

JISC

An Investigation into the Feasibility of a Cross-Jurisdiction Common Access Management Federation Agreement

Jason Campbell



Contents

Important Disclaimer	2
Introduction	4
Scope	4
Context.....	4
Analysis of Service Provider Attitudes.....	7
Analysis of Access Management Federation Attitudes	8
Analysis of the Legal Context	9
Analysis of Existing Federation Agreements	12
Future Developments.....	15

Introduction

This is the final report of the JISC Legal investigation into the feasibility of a cross-jurisdiction common access management federation agreement. Its purpose is to evaluate the likely success of framing a common template or templates for access management agreements which can be adopted across a number of jurisdictions.

This project is funded under JISC's Access Management Transition programme, and thanks are due to Jane Charlton, the JISC Access Management Outreach Coordinator, for her guidance, feedback and patience.

The report endeavours to analyse the legal position as it stood at 1 May 2008.

Scope

The project considers the legal and organisational barriers to the adoption of common agreements in relation to federation-identity provider and federation-service provider agreements, and in relation to interoperability agreements between national federations. This analysis of barriers is with a view to gauging the feasibility of the adoption of a common template agreement or agreements. There are a number of reasons why such commonality would be beneficial but there is a focus here on gaining the maximum sign-up of service providers to national access management federations.

This report does not consider the technical issues of federation operation, service infrastructure, choice of software, or methods of interoperability.

Further, this report will not instruct federations, service providers or users as to the degree of risk they should be willing to bear, or to the benefit or detriment of a particular licence term over another. The negotiation of licences and contractual terms must be a matter of agreement between the parties, according to their particular circumstances, objectives and willingness to assume responsibilities.

Context

At the present time, access management federations can be found at various stages of development. The furthest developed federations have progressed beyond early stages and are showing signs of embedding and stability, though are still seeking a critical mass of service providers. At the same time, less developed federations continue to progress beyond the early stages of establishment.

The range of development between federations is likely to affect the acceptability of adopting a common template. A well-established federation will need good grounds for undoing previous development, and accepting compromises. It will mean going back to those who have already signed up, or are in the process of doing so, and undertaking consultation and possibly negotiation once more. On the other hand, the adoption of a common template is likely to accelerate the progress of less developed federations.

Given the most developed federations are likely to be seen as leaders, it could be that their existing agreements are likely to be the ones which most inform the development of a common template. This may make the effort in changing over more palatable. However, most importantly is the identification and promotion of the benefits expected to be gained.

In previous work done in this area, it was concluded that 'the divergent national federation policies in place (particularly in Europe) could hinder operability'¹.

In an area of development where technical standards are paramount to the operation of seamless systems, it should be noted that other differences may also form barriers. Uncertainty can act as much as a barrier as incompatibility, in respect to interpretation of agreements (and in particular, responsibilities).

To this end, the Curtis+Cartwright report recommended that JISC works in partnership with others to 'encourage, as far as possible, concurrence between national federation policies to support future inter-federation interoperability'².


However, the benefits would assist not only interoperability, but also the joining of multiple federations by service providers.

¹ Curtis+Cartwright Consulting, *Federation access management: international aspects*. June 2007, paragraph 14

² *Ibid.*, paragraph 19

To this end, JISC Legal has investigated whether in legal and organisational terms, the development and adoption of common access management federation agreements; in considering the feasibility of concurrence, the following degrees of integration have been evaluated as outputs:

- A single set of templates adoptable as-is by participating federations in any jurisdiction
 - A set of adaptable templates adoptable with local variation by participating federations
 - A framework template, with detailed development left to participating federations
 - A verification or information scheme, certifying that federation agreements meet certain criteria
 - Independently developed federation agreements (as present)
- Most concurrence



Most divergence

Adoption of approaches with high degrees of concurrence is likely to lead to the greatest disruption to the present state of affairs. It is therefore clear that these approaches are only feasible if the federations involved are strongly committed to the achievement of convergence and its benefits.

