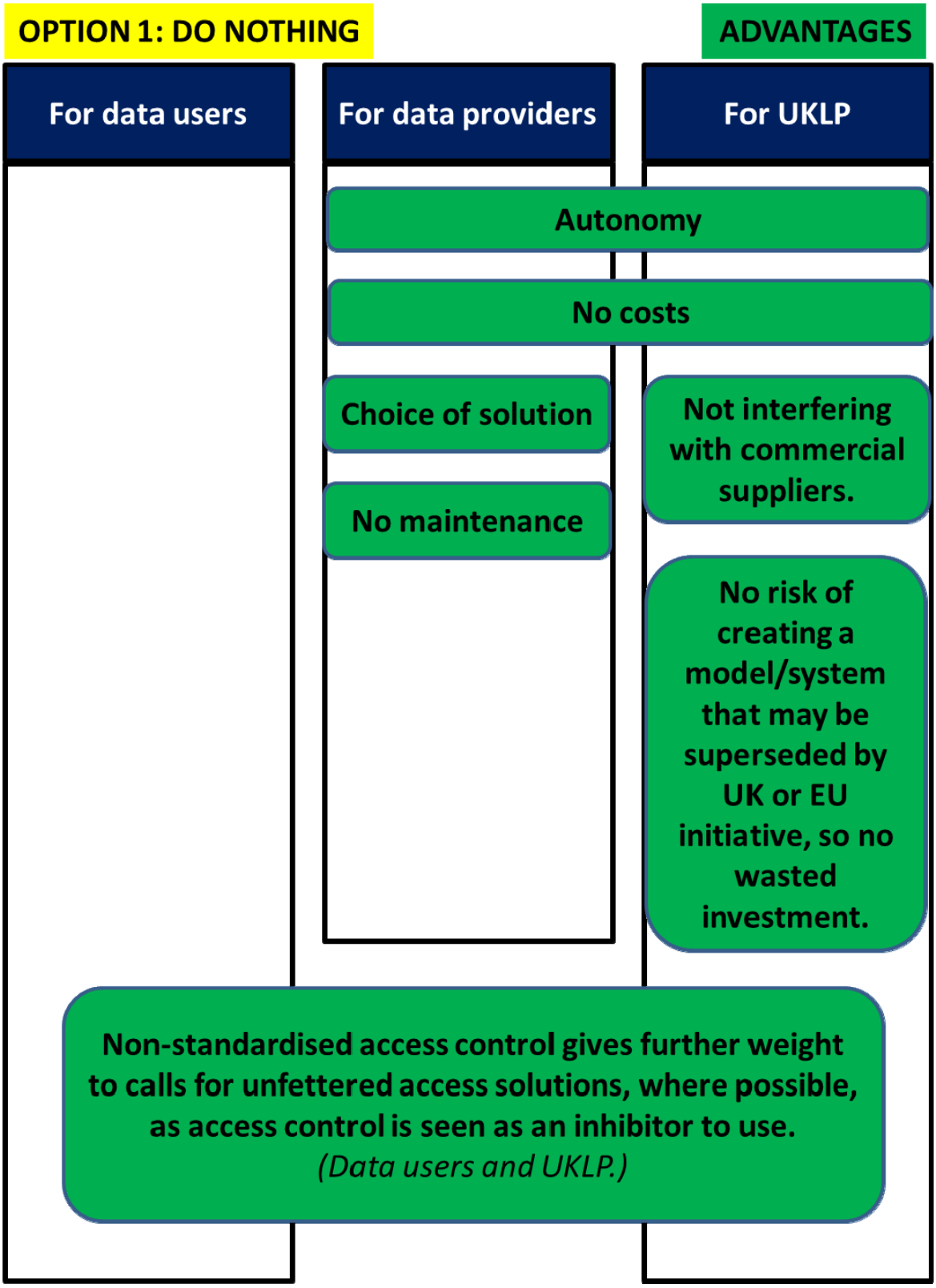
Licensing models are offered and concluded using the online Licence Shop.

