This article appeared in a journal published by Elsevier. The attached copy is furnished to the author for internal non-commercial research and education use, including for instruction at the authors institution and sharing with colleagues.

Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.

In most cases authors are permitted to post their version of the article (e.g. in Word or Tex form) to their personal website or institutional repository. Authors requiring further information regarding Elsevier’s archiving and manuscript policies are encouraged to visit:

http://www.elsevier.com/copyright
Enabling decentralised management through federation

Kevin Feeneya*, Rob Brennana, John Keeney, Hendrik Thomasa, Dave Lewisa, Aidan Boranb, Declan O’Sullivana

aSchool of Computer Science and Statistics, Trinity College Dublin, Dublin 2, Ireland
bBell Labs Ireland, Alcatel-Lucent, Blanchardstown Industrial Estate, Blanchardstown Dublin 15, Ireland

ABSTRACT

Cross-domain management is an increasingly important concern in network management and such management capability is a key-enabler of many emerging computing environments. This paper analyses the requirements for management systems that aim to support flexible and general capability sharing between autonomously managed domains. It introduces a novel Layered Federation Model (LFM) to structure this requirements analysis and describes the Federal Relationship Manager (FRM) which instantiates several layers of this model. The FRM combines semantic mapping management and authority management technologies to help solve several of the general management problems that are encountered whenever organisations enter into capability sharing agreements. An overview of related work on federation and the technical underpinnings of our approach are discussed and our work’s particular relevance to real world problems is explained through two service-centric use cases which involve the end-to-end delivery of a multimedia stream to a user’s home across several independent operators. Finally, experimental results are presented to highlight the practical advantages of our approach.

© 2010 Elsevier B.V. All rights reserved.

1. Introduction

The emergent challenge of planetary scale IT infrastructures that blend and shape networks, services, smart devices and sensors is one of heterogeneity driven not primarily by technological factors but by organisational diversity. The always-on, multi-mode, loosely-coupled, user-centric nature of modern communications and the diversity of operator business models ensure that end-to-end service provision frequently crosses heterogeneous management domains. Increasingly the service delivery path incorporates non-traditional communications resources, such as devices in a consumer’s Home Area Network (HAN), which are highly unlikely to be managed resources in the sense of supporting traditional OAM (Operations, Administration and Maintenance/Management) models, interfaces or inter-operator legal frame-

works. New resources also exhibit a daunting diversity and dynamism compared to more tightly-controlled, vertically-integrated, operator-bundled consumer offerings of the past.

The modern operator landscape presents an increasingly complex topology of organisational forms. Companies are often embedded within complex webs of relationships with suppliers, collaborators, peers, competitors and a variety of other third parties. These broader organisational forms are described variously as ‘supply chains’, ‘virtual organisations’, ‘value networks’, ‘collaborative business networks’ and other subtly variegated descriptive terms. While the significance of any particular cross-organisational model in this taxonomy of organisational forms as discussed in the business management literature (e.g. [10]), is open to debate, the increasing importance of management approaches which cross-organisational boundaries and attempt to apply coherent solutions and management models across multiple independent organisations is clear.
The challenge does not only lie in the technological aspects of enabling cross-domain communication. Advances in standardised technologies such as Service Oriented Architectures (SOA), drawing on older technologies such as RPC and Component-Based Software Engineering (CBSE) models, provide easy-to-use plumbing to physically access services in other domains, in a secure and auditable manner. However, these approaches require extensive pre-negotiation and advance coordination. The fundamental problem being addressed here is how to support more agile and dynamic creation of cross-domain organisational agreements to enable capabilities to be shared between parties. Of particular importance is the problem of managing access between diverse systems to support fine-grained sharing of capabilities, through the lifecycle of the agreement. Another major issue is one of semantic interoperability (rather than data-level or network-level interoperability). Even where semantic web services [35] are used to facilitate semantic descriptions of services, the semantic descriptions must be compatible and pre-agreed. Where technologies like CMDBf [11] can provide a federated view of heterogeneous data-stores, the identification of capabilities to share, and management of access to them is still a major overhead in creating and maintaining such agreements.

Mature approaches to systems and telecommunications management such as ITIL [1] or eTOM [2] have always been driven by both the technological and organisational challenges of the domain. However, despite long established signalling and media interconnects between operators supported by standardised protocols, SLAs and legal agreements, progress on B2B interfaces at the operational level has been limited [24]. One of the reasons for this is the costly and limited integration of modern OAM systems even within a single operator network due to the proliferation of vendor, FCAPS [3] functional or network type stovepipes within a domain [25]. This leads to high integration costs and inflexible, brittle systems. Even agile mechanisms to dynamically define contracts and SLAs between organisations (e.g. [20]) require shared infrastructure and common semantics, and are limited to relatively static, course-grained, producer-consumer style relationships. The emergence of new types of distributed systems – autonomic, mobile and planet-scale networked applications has, if anything, served to further increase the focus on managing applications that cross-domains of authority. Innovative operators and equipment vendors have embraced this trend with a plethora of new open service APIs for the network, e.g. Alcatel-Lucent’s OpenAPI, GSMA OpenAPI and Ribbit, but it is unclear how or if these efforts will support multi-operator service and network management beyond critical functions such as billing or how such open APIs can be leveraged in conjunction with non-traditional communications resources such as the media playback capabilities of the HAN to provide end-to-end assurance and QoE guarantees.