At present, it is not clear where the leadership will come from in order to bring federations together to adopt common standards. Although discussion, cooperation and some coordination takes place through a number of organisations and forums, this may not be sufficient to ensure the coordination that needs to take place to enable an approach leading to a high degree of convergence.

It is also clear that federations from other jurisdictions not included in this study may be interested in adopting common agreements, partly to benefit from convergence, and partly to speed up the process of developing agreements independently and from scratch.

The adoption of common frameworks and templates would have the effect of imposing compromises on some if not all of the participants. An evaluation was conducted of the benefits of convergence against the benefits of independent development of agreements, and the result of this analysis is as stated below:

Benefits of convergence	Value of benefit
Aids interoperability between federations	High
Minimises agreement acceptance difficulties for service providers and federations	High
Reinforces knowledge of agreements	Low
Minimises focus on differences of policy	Low

Benefits of independence	Value of benefit
May avoid a highly legalistic approach	Medium
Allows adaptation to local situation	Low

Recommendation: There is a substantial advantage in the standardisation of access management federation agreements across jurisdictions, both at the individual national federation level, and at the federation interoperability level.

Looking to the objectives which are likely to drive the process of convergence, the following successful outcomes and failure outcomes can be identified:

Success scenarios	Failure scenarios
Federations undertaking agreement revision processes to adopt new common agreement	Few or no federations undertaking agreement revision processes to adopt new common agreement
Increased sign-up of service providers to national federations due to lower entry barrier	Federations making substantial changes to the common templates before adoption
Minimum focus on agreements, with risk managed in perspective	Agreements remaining an issue whilst federations and interoperability develop, with risk blown out of perspective

There is evidence to suggest that peering is taking place by way of informal bilateral or multilateral agreements between federations. This is likely to be ad hoc and is likely to be unsustainable when scaled up.

In order to achieve certainty and credibility, it is clear that a more consistent approach needs to be adopted. However, an important prerequisite is sufficient convergence at national federation level in order to make dealing with interoperability agreements manageable:

One [interoperability] model is where identity providers within a federation can gain access to specific services within another federation by exposing the federation metadata to that federation ... This model could work where federation policies are very similar and little trust is required.

Overall, it is clear that this is a time when the development of common agreements is preferable to independent, ad hoc adoption by individual federations. However, the success of this activity is likely to depend on the perception of benefits by federations with existing agreements.

Analysis of Service Provider Attitudes

In order to determine service provider attitudes, JISC Legal conducted a small-sample survey of key service providers. The responses received were from large publishers, being the service providers most likely to be faced with cross-jurisdictional issues. However, this analysis will additionally conclude with a consideration of issues for smaller providers.

From the survey feedback and other evidence, it appears that, although service providers are in favour of consistency and coherency they are nonetheless used to dealing with a variety of agreements. For example, one respondent stated:

‘the agreements presently in place ... are quite diverse – some are more extensive than others, yet others are more generic, and yet others are nothing but a ‘we promise not to break stuff’ memorandum.’

The burden placed upon large publishers due to the variety of agreements is likely to be mitigated by them having the legal expertise ‘on tap’ to review such agreements, and the experience to be able to decide whether a proposed agreement contains anything of concern or out of the ordinary.

Publishers have expressed a preference against overly bureaucratic or legalistic frameworks, though they expect certain basic criteria to be met. Likewise and unsurprisingly, they would oppose any more onerous provisions which may be put upon them in terms of liability or data protection:

‘The only thing we want to avoid is making things “heavier” in terms of data protection and liability.’

From the service provider point of view, a straightforward agreement appears favourable to an ‘every possible contingency’ agreement and an agreement which attempts to shift the burden of data protection risk and bearing of liability onto the publisher.

Smaller publishers and non-publisher service providers will be even less likely to take on increased liability and more onerous data protection and other regulatory provisions. They are less likely to be able to deal efficiently with a large range of agreements, and therefore might benefit most from common agreements being adopted in different jurisdictions.

Recommendation: Federations must ensure that service providers are consulted with regards to the development and adoption of common agreements, and are lobbied with regards to the benefits of a cross-jurisdiction common template in reducing the overhead associated with signing up to multiple federations.