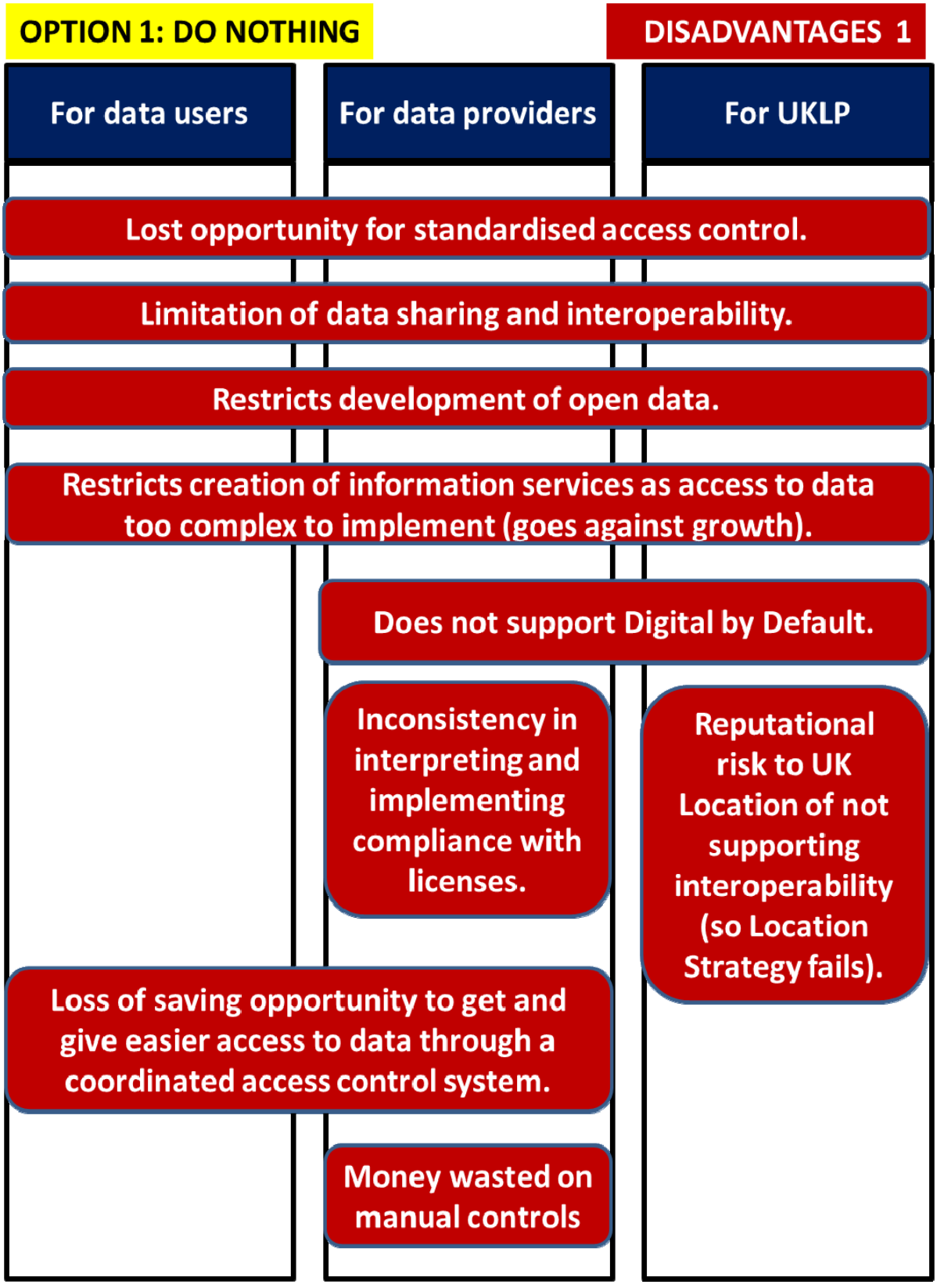
A variety of authentication methods may be offered, depending upon the web service.

