

AAA, Middleware and DRM

Preface

In July 2004 the Treasury, Department of Trade and Industry (DTI) and the Department for Education and Skills (DfES) published the "Science and Innovation Investment Framework 2004-014", which set out the government's ambitions for UK science and innovation over that period, in particular their contribution to economic growth and public services.

A section of the Framework addressed the need for an e-infrastructure for research. It proposed an Office for Science and Innovation (OSI) lead steering group to focus discussion and assess requirements for its development.

To implement this recommendation, the OSI steering group was formed and commissioned a study to help inform the process of achieving the objectives set out in the Framework document. The study was tasked with establishing a high-level "road map" of the current provision of the UK's "e-Infrastructure" to support research, and in doing so help define the development of this infrastructure.

The steering group subsequently formed six working groups to develop this road map of the e-Infrastructure in greater detail in specific areas. These working groups were tasked with producing the following reports:

1. Information creation and data creation
2. Preservation and curation
3. Search and navigation
4. Virtual research communities
5. Networks, compute power and storage hardware
6. Middleware, AAA (authentication, authorization, accounting) and digital rights management

The individual reports are intended to represent the informed opinion of the working groups and their contributors and to guide discussion and future development of the e-infrastructure. The working groups have worked closely together. Although each report is free-standing, a synthesis of all the reports and major issues has also been produced which will provide a framework for any potential departmental bids in the next Comprehensive Spending Review in 2007 and for future planning and development of the e-infrastructure for research.

Prue Backway
Office for Science and Innovation
Department of Trade and Industry

Executive Summary

AAA (Authentication, Authorisation and Accounting), Middleware and DRM (Digital Rights Management) form part of the core fabric of a distributed, heterogeneous e-infrastructure that is the vision of the Science and Innovation Investment Framework. They are the 'invisible mechanisms' on which many users rely, but that can act as barriers to the user experience through poor implementation, lack of understanding or confusing policy and practise.

This report summarises the findings of the AAA, Middleware and DRM working group formed by the DTI Steering Group to explore requirements for these areas of work and to make appropriate recommendations as to future development requirements to ensure a robust infrastructure and reliable user experience. A total of 28 recommendations are made within this report, which can be summarised within the following high-level recommendations and messages:

- Work to inform service and software requirements must continue to be supported. The three areas covered by this report are at very different levels of maturity within the UK, but all will benefit from ongoing review and scoping. Recommendations in this area include the need to support networks of excellence, technology review and scoping to improve authentication and authorisation tools and services, and work to explore the role of these technologies and processes within existing infrastructures such as the RAE.
- Technology and service development is still required. Whilst significant investment has been made within the UK to support technology development for next generation infrastructures, ongoing support is required to serve the evolving requirements of the research process. Many of the recommendations in this area are to support new ways of working, such as Virtual Organisations, or to support individuals working outside of existing institutional boundaries.
- To achieve take-up, work to change practise should be supported. New technologies can only be successfully implemented when supported by coherent, consistent and well considered policies and practise. Recommendations in this area support the changing role of both the institution and the user, and look towards widening participation within research.
- The importance of social interaction and technology impact should not be overlooked. The complex technological and policy requirements of AAA, Middleware and DRM often divorce developments from the user. Recommendations in this area address this issue by looking at the development of business models, social process studies and take-up support.

Contents

Preface	2
Executive Summary	3
Theoretical Ideal	6
Current Position and Plans	7
Authentication, Authorisation and Accounting	7
Middleware	10
Digital Rights Management	12
Options for the Future	14
Authentication, Authorisation and Accounting Requirements	14
Middleware Requirements	18
Digital Rights Management Requirements	20
Recommendations	23
Appendix A: Working Group Membership	24
Appendix B: Glossary	25
Appendix C: References	27

Introduction

In describing the facilities that an e-Infrastructure should provide, the “Survey of the UK’s current e-Infrastructure Provision for Academic Research” highlights a series of supporting mechanisms:

“Behind these facilities are further vital but often invisible mechanisms which make all of this work, in as coherent and reliable a manner as possible...”¹

The three service components described in this report provide exactly this backbone and as such are vitally important in making an e-Infrastructure functional in the manner described by the survey. Authentication, authorisation and accounting (AAA), middleware, and digital rights management (DRM) are the core fabric of a heterogeneous, distributed e-Infrastructure that will help meet the vision for research as laid out in the Science and Innovation Investment Framework 2004 – 2014².

All three of these components are at very different stages of development within the UK. The service critical nature of authentication, authorisation and accounting has led to significant developments in line with international programmes of work such as the JISC Federated Access Management initiative³ and the UK Grid Certificate Authority⁴. Whilst robust next generation services are emerging in this sphere, further development is needed to ensure that the full requirements of an e-Infrastructure can be met.

Middleware as an area is more problematic to define as the term is applied in many different contexts. Whilst defining the precise definition of middleware is difficult, it is clear what middleware must be able to do in order to support the proposed e-Infrastructure: it should enable the e-Infrastructure to be robust, reliable and resilient, it should be based on open standards and have backwards compatibility and it should be based on a service-oriented approach. This report focuses on areas of middleware that can directly support these requirements.

Whilst digital rights management and related topics such as intellectual property rights (IPR) are governed by clear laws and policies, most end-users are still poorly supported in interpreting these in to every-day working practise. This lack of end-user understanding combined with potential significant legislative changes and challenges to the scope of the law created by new initiatives such as Virtual Organisation means that much effort is required to successfully implement digital rights management within the e-Infrastructure.

This report has focused on each of the three service components in the context of the current environment as described above. As such advancements in the short and medium term for some areas are likely to be greater than in other areas. It is important that the current context and the reality of the existing institutional infrastructure within the UK are kept at the forefront of debate surrounding future vision.

¹ Lord, Philip and Macdonald, Alison. Survey of the UK’s current e-Infrastructure Provision for Academic Research. September 2005.

² Science and Innovation Investment Framework, 2004 – 2014. July 2004: <http://www.hm-treasury.gov.uk/media/95846/spend04_sciencedoc_1_090704.pdf>.

³ JISC UK Access Management Federation Initiative: <<http://www.jisc.ac.uk/federation.html>>.

⁴ UK Certificate Authority: <<https://ca.grid-support.ac.uk/>>.

Theoretical Ideal

The following statement is proposed as a theoretical ideal of how a user may wish to engage with authentication, authorisation, accounting, middleware and digital rights management within an e-Infrastructure. It is a single user point-of-view, and by its nature will not cover all of the detailed requirements of the multiple stakeholders within this environment.

"First thing in the morning I log in to my office computer at home using my usual username and password. Since the network at work knows where I am and what system I am using, that allows me to access everything I need for my normal work: e-mail, internal files, company calendar and so on. If I were working from a hotel then I would also need to give the one-time password from my keyring. I receive an e-mail asking me to update information regarding a project I manage on the institutional finance system, so I switch to my role as system administrator. To get administrator access I need to enter the password from my keyring. When I have updated the relevant information I drop back to normal user access. At lunchtime I need to work on an essay for a course I am studying at another university, so I drop into my student role (the university checks with my employer that I have already logged in, so I don't need to enter any passwords) which lets me contact my tutor and run a couple of searches on a commercial database. As part of my research I need to run a visualisation simulation and so I submit a job to the National Grid Service. I am allowed to submit this job as I have credit available in my institutional account, which controls Grid usage. I receive confirmation of the job request on my mobile phone and that evening I receive another notification that my job has completed. In the afternoon I get a call from a colleague I met at an international conference who would like me to join a quick video-conference he has set up. Since I am already logged in the collaboration system recognises me and allows me to join the conference and add comments to a document we are developing together. When the paper is finished next week, I will submit it to my institutional repository along with the relevant supporting research data."

Current Position and Plans

The following table gives an overview of known developments and development plans within the UK and related communities. This list is not intended to be exhaustive, but aims to highlight the most important areas in relation to this study and the needs of the Science and Innovation Investment Framework.

Authentication, Authorisation and Accounting

Activity	Description	Scale	Current Expenditure	Future Plans	Developments in other countries
UK HIGHER EDUCATION					
e-Science CA (NGS)	The UK e-Science Certification Authority (CA) provides X.509 certificates for the UK e-Science community and is being run as part of the Grid Operations Support Centre funded by the Research Councils' core e-Science programme	Approximately 1000 users and 2000+ hosts.	Unknown	JISC funded projects to link Certificate Authority and Access Management Federation Proposed JISC development plan for further work on levels of assurance within certificates Proposed JISC development plan for CA development plan	Models for national CAs to serve the e-Science community can be found throughout all of the major countries involved in grid development and deployment The IGTF is the International Grid Trust Federation. It is a federation of the three PMAs (Policy Management Authorities) in the world (EUGridPMA (EU-and-friends), TAGPMA (the Americas, north and south), and APGridPMA (Asia/Pacific)
Athens	Athens provides the current, centralised access management system for UK HE and FE, providing Athens user accounts for access to third party resources	3.5 million user accounts within the HE and FE sector	JISC support of approximately £650,000 per annum, plus a charging model for publishers	Eduserv Athens a partner in federated access management developments	Few national systems exist in other countries using a similar model to Athens
Federated Access Management	JISC is implementing the UK Access Management Federation at UKERNA to support devolved authentication for HE and FE. The DfES has recently agreed plans to roll-out for the schools sector	To cover HE, FE and schools sectors	Seed funding of £1.1 million for two years, decreasing to approximately £500,000 per	Committed transition plan for 2006 – 2008, becoming a full service in July 2008 Planned JISC	Gaining international momentum. Known plans in US, Australia, Netherlands, Spain, Finland, Norway, and Switzerland. Engagement from France and Germany

			annum	development to enhance core service: TERENA SCS and Virtual Home for Identities.	
Ad-hoc solutions	Ad-hoc access management solutions such as IP restricted access, username and password built in to systems, including identity management and single sign-on solutions	Unknown	Unknown	Unknown	Problem space is well established internationally
RADIUS for roaming	UKERNA launching JANET Roaming Service to allow users visiting institutional campuses to log-in using their own institutional username and password. Based on RADUIS technology, and eduRoam policies	Currently small trial but aimed to serve all JANET sites	Unknown	Plans tabled to provide a bridge between JANET Roaming and the UK Federation	eduRoam established throughout Europe and Australia, with interest from US
Accounting	UK standards based on Counter project. Current Athens system provides accounting information to institutions	UK HE and commercial providers	Unknown	JISC development plans to examine accounting, auditing and diagnostic requirements across e-Infrastructure and repositories	Useful report from Swiss NREN – SWITCH – detailing accounting plans
Grid Accounting	Grid Accounting is still immature, but a number of projects have made some progress in implementing usage recording systems (metering). This work has fed back into the GGF standards procedure and standards are appearing (GGF Usage-Record Working Group)	Accounting tools being developed and used by some Grid projects, including NGS, EGEE, OSG, SweGrid and TeraGrid	Unknown	Developments will continue, for example in EGEE (APEL and DGAS tools)	Ongoing interest in exchange of interoperable accounting records
TECHNOLOGY DEVELOPMENT					
SAML	SAML – Security Assertion Mark-Up Language – was designed to meet the needs of interoperable single sign-on. SAML 2.0 has recently been released. It is the standard used by the Shibboleth implementation	Supported by Liberty Alliance – and OASIS standard	Unknown	Ongoing development plans	Ongoing interest as a major international standard
Authorisation Tools	Various tools have been created to help manage user information to address authorisation transactions. Two are of particular relevance and prominence: PERMIS (Privilege and Role Management Infrastructure	Tools used by various institutions internationally	Unknown	Software packages well embedded within communities – planned further development for both tools	Ongoing international interest

	Standards) and VOMS (Virtual Organisation Membership Service)				
WS-Security (Fed, Trust etc)	WS-Security is a specification that provides enhancements to SOAP messaging to protect the confidentiality of the message and to authenticate the sender. It also describes how to associate a security 'token' with this message – and works with other standards such as X.509 and SAML. Six new specifications support WS-Security are being examined (Policy, Trust, Privacy, Secure Conversation, Federation, Authorization)	Supported by Microsoft and IBM – an OASIS standard	Unknown	Continued development, particularly WS-Security, WS-Trust and WS-Fed.	Ongoing interest as a major international standard
Identity Management	Identity Management is gaining momentum from federated access management developments. There are two main drivers – the need for well-defined identity management internally to support federated access management, and the wish to federate identities as well as access	Four developments of interest to UK HE: Liberty Alliance Microsoft InfoCard Higgins A-Select	Unknown	Development in each of the main players	International representation behind all of these initiatives apart from A-Select which is a Dutch initiative
OTHER UK SECTORS					
NHS	AAA remit of Technical Architecture Design Group for National Library for Health (NLH) electronic delivery (England). Looking towards Smartcard technologies, but interested in working with UK HE NHS Wales is not following the lead of NHS England. Their authentication strategy is being developed by the Welsh Assembly's Informing HealthCare programme and its Access to Knowledge (A2K) project	NHS-England NHS-Wales	Unknown	Design of new architecture for National Library for Health Design of new architecture for A2K project	Unknown Unknown
UK Government	Cabinet Office Chaining a PAN Government Identity Management SIG – keen interest in federated access management	UK Public Sector	Unknown	Special Interest Group to make recommendations	US Government Authentication based on Federated Access Management – working with Internet2
Museums and Archives	No known co-ordinated approach to AAA in this field	Unknown	Unknown	Unknown	Unknown

Middleware

Activity	Description	Scale	Current Expenditure	Future Plans	Developments in other countries
UK HIGHER EDUCATION					
Core e-Science Programme Middleware Demonstrators	The Core e-Science Programme funded a range of middleware demonstrator projects	15 demonstrator projects	£6.5 million	Unknown	Unknown
OMII	The Open Middleware Infrastructure Institute was funded by the e-Science Core Programme. Its remit is to harden and support key middleware components within e-Science	UK Centre serving HE community	Initial grant £6.5 million, new grant of £9.4 million agreed Proposed JISC development contribution	Recent grant renewal including two further OMII-nodes to broaden work across UK	NSF Middleware Initiative, OMII-Europe, OMII-China
Production Grids such as NGS and GridPP	Production Grids are important in terms of delivering middleware software and services. Within the UK the National Grid Service and GridPP are the most prominent services in this area	UK wide (NGS) UK Particle Physicists (GridPP)	Unknown £32 million over 6 years	JISC and e-Science Core Programme continue to invest in and develop the NGS	Various production Grids developed internationally
JISC e-Framework	The primary goal of the JISC e-framework is to produce an evolving and sustainable, open standards based service oriented technical framework to support the education and research communities. This includes a wide range of 'common services', or middleware components	Integral part of JISC and DEST development programmes		New development programmes within JISC development	Joint initiative with Department of Education, Science and Training in Australia and input from SURF in Netherlands
JISC IE Shared Infrastructure	The JISC Information Environment technical architecture specifies a set of standards and protocols that support the development and delivery of an integrated set of networked services that allow the end-user to discover, access, use and publish digital and physical resources as part of their learning and research activities. This includes a shared infrastructure of national and distributed services	UK HE and FE sectors		New development strategy for shared infrastructure recently released	Unknown
TECHNOLOGY DEVELOPMENT					
Globus Alliance	The Globus Alliance is a community of organizations and individuals developing fundamental technologies behind the Grid,	International	Funded through government research and	Current release of toolkit 4.0, further releases as yet	Globus is an international partnership

	which lets people share computing power, databases, instruments, and other on-line tools securely across corporate, institutional, and geographic boundaries. The Globus Toolkit is an open source software toolkit used for building Grid systems and applications. The Open Grid Services Architecture (OGSA) represents an evolution towards a Grid system architecture based on Web services concepts and technologies		development programmes	unscheduled	
European Projects such as EGEE	The Enabling Grids for E-sciencE (EGEE) project is funded by the European Commission and aims to build on recent advances in grid technology and develop a service grid infrastructure which is available to scientists 24 hours-a-day. The middleware activities in EGEE focus primarily on re-engineering existing middleware functionality, and middleware is released via gLite	European	64 million Euro EU funding	Four years project funding secured, now in second of two year stages	European and industry partners in EGEE
OTHER UK SECTORS					
UK Government	Supported through various channels such as the e-Government Interoperability Framework, the e-Government Unit and the Chief Information Officer Council. Government Gateway launched as 'middleware infrastructure'	UK public sector	Unknown	Unknown – focus on 'shared services' within Chief Information Officer Council	Unknown
NHS	Various projects exist within National Programme for IT and Connecting for Health programmes	Health sector	Unknown	Connecting for Health programme started April 2005	Unknown
Museums and Archives	Unknown	Unknown	Unknown	Unknown	Unknown