Analysis of Access Management Federation Attitudes

In order to determine federation attitudes, JISC Legal conducted a small – sample survey of relevant access management federation representatives. Despite being a small – sample survey, we believe that the responses are representative of attitudes in general.

It is clear that national federations are conscious of the benefits that would come from the adoption of common agreements. However, the success of such activity will depend on the extent to which existing, established federations are willing to undertake the process of bringing in a new agreement.

The survey showed that all federations have at least some service providers signed up from a different jurisdiction, with proportions ranging from a few percent to around 15%. Most federations reported that some service providers have had some difficulty in evaluating or accepting the federation's agreements and/or policies.

Most federations expressed a willingness to revisit their present agreements, or to adopt new ones, in order to achieve the benefits associated with the adoption of a cross-jurisdiction common template. However, one established federation thought it unlikely that it would either revise its current agreements or adopt a new one. The federations which expressed a willingness to change in order to benefit from a common template were of the opinion that the likely timescale for this would be 1–3 years, rather than in the very near future, or in the longer term. This could be an issue for the feasibility of a common template, as the larger the membership a federation has signed up, the more onerous it may be to revise or adopt their existing agreements. Likewise, most federations were prepared to be flexible with respect to readjustments of data protection requirements, language and liability allocation in order to achieve compromise for the purposes of a common template. However, the more established federation rated it unlikely that much change would be accepted.

From the survey and subsequent discussion, it is clear that whilst some federations have ready access (either in-house or available ad hoc) to legal and organisational support, others do not have such assistance.

From this analysis, it seems the adoption of a cross-jurisdictional template will be most attractive to federations whilst in their early development. If established federations are unwilling to adopt a common template, this will dilute the benefit with regard to inter-federation agreements. If a common template is adopted as a de facto standard, however, it could be that force of numbers, plus pressure from international service providers, gives federations maintaining 'independent' agreements sufficient good reason to adopt the common template in future.

Recommendation: Development of the cross-jurisdiction common template should include emphasising the general benefit to be gained from the adoption of such a template, both at the member level and the inter-federation level. This should be accompanied by lobbying of more established federations in order to ensure their support.

Analysis of the Legal Context

As part of its investigation, JISC Legal has analysed the areas of law which either require to be addressed as part of access management federation agreements, or which are commonly included in such agreements.

Intellectual Property Rights

Authentication and Authorisation Infrastructure (AAI) will typically be used to manage user access to resources dependent on the contractual right (licence) held. An infringement of intellectual property will usually take place where a user is incorrectly permitted to access copyright-protected resources. The licensing of resources to users takes place between the service provider and identity provider, without the involvement (in legal terms) of the federation organisation. However, the service provider may lose trust in a federation if it recognises intellectual property breaches taking place, irrespective of responsibility.

An intellectual property issue may arise in relation to the federation in the case where it is the erroneous operation of the federation's AAI which allows a user to access materials without the relevant right. This could give rise to a liability as secondary infringement of copyright, as breach of a contractual obligation (the federation agreement with the service provider) or as actionable negligence for failing to take reasonable care.

Contractual relationship issues

Federation agreements will typically have contractual status. This requires that the parties involved are constituted as legal entities having the power to enter into a contract. This may be an issue in relation to federations formed by loosely cooperating bodies. The agreements must be in a form recognised by the applicable law as capable of forming a contract, and the parties must have sufficient notice of all the relevant terms and conditions pertaining to the obligations prior to contract.

There may further be issues of the validity of certain terms, particularly in relation to the limiting of liability, which may be subject to legal controls (such as those under the Unfair Contract Terms Act 1977 in the UK).

Allocation of responsibility and liability issues

Legal systems typically allow, with some restrictions, the allocation of risk by way of contract. This allows federations to specify which party will be liable in the event of a particular type of breach of the agreement, or other actionable loss. In the event of a breach of contract, or of negligence occasioning loss to a third party, such statements provide certainty in terms of responsibility.

Typically, the party responsible or most responsible for control of a certain activity will be the one responsible for actionable loss as a result of breach of a legal duty. However, parties may wish to alter this position for one of a number of reasons, such as the nature of the parties involved, the overall relationship of the parties, and if one party is better placed to bear the risk and if relevant, to insure against that particular loss.

It is suggested that in the case of a cross-jurisdiction common template, the parties are most likely to accept that each party bears the responsibility of the consequences of its activities, without substantial alteration of this default position. It is therefore the case that the provisions in an agreement will merely reiterate the default position.

Data Protection issues

As a result of the European Data Protection Directive, the member states of the European Union are required to have implemented laws which protect the accuracy and security of personal data (information about living persons). Beyond the European Union, other jurisdictions may have laws which protect personal privacy in different ways. Typically, an organisation in one jurisdiction acting within another jurisdiction must comply with that second jurisdiction's data protection and/or privacy laws. In the case of identity management systems, the identity provider will typically hold personal data about users. Where the system invokes propagation of information that could identify a living individual, this will represent a transfer of personal data, and compliance with data protection/privacy laws must be ensured.

The following table sets out a brief description of the data protection laws pertinent to each of the jurisdictions considered:

Denmark
Act on Processing of Personal Data (Act No. 429 of 31 May 2000) www.datatilsynet.dk/english
The data protection legislation of Denmark implements the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU Directive). The act was amended last on 1 July 2007 and it replaces the Public Authorities Registers Act and the Private Registers Act. The Office for Personal Data Protection is responsible for exercising surveillance over the processing of data to which the act applies.
Finland
Personal Data Act (523/1999) www.tietosuoja.fi/27305.htm
The first data protection act, Personal Data File Act 1988, was aimed at preventing violations of integrity at all stages of data processing. The new act, Personal Data Act (523/1999), replaced this act but the basic principles of protection of privacy remained unchanged. It includes some constitutional reforms, lays more emphasis on the basic rights and freedom of individuals in the processing of data and accommodates the EU Directive. The supervisory authority dealing with compliance of the data protection legislation in Finland is The Data Protection Ombudsman/The Data Protection Board.
France
Act No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (Amended by the Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data) www.cnil.fr/index.php?id=4
The Act 2004-801 of 6 August 2001 modified legislation Nr. 79-17 of 6 January 1978 incorporating the EU Directive into national laws. CNIL (Commission Nationale de l' Informatique et des Libertes or French National Commission for Data Protection and the Liberties) is the supervisory authority dealing with data protection compliance in France.
The Netherlands
Personal Data Protection Act 2000 (Wet Bescherming Persoonsgegevens) www.dutchdpa.nl/documenten/en_wetten_wbp.shtml
The act came into force on 1 September 2001 to implement the EU Directive into Dutch law. The Dutch Data Protection Authority (DPA) is responsible for overseeing the processing of personal data under the act.
Norway
Personal Data Act 2000 www.datatilsynet.no.htest.osl.basefarm.net/templates/Page____194.aspx
The Data Register Act of 1978 was made obsolete by the Personal Data Act of 2000. The act came into force on 1 January 2001. The act was passed in order to bring the Norwegian law on data protection in line with the EU standards. The purpose of the act as given in section 1 is 'to protect natural persons from violation of their right to privacy through the processing of personal data'. The Data Inspectorate is responsible for enforcement of the act.
Sweden
Personal Data Act 1998 www.datainspektionen.se/in_english/personal_data.shtml
The Personal Data Act implements the EU Directive and it came into force on 24 October 1998. It replaces the Swedish Data Act 1973. The current act does not apply to data processed prior to 1998. Data processed prior to enactment of the new act is still regulated by the act of 1973. As per section 1 of the Personal Data Act the purpose of the act is 'to protect people against their personal integrity being violated by the processing of personal data'. The Data Inspection Board is the supervisory authority as regards the processing of personal data.

Switzerland

Federal Law on Data Protection of 19 June 1992 www.edoeb.admin.ch/org/00828/index.html?lang=en

The act came into force on 1 July 1993. Although Switzerland is not a member of the EU, the principles of the data protection legislation are similar to those applied by the other EU member states. As per the general information on the act available in the web link to the act, it extends the protection of private persons provided by the Swiss Civil Code and regulates in a detailed manner the processing of data by Federal authorities.

Article 1 of the Act aims 'to protect the privacy and fundamental rights of the person on whom data is processed'. The Federal Data Protection and Information Commissioner (FDPIC) is the body that supervises the compliance of Federal Authorities with the act.

United Kingdom

Data Protection Act 1998

The Data Protection Act 1998 came into force on 1 March 2000. It regulates the obtaining, holding, using, processing and disclosing of information relating to individuals. The act applies both to manual data and to data processed by computers. The act requires that those processing personal information notify the Information Commissioner's Office (ICO) that they are doing so, unless their processing is exempt.

United States of America

Safe Harbor Agreement www.export.gov/safeharbor

There is no comprehensive data protection legislation in the US. Instead the US has developed a 'safe harbor' framework which provides seven safe harbor principles. It is voluntary for organisations to join the safe harbor framework. Organisations joining the safe harbor are certified as providing 'adequate' protection under the terms of the EU Directive 95/46/EC so as to legally comply with the transfer of data between countries.

Identification of the applicable law

Where activities take place across jurisdiction borders, or involve parties in different jurisdictions, the rules of private international law specify under which law and in which jurisdiction any disputes will fall to be decided. Each country has its own rules of private international law which will decide upon applicable jurisdiction (which country's courts could decide the matter) and applicable law (which jurisdiction's laws will apply). It can be noted that these are two separate issues and a dispute subject to one country's laws may be decided by a court in another country.

In relation to non-consumer contracts, such as federation agreements, the parties are commonly permitted to specify under which jurisdiction and law they wish their contract to be subject. Some jurisdictions insist that the selection be limited to those jurisdictions to which there is a connection by virtue of the contract or the parties. Therefore a party in jurisdiction A contracting with a party in jurisdiction B for the performance of services in jurisdiction C may be restricted to those jurisdictions. In the event of the parties not specifying a choice of law, default rules will apply to allocate jurisdiction and law. The explicit selection of a jurisdiction and applicable law as part of the agreement will increase certainty and remove a potential area for dispute.

In relation to federation agreements with identity providers and service providers, there will typically be an expectation that the law and the jurisdiction of the federation's jurisdiction will apply. However, the submission of a confederation agreement or a peering agreement to a single jurisdiction is likely to be more contentious.

Recommendation: The common template should specify, in relation to service provider agreements, that the legal system of the federation is the applicable law and jurisdiction of the agreement.

Recommendation: In relation to inter-federation peering agreements, the common template should specify that any dispute or disagreement between the parties will be settled according to the law and jurisdiction of the party against which the dispute or disagreement lies.

Analysis of Existing Federation Agreements

JISC Legal analysed national federation agreements in place in nine jurisdictions, in order to determine the current degree of variation of content, structure and approach.

It should be noted that analysis was made of the agreements publicly available as at autumn 2007. Several of the agreements were in development at that point, and updated versions are now available. However, this analysis shows agreements at the various stages of development that are likely to be found across jurisdictions (including those not considered as part of this study).

Variation of content

Analysis of the agreements applicable to the nine federations involved in this study revealed, for the most part, similarity of content. This broadly mirrors the content suggested in the Liberty Alliance Project's Contractual Framework Outline for Circles of Trust³. As noted in the preliminary work on policy in establishing the Kalmar Union:

'Preliminary comparisons of these policies ... make evident that the similarities far outnumber the differences. Furthermore, many of the differences appear to be caused by chance rather than by choice⁴.'

Study of the nine agreements bore this out. The following table gives an outline analysis of the agreements' content:

Organisation	France (CRUJ)	UK (AMF)	Netherlands (SURF)	Denmark (DK-AAI)	USA (InCommon)	Finland (HAKA)	Switzerland (SWITCH-AAI)	Sweden (SWAMI)	Norway (UNINETT)
Organisation	✓	✓	✓	✓	✓	✓ ^a	✓	✓	✓
Joining	✓	✓	✗	✓	✓	✓ ^a	✓	✓	✗
Withdrawing	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP/SP Relationship	✓	✓	✗	✓	✓	✓	✓	✓	✗
Updating	✓	✓	✗	✓	✓	✓	✗	✓	(✓)
Cert. Auths	✓	✗	✗	✗	✗	✓	✗	✗	✗
Responsibility	(✓)	✓	✗	(✓)	✓	✓	✓	✓	✓
Disclaimer	✗	✓	(✓)	✓	✓	✓	✓	✓	(✓)
Logging	3 mths	3-6 mths	✗	✗	✗	✓ not spec	✗	✗	✗
DP	✓	✓	✓	✗	✓	✓	✓	✓	✓
Limited use of attributes	✓	✓	✓	✓	✓	✓	✗	✗	✗
Formality	2/4*	4/4	2/4	2/4	4/4	2/4	3/4	2/4	2/4
Development	4/4	4/4	2/4	1/4	4/4	3/4	2/4	3/4	2/4
Jurisdiction	✗	England	✗	✗	Delaware	Operator domicile	Swiss law	✗	Norwegian law
Dispute Res	✗	✓	✗	✗	✓	✗	✓	✗	✗
Insurance	✗	✗	✗	✗	✓	✗	✗	✗	✗

³ Liberty Alliance Contractual Framework Outline for Circles of Trust, www.projectliberty.org/liberty/files/whitepapers/liberty_alliance_contractual_framework_outline_for_circles_of_trust

⁴ Tveter, WM. Melve, I. and Linden, M. *Towards interconnecting the Nordic identity federations*. 2007

Key to terms and symbols used

✓ included in agreement (✓a included in appendix)

[✓] partially addressed in agreement

✗ not included in agreement

* though the agreement states it is to have no legal sanction

Organisation records whether the agreement describes the organisational structure of the federation (such as the relationship between the members, service providers, identity providers and the federation itself).

Joining records the process by which service providers become members of the federation in order to provide resources via authenticated and/or authorised access management.

Withdrawing records the process by which a member can withdraw from the federation, and specification of any related notice period that is required.

IP/SP Relationship records whether the agreement specifies the links and obligations between identity providers and service providers.

Updating records whether a mechanism is specified for the evolution of the agreement, and what procedures are provided to incorporate such changes.

Cert. Auths records whether the agreement deals with the identification of certification authorities.

Responsibility records whether the agreement allocates duties to the parties, and the consequences of failure to perform those duties as stated.

Disclaimer records the inclusion of a disclaimer of liability or other limitation of liability in favour of one or more parties to the agreement.

Logging is the specification of whether, and for how long, information about user access via the federation is kept.

DP records whether the agreement contains provisions related to the protection of personal information.

Limited use of attributes specifies whether the parties commit themselves to passing only non-DP information whenever possible, and that the attributes will only be used for the purposes of access management.

Formality shows a broad grading of the legal formality of the document, with 1=informal, 2=business-type language, 3=formal, 4=legalistic.

Development shows a broad grading of the character of the document, on a scale of 1=draft-like, 2=simple with further development expected, 3=generally complete, 4=fully developed.

Jurisdiction records whether the agreement specifies the jurisdiction and applicable law of the contract.

Dispute Res records whether the agreement refers to a non-court procedure (such as arbitration or mediation).

Insurance records whether a party or parties are required to insure activities carried out under the agreement.

This study considered which parts of federation access management agreements were legally 'active' clauses (ones which created or altered the parties' obligations), which were 'passive' provisions (ones which simply reiterated what the situation would have been anyway) and which were 'operational' provisions (which gave details of what needed to happen to make federated access management work).

Current agreements do not contain a substantial number of 'active' clauses. The majority of content states what the case would be by default, or states under a title 'responsibilities' what is needed for the infrastructure to operate. This often makes agreements look more complex legally than needs to be the case, and introduces an increased cost of having the agreements analysed. It is therefore suggested that a structure which makes clear what the legally active provisions are should be adopted.

Recommendation: It is recommended that the common template clearly differentiates the legally active provisions (which will require scrutiny and risk evaluation by parties to the agreement) from legally passive requirements and procedural requirements.

The analysis has shown that, as yet, national federation agreements do not typically address the particular legal issues which might arise related to out-of-jurisdiction members.

Recommendation: Development of the common template should consider the legal effects and consequences of the signing up of out-of-jurisdiction members to a national federation.

Variation of structure

As part of its study, JISC Legal analysed the various approaches to the structuring of the existing agreements. It found a significant diversity amongst the nine federation agreements studied.

Some are presented as single documents, some as agreements with appendices, and some as multiple documents. There is also variety as to the extent to which service provider agreements and identity provider agreements are presented separately.

However, in general, the structure of the agreement will have no bearing on its legal effect. The only exception to this is where interpretation of a provision depends on its context. That context does include its place in a structure; for example, a statement that a party has to supply certain data may be interpreted differently if contained in an 'Obligations' section than if it appeared in an 'Operational Procedures' section.

Analysis of the existing agreement structures shows that differences appear cosmetic, and there is nothing that suggests that differing structures have been intentionally adopted as the result of divergent approaches. Rather, they seem to be simply the result of different ways of setting out the provisions. It is therefore considered that the adoption of a different structure of agreements is unlikely to represent a barrier in itself.

Recommendation: The structure of a common template agreement is unlikely to have an impact on its legal effect. The common template should therefore be in the most user-friendly structure, with clear differentiation of active legal provisions from statements which reinforce the default position, and technical and procedural provisions which allow the federations to operate.

Variation of approach

A more significant (and potentially difficult) variation arises in relation to the differences in approach to the formality of the federation agreements. At one end of the scale, one federation agreement states:

'These responsibilities ... should not be interpreted as rules intended to assign financial or legal sanctions against those who transgress, but more as a system of "best practices".'

On the other hand, a number of other federation agreements reviewed adopt a formal legal approach. These differences of approach may be simply a product of the particular processes by which the agreements were devised, or may reflect differing risk cultures. Where differences rest on attitudes to risk and expectations of formality, this is an area in which compromise may be more difficult.

A review of the existing access management federation agreements shows a variety of formality and maturity of development.

Differences between current national federation agreements are generally insignificant in terms of content and structure. However, a diversity of approach to the legal formality of the agreements exists, and this is an issue on which compromise will need to be reached in order to develop a common template.

Recommendation: If the benefits of a common template are to be achieved, federations will have to compromise on the type of agreement they expect, particularly in respect to the degree of legal formality. It is recommended that the level of formality to be adopted is that which maximises ease of comprehension.

Future Developments

A mechanism will be needed to ensure that the common template can be updated in the light of future developments. The wish to add further jurisdictions, changes in technology and changes in the law may all require a change to such a document.

As a first observation, the necessity of change is likely to depend on the approach adopted with regard to the legal formality of the document. A broader, less legalistic approach is less likely to require frequent updating than a legally detailed one.

Beyond this, it will be necessary to find a mechanism to identify any relevant changes in law, technology or federation practice which make it necessary to update the common template or templates. In order to ensure this happens, an organisation representative of cross-jurisdiction federation interests will need to take on such responsibility, with a procedure to negotiate and disseminate updates to the agreements.

It should be noted that in the event of some federations updating their agreements, whilst others continue with a previous version, some degree of convergence will be lost. This may very well be unavoidable, given the independence of national federations. Although it is unlikely that any body will emerge that will require updating to maintain convergence, a strong cross-federation body championing the cause of convergence and consistency may go some way to ensure the greatest degree of harmonisation.

Recommendation: Any common agreements will need to be reviewed periodically to ensure their currency and relevancy in relation to legal and technological change. This should be undertaken by a body representative of the participating federations.

An Investigation into the Feasibility of a Cross-Jurisdiction Common Access Management Federation Agreement

Further information about JISC:

Web: www.jisc.ac.uk

Email: info@jisc.ac.uk

Tel: +44 (0)117 33 10789