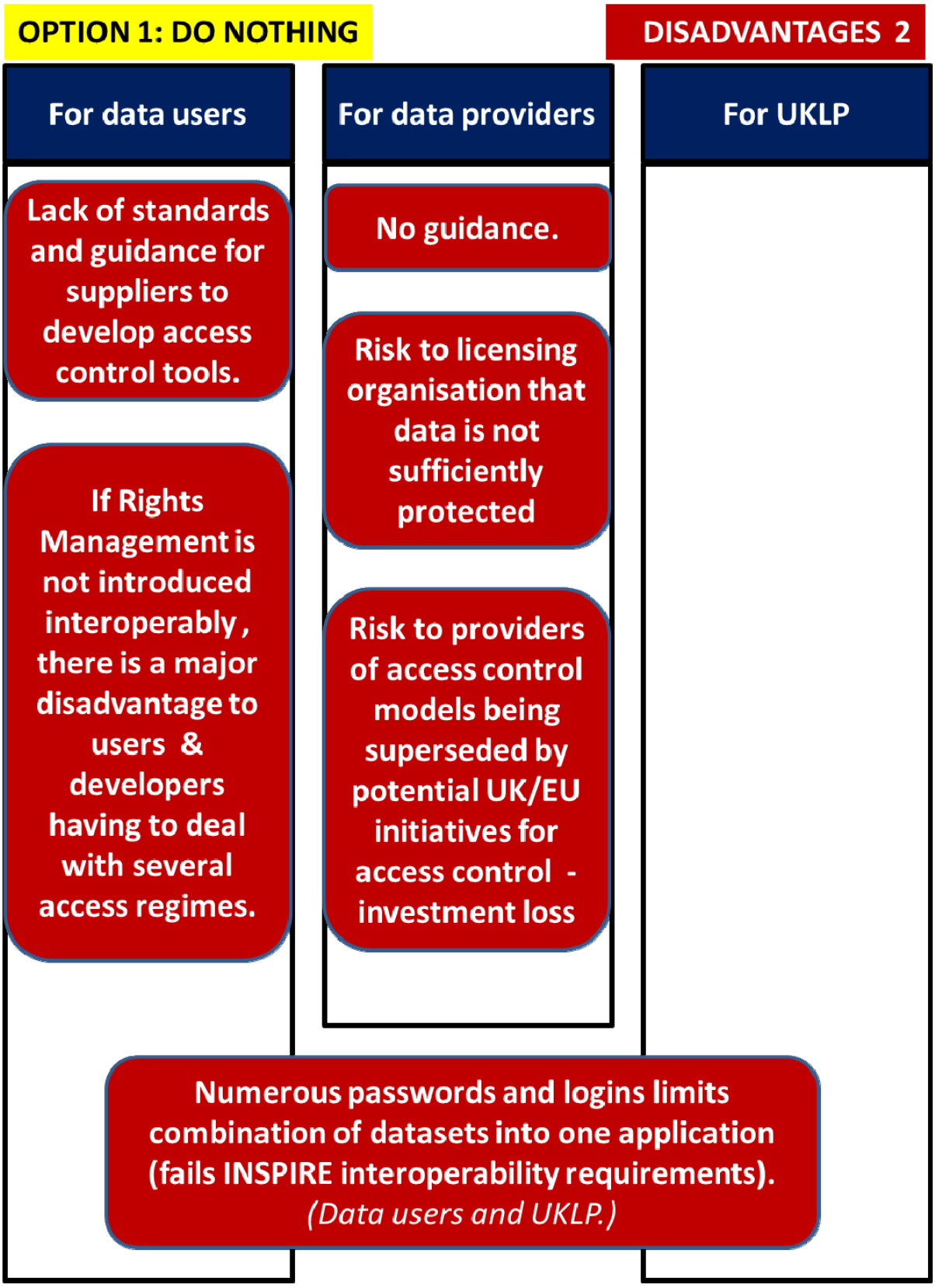
The Gateway User configures their client application to use the proxy with the selected authentication method.

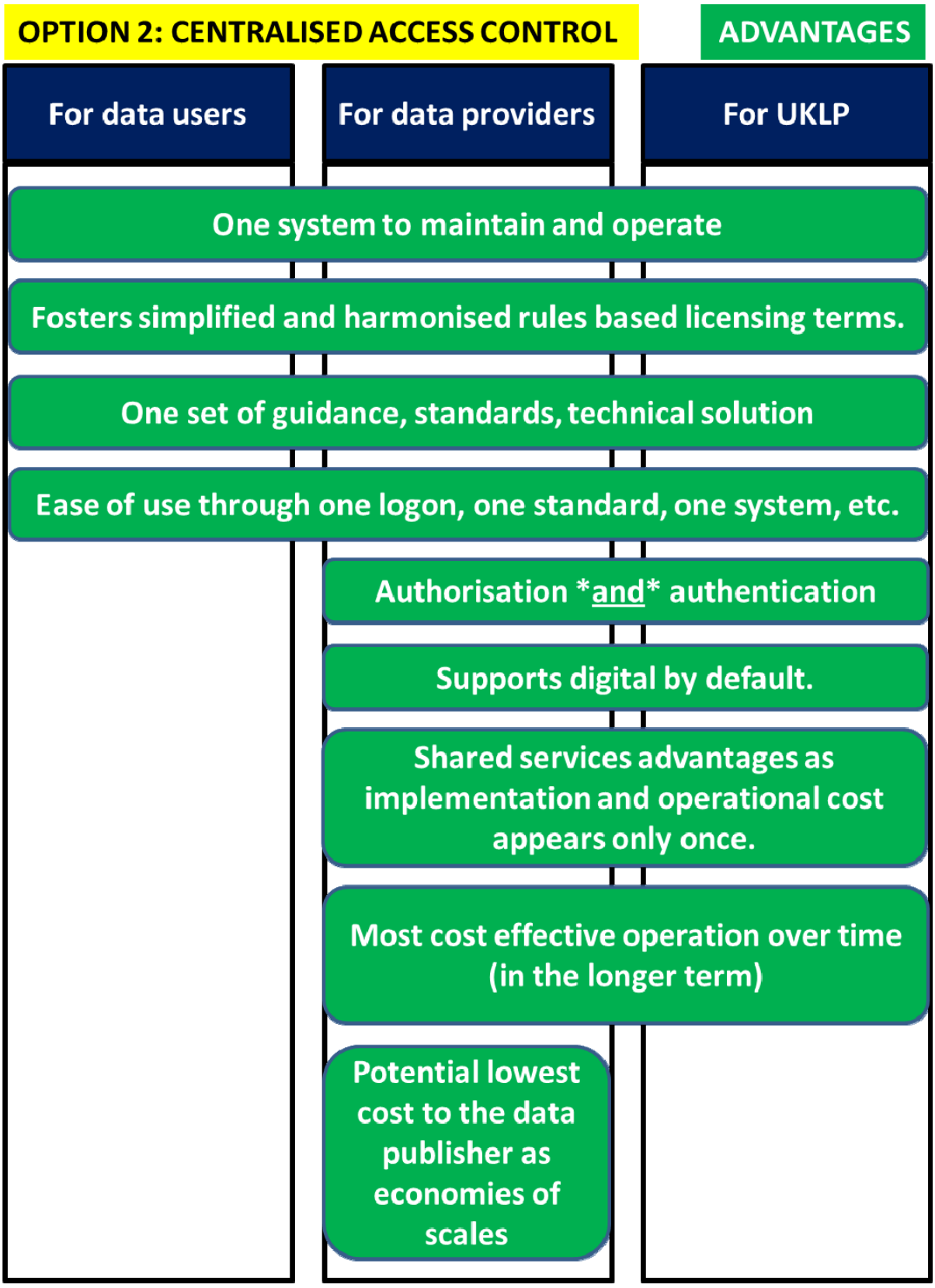
Proxy service URLs can be permanent, or time-restricted.

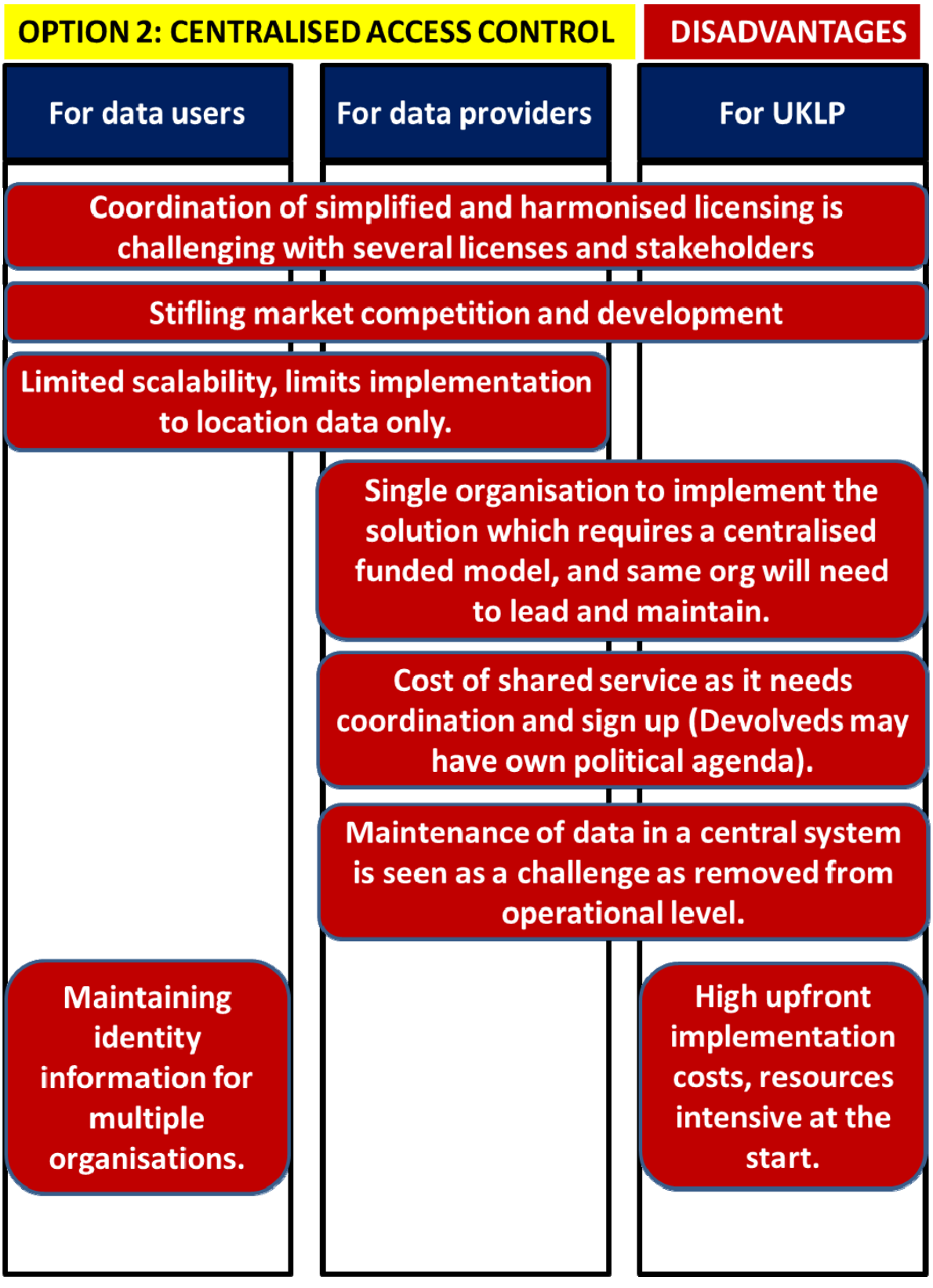
# ANNEX D. ADVANTAGES AND DISADVANTAGES OF THE OPTIONS

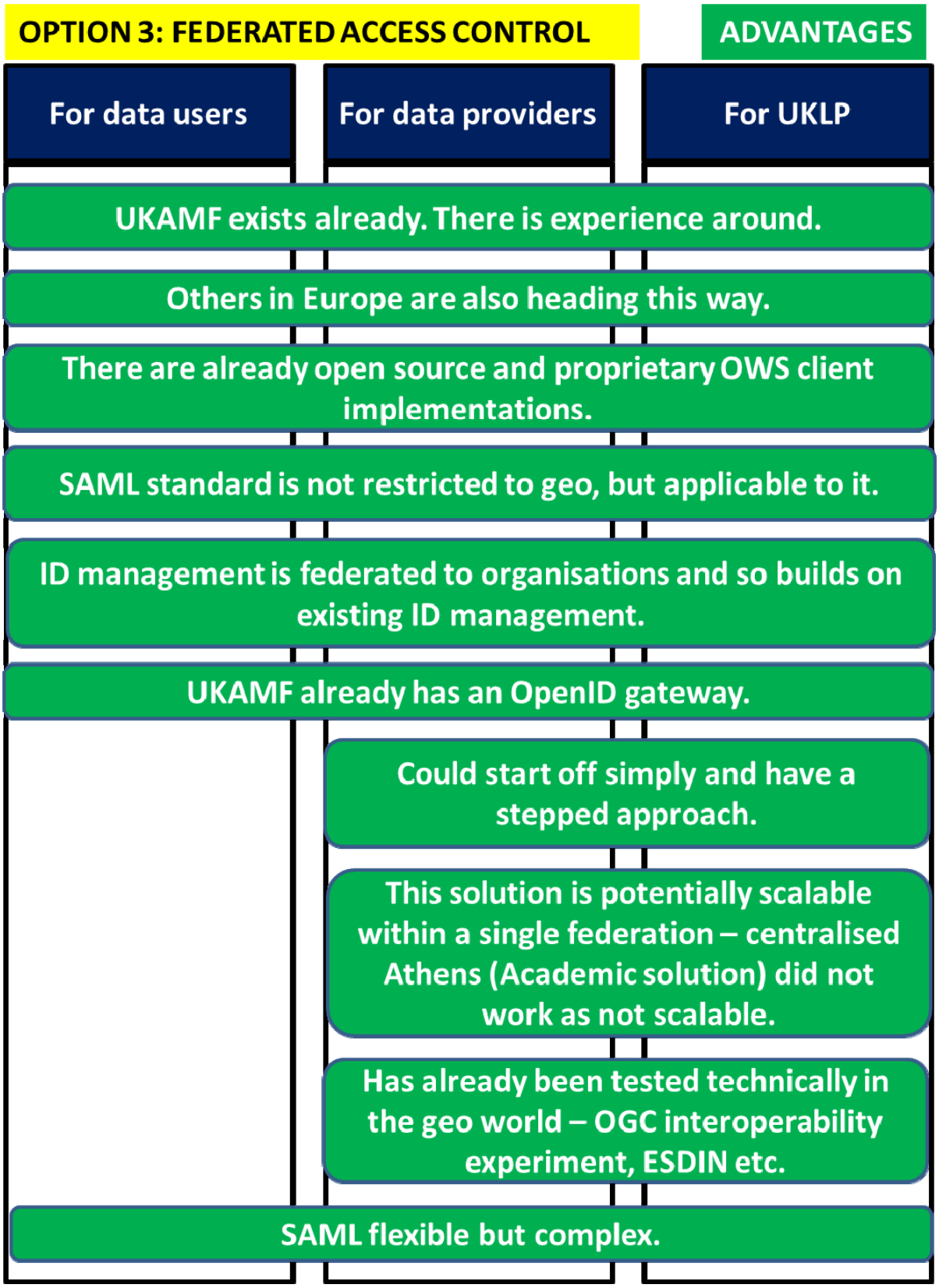


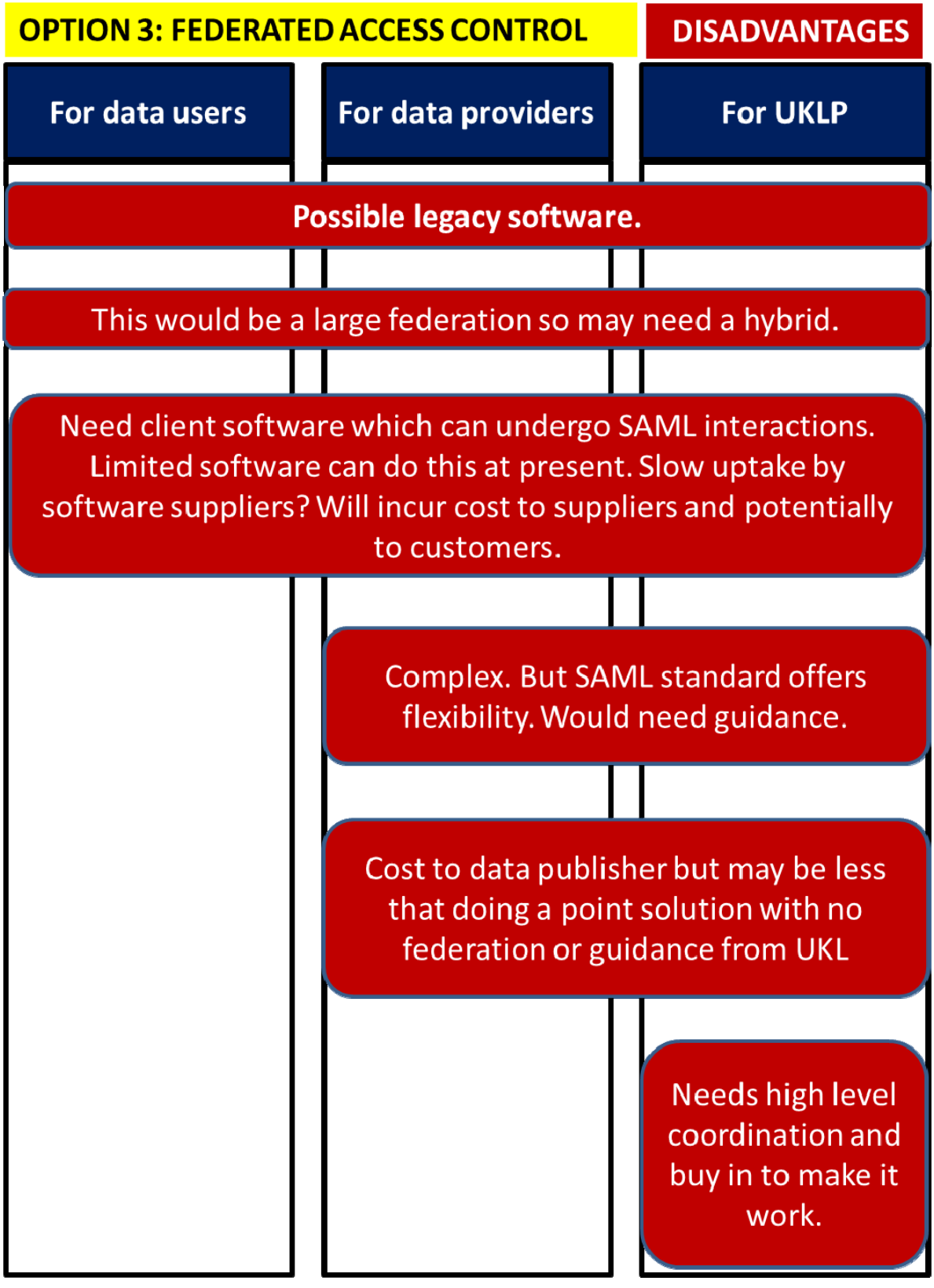

OPTION 1: DO NOTHING
DISADVANTAGES 1
For data users
For data providers
For UKLP
Lost opportunity for standardised access control.
Limitation of data sharing and interoperability.
Restricts development of open data.
Restricts creation of information services as access to data too complex to implement (goes against growth).
Does not support Digital by Default.
Inconsistency in interpreting and implementing compliance with licenses.
Reputational risk to UK Location of not supporting interoperability (so Location Strategy fails).
Loss of saving opportunity to get and give easier access to data through a coordinated access control system.
Money wasted on manual controls


OPTION 1: DO NOTHING
DISADVANTAGES 2
For data users
For data providers
For UKLP
Lack of standards and guidance for suppliers to develop access control tools.
If Rights Management is not introduced interoperably, there is a major disadvantage to users & developers having to deal with several access regimes.
No guidance.
Risk to licensing organisation that data is not sufficiently protected
Risk to providers of access control models being superseded by potential UK/EU initiatives for access control - investment loss
Numerous passwords and logins limits combination of datasets into one application (fails INSPIRE interoperability requirements).
(Data users and UKLP.)


OPTION 2: CENTRALISED ACCESS CONTROL
ADVANTAGES
For data users
For data providers
For UKLP
One system to maintain and operate
Fosters simplified and harmonised rules based licensing terms.
One set of guidance, standards, technical solution
Ease of use through one logon, one standard, one system, etc.
Authorisation *and* authentication
Supports digital by default.
Shared services advantages as implementation and operational cost appears only once.
Most cost effective operation over time (in the longer term)
Potential lowest cost to the data publisher as economies of scales


OPTION 2: CENTRALISED ACCESS CONTROL
DISADVANTAGES
For data users
For data providers
For UKLP
Coordination of simplified and harmonised licensing is challenging with several licenses and stakeholders
Stifling market competition and development
Limited scalability, limits implementation to location data only.
Single organisation to implement the solution which requires a centralised funded model, and same org will need to lead and maintain.
Cost of shared service as it needs coordination and sign up (Devolveds may have own political agenda).
Maintenance of data in a central system is seen as a challenge as removed from operational level.
Maintaining identity information for multiple organisations.
High upfront implementation costs, resources intensive at the start.


OPTION 3: FEDERATED ACCESS CONTROL
ADVANTAGES
For data users
For data providers
For UKLP
UKAMF exists already. There is experience around.
Others in Europe are also heading this way.
There are already open source and proprietary OWS client implementations.
SAML standard is not restricted to geo, but applicable to it.
ID management is federated to organisations and so builds on existing ID management.
UKAMF already has an OpenID gateway.
Could start off simply and have a stepped approach.
This solution is potentially scalable within a single federation – centralised Athens (Academic solution) did not work as not scalable.
Has already been tested technically in the geo world – OGC interoperability experiment, ESDIN etc.
SAML flexible but complex.


OPTION 3: FEDERATED ACCESS CONTROL
DISADVANTAGES
For data users
For data providers
For UKLP
Possible legacy software.
This would be a large federation so may need a hybrid.
Need client software which can undergo SAML interactions. Limited software can do this at present. Slow uptake by software suppliers? Will incur cost to suppliers and potentially to customers.
Complex. But SAML standard offers flexibility. Would need guidance.
Cost to data publisher but may be less that doing a point solution with no federation or guidance from UKL
Needs high level coordination and buy in to make it work.