The focus of past standardisation has been on long-lived (typically measured in years) management systems integration supported by common resource models (e.g. the Tele-Mangement Forum’s SID [4]), often based on green-field assumptions and perhaps implying support for a limited and pre-defined set of specific business models (e.g. TINA [5]). In contrast, the work described here assumes that the management systems to be interconnected are already deployed and use heterogeneous resource models, that interconnection takes place in a dynamic environment where instead of extensive integration, minimal and appropriate integration for the current task is negotiated by management systems as part of a wider “federation” of co-operating systems delivering end-to-end services. In this work, the term federation is employed as a general term for describing agreements that support cross-organisational capability sharing (as explained in Section 3.1). Thus, defining mechanisms for the establishment of a common semantics for describing management capabilities and communications resources is given much more weight than building yet another “common” resource model. To enable the distributed delegation of local configuration, service execution or monitoring capabilities a rule or management policy-based approach is used for the exchange of management requests. The goal of this research, from a business point of view, is to provide a lightweight relationship-management infrastructure which can conveniently support whatever business models and pricing/billing mechanisms are agreed between the participating organisations.

This research builds upon the authors’ previous work in developing decentralised policy based management systems [18], semantic mapping [51] and ontology-driven data integration [7]. The key innovations introduced in this paper are: a novel layered federation model which partitions the important aspects of inter-organisational relationships into six distinct aspects, each of which maps neatly to a technological platform that enables convenient implementation; an approach to describing shared capabilities with RDF [46] that allows deterministic management rules to be applied on top of an open and extensible RDF graph; a FRM architecture which brings this work together by combining semantic mapping management and authority management in a unified system that helps solve several of the general management problems that are encountered whenever organisations enter into resource sharing agreements. The rest of this paper is structured as follows: Section 2 provides an overview of related work on federation and the technical underpinnings of our approach; Section 3 describes two service-centric use cases for operator – HAN owner federation to capture system requirements from which a general layered federation model is derived; Section 4 presents our current work on a “federal relationship manager” that implements a sub-set of the layered federation model functionality and presents some experimental results; Section 5 describes our conclusions and plans for future work.

---

3 The OSI management functional areas of Fault, Configuration, Accounting, Performance and Security.
5 Telecommunications Information Networking Architecture Consortium.
2. Background

As business applications and processes that span organisations have become more prevalent, problems with the management of such applications and processes across multiple management domains using heterogeneous management technologies have become more apparent. Much of the research on cross-organisational management has focused on the specification of contracts and agreements between organisations, which then must be monitored and enforced by both parties, in particular focusing on service levels agreements (SLAs) \[5,20,30,41\]. SLA-driven, cross-organisation management is typically divided into two phases – SLA negotiation and specification, and then the runtime monitoring SLA fulfillment and delivery, with associated management actions to ensure that the service is being delivered appropriately. Traditionally, defining an SLA is a slow and tedious process requiring complex language and protracted negotiation. Approaches at defining SLAs in machine interpretable formats have enabled the dynamic interpretation and evaluation of SLAs (see \[41\] for a comparison of formats). However, there has been little progress in the field of automated or dynamic negotiation of SLAs outside of the field of cloud or grid computing \[23,56\].

In this work, we support such cross-domain management by using Policy Based Management (PBM). PBM is an increasingly popular method for combining flexibility with efficiency in systems and network administration \[8\]. In PBM systems, decisions about the behaviour of the system are specified as rules, often expressed in a high level language, which are then mapped into concrete behaviours by the policy system. However, PBM systems have primarily been focused on automating management decision within single organisations, so the organisational modelling abstractions currently used, e.g. roles \[47\] and domains \[48\], reflect centralised organisational concerns.

Although most research in policy languages and architectures has focused on centralised management within an organisation, these models are increasingly being extended and enhanced to include constructs and architectures that support cross-organisational management. For example, Organisational Based Access Control (OrBAC) \[15\] is an access control policy model that is explicitly designed to allow management policies to be applied in a multi-organisational setting. X-federate \[6\] goes one step further in that it incorporates a policy language, an UML-based meta-model and enforcement architecture, and a common policy authoring process designed to help administrators from related organisations to arrive at mutually interoperable management system configurations. However, these attempts to support federated multi-organisational management through policy languages and frameworks generally assume that the participating organisations will adopt a common architecture, common policy languages, common data-models or even common policy-authoring processes, thereby conflicting with the objective of allowing individual parties to maintain their autonomy and privacy \[54\]. While such approaches may be well suited for situations where the participating organisations are intimately related, but still maintain minimal coupling between their management systems, there are many situations where organisations wish to federate to share resources (and their management) with one another without having to adopt common management systems across the federation. For example, telecommunication providers are generally concerned with finding easier and better ways that they can inter-connect, pass traffic between one another and share management information, e.g. for billing or fault rectification. However, they typically have their own complex management systems, models and architectures that have been expensively developed. In many cases, the advantages of greater manageability with a shared federation-wide policy system is far outweighed by the cost of moving from their current systems, even were such close cooperation encouraged in such a highly competitive environment.

Ongoing research has also attempted to address the problem of managing such cross-domain applications and services by proposing common models, processes, frameworks and platforms (e.g. \[19\]). Attempts have been made to define new management information modelling and service modelling languages to act as a lingua franca between heterogeneous network management models. Notable amongst these are the Distributed Management Task Force’s (DMTF) Common Information Model (CIM) schema \[9\] and the TeleManagement Forum’s NGOSS technology neutral architecture \[39\]. However, a lack of a strong interoperability mechanism and reliance on conformance to poorly subscribed industrial agreements effectively demote these to the status of yet further management knowledge formats, with which other schemes need to interoperate.

In contrast to the top-down approach that is implicit in current cross-organisational policy systems, there is growing research interest in bottom-up approaches. Such approaches require semantic mapping between resource descriptions, management capabilities and administrative concerns across heterogeneous management domains. Resolving the semantic differences can be eased by explicit meta-models that can be extended without necessitating reimplementation of management systems. Although some progress has been made in previous approaches (e.g. OSI management, CIM \[9\] and DEng \[49\]) it has been the standardisation of meta-data modelling on the WWW and the availability of associated general purpose information modelling tools that has resulted in the greatest advances in interoperability. These meta-models were initially based on open XML schemas processed by general-purpose parsers and transformation processes, but more recently Semantic Web languages (e.g. RDF and OWL \[31\]), and associated general purpose logic reasoners have become popular. For example, the FUSIO system \[50\] uses a semantic-based approach to expose RDF encoded management data from underlying heterogeneous management systems in a loose schema-less manner. This has evolved from an earlier non-semantic service-oriented (WSDM) integration platform for monitoring \[19\].

However, the actual conceptualization of a domain and the subsequent explication in an ontology (or other modelling) language is a very heterogeneous process \[12\]. For example, conceptual heterogeneity between ontologies
arises due to the natural diversity of human viewpoints involved in modelling a domain [16]. For example, two ontologies could differ because they provide a more or less detailed description of the same domain [21]. The different levels of heterogeneities [43] are major obstacles to the promise of interoperability of knowledge on ontologies [31]. A common approach to mitigate the effect of heterogeneity is to discover the specific correspondences between related ontologies and to document them using an appropriate ontology mapping expression [21,40,42]. Kalfoglou and Schorlemmer define ontology mapping as the task of relating the vocabulary of two ontologies sharing a domain in such a way that the structure of ontological signatures and their intended interpretations are respected [26]. Due to the heterogeneity of ontologies, many ontology mapping scenarios can aid interoperability, e.g. ranging from simple conversion mappings to complex structural mappings [32].

In recent years the research on ontology mappings has made remarkable progress [16,17,42] but the creation process and application of ontology mappings is still a complex and time-consuming task [26,42], particularly for system integration where mappings may be required at the technology-level, service-level and business-level [38]. Instead of recreating the same or similar mappings repeatedly it may be more beneficial to discover existing mappings and if appropriate to reuse them [17]. An analysis of the lifecycle of a particular ontology mapping [42,51] helps to understand how the mapping was created, what information was used, what meta-data describes the mapping, and ultimately how re-usable that mapping may be. Publications on ontology mapping meta-data are relatively rare [16,26,42,51] and currently all phases of the ontology mapping lifecycle are poorly documented. The practical scalable deployment of ontology mappings to support ontology-based integration of systems, and the associated maintenance and evolution of the mappings and the systems that rely on them is a complex problem [3,4,22]. Failure to cope with their maintenance can lead to scalability issues [7,1] which impact the performance of the system. However, modelling the dependencies between the mappings and system elements can ease the maintenance and evolution of such systems to some degree [28,36].

The transformation of standardised management information meta-models into OWL has been shown to have a benefit in achieving a degree of semantic interoperability between models conforming to these different standards (e.g. SMI, GDMO and CIM) both in modelling tools [34] and at runtime [29,33]. Semantic interoperability techniques have also been exploited during SLA and contract negotiations in cross-organisation grid applications [56]. The integration of policy-based management and semantic modelling is already an active research area [27,52]. The predominant aim to date has focused on the increased expressiveness that ontology-based reasoning can offer a given policy language [44,53]. In contrast, in this work we focus on a mechanism by which internal policy semantics of a domain are mapped onto semantics that are negotiated and maintained as part of membership of a federation.

3. Use cases and a layered federation model

The impracticality of cross-domain management approaches that presuppose common policy systems, information models and management processes becomes readily visible when the requirements are considered for the sorts of cross-organisational cooperation that will be needed to deliver even the most basic of services to emerging computing environments. In order to highlight these requirements, and the insufficiency of current management approaches, we have developed simple use-cases that involve the delivery of a basic service to a Home Area Network (HAN) device. The service, called StreamToHAN, enables a real-time, high-quality video stream (e.g. IPTV over SIP or a store and forward-style shared DVR) to be delivered from a mobile phone terminal to a media rendering device within a HAN. The service delivery is considered in two different contexts, differentiated by the distribution of service control and execution resources and the underlying organisational arrangements that exist between the operators and the HAN owner to support the service. In each case, the relationships, and hence the ability to interwork in both the management and control planes within the context of a negotiated scope, are supported by a service called the Federal Relationship Manager (FRM). The design and implementation of the FRM is discussed in detail in Section 4, but for the purpose of this discussion, it can be considered to provide capabilities that support federal relationships between participants in end-to-end service delivery, including semantic interoperability services such as mapping discovery that enable the inter-domain operation and management of these capabilities.

In the first use case, the StreamToHAN service control point is provided by a mobile network operator, perhaps as an IMS service. There are two federations involved in the service delivery – a federation of operators (OF) and a federation between the customer who owns and controls the HAN and their local network operator (OCF), the provider of their gateway/router and network connectivity. The OF serves to provide network operators with a means of managing the capabilities that they expose to one another – this covers basic traffic routing capabilities but also includes higher-level capabilities, such as the ability to set configuration policies or invoke services such as media playback within particular HANs.

The OCF represents a simple means by which the customer can delegate management authority over the capabilities in their HAN, on a case by case basis, to their network provider in the interest of receiving improved customer support, an increased range of services and ease of use for their HAN. These capabilities, or specific sub-sets of them, can then be made available by their local operator to other network operators through the OF (although probably in an aggregated, anonymised form). Thus, the mobile operator in Fig. 1 has access to these capabilities through the OF when executing the StreamToHAN service.

In the second use case, service control is provided by a third party service provider. There are two extra federations involved in addition to the two federations from
the first use case. There is a federation between the service provider and the network operator (SOF). This federation allows the network operator to make the capabilities shared between the OF to be made available to service providers, including capabilities representing devices in the HANs of individual subscribers. This scenario also requires a federation to exist between the customer and the service provider (i.e. the customer has to sign up to the service) (see Fig. 2).

It should be noted that, although these scenarios contain concrete examples of patterns of inter-organisational relationships, they do not assume any particular business case, nor do they presuppose that the organisational arrangements outlined in the scenarios above are the best way of solving the problems in delivering such services. Rather, they are intended to be a reasonably realistic sample of the types of inter-organisational arrangements that exist in the real world. None of these organisational arrangements presuppose any billing model – the FRM is a policy based management framework and it provides several ways in which billing and business models can be supported – membership of a federation can depend upon
payment, use of any particular shared capabilities can be metered or the business model can be agreed independently of the technical infrastructure through pre-existing contracts. The goal of this research, from a business point of view, is to provide a relationship-management infrastructure which can conveniently support whatever business models and pricing/billing mechanisms are agreed between the participating organisations.

3.1. A definition of a federation

Before going on to discuss the technical details of the FRM system, it is worth clarifying in more detail what is meant here by the concept of a federation. This term is commonly employed in the IT management literature, however, in many cases, what exactly is meant by the term is rather vague. For the purpose of this paper, a federation is considered to be a persistent organisational agreement which enables multiple autonomous entities to share capabilities in a controlled way. The four important points to take from this definition are firstly that the federation brings together autonomous entities – organisations or individuals endowed with sovereign decision making power over the resources that they own or control. This distinguishes the federation from the centralised organisation, which are often made up of multiple entities themselves – divisions, departments, teams and so on all the way down to the individuals, but the organisation’s management hierarchy exercises coherent decision making power over the resources of the organisation.

The second important point in the definition flows from the first. Because there is no paramount authority governing the organisational arrangement between the entities, the federation exists by virtue of the agreement of its members. The members are autonomous and thus can choose to leave the federation if they please. Hence, if the arrangement is to be viable, it is important that its nature, structure and evolution are agreed by its constituents. Furthermore it is important that the value delivered to the constituents from their federal membership is transparent and clear to each of them as, if this is not the case, they are likely to leave.

The third important point is that federations exist in order to enable the controlled sharing of capabilities between autonomous entities. The term “capability” is here used in the widest possible sense – it could refer to something as simple as a channel which enables communication between organisations. The term ‘sharing’ is not meant to imply any specific regime by which access to members’ capabilities will be granted. In this context, controlled capability sharing simply means that parties to the federation may be given access to capabilities which they would not otherwise possess (but this access may be constrained by the entity that grants access). The final point of significance is that federations are persistent. This is not meant to imply that they are permanent or that they must last any particular period of time. It simply serves to distinguish them from simple transactions or simple interactions between autonomous entities. The federation persists beyond a single transaction. Hence the federation will have a life-cycle.

3.2. A layered federation model

In this work, the term federation is employed as a general term for describing cross-organisational capability sharing. However, organisational arrangements between autonomous entities vary widely in scope and can be complex and multi-faceted. Thus, models of federations must be capable of capturing and reflecting the most important factors that vary across such arrangements if they are to be capable of modelling the evolving, dynamic nature of such arrangements in the real world. The Layered Federation Model, pictured in Fig. 3, is a general-purpose high-level conceptual model of the components of a federal agreement. The model is decomposed into layers, with each layer representing one aspect of the organisational arrangement. This layered model should not be confused with a communications stack – each layer builds upon the lower layers and depends upon them, but in some relationships there may be cross-layer interactions and layers may be empty. Its main purpose is to serve as a useful model for the decomposition of federal relationships in order to render their definition and maintenance more transparent. The layers represent the most important aspects of organisational relationships that successful persistent organisational relationships require, with their relative positioning in the layered model representing the dependencies between the various elements that constitute such an agreement.

3.2.1. Trusted communication layer

Distributed federal relationships are based on communications. A basic requirement for any sort of communication between autonomous entities is a channel with sufficient security measures to satisfy both parties’ requirements for the current dialog. This requires them to agree on communications protocols, security mechanisms and even applications. These requirements cover issues such as identification, authentication, privacy and integrity of communication. These concerns form the most fundamental layer of our federation model because all higher level agreements and interactions depend upon them.

3.2.2. Federal relationship definition layer

The relationship definition layer supports the definition and transmission of the basic rules that govern each organisation’s relationships with other organisations within the federation. This provides a generic layer in which rules concerning membership of the federation, sharing of capabilities (and their revocation) can be negotiated and agreed. For example, in certain situations an organisation may make its resources available to third parties through federal arrangements which require the third party to reciprocate by sharing some resource that it controls or the organisation may require certain guarantees regarding the continued availability of shared resources or, conversely, that shared resources can be unshared when they are required.

3.2.3. Shared semantic layer

Federations, as we understand them, exist to allow autonomous organisations to share capabilities. However,
any particular organisation will generally have its own addressing mechanisms and semantics for describing the resources that it controls and the capabilities that they support. If these resources are to be made available to third parties, the third party needs to be able to understand how these resources correspond with its own internal view of the world. The shared semantic layer thus serves to provide a mapping between the semantics used internally by each party to the federation to describe their resources and capabilities to those used by the other parties. This could be achieved by means of a standardised federal semantic language, or it could be achieved by each party mapping directly between their internal semantics and that of the other parties to the federation. What is important is that there is some means by which the mapping is managed.

3.2.4. Shared capabilities layer

Having established sufficiently secure communications, a general resource sharing regime and shared semantics with respect to resources, the prerequisites are in place to allow capabilities to be shared. The capability sharing layer is concerned with enabling members of federations to manage the dynamic set of capabilities that are shared between them. This includes providing a means whereby members of the federation can add and remove capabilities from the pool available to other parties in the federation, as well as allowing other parties to discover which capabilities are available for use at any particular time. Such dynamic facilities are crucial if the federation is to be viable over time – it is common to find that a resource controlled by an organisation is suddenly needed for some function or that traffic spikes and so on, such agreements can only really be meaningfully checked over significant periods of time. The Monitoring and auditing layer is thus the top layer of this federal model. It is responsible for providing members of the federation with detailed monitoring of their compliance and that of counter-parties to federal agreements. Since such arrangements are based on the voluntary agreement of autonomous entities, it is particularly important that all parties are provided with sufficiently rich information which allows them to clearly understand the costs and benefits of their membership in the federation.

4. Federal relationship manager

The Layered Federation Model (LFM), described above, is an abstract model which serves to decompose federal relationships into a number of inter-dependant layers. There are a wide variety of technologies which could
potentially be used to implement a software system that could support the management of such relationships. For example, the Ponder framework [14] constitutes a policy specification language and a java-based policy deployment and enforcement architecture which has, in theory at least, the flexibility to describe whatever rules are required in any domain; XACML constitutes an extensible XML based policy language along with a general architecture for the integration of access control policy management into any network or application. It would be possible to implement a software system to support the LFM based on a wide variety of policy languages, architectures or information models as there are many that are sufficiently expressive to model, encode and deploy a LFM instantiation. In the case of Ponder, for example, although there is no explicit support for the concept of a federation, any given federal relationship could be encoded by appropriately combining a set of the language’s domains, groups, management structures, roles and relationships with an appropriate set of policy rules. However, there are several reasons why using any of these solutions to support an implementation of the LFM would be problematic. Most importantly, such approaches tend to be relatively heavyweight as they are premised on the assumption that all prospective parties have adopted a relatively complex set of common technologies prior to even investigating any possibilities of collaboration. Thus, they are only viable solutions to support cross-organisational collaborations when all of the organisations involved use a common policy language (e.g. Ponder, XACML) or information model (e.g. DENg) to govern their federal interactions. In the real world, particularly in the telecommunications sector, organisations tend to have diverse deployed management systems, information models and network architectures, and even when a common uniform platform can be agreed for a federation, the costs of mapping from internal models to those used by the federation are considerable.

When designing systems to help manage the sharing of capabilities across organisational boundaries, a useful rule of thumb is that the greater the requirement for common technology, models and processes that do not already exist across the federation, the greater the barrier to adoption of the technology. Thus, when considering the problem of providing technical tools to support the management of such relationships, our goal is to support as many of the aspects of the LFM as is possible, while minimising the requirement for common technologies, models and processes across the participants. Our FRM is designed as an interconnector between existing management systems and existing semantic spaces, rather than a universal model that must be applied across the entire network of relationships. The goal of the FRM is to encapsulate the common technical infrastructure that an organisation must adopt in order to manage and maintain an arbitrarily complex set of federal relationships. It does not mandate any particular policy language, information model, management structures or processes across federal relationships. The FRM is based upon the confluence of two hitherto distinct research strands within the Knowledge and Data Engineering Group in Trinity College Dublin within the FAME project – the ontology mapping framework [42] and the Community Based Policy Management System (CBPMS) [18]. Together they provide a basic framework upon which a FRM can be built that instantiates the LFM above.

4.1. The community-based policy management system (CBPMS)

The CBPMS is a general purpose policy management framework designed to provide a flexible and secure authority management capability that is policy language and information-model neutral. The CBPMS supports decentralised management through delegation of capability authorities. Capability authorities are references to nodes on a capability–authority tree, and this tree is implemented as a service which can be deployed by the owner of any resource that is to be shared. What makes the CBPMS particularly suitable for application in this domain is that these capability authorities are higher-level constructs than permissions – the standard unit of most access control and management policy systems – and that they are structured. This allows, for example, a telecommunications service provider to grant StreamToHAN access to a partner to all of their customers (or whatever subset they require) via a single delegation of a capability authority rather than having to specify individual permissions for each user which is impractical on such a scale.

Fig. 4 shows a montage of two screen shots from the CBPMS management system. The panel on the left shows a fragment of the domain map, from the point of view of an operator in the StreamToHAN scenario and the panel on the right shows a section of the service operator’s capability authority model. Federations are established through invoking the CBPMS federate primitive which creates an association between domains. Capabilities can be shared with federated domains by delegating collections of nodes from the capability authority tree to associated nodes. When compared to the standard role and rule-based approach to policy management, capability authorities yield considerable gains in terms of the size of the policy search space that must be traversed for policy decisions. The ordering of capability authorities partitions the policy search space. Fig. 5 shows the practical advantages that this ordering brings in terms of the size of the policy search space that must be traversed. The experiment involved randomly generating equivalent sets of policies within a CBPMS implementation and a standard role-based policy system and comparing their performance over a large number of simulations. In large, complex, cross-domain service delivery scenarios, such gains are extremely important, since many such services have relatively low tolerance for delays in establishing the connections and even lower tolerance for delays in service delivery.

4.2. The semantic mapping framework

The semantic mapping framework illustrated in Fig. 6 (extended from [42]) spans ontology mapping creation,
through use and reuse, to evolution and management. This framework is deployed within the FRM to enable the effective and efficient creation and management of mappings between domains to increase understanding of shared capabilities across federations. For example, in the StreamToHAN scenario this would include (a) the capabilities shared within federations (typically network or service resources), (b) the context used in communication services, and (c) the policies used to express governance over the capabilities.

Current ontology mapping approaches can be characterised as: “knowledge engineers” engaging in “one shot” processes that result in static “one size fits all” mappings which are then published for indiscriminate use. In contrast, the ontology mapping process deployed in our framework is designed to: (a) cope with the diversity of actors involved in managing a federation (i.e. not always specialist knowledge engineers with specialist tools) [13]; (b) allow for the diversity of ontology mapping execution deployments; (c) enable rich annotation of ontology mappings through meta-data (see below); (d) enable sustainable and scalable deployment of mappings through dependency modelling [7]. Aspects (a) and (b) are advances in active research areas, however, aspects (c) and (d) contribute to research topics that have been heretofore neglected but are critical to industrial uptake and deployment.

In order to support the use, reuse, and evolution of ontology mappings, meta-data documenting the ontology mapping lifecycle is needed. In our system, this meta-data are collected and processed by a combination of automatic extraction from the ontologies and mappings and manual entry of meta-data by the stakeholders. In addition, the collected meta-data can be exported in an ontology-based representation that supports ontology mapping meta-data processing and interoperability. Our meta-data model is based upon an extensive evaluation in 2009 of meta-data support for management of ontology mappings in 13 mapping creation and management tools [51]. The Goal Question Metric (GQM) method was applied as an established method for structured and replicable evaluation of software products [2]. The 31 evaluation criteria established in [51] formed the basis for subsequent meta-data model development.

The meta-data model is under incremental validation through application to use-cases such as our StreamToHAN scenario. Mapping discovery is important for StreamToHAN when a new media device appears in the HAN, for example due to a purchase by the HAN owner from a third party. If the capabilities offered by this device are not already sufficiently described within the operator–customer federation then some form of mapping will be required to allow the customer to share those capabilities. Given a large network of customers or access to a global source of potential mappings like the Semantic Web it is very likely that another customer has already deployed these capabilities and performed the expensive task of creating suitable mappings for them. Hence efficient mapping discovery and subsequent re-use can potentially ease the deployment and integration costs. Evaluation of the potential for re-use can be separated from discovery and is the domain of machine-based mapping reasoning and recommendation enabled by our ontology-based representation of the mapping meta-data.

In order to evaluate the meta-data’s ability to augment discovery, a set of common mapping discovery tasks were defined (e.g. find mappings for a specific pair of named

![Fig. 4. CBPMS domain relationship and capability authority model screenshots.](image)

![Fig. 5. Simulated cost of CBPMS as against RBPMs with respect to policy search space size.](image)
ontologies, in a specific mapping file format), and then validated by a survey of 15 independent domain experts. This allowed lab-based, automated information retrieval tests to be run to establish if the retrieval effectiveness and efficiency was improved by using a semantic model of the ontologies, mapping features and life-cycle information. For this purpose an ontology mapping management framework (Moom) was built as a plug-in module using the Drupal content management system and supporting a SPARQL-based [45] mapping discovery mechanism. SPARQL, the RDF query language, is used to query the mapping repository which is a knowledge base expressed in OWL/RDF. Ontology mapping files stored in the Moom repository were analysed to suggest automatically extracted mapping meta-data fields and a knowledge engineer was able to verify these fields and enter additional meta-data. In the experiment, a file-based finder of the mapping files was compared to the metadata-based finder. These experiments have shown that the metadata-based approach has the same or better Recall and Precision than the file-based finder and that some discovery tasks were impossible with the file-based approach (e.g. due to the greater variety of search terms available in a meta-data based approach). Non-functional performance improvements were also demonstrated – Fig. 7 shows a comparison of query times for the 15 tasks identified in the scenario. Reduced query complexity was also shown. These findings, showing improvements in both the functional and non-functional properties of the system, provide evidence that our approach of defining a richer, ontology-based meta-data model for mappings is superior to the minimal meta-data defined by the other 13 mapping tools we surveyed [51]. Efficient mapping discovery and re-use are key enablers to building flexible federation systems that will be able to deal with a realistic diversity of model schemata that are changing over the federation lifecycle in an implementable fashion.

4.3. Combined FRM architecture

Fig. 8 shows the basic design of the FAME FRM. At its core it bundles together a semantic mapping framework with the CBPMS authority distribution system. It operates according to the following pattern: the relationship-management
service (as shown in Fig. 4), which can be controlled by resource/capability and relationship policies in the local network management system (NMS), allows an organisation to form relationships and share capabilities with third parties and make them available through a web-service-based API. Standard mechanisms for establishing trusted communications, for example [55], is assumed. Federation relationship negotiation is currently a manual process but federations can be programmatically initiated, maintained and terminated. Establishing a shared semantics for the federation is normally done incrementally throughout the federation lifecycle since the system depends on “just enough” semantics driven by the actual capabilities shared (whether imported or exported) within the federation at the current point in time. For example, a StreamToHAN customer may need to augment the shared semantics of an operator–customer federation when new devices with new capabilities are deployed in the HAN. Thus the “Capability Publication and Discovery” mechanism of the FRM is central to driving semantic convergence. This is implemented via linked-data style RDF publication on an authenticated SPARQL endpoint. Hence a minimal common OWL-based semantics are defined for federations, capabilities and capability authorities. However, these are

Fig. 7. Comparison of query times for file-based and metadata-based mapping searches.

Fig. 8. FAME Federal Relationship Manager.
published as RDF statements with a collection of associated RDF describing the web-service based entry point to those capabilities. This loose coupling allows for redundancy of capability authority definition and supports SPARQL-based discovery. Authentication is required since capability browsing is limited to a specific federation context and hence a specific capability representation. There is also a lightweight XMPP-based "presence" service supported to allow for notification-based capability discovery. Upon discovering new capabilities or during federation formation the semantic mapping framework can be used determine and manage appropriate mappings, or at least to identify capability descriptions that require user support to enable interoperability.

Capability sharing is itself enabled through the CBPMS architecture which maintains a distributed capability delegation graph and provides a Policy Decision Service to resolve policy evaluation requests (both locally for exported capability authority policies and remotely for imported capability authority policies).

The semantic mapping framework also allows organisations to map capabilities that have been shared by third parties to their own local information models and to manage these mappings too as they change over time. The FRM provides an extremely useful capability for cross-organisational management: It processes any requests for capability use from third parties, validates these against its internal relationship model, maps them to the local semantic space and delivers the request, in a locally comprehensible language, to the local management system – which can then do whatever it wants with the request, safe in the knowledge that the FRM has guaranteed that the request is consistent with capability sharing agreements that the organisation has entered into. In essence the FRM provides the middle 3 layers of the LFM (relationship definition, shared semantics and shared resources) and allows the 5th and 6th layers to be provided by the management systems of the various participants.

The FRM configuration operates as a run-time filter on capability invocations by third parties, which enforces security checks on all invocations and translates them into a representation that allows them to be directly invoked internally. The configuration is deployed as a sequence of lightweight filters, as shown in Fig. 9. The lower track shows how meta-data are consumed and transformed by the FRM runtime, while the invocation data are transformed along the upper track.

5. Conclusions and future work

This principal aim of this work is the development of a management framework which facilitates more agile sharing of ICT capabilities between autonomous organisations with heterogeneous deployed systems. Critical to the achievement of this goal is that the framework remains lightweight in terms of the common technical infrastructure that must be deployed by participants, the overhead of establishing and administering federations, and the operational overhead of the federated management system on runtime service delivery. The work described in this paper has described several concrete advances in our progress towards this goal.

The design and implementation of the FRM has illustrated how semantics and authority management technologies can be successfully combined to manage the distribution of complex capabilities between independent organisations with heterogeneous underlying IT systems and management information models, in such a way that they can conveniently integrate the imported capabilities with their existing management systems. The use of open-world semantic web languages – OWL and RDF – to describe capabilities helps to minimise the technical barrier to entry, as participants in federations only need implement support for those capabilities that they are interested in, without removing the ability to describe arbitrarily complex capability semantics. Furthermore, the meta-data based semantic mapping framework implemented in the FRM also helps to ease the administration overhead of federations throughout their lifecycle by providing both functional and non-functional improvements in the ease of mapping management and reuse. The CBPMS relationship map and capability authority model deployed to manage the distribution of authority for capability usage across federations is inherently simple and lightweight to maintain over time, having been developed and successfully applied in problem domains where management resources are more constrained – such as collaborative management of the resources of internet communities and consumer-management of information sharing [18].

In this paper, we have shown that our use of the capability authority graph to model policy can reduce policy-search overhead by an order of magnitude – reducing the runtime overhead of deploying the FRM by a similar margin compared to standard role-based policy systems. This measure is particularly important in this context – as
shared capability authorities may need to be processed by multiple management systems as they pass through different domains along their delivery path.

The definition of federation and the LFM that we have introduced in this work have been developed alongside our engineering work to allow us to break inter-organisational relationships down into dependant layers to render their definition and maintenance more tractable and transparent. This LFM model has proved invaluable in analysing a series of use-cases developed in collaboration with our industrial partners on the FAME project. The utility of this model is accentuated by the fact that its layers proved easy to map to technical implementations. The FRM implementation described in this paper only partially covers the LFM layers— the trusted communications layer is assumed – and the integration work on that LFM component is ongoing.

Furthermore, although our FRM implementation supports easy integration with local management systems, it assumes that the formation of relationships, the structure of federations and the definition of operational rules to govern the capabilities shared across them is a manual task. The FRM provides tools that facilitate such interactions, but it does not support automated federation discovery and negotiation. For the current work, we have assumed that entities have some means of discovering third parties that they would like to form federations with and communicating with them about the capabilities that they offer. How they do so is beyond the scope of this work which addresses the problem of how entities can form federations with third parties once they have come to the conclusion that sharing some resources with that third party is potentially desirable. A continuing focus of our research is the limits to which it is practicable to automate the negotiation and formation of federal relationships between autonomous entities. The first phase of this work will be limited to selection of pre-existing federation templates such as the operator–customer federation type and federation roles from the StreamToHAN scenario.

Although the use-cases described in this study are relatively realistic and correspond closely with the capability sharing agreements that service providers offer and wish to offer in order to deliver services to emerging computing environments, the real world tends to be more complex. In addition to network and service providers, there are numerous other parties who hold some stake or other in such services. Device and service providers often, in practice, control some of the capabilities that exist within a domain such as the HAN and they form agreements with one another which can be complex. Another strand of our continuing research is the application of the FRM to more complex multi-organisational arrangements which involve an increasing number of autonomous organisations.

Acknowledgements

This research is partially supported by the Science Foundation Ireland (Grant 08/SRC/11403) as part of the Federated, Autonomic End to End Communications Services Strategic Research Cluster (www.fame.ie).

References


Kevin Feeney is a research fellow in the knowledge and data engineering group (KDEG), Trinity College Dublin (TCD), Ireland. His research focuses on distributed and decentralised management systems. He has spent the last 13 years modelling, designing and developing distributed systems, spread evenly across industry and academia, in areas spanning everything from telecommunications and financial systems to consumer internet applications.

Rob Brennan is a research fellow in the knowledge and data engineering group (KDEG), Trinity College Dublin (TCD), Ireland. His research interests include semantic interoