

Mapping security services to the e-Framework

Final report

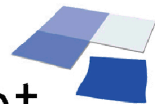
CC331D004-1.1

9 June 2009

Cover + 20 pages

Dr Max Hammond
Dr Claire Davies

curtis+cartwright



Curtis+Cartwright Consulting Ltd

Main Office: Surrey Technology Centre,
Surrey Research Park, Guildford
Surrey GU2 7YG

tel: +44 (0)1483 685020
fax: +44 (0)1483 685021
email: postmaster@curtiswright.co.uk
web: <http://www.curtiswright.co.uk>

Registered in England: number 3707458

Registered address:
Baker Tilly, The Clock House,
140 London Road, Guildford,
Surrey GU1 1UW

Executive summary

- 1 The objectives of this project were to contribute UK security functionality documentation to the e-Framework and to compare and contrast the security mechanisms in place across the partner countries in the e-Framework to support increased interoperability. This project was not tasked to review the e-Framework, and has not undertaken that activity; but we have made some observations in this document which represent those of a contributor rather than a reviewer.
- 2 The project was split into three phases: 1) initiation and landscape study; 2) documenting core UK security services; 3) synthesis and reporting. We discussed and agreed all outputs with the JISC Programme Manager.
- 3 The intended audience for this document is JISC (Sections 1, 2, 3 and 4 are most relevant) and the wider community (Sections 1 and 5 are most relevant).

Project outputs

- 4 The landscape study provided a useful (and necessary) analysis of the progress that the international partners had made toward documenting their security architectures, and collated information on the security approaches of the UK e-Science grid and the UK federation. From this preliminary work, it became clear that there was not enough security documentation on the e-Framework from the international partners to meet the original objectives of this project. Accordingly, the focus shifted to documenting further UK security functionality. We have submitted a range of documentation to the e-Framework (see Section 3 and Annex B).

Key findings

- 5 The key findings are set out in full in Section 4 and are, in summary:
 - The e-Framework takes time to understand and the available documentation and support does not always help clarification.
 - The overheads for documenting should be minor if the e-Framework is incorporated in the design process from the outset, although it is difficult and time-consuming to retrospectively document existing real-world functionality.
 - The e-Framework review process did not operate in a timely manner for our project.
 - Not every development project is suitable for documenting on the e-Framework. Functionality that does not consist of much machine-to-machine flow, and where there are few service interfaces, do not fit well with the e-Framework model.
 - Using the e-Framework to compare security functionality across partners is not currently possible as there is not enough relevant e-Framework documentation published.
 - The e-Framework is not the most appropriate way of analysing security interoperability - the challenges frequently lie at policy or conceptual levels which are not adequately represented within the e-Framework.

Guidance to projects contributing to the e-Framework

- 6 Some guidance to potential e-Framework contributors is provided in Section 5. In summary:
 - Not every project/service should contribute to the e-Framework; suitability should be assessed and agreed with JISC on a per project basis.

- The e-Framework is most beneficial for service-based systems with reusable interfaces.
- Trying to document project outputs for the e-Framework at the conclusion of the project is not the most effective approach. If the e-Framework is incorporated into the design process from the outset it can provide a structure to help with developing reusable software; used in this way, the overheads should be minimal.
- The e-Framework model can lead to spiralling complexity in documentation. It is important to apply good diagramming practice to the development of SUMs: consider their scope carefully, and show the important information without unnecessary detail.

Working with the e-Framework

- 7 This project has worked with the e-Framework to reflect on the key findings (Section 4) and the guidance outlined in Section 5.
- 8 The e-Framework is committed to learning from experiences to improve its approach, and the findings from this project have informed the evolution of the e-Framework, and the outputs will be factored into the community focussed validation of the e-Framework technical approach which is scheduled from June-December 2009. Annex C provides an update from Ian Dolphin (Director of the e-Framework) on how the e-Framework has evolved since this project was completed and how this project has informed these changes.

List of contents

Executive summary	1
Document history	3
List of contents	3
1 Introduction	5
1.1 General	5
1.2 Background	5
1.3 Overview of the project	6
1.4 Document overview	6
2 Methodology	7
2.1 General	7
2.2 Phase 1: initiation and landscape study	7
2.3 Phase 2: documenting core UK security services	7
2.4 Phase 3: synthesis and reporting	8
3 Project outputs	9
3.1 Landscape study	9
3.2 e-Framework documentation	9
3.3 Final report	10
3.4 Completion report	10
4 Project findings	11
4.1 Summary of findings	11
4.2 Implications for future work	12
5 Guidance for projects contributing to the e-Framework	13
5.1 Introduction	13
5.2 The pressure to contribute	13
5.3 Deciding whether to contribute	13
5.4 The e-Framework model	14
5.5 Summary	15
A List of abbreviations	17
B Submitted e-Framework documentation	19

Document history

Version	Date	Description of Revision
0.1	29 December 2008	Draft for internal review
0.2	6 January 2009	Revised draft for internal sign-off
1.0	8 January 2009	Draft for review by James Farnhill
1.1	8 June 2009	Issue version incorporating comments from a meeting with the e-Framework

This page is intentionally blank

1 Introduction

1.1 General

1.1.1 This report has been prepared by Curtis+Cartwright Consulting Ltd. The report documents the project's methodology, its outputs and its key findings. It is the final deliverable of a JISC project funded under the e-Infrastructure programme (2006-2009) to map security functionality in the UK education and research community to the e-Framework.

1.1.2 This is the issue version of the document (v1.1).

1.2 Background

Security functionality in the UK education and research community

1.2.1 JISC's aim is to support secure¹ access to the resources it procures on behalf of the UK education and research community, and thereby maintain the trust of the users, service providers and institutions.

1.2.2 Much of the infrastructure within which resources are stored and (potentially) from which resources are accessed is beyond JISC's control, for example institutional networks and the Internet. Accordingly, JISC does not have responsibility for the security of the resources it procures but does provide some centralised security functionality to support access to these resources in a secure manner. This centralised security functionality includes:

- **The UK Access Management Federation for Education and Research (the UK federation):** the UK federation was launched in November 2006 and provides a framework within which registered organisations, institutions and individuals can exchange information to support secure access to resources.
- **The National Grid Service (NGS) Certification Authority (CA)** provides X.509 certificates for the UK e-Science community. The CA is part of the NGS project, funded by JISC, Engineering and Physical Sciences Research Council (EPSRC) and the Science and Technology Facilities Council (STFC).

The e-Framework

1.2.3 The primary aim of the e-Framework² is to facilitate technical interoperability within and across the education and research community through improved strategic planning and implementation processes. It is an evolving knowledge base containing technical documentation of e-infrastructure, both in use and in development. The e-Framework supports reuse of functionality and a service-oriented approach to design. The service-oriented approach dictates that functionality is grouped around business processes and packaged as interoperable services.

1.2.4 The e-Framework is organised as five domains: learning and teaching; research; administration; IT Services; libraries and common. Security functionality crosses all of these domains. It is intended that documented security functionality can be reused by the e-Framework community when developing and implementing services across these domains (eg to provide access controls for an administrative service). Documenting security

¹ Covering confidentiality, integrity and availability.

² See <<http://www.e-framework.org>>

functionality in a common way will also support interoperability between different communities (*eg* interaction between different national access management federations).

1.3 Overview of the project

1.3.1 JISC has funded a large number of projects in recent years that have focused on secure access to information resources.³ Similar work has been conducted by JISC's international e-Framework partners, including recent initiatives in Australia and New Zealand which have mapped aspects of their respective security federations to the e-Framework. Accordingly, the objectives of this project were to:

- contribute UK security functionality to the e-Framework;
- compare and contrast the security mechanisms in place across the partner countries in the e-Framework to support increased interoperability.

1.3.2 It was also anticipated that as we would be submitting a large amount of documentation to the e-Framework this project could reflect on the experiences of contributing to the e-Framework (*ie* documenting, submitting and getting approval to publish). It was hoped that our experiences would benefit future projects submitting documentation to the e-Framework. We were explicitly not asked to review the process – we have only made observations based on our experiences.

1.3.3 The anticipated outcome of the project was an international picture of service based security measures in support of their respective education and/or research communities. This will allow the e-Framework partners to maximise benefit and value by making best use of the available resources and minimising duplication of effort.

1.3.4 This project commenced in February 2008 and was split into three phases:

- Phase 1: initiation and landscape study;
- Phase 2: documenting core UK security services;⁴
- Phase 3: synthesis and reporting.

1.3.5 The objectives and approach are set out in full in the project plan on the project's website.⁵

1.4 Document overview

1.4.1 The remainder of this document is structured as follows:

- Section 2 sets out the approach taken to the project;
- Section 3 provides an overview of the project outputs;
- Section 4 summarises the project findings;
- Section 5 provides guidance to the community for submitting documentation to the e-Framework.
- Annex A provides a list of the abbreviations used in this document;
- Annex B presents a full list of the documentation that has been developed by this project and submitted to the e-Framework.

³ For example projects within the Authentication, Authorisation and Accounting (AAA), Core Middleware and e-Infrastructure programmes.

⁴ The scope was limited to the systems and policies of the UK Access Management Federation and the National grid Service Certification Authority (NGS CA), and preceding JISC projects funded under the e-Infrastructure programme and the Access Management programme.

⁵ See <<http://www.jisc.ac.uk/whatwedo/programmes/einfrastructure/mappingsecurityservices.aspx>>

2 Methodology

2.1 General

2.1.1 This was a largely exploratory project, so an iterative approach to information capture, documentation and validation was taken where possible in order to meet the project objectives.

2.2 Phase 1: initiation and landscape study

2.2.1 The Landscape Study provided the foundation for the rest of the project. It was therefore important to ensure that the information contained within it was an accurate representation of the current landscape, and that it fitted with JISC's and the e-Framework's goals for documentation of UK security functionality. We achieved this by:

- engaging with key stakeholders to understand current systems and documentation;
- consulting with the JISC, the e-Framework Technical Editor, the international partners, the UK federation and the NGS to formally review the Landscape Study;
- placing the document on the e-Framework Community Wiki for wider comment.

2.2.2 The Landscape Study highlighted that there was minimal security documentation on the e-Framework from the international partners. This made it impossible to meet the objectives for Phase 3 (see assessment in sub-section 2.4).

2.3 Phase 2: documenting core UK security services

2.3.1 The e-Framework is a relatively new entity which is bringing together diverse national and international communities. Due to the limited numbers of existing contributions on the e-Framework, especially those specific to grid computing, some interpretation and judgement was required to define and write this project's contributions. We allocated significant effort to understanding the concept of the e-Framework, to understand how real-world systems may be represented on it, and finally to document these systems in e-Framework format.

2.3.2 The Landscape Study proposed an approach to documentation which had been reviewed by stakeholders. In particular, decisions had to be made on the level(s) of abstraction, boundaries and perspectives used (*eg* specificity, grouping of functional elements, and how to present the information). A number of potential challenges and issues which might be encountered during the documentation process were also identified. The list of documentation was later refined as our knowledge of the e-Framework progressed, and we started producing documentation.

2.3.3 We discussed and prioritised the documentation to be produced in conjunction with the JISC Programme Manager and other key stakeholders. It was originally intended that we would submit an initial set of documentation to the e-Framework for review, then use the comments from the e-Framework Integrity Group (the eFIG) to inform any further documentation we wrote. However, this was not possible due to the length of the review period. We have withheld some effort to address comments on the documentation after the project has formally closed.

2.4 Phase 3: synthesis and reporting

2.4.1 This phase of the project was originally meant to comprise:

- **SUMs comparison:** a comparison of the UK, Netherlands, NZ, and Australian security SUMs to identify similarities and differences between systems;
- **Final report:** a final report providing a high-level view of the international security landscape and ongoing developments, identify interoperability “pain points”.
- **Roadmap:** a roadmap to help JISC understand subsequent activities to undertake and recommendations for further work.

2.4.2 However, not all of this work could be completed for the following reasons:

- **SUMs comparison:** there are currently not enough security SUMs on the e-Framework from the international partners to allow a comparison with the UK functionality (see Section 4 for further information). It is likely that the information required has been documented locally by the international partners, but has not yet been documented for the e-Framework. However, collecting this information was not considered to be a productive way to use the remaining effort from this project, neither by JISC nor the project team.
- **Final report:** a high-level view of international developments was provided in the landscape study, and nothing more could be added in Phase 3. Interoperability pain points cannot be identified as the documentation is not available on the e-Framework.
- **Roadmap:** the UK federation and the NGS are now well established and are addressing necessary technical developments themselves; projects addressing the interoperability between the NGS and the UK federation are already being funded by JISC. In absence of a comparison with the international partners’ security functionality and an analysis of interoperability, there is currently no future work that we can recommend in addition to that currently being undertaken by the UK federation, the NGS and JISC.

2.4.3 Following discussion with the JISC Programme Manager, it was decided that the effort for Phase 3 would be devoted to completing further e-Framework documentation, in particular including the wider NGS (*eg* the use of proxy certificates) which offer some interesting examples of machine-to-machine flow.

2.4.4 The other deliverables for this phase are a Final Report (this document) and a Completion Report.

3 Project outputs

3.1 Landscape study

3.1.1 A Landscape Study⁶ was produced which formed the foundation for the rest of the study. It provides a high-level synopsis (as of September 2008) of:

- the e-Framework partners' security functionality and e-Framework documentation;
- the UK federation and the NGS CA security policies and systems.

3.2 e-Framework documentation

3.2.1 This project has written and contributed a wide range of Service Usage Models (SUMs) and Service Genres to the e-Framework for the UK federation, the NGS CA and the wider Grid. These are summarised in the table below. Annex B provides further details of the documentation.

Title	Document type	Status
UK federation: top-level view	SUM	Published on e-Framework
UK federation: manage users	SUM	Submitted
UK federation: use services	SUM	Published on e-Framework
NGS CA: issue certificate	SUM	Comments received and incorporated; awaiting publication
NGS CA: renew certificate	SUM	Submitted
NGS CA: user-revoke certificate	SUM	Submitted
Virtual organisations on the Grid	SUM	Submitted
Proxy access to grid resources	SUM	Submitted
Cryptography	SUM	Submitted
Certify	Service genre	Submitted
Decrypt	Service genre	Submitted
Encrypt	Service genre	Submitted
Generate entropy	Service genre	Submitted
Hash	Service genre	Submitted
Issue	Service genre	Submitted
Sign	Service genre	Submitted
Verify	Service genre	Submitted

Table 3-1: list of e-Framework documentation produced by this project

⁶ Mapping security functionality to the e-Framework: landscape study. Curtis+Cartwright Consulting Ltd. v1.0. 2 September 2008.

3.3 Final report

The final report (this document) summarises what the project has done and what it has achieved, including a discussion of the methodology, outputs, key findings and guidance for projects submitting to the e-Framework.

3.4 Completion report

- 3.4.1 A completion report,⁷ an internal document for JISC stakeholders, was produced to “sign-off” the project and document the observations of the project team whilst undertaking it.

⁷ *CC331D003: Mapping security functionality to the e-Framework: completion report.* Curtis+Cartwright Consulting Limited.

4 Project findings

4.1 Summary of findings

The e-Framework takes time to understand

- 4.1.1 The e-Framework is complex and it is difficult to gain quickly a good understanding of the e-Framework in order to assess how a project may contribute. The available documentation and support does not always help. Furthermore, there are currently very few published SUMs, genres and expressions on the e-Framework to guide potential contributors; what has been published is not consistent neither in terms of content nor approach. Significant time and effort is required to work out the best way to develop documentation. Our experience suggests that applied guidance illustrating real systems documented using the e-Framework model would be useful.

The overheads for documenting should be minor if the e-Framework is incorporated in the design process from the outset

- 4.1.2 It is difficult and time-consuming to document retrospectively existing real-world functionality using the e-Framework templates. If the e-Framework is incorporated into the design process from the outset it can provide a structure to help with developing reusable software. Used in this way, the overheads should prove minor.

Not every development project is suitable for documenting using the e-Framework

- 4.1.3 Functionality that does not consist substantially of machine-to-machine flow, and where there are few service interfaces, does not fit well with the e-Framework model and is difficult to document effectively. Section 5 provides guidance about what functionality is most appropriate to document in the e-Framework.

Using the e-Framework to compare and contrast security functionality across partners is currently not possible

- 4.1.4 Although all of the partners are committed to the e-Framework, there is currently not enough documentation in the e-Framework to allow a comparison of security functionality of the international partners, and some partners do not have any immediate plans for documentation. It is also evident that the partners' documented security functionality is all related to federated access management (there is currently no grid functionality documented), and what documentation there is does not represent complete or current systems:
- **Australia** has relatively well advanced plans to populate the e-Framework, however, only the Meta Access Management System (MAMS) project (precursor to the Australian Access Federation (AAF)) has been documented as a SUM. A broader AAF SUM which builds on the MAMS SUM is in development.
 - **New Zealand** has an Identity and Access Management (IAM) SUM on the e-Framework which provides the mechanisms for identities to be managed within an Identity Provider (IdP) that is providing an authenticate service. There are no plans to add any further documentation to the e-Framework over the next few months.

- **the Netherlands** does not currently have any security documentation on the e-Framework. The SURFfederatie is in its early stages, and the big challenge for the Netherlands in developing e-Framework documentation is “learning by doing”.

The e-Framework is not the most appropriate way of analysing security interoperability

- 4.1.5 The e-Framework probably does not represent the best approach to analysing interoperability opportunities and challenges in existing security infrastructures: interoperability challenges frequently lie at policy or conceptual levels which are not adequately represented within the e-Framework.

4.2 Working with the e-Framework

- 4.2.1 This project has worked with the e-Framework to reflect on the key findings (above) and the guidance outlined in Section 5.
- 4.2.2 The e-Framework is committed to learning from experiences to improve its approach, and the findings from this project have informed the evolution of the e-Framework, and the outputs will be factored into the community focussed validation of the e-Framework technical approach which is scheduled from June-December 2009. Annex C provides an update from Ian Dolphin (Director of the e-Framework) on how the e-Framework has evolved since this project was completed and how this project has informed these changes.

4.3 Implications for future work

- 4.3.1 In terms of UK security functionality in the education and research sector, we have now documented the main security functionality for the NGS CA, wider NGS and the UK federation as SUMs on the e-Framework. We do not recommend that any further documentation is produced for extant systems as the overheads are high; it would be more useful to reflect on how the e-Framework should develop and consider how the current documentation might best be used.
- 4.3.2 Projects addressing the interoperability between the NGS and the UK federation are already being funded by JISC, and are required to document the outputs on the e-Framework. The guidance provided in Section 5 may be helpful to these (and other) projects developing e-Framework documentation.
- 4.3.3 Projects which are developing new code and which have a service-based structure (interfaces which are likely to be reused) should use e-Framework documentation as the basis for the initial architectural design of their system and contribute to the e-Framework (see Section 5 for further information).
- 4.3.4 If the international partners continue to be committed to working together, and a “common global infrastructure” remains an aspiration, it will be important that a view of the international security landscape is developed in the future. This should include identification of similarities, differences and analysis of interoperability “pain points”. This could be done as a future project independently from the e-Framework, coordinating effort to gather the necessary information.

5 Guidance for projects contributing to the e-Framework

5.1 Introduction

5.1.1 This section provides guidance to those projects that wish to submit content to the e-Framework, and also to potential bidders who have been asked to consider whether their projects could contribute to the e-Framework. The guidance is based on our experience of contributing documentation to the e-Framework over the last 12 months – it is not intended to replace the extensive information available on the e-Framework website.⁸

5.2 The pressure to contribute

5.2.1 Most JISC Invitations To Tender (ITTs) or Calls for technical projects now contain a reference to the e-Framework, often requiring respondents to identify how they will “map” or “contribute” the outputs from the project to the e-Framework.

5.2.2 It is difficult to gain a good understanding of the e-Framework quickly in order to assess how a project may contribute to it. There are currently very few published SUMs, genres and expressions on the e-Framework to guide people, and what is there is not consistent in terms of content or approach. Also, the term “map” implies that the e-Framework is a normative architecture, when it is not.

5.2.3 Consequently, most respondents are obliged to state how they will contribute outputs with little understanding of the e-Framework. The e-Framework can, however, be seen by project managers as a useful focus for planning and recording technical outputs, rather than as an additional burden.

5.2.4 In the following sub-sections we have tried to provide some guidance which will aid e-Framework contributors.

5.3 Deciding whether to contribute

What should go in?

5.3.1 The e-Framework is well-suited to service-oriented design, where system elements have well-defined interfaces which are likely to be reused. It is not an ideal repository for business process analysis, although some analysis is required to support submissions. It is also not intended to be a repository for documentation of existing systems which are well-documented elsewhere (*eg* Shibboleth).

5.3.2 To get the most benefit from the e-Framework, it is best to use the e-Framework approach during the initial planning for your project – considering how to design and implement “services”. If your project outputs are likely to include reusable services, it is likely to be worth contributing to the e-Framework.

5.3.3 When responding to an ITT, we believe that “the outputs are not likely to be appropriate for contribution to the e-Framework” should be a valid response. This statement should be justified in the proposal, and it may be helpful to review and agree this decision with JISC once the project is underway.

⁸ <<http://www.e-framework.org>>

How to develop e-Framework documentation

- 5.3.4 The e-Framework document templates demand analysis of the overall business requirement, the business processes which support the overall requirement, the functionality of the system which will provide these business processes, and the structure of the system which implements the functionality. The e-Framework is not concerned with implementation specifics, but it is the opinion of this project that e-Framework SUMs and Service Expressions must contain some implementation details; the choice of how to arrange services is an implementation artefact.
- 5.3.5 The e-Framework documents support a structured approach to software development, and if a methodology which is consistent with e-Framework documents is used, there is likely to be little additional work needed to contribute. Most software development follows this process of requirements analysis, architectural design, and code generation – but possibly without documenting each stage.
- 5.3.6 There is much content on the e-Framework website about the goals of the e-Framework, the types of e-Framework documentation, the submission and review process and templates for documentation. The e-Framework also has a Community Wiki, but there are few active participants at the time of writing. The Technical Editor and the eFIG review all documentation submitted to the e-Framework prior to publication. Early contact with the Technical Editor is recommended to help develop a view as to how to use the e-Framework.

5.4 The e-Framework model

- 5.4.1 The e-Framework model has a shallow structure consisting of Service Expressions, Service Genres and Service Usage Models. As, at the time of writing, there is still debate within the e-Framework programme around the conceptual basis of these components, projects contributing to the e-Framework will need to accept that there is some uncertainty in the best approach to take.
- 5.4.2 The document structure lends itself to clear documentation of service-oriented architectures (seeing a service as a bundle of related functionality), but recent guidance from the e-Framework sees services as abstract and discrete functions (rather than functionalities) – this can easily lead to spiralling complexity within documentation.⁹
- 5.4.3 We believe that good practice in diagramming transfers directly to e-Framework SUMs – the information which is necessary to understand the concept should be shown, and the detail hidden. Within the e-Framework concept, the detail may be hidden as a nested SUM, or as a service (expression or genre). We have used the graphical modelling languages UML and BPMN extensively within the SUMs we have generated; we believe that they are excellent tools for transferring structural and process flow information.
- 5.4.4 Overall, the approach should probably be: “what is the best way to share the important information from my project – the concepts, the structure and the detail of the interfaces?” Complex systems should be broken up into manageable chunks, rather than seeing e-Framework documentation as the place to store the full detail of the systems.

⁹ For example, Shibboleth IdP could reasonably be described as a service: it presents an interface with a range of well-defined behaviours. However, current e-Framework guidance is that services should reflect simple nouns, and the functionality of Shibboleth IdP is more complex than this. Shibboleth IdP could be represented as a SUM, but then the structure of Shibboleth IdP would need to be documented although none of its elements are individually reusable.

5.5 Summary

5.5.1 To summarise:

- Not every project/service should contribute to the e-Framework; suitability should be assessed and agreed with JISC on a per project basis.
- The e-Framework is most beneficial for service-based systems with reusable interfaces.
- Trying to document project outputs for the e-Framework at the conclusion of the project is not the most effective approach. If the e-Framework is incorporated into the design process from the outset it can provide a structure to help with developing reusable software; used in this way, the overheads should be minimal.
- The e-Framework model can lead to spiralling complexity in documentation. It is important to apply good diagramming practice to the development of SUMs: consider their scope carefully, and show the important information without unnecessary detail.

This page is intentionally blank

A List of abbreviations

AAF	Australian Access Federation
BPMN	Business Process Modelling Notation
CA	Certification Authority
CM	Core Middleware
eFIG	e-Framework Integrity Group
EPSRC	Engineering and Physical Sciences Research Council
IAM	Identity and Access Management
IdP	Identity Provider
ITT	Invitation To Tender
JISC	Joint Information Systems Committee
MAMS	Meta Access Management System
NGS	National Grid Service
RA	Registration Authority
SOA	Service Oriented Architecture
SP	Service Provider
STFC	Science and Technology Facilities Council
SUM	Service Usage Model
UML	Unified Modelling Language

This page is intentionally blank

B e-Framework documentation

B.1.1 The e-Framework documentation that was developed as part of this project is shown in the following table. Note that where the status is 'submitted', the documentation was originally submitted to the e-Framework between August 2008 and January 2009, but due to changes in the e-Framework submission process they are awaiting review.

Title	Document type	Description	Status
UK federation: top-level view	SUM	This SUM provides a high-level view of the UK federation business processes, outlining the processes that are in place in order to manage UK federation members, federated Service Provider (SP) and Identity Provider (IdP) entities, user management, service usage and support and monitoring activities. This SUM provides cohesion for the lower-level UK federation SUMs, which provide more detail on the processes supported by the UK federation.	Published
UK federation: manage users	SUM	This SUM outlines the processes surrounding the membership lifecycle for users of federated resources. Some of these processes will be similar to those employed by other nations' federations, and may be informative to organisations who wish to interact with the UK federation.	Submitted
UK federation: use services	SUM	This SUM outlines the processes by which registered users are authenticated and authorised to gain access to federated resources. This process is likely to be representative of that used by other nations' federations and may be informative to organisations who wish to interact with the UK federation.	Published
NGS CA: issue certificate	SUM	Issuing a certificate to a user is an essential prerequisite before that user can use grid resources. This SUM provides the process by which public key cryptographic certificates are issued to users of the grid, co-ordinating the user, RA and the CA.	Comments received and incorporated, awaiting publication
NGS CA: renew certificate	SUM	Certificates are issued with a finite period of validity. This SUM sets out the process by which these certificates are re-issued to users of the grid at the end of the certificates validity.	Submitted
NGS CA: user-revoke certificate	SUM	An important function within a public key infrastructure is the ability to revoke a certificate. This SUM covers the case where a user has initiated the revocation of his or her own certificate.	Submitted
Virtual organisations on the Grid	SUM	This SUM describes a method of generating Attribute Certificates (ACs) containing authorisation information for entities identified by a Public-Key Infrastructure (PKI). Specifically, ACs setting out membership and role of groups within a Virtual Organisation (VO) are generated, to enable Role-Based Access Control (RBAC) by relying parties. This SUM contains the processes necessary for managing VOs, for managing the users within those VOs, and for generating ACs.	Submitted

Table B-1 (part 1 of 2): list of e-Framework documentation produced by this project

Title	Document type	Description	Status
Proxy access to grid resources	SUM	This SUM shows how a RFC3820-compatible proxy service (as implemented by the MyProxy software) can facilitate access to grid resources	Submitted
Cryptography	SUM	"Crypto" is a basic technique which currently underpins all secure communication on the internet. It provides the raw tools which allow communications and files to be encrypted and decrypted, and their authenticity confirmed. This SUM provides a simple model of the key processes involved in providing crypto functionality.	Submitted
Certify	Service genre	Certification is the process by which some object is certified as being created, validated or approved by an organisation, individual or system. This service genre describes the function to certify an object as authentic.	Submitted
Decrypt	Service genre	Decrypt represents a fundamental capability which can support the confidentiality and authenticity of electronic information. Encryption (and hence decryption) underpins all secure online communications. This genre provides the function to decrypt a ciphertext object using a key to generate a plaintext object.	Submitted
Encrypt	Service genre	Encrypt represents a fundamental capability which can support the confidentiality and authenticity of electronic information. This genre provides the function to encrypt a plaintext object using a key to generate a ciphertext object.	Submitted
Generate entropy	Service genre	The ability to generate randomness is necessary for a range of tasks, and especially cryptography. This service genre provides a source of entropy.	Submitted
Hash	Service genre	This genre provides only one function: to generate a hash for an object. Hashing data is an important capability which supports integrity and digital signatures. A cryptographic "hash function" is a transformation which takes input data of arbitrary length and generates a "hash" of fixed length. Hashing is used within most secure communication and digital signature applications.	Submitted
Issue	Service genre	The Issue service genre covers the transfer of possession (although not necessarily ownership) of an object from one entity to another. This MAY include providing a mechanism for the recipient to collect the object. The data object MAY be a representation of a physical object, in which case the data object will not be transferred to the recipient.	Submitted
Sign	Service genre	This genre provides only one function: to sign an object using a provided key. Sign represents an important capability which can support assurance of the authenticity of electronic information.	Submitted
Verify	Service genre	The Verify service genre checks that an object or set of objects comply with a set of criteria. This is a common requirement, with an extremely broad range of possible implementations. Most implemented code implements some verification; this service genre is intended to be used where it is appropriate to have this functionality exposed as an interface.	Submitted

Table B-1 (part 2 of 2): list of e-Framework documentation produced by this project

C Evolution of the e-Framework

C.1 Introduction

- C.1.1 In May 2009 the Curtis+Cartwright project team, together with James Farnhill, met with the Director of the e-Framework (Ian Dolphin) and the JISC Programme Manager for the e-Framework (Alex Hawker) to reflect on this project and to support the e-Framework's commitment to learning from experiences to improve its approach.
- C.1.2 The meeting was very productive, and the statement below provides an update on how the e-Framework has evolved since this project was completed and how this project has informed these changes.

C.2 e-Framework statement (Ian Dolphin, June 2009)

- C.2.1 The e-Framework has continued to evolve during the course of, and immediately following the "Mapping Security Services to the e-Framework" Project. The experience of the project has informed this evolution, and its outputs will be factored into the community focussed validation of the e-Framework technical approach which is scheduled from June-December 2009. It should be acknowledged, however that the continued evolution of the e-Framework technical approach and partnership presented the project with something of a "moving target".
- C.2.2 The e-Framework Partnership has taken the perspective that a broad community focussed validation of the soa-related technical work undertaken over the last three years was necessary to ground that work in the reality of soa adoption within the sector. Such a review, however, could not take place effectively until both a clear rationale, and an overarching technical model were available to the community. A significant proportion of effort within the soa-related strand of e-Framework Partnership activity over the nine months prior to June 2009 has therefore aimed at the production of these two elements. The validation process will have a three-fold emphasis; on the rationale underpinning the work, on the overall approach embodied in the technical model, and on the utility of the submissions to the international knowledgebase. One aspect of validation will be to test the applicability and utility of these general elements against the specifics of domain or work area practice. MSSeFP provides valuable initial evidence to this process in the area of security.
- C.2.3 MSSeFP reported on several aspects of the e-Framework submission process which were, and are, less than perfect. There is, of course, an aspect of this which is covered by the elements - rationale and technical model - reported above. It is undoubtedly also the case that comprehensive training materials are required to reduce complexity for the community. Alongside the validation process, therefore, there is a specific strand of work across the partnership to produce a programme of materials to support the evaluation and adoption of the e-Framework technical approach.
- C.2.4 It remains the case that the adoption of service oriented approaches and Service Oriented Architecture has been slower within the sector than was anticipated when this work began. There are many factors interacting to produce this effect - technical, economic and cultural. The speed of adoption, and subsequent lack detailed experience within the sector has acted, however, to highlight flaws in the e-Framework submission process itself which have been noted by MSSeFP, principally the significant time lag between submission, feedback and publication. Given the slow adoption of soa/SOA within the sector, and a review process which focussed on the review of submissions from the perspective of detailed soa/SOA technical expertise, this lag is hardly surprising. The maturity of soa adoption within the

sector produced relatively few "experts" to act as reviewers, whilst the number of submissions from funded projects - many producing submissions as they concluded - produced an unmanageable "bulge" which the review process simply could not deal with in a timely manner. This was compounded by the impact of project grant agreements which effectively mandated the production of e-Framework submissions before the experience, context or objectives of the project were fully understood.

- C.2.5 In recent months, the e-Framework has taken steps to resolve these issues.
- C.2.6 Firstly, the the situation where projects are mandated to produce submissions is being modified considerably. In the future, the emphasis will be on the e-Framework Community Engagement Team working collaboratively with Programme Management and projects themselves to determine where a project can make a meaningful and effective submission.
- C.2.7 Secondly, the submission process has been amended. The e-Framework Integrity Group, which previously undertook both the development of both the e-Framework Technical Model and the review of submissions has been abolished. Two groups, one responsible for the development of the model, and one responsible for the review of submissions have been formed. The Technical Review Group will consist both of experts in soa and SOA, but also a more broadly based range of experts in a range of specific domains and work areas. The core task of this group is to determine whether a submission is suitable for sharing in the international knowledgebase (Editorial staff will check that the essential components of a submission are present). Comments from reviewers, together with the submission, will then be published for community review and assessment. The emphasis forthwith will be on enabling a learning dialogue on soa/SOA adoption within the educational community, and the transfer of experience and knowledge between work areas and domains. That dialogue will, of necessity, be as open as possible.
- C.2.8 It should be noted that whilst some of these changes are in place, others remain in the process of implementation, or are yet to be established. It should be noted further that this change takes place against a broader backdrop of change within the e-Framework Partnership itself. This change is reflected in a revised mission statement and profile,¹⁰ and is being accompanied by a broadening of strategic engagement in the partner countries.

¹⁰ <<http://www.e-framework.org/AbouttheInitiative/tabid/688/Default.aspx>>