Digital Rights Management

Activity	Description	Scale	Current Expenditure	Future Plans	Developments in other countries
UK HIGHER EDUCATION					
Open Access Agenda	The Open Access agenda is being pursued by various bodies across the UK to encourage self publication of scholarly communications. This includes initiatives such as the 'author pays' model	Supported by various groups throughout the UK	Unknown	Many organisations planning Open Access policies	International agenda well established
JISC Intrallect Report	A significant study in to DRM undertaken by JISC in early 2004	Study of UK requirements	£25,000 study	Recommendations taken forward by IPR consultants	Unknown
JISC IPR Consultancy	Consultants working on behalf of JISC and its community to both inform and update on DRM issues and recommend development areas	UK wide		Ongoing consultancy	Unknown
License Expression Working Group	The National Information Standards Organization, Digital Library Federation (DLF), EDItEUR, and Publishers Licensing Society (PLS) have agreed to form a License Expression Working Group to develop a single standard for the exchange of license information between publishers and libraries.	Working group with international representation	Contributions in the form of members time	Recommendations from working group to define future development plans	International membership on group
TECHNOLOGY DEVELOPMENT					
License Expression Languages	A License Expression Working Group has been formed by the Digital Library Federation and the Publishers Licensing Society to work towards a standard agreed License Expression Language	International membership	Voluntary contributions	To make formal standard recommendations	International membership on working group
DRM Systems	Many commercial companies are using DRM systems to help enforce DRM policies. They are largely unpopular as they are felt to unreasonably restrict user rights	International commercial	Unknown	UK and EU governments reviewing place and application of DRM systems	International interest and development
'Commons' Developments	Creative Commons started with the vision of creating flexible copyright licenses for creative work. Licenses that meet UK legal requirements now exist. Science Commons now seeks to extend this vision to all scientific data	International	Ongoing financial support from governments and foundations	Extending international remit, supporting projects such as Science Commons	International development well advanced
OTHER UK SECTORS					

UK Government	The All Party Parliamentary Internet Group (APIG) is currently undertaking a public inquiry on Digital Rights Management (DRM), with a report to be published in April. As part of the pre-Budget, the Chancellor Gordon Brown announced that he has commissioned an independent review into intellectual property rights in the UK	UK public sector	Unknown	12 month IPR review starting in January 2006. APIG enquiry report to be published in April	EU Commission publishes regular reports on DRM and IPR issues
NHS	Unknown	Unknown	Unknown	Unknown	Unknown
Museums and Archives	Unknown	Unknown	Unknown	Unknown	Unknown

Options for the Future

It is clear that the current and known developments in all three of the fields discussed in this report will not allow for the full provision of the theoretical ideal as shown in section three of this report. As such, the working group has identified a series of requirements to enable e-Infrastructure provision to move closer to this theoretical ideal over the next five years. This report does not attempt to look further ahead than this due to the fast-changing nature of both the research and technical environment that we currently work in.

Each section below sets out a development requirement, and explains the current position for this requirement. Where clear work areas can be identified, these are described along with an appropriate justification, benefit statement and risk analysis.

Authentication, Authorisation and Accounting Requirements

A. Strong federated access management system within the UK with institutionally centralised authentication

JISC will be launching the UK Federation Access Management for Education and Research in September 2006. This service will initially focus on meeting the current main requirement for access management within the UK in terms of access to commercial resources. As the service grows in capacity, federated access management will be increasingly used in other scenarios such as access to non-commercial resources including e-learning and core research material and access to internal resources within institutions. Ongoing support will be need for these activities.

The following work areas are proposed:

Recommendation 1	
Work area:	<i>Supporting the federated access management requirements of Virtual Organisations</i>
Description:	Federated Access Management can greatly support the needs of Virtual Organisations, but further work is needed to allow VOs to fully exploit this potential. A programme of work is proposed to support the requirements of Virtual Organisations including: use of multiple attribute authorities within institutions, support for fine-grained authorisation, and Federation membership models for Virtual Organisations
Justification:	Virtual Organisations define the major requirements of the evolving e-Infrastructure. It is essential that they are fully supported in national developments
Benefit:	Virtual Organisations supported earlier in development cycle than previously expected
Risks:	Lack of understanding of VOs within institutions

Recommendation 2	
Work area:	<i>Changing Practises: the Institution as Service Provider</i>
Description:	Federated Access Management challenges institutions to rethink their capabilities by encouraging them to position themselves as Service Providers, sharing data securely with partners. Support will be needed to enable institutions to understand and adopt this approach
Justification:	e-Learning and e-Research developments all require institutions to take this position
Benefit:	Full exploitation of the potential of e-Research and e-Learning collaborations

Risks:	Lack of capability and management within institutions
--------	---

Recommendation 3	
Work area:	Virtual Home for Identities
Description:	A 'Virtual Home for Identities' allows users without home affiliations to participate in collaborations protected by a Federation
Justification:	Many research partners (visiting professors, commercial partners etc.) may have no affiliation but wish to access secure data. Institutions are often forced to (inappropriately) give such users institutional status to allow for collaborative activities
Benefit:	Ability to collaborate widely without breaking institutional membership policy
Risks:	Poorly defined policy for use could over-burden system

Recommendation 4	
Work area:	Server Certificate Service
Description:	Federated Access Management requires all Identity Providers and Service Providers to have a Server Certificate. Provision of a central service could make issue and renewal of such certificates far simpler, and reduce the support burden for the Federation
Justification:	Reduces the support burden of the Federation and has broader applicability for wider server certificate use
Benefit:	Central system offering certificates at a fair price and reduced administrative burden
Risks:	Demand for other use scenarios could impact on scale of service

B. Support for levels of assurance for applying appropriate authentication to resources

The UK currently offers two strengths of authentication: username / password through Athens and certificate access through the Certificate Authority. Application of strength is defined through the environment in which the resource sits rather than its worth. Work is needed to provide appropriate strength of authentication to all resources against a defined level of assurance.

Recommendation 5	
Work area:	Level of Assurance: UK Definition of LOA
Description:	Before Levels of Assurance can be applied, an agreed standard for expressing levels will need to be defined
Justification:	Required for strength of authentication to be appropriately applied. Important in other sectors, particularly NHS and Government
Benefit:	Appropriate authentication for the appropriate resource
Risks:	Failure to reach agreement on levels required

Recommendation 6	
Work area:	Expressing Level of Assurance
Description:	Both the UK Access Management Federation and the UK CA will need to be able to express and manage LOA as part of the authentication process
Justification:	Development work is required to implement this advanced functionality within both services
Benefit:	National services offering Level of Assurance as part of core functionality
Risks:	Lack of definition standard (see recommendation 5)

Recommendation 7	
Work area:	Appropriate Level of Assurance
Description:	Authentication strength is currently defined by the environment offering a service or resource, rather than by the worth of the resource. A review of application of strength of authentication against research resources is proposed
Justification:	Application of appropriate levels of assurance will open up access to resources to wider groups of users that may not wish to apply for strong tokens (such as Grid certificates)
Benefit:	Wider take-up of resources

Risks:	Confusion over appropriate authentication mechanisms for both users and resource providers
--------	--

C. Integration of existing access management systems within UK education

There are currently four access management systems operating within the UK: the Grid Certificate Authority, the Athens authentication system, the UK Access Management Federation and the Janet Roaming Service. Whilst each of these services satisfies a particular unique set of requirements, interactions between these services will be essential to meet the theoretical ideal described in this paper.

Recommendation 8	
Work area:	<i>Appropriate Use of PKI</i>
Description:	Take-up of PKI technologies is still limited within the UK despite the functionality it can offer. Funding for Early Adopters of PKI technologies is proposed to help 'kick-start' use of PKI within the UK where it can be usefully applied. This should include the development of JISC projects such as the TIES2 and DCOCE reports
Justification:	Institutions within the UK need direct support at the implementation stage for this technology to achieve wide take-up and use within the UK
Benefit:	Advanced technologies to support research process
Risks:	Lack of skills and knowledge within institutions

Recommendation 9	
Work area:	<i>Bridging Network and http Access</i>
Description:	True Single Sign-On has yet to be achieved as different technologies are used to gain network and http authentication. Solutions have been proposed to bridge this technological divide, but work is needed to prove requirements within the UK
Justification:	A fully scoped requirement statement will be essential before taking this work forward to service within the UK
Benefit:	Identified need before development
Risks:	Delay in provision of service

Recommendation 10	
Work area:	<i>Federated Access Management and the UK CA</i>
Description:	JISC has funded development to provide a 'bridge' between the UK CA and the UK Access Management Federation. Work will be required to fully embed this service within the UK, and to support user training and awareness
Justification:	Support for user training and embedding will enhance the development funds spent on this service
Benefit:	User education and awareness
Risks:	Delay in developments

D. Delegated authorisation

Whilst centralised authentication is appropriate within an institutional context, centralised authorisation will limit and restrict the needs of research groups to run and develop services. Models are emerging that support delegated authority for authorisation, but further work is required to provide the full functionality needed to support research groups within Virtual Organisations.

Recommendation 11	
Work area:	<i>Authorisation Tools Analysis</i>
Description:	Many tools have been developed to support authorisation functions within virtual organisations and institutions. An analysis of current developments, functionality and gaps is proposed in conjunction with the National Grid Service
Justification:	Authorisation is a key requirement within the e-Infrastructure. Coherence in

	terms of development and available tools is required to achieve the functions required by institutions and VOs
Benefit:	Clear understanding of development achieved and requirements outstanding
Risks:	Lack of buy-in from software developers

E. Ability to work across federations in both academic and commercial domains

National Federated Access Management Systems are in development on an international scale, including major developments throughout Europe, the US and Australia. To truly benefit from the potential of this progress, the UK will need to contribute to international debate and agreement on standards, policies, processes and best practise.

Recommendation 12	
Work area:	Support for UK participation in national developments
Description:	A formal body of effort for UK participation in national developments in federated access management is proposed as part of the (evolving) Core e-Science Programme Security Network
Justification:	For the UK to participate fully in national developments, a coherent and supported voice within these developments will be required
Benefit:	Coherent messages from the UK
Risks:	Lack of buy-in from major players within the UK

F. Personal / multiple identity management tools and training

Identity Management developments are occurring on three levels: to support intra-institutional, inter-institutional and personal requirements. As part of the UK Access Management Federation, institutions are required to review and standardise the way in which they manage user identities and support is required for this process. As part of collaborative efforts, the concept of Federated Identity Management to allow secure sharing of detailed information is emerging but its role within education and research is yet to be defined. Finally, users are increasingly finding the need for personal identity management tools to support multiple-affiliation and lifelong affiliation models.

Recommendation 13	
Work area:	Identity Management Review
Description:	A review of the key players within the Identity Management sphere, including Microsoft InfoCard, the Liberty Alliance and other open source applications is proposed
Justification:	In order to best support developments within Identity Management for education and research, a full audit of options is essential
Benefit:	Informed development decisions
Risks:	Changing landscape may make information quickly out of date

Recommendation 14	
Work area:	Identity Management beyond the Institutional Boundaries
Description:	Development work to support inter-institutional and personal identity management requirements within the e-Infrastructure
Justification:	New models of identity management will be essential for moving beyond the boundaries of user-institution relationships within research
Benefit:	Cutting edge development
Risks:	Backing the wrong technological solution

G. Accounting, auditing and diagnostics tools

For an e-Infrastructure to operate successfully, tools for auditing, accounting and diagnostics will be essential for a variety of tasks such as gathering usage statistics, measuring quality of service, and supporting billing and account allocation. Although many services within the Grid and within individual institutions currently create service logs, there are a lack of tools to support analysis and application of this data in the current environment, and a lack of tools to track full workflow across institutions and services.

Recommendation 15	
Work area:	<i>Institutional Business Models in a Changing e-Infrastructure</i>
Description:	Developments to create an e-Infrastructure must take into account the institutional role and the need for e-Research to be aligned to institutional policy in terms of support, user rights and responsibilities, structures, authorities, and institutional service provision
Justification:	e-Research functions rely on existing institutional infrastructure
Benefit:	Synergy between institutional and e-Research processes
Risks:	Lack of buy-in from institutions

Recommendation 16	
Work area:	<i>Virtual Organisation Management Tools</i>
Description:	For Virtual Organisations to be successful, they need to have well-defined business, or e-administration processes that can interoperate with existing institutional and national infrastructure. Work is needed to enhance current research and development in this area, such as the TrustCoM project
Justification:	Without a formal and well-defined business process that interoperates with existing institutional infrastructure Virtual Organisations will not be successful
Benefit:	Builds on and interoperates with existing business models
Risks:	Lack of buy-in from institutions

Middleware Requirements

H. Embedding and support for production middleware

Middleware outputs are produced by a range of bodies from large organisations such as Globus to small research projects. Whilst the UK cannot finance full support models for all middleware developments, it can provide support for institutions in adopting and embedding the outputs available to them.

Recommendation 17	
Work area:	<i>UK Focus</i>
Description:	Whilst various groups within the UK track international middleware developments, there is no single focus for information about developments and how they might be exploited within the UK. Such a role is proposed to provide this focus and to co-ordinate UK contributions to international forums such as the Global Grid Forum
Justification:	Coherence of message and information
Benefit:	Single point of information for UK researchers
Risks:	Lack of take-up

I. Provide sustainable routes for required services

High-level middleware can be defined as the core functions that are ubiquitously required within the e-Infrastructure such as authentication and

authorisation, service registry and workflow. Within the UK, the Open Middleware Infrastructure Institute (OMII) has begun the task of providing robust, reliable and resilient versions of these core elements. This is an inevitably costly process. Other sustainability models include community-supported developments such as open-source libraries.

Recommendation 18	
Work area:	<i>Support for Sustainability: OMII and Supporting Models</i>
Description:	As part of its recent funding, the OMII model has expanding to include 'nodes' at the University of Manchester and the University of Edinburgh. Following on from successful review of this process, additional nodes are proposed focussing on wider support models such as building community support for open source libraries not included in the OMII full support model
Justification:	Identified as a critical activity in the e-Infrastructure Roadmap document
Benefit:	Guaranteed software support mechanisms
Risks:	Choice of software: backing the wrong models

Recommendation 19	
Work area:	<i>Management of 'data heavy' users</i>
Description:	As with any service, Grid technologies are used more heavily by a small group of users than typical usage scenarios. This work package will investigate appropriate mechanisms for supporting these users whilst minimising impact on typical users at both an institutional and national service level
Justification:	Appropriate management of such users will enhance service quality for all users
Benefit:	Service at best level for all users
Risks:	Risk of having to impose limits on data heavy users

Recommendation 20	
Work area:	<i>Community Software Development: Social Process Study</i>
Description:	Community Software development is a familiar activity within research projects, but its overall impact on and place within the research process is unclear. A study to analyse the social process and impact of community software development on academic research is proposed
Justification:	It is important to understand the place of technology processes within the changing research environment
Benefit:	Clearer understanding of the role of community software development
Risks:	Lack of buy-in from research councils and funding bodies

J. Tools for both inter- and intra- Grid requirements

Much of the focus of Grid technologies has been on large-scale collaborations across institutional and geographical boundaries using national service functionality such as the National Grid Service. Whilst this notion of open shared distributed computing is attractive, many developments will still take place within 'intragrids' or closed grid environments. Such developments will inevitably create requirements for different tools and technologies to gain the benefits of Grid innovation within a closed environment.

Recommendation 21	
Work area:	<i>The University Intragrid</i>
Description:	A programme of work to establish requirements and initiate development for intragrid tools, and to analyse how these can be supported alongside intergrid in the context of sustainability models such as OMII
Justification:	Intergrid models will not meet the full requirements of researchers in certain disciplines, such as medical researchers or institutions in terms of extent of ability to openly share compute resources
Benefit:	Ability to apply either inter- or intra- grid models in appropriate scenarios
Risks:	Closed environments at odds with open models of Grid developments

K. Organisational take-up across user communities

Take-Up of Grid and e-Research technologies is still at a relatively low level within the UK. Whilst initiatives such as e-Science Core Programme have had a significant impact in terms of raising the profile and use of the National Grid Service and related middleware technologies, ongoing support is needed to enable all research organisations within the UK to participate.

Recommendation 22	
Work area:	<i>Organisational Take-Up Analysis</i>
Description:	An analysis of take-up of Grid technologies across UK educational and research establishments
Justification:	Will justify the need for new developments and ongoing support for e-Science activities beyond the core programme
Benefit:	Clear picture of current status and evidence to support future engagement of institutions
Risks:	Difficulty in finding appropriate contacts within institutions

Digital Rights Management Requirements

L. DRM workflow across international boundaries

One of the major benefits of Grid technology is the ability to exploit resources on distributed networks internationally. This in turn means that research processes can be run and created on an international basis – raising issues about the application of digital rights management laws in different countries.

Recommendation 23	
Work area:	<i>Grid Workflow and DRM: Case Studies</i>
Description:	Case Studies that track real research processes across international boundaries with contributions from various researchers within Virtual Organisations are proposed, reflecting on potential DRM, IPR and license issues at several points in the research process
Justification:	By analysing real cases, a full picture of the implications of DRM workflow can be assessed
Benefit:	Better understanding of implications for international Grid developments
Risks:	Difficulty to define applicable laws in different countries

M. Commons

Creative Commons licences were created to help content creators express how they wished their work to be used in a user friendly manner. The initiative has gained ground on an international basis, and UK versions of the Creative Commons licences are now available. Work has begun in complementary areas, such as Scientific Commons which is exploring the wider implications of scientific data creation and use.

Recommendation 24	
Work area:	<i>Personal Digital Rights Management</i>
Description:	Initiatives such as Creative Commons allow creators more control over their IPR, but support is needed to help users understand how to protect and promote their work, and the impact that institutional affiliation or publication may have on their rights. A user engagement programme is required to support this process
Justification:	DRM and IPR is a specialist area – stakeholders will only be willing to engage in these activities if full support is offered
Benefit:	Wider take-up and appreciation of initiatives such as Creative Commons

Risks:	Lack of user and institutional buy –in
--------	--

Recommendation 25	
Work area:	<i>Creating IPR: Research Developments within Institutions</i>
Description:	Maximising the potential of the full range of research outputs within an institution is rarely achieved. Whilst researchers are creating a wealth of resources, such as datasets, software developments and scholarly communications, the institution often fails to maximise internal use and external exploitation – often failing to secure simple read access to scholarly works. A short programme of work is proposed using groups of researchers within institutions as case studies
Justification:	Support for institutions in maximising the benefits of assets
Benefit:	Benefits for institution and individual researchers in greater use of assets
Risks:	Few existing structures within institutions to support this process

N. Open Access and RAE

Open Access publication through institutional repositories and the wider Open Access agenda is changing the scholarly communications workflow. There are opportunities for institutional repositories to play a part within the Research Assessment Exercise, but questions about quality control would need to be resolved for such an agenda to be taken forward.

Recommendation 26	
Work area:	<i>Open Access Within the RAE</i>
Description:	This work area will explore options for securing quality assurance at level that could be acceptable to the RAE process within institutional repositories. This may include the use of digital signatures, control of submission, internal ratification of accuracy etc.
Justification:	This process would benefit both institutions and the full RAE process
Benefit:	Streamlining processes
Risks:	Not achieving buy-in from RAE

O. DRM and authorisation

Authorisation and Digital Rights Management have the same goal: to express who can access what. Whilst the two processes have distinct roles in the process of resource usage there are inevitable points of interaction, particularly within DRM systems.

Recommendation 27	
Work area:	<i>Authorisation and DRM Study</i>
Description:	This study will review the full DRM lifecycle as described in the JISC Intrallect report, and the points at which authorisation and DRM systems and languages interact. It will look for potential areas of non-interoperability and provide recommendations for an inclusive workflow
Justification:	Authorisation and DRM should not be seen as competing technologies but as interoperable options for resource sharing
Benefit:	Clarity on application of both technologies
Risks:	Danger of competing ‘camps’

P. IPR and Virtual Organisations

Whilst IPR and DRM models for researchers within institutions are still badly understood, the new models of Virtual Organisations challenge these very structures. Collaborative research developments between teams of research members across international boundaries and documented through shared

tools do not fit the models for DRM and IPR enforcement that are currently applied as part of the researcher-institution contract.

Recommendation 28	
Work area:	<i>IPR and Virtual Organisations</i>
Description:	As researchers become more involved in working within Virtual Organisations, there will be more challenges to the existing contractual arrangements between researchers and affiliated institutions in terms of Intellectual Property Rights. Case Studies to investigate alternative models for IPR within VOs are proposed
Justification:	Such issues should be addressed as early as possible in the evolution of Virtual Organisations to prevent barriers occurring in the future
Benefit:	Growing use of Virtual Organisation models
Risks:	Study may slow down innovation in VOs

Recommendations

The 'Options for the Future' appraisal makes 28 fine-level recommendations for future development activities. These individual work areas have not been costed as various models exist for taking the work forward. Whilst this study should not be considered as a structure for funding proposals or as a bid for potential funding, it is worth noting appropriate structures under which development work could be taken forward. Four themes have been identified that cut across the development work described and have the potential to be scoped as working areas. These are:

Theme	Recommendation references
Work to inform development requirements	7,9,11,12,13,25,26,27
Technology and service development	1,3,4,6,14,16,18,21
Changing practise	2,5,8,10,17,19
Social and impact studies	15,20,22,23,24,28

In addition to the development recommendations, the working group would like to make the following recommendations:

- Timescales: this report attempts to identify the requirements for AAA, Middleware and DRM within the timeframe of the Science and Innovation Investment Framework which looks forward to 2014. Proposing requirements across such as long timescale within as fast-moving technological environment is a high risk strategy, and it will be important for proposals to be reviewed on a frequent basis. A review every two years is suggested.
- Cross-working and synergies: the working parties attached to the e-Infrastructure Steering Group have been working independently of each other, and there will inevitably be duplication of information and proposals across reports. It is recommended that time is taken to review the reports against each other and to identify duplications and synergies.
- User benefits and applications: it will be important to further scope the benefits and justification for work areas and to ensure that a clear user / stakeholder perspective is retained across e-Infrastructure planning and report. It is recommended that clear user cases be developed from 'theoretical ideal' statements.
- International synergy: it will be important for the UK to recognise international developments, not only in individual areas as shown in 'current and known plans' but also at a strategic level in terms of planning for e-Infrastructure. It is recommended that updates on international developments, such as the US cyber-infrastructure initiative, be pursued by the Steering Group.
- Definitions and vocabulary: all of the working group reports will be using terminology such as 'e-Infrastructure' and 'Virtual Organisations'. It will be beneficial to overall developments to agree a shared definition of these terms to ensure that the same application is used across the working groups. A shared glossary for the reports is proposed.

Appendix A: Working Group Membership

Membership of the AAA, Middleware and DRM working group:

Leona Carpenter: Consultant, Joint Information Systems Committee

David Chadwick: Professor of Information Systems Security, University of Kent

Andrew Cormack: Chief Security Advisor, UKERNA

David DeRoure: Head of Grid and Pervasive Computing, Southampton University

Brian Gilmore: Director of Computing Services, University of Edinburgh

Nicole Harris: Programme Manager, Joint Information Systems Committee

Jens Jensen: CA Manager, Rutherford Appleton Laboratory

David Kelsey: Head of Particle Physics Computing, Rutherford Appleton Laboratory (EGEE / GridPP)

Brian Matthews: Rutherford Appleton Laboratory

Andrew MacNab: Coordinator of Security Middleware Groups, GridPP & Manchester HEP, Manchester University

Charles Oppenheim: Professor of Information Science, Loughborough University

John Paschoud: Projects Manager, London School of Economics

Appendix B: Glossary

APEL	EGEE Accounting Application
APIG	All Parliamentary Internet Group (UK Government)
A-Select	A-Select is a framework that allows users to authentication by several means with Authentication Service Providers such as universities and banks
Athens	Access Management System serving UK Higher and Further Education through JISC contract
Authentication	The act of confirming that someone is who they say they are
Authorisation	The process which confirms what a user may access
Certificate Authority	A trusted third party which issues digital certificates for use by other parties
CIO	Chief Information Officer Council
Connecting for Health	NHS Scheme to implement modern computing services for patient care and services
Creative Commons	A non-profit organisation offering a range of license formats as an alternative to copyright
DEST	Department of Education, Science and Training in Australia
DGAS	Distributed Grid Accounting System
DLF	Digital Library Federation
DRM	Digital Rights Management
eduRoam	A RADIUS based architecture to allow users to 'roam' between institutional campuses using their home credentials to gain access to services
EGEE	Enabling Grids for E-Science
e-Government Interoperability Framework	The e-GIF defines the technical policies and specifications governing information flows across government and the public sector
E-Government Unit	Cabinet Office Unit responsible for formulating IT strategy and policy for UK Government and public sector
e-Infrastructure	Term used to described the vision for next generation IT infrastructures for research describe in the Science and Innovation Investment Framework
Federated Access Management	Federated Access Management builds a trust relationship between Identity Providers (IdP) and Service Providers (SP). It devolves the responsibility for authentication to a user's home institution, and establishes authorisation through the secure exchange of information (known as attributes) between the two parties
gLite	Middleware toolkit from EGEE
Globus Alliance	Research project developing a software infrastructure for distributed computing on a world-wide scale
GridPP	UK Particle Physics grid
Higgins	a framework that will enable users and enterprises to integrate identity, profile, and relationship information across multiple systems
IGTF	International Grid Trust Federation

IPR	Intellectual Property Rights
JANET	Joint Academic Network
JISC	Joint Information Systems Committee
JISC / DEST e-Framework	The primary goal of the initiative is to produce an evolving and sustainable, open standards based service oriented technical framework to support the education and research communities
JISC Information Environment	a range of services, tools and mechanisms for colleges and universities to exploit fully the value of online resources and services
Liberty Alliance	The mission of the Liberty Alliance Project is to establish an open standard for federated network identity through open technical specifications
Microsoft InfoCard	Codename for current Microsoft developments for identity management solutions
NGS	National Grid Service
NHS National Programme for IT	Framework for IT provision under which 'Connecting for Health' is run
NISO	National Information Standards Organization
NREN	National Research and Education Network
OASIS	Organization for the Advancement of Structured Information Standards
OGSA	Open Grid Services Architecture
OMII	Open Middleware Infrastructure Institute
Open Access	Open Access publishing, where the author (usually the author's research funder or institution) pays the publication costs, has been proposed as an alternative to a subscription-based model
PERMIS	Privilege and Role Management Infrastructure Standards
PKI	Public Key Infrastructure
PLS	Publishers Licensing Society
PMA	Policy Management Authority
RADIUS	a server for remote user authentication and accounting
SAML	Security Assertion Mark-Up Language
Science Commons	A Creative Commons project to extend licenses to serve all scientific resources
SOAP	Simple Object Access Protocol
SWITCH	Swiss NREN
TERENA	Trans European Research and Education Networking Association
TERENA SCS	TERENA Server Certificate Service
UKERNA	UK Education and Research Network Association
Virtual Organisation	The structure which 'organises' a group of researchers and other end-users collaborating across institutional boundaries
VOMS	Virtual Organization Membership Services
WS-Security	A means for applying security to web services by incorporating features in to the header of a SOAP message
X.509	a PKI standard

Appendix C: References

APIG:	< http://www.apig.org.uk/ >.
A-Select:	< http://a-select.surfnet.nl/ >.
Athens:	< http://www.athensams.net >.
Chief Information Officer Council:	< http://www.cio.gov.uk/ >.
Connecting for Health:	< http://www.connectingforhealth.nhs.uk/ >.
Counter:	< http://www.projectcounter.org/ >.
Creative Commons:	< http://creativecommons.org/ >.
DEST:	< http://www.dest.gov.au/ >.
DLF:	< http://www.diglib.org/ >.
eduRoam:	< http://www.eduroam.org/ >.
EGEE:	< http://public.eu-egee.org/ >.
e-Government Interoperability Framework:	< http://www.govtalk.gov.uk/schemasstandards/egif.asp >.
E-Government Unit:	< http://www.cabinetoffice.gov.uk/e-government/ >.
e-Science Core Programme:	< http://www.rcuk.ac.uk/escience/ >.
Globus Alliance:	< http://www.globus.org/ >.
Grid Operations Support Centre:	< http://www.grid-support.ac.uk/ >.
GridPP:	< http://www.gridpp.ac.uk/ >.
Higgins:	< http://www.eclipse.org/higgins/ >.
JISC:	< http://www.jisc.ac.uk/ >.
JISC Intrallect Report:	< http://www.intrallect.com/drm-study/ >.
Liberty Alliance:	< http://www.projectliberty.org/ >.
License Expression Working Group:	< http://www.niso.org/committees/License_Expression/LicenseEx_comm.html >.
Microsoft InfoCard:	< http://msdn.microsoft.com/windowsvista/building/infocard >.
NGS:	< http://www.ngs.ac.uk/ >.
NHS National Programme for IT:	< http://www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/NationalITProgramme/fs/en >.
NHS:	< http://www.nhs.uk/ >.
NISO:	< http://www.niso.org/ >.
OASIS:	< http://www.oasis-open.org/home/index.php >.
OMII:	< http://www.omii.ac.uk/ >.
PERMIS:	< http://www.permis.org/ >.
PLS:	< http://www.pls.org.uk/ >.
RADIUS:	< http://www.gnu.org/software/radius/radius.html >.
SweGrid:	< http://www.swegrid.se/ >.
SWITCH:	< http://www.switch.ch >.
TeraGrid:	< http://www.teragrid.org/ >.
TERENA:	< http://www.terena.nl >.
UK e-Science Certificate Authority:	< https://ca.grid-support.ac.uk >.
UKERNA:	< http://www.ukerna.ac.uk >.
VOMS:	< http://edg-wp2.web.cern.ch/edg-wp2/security/voms/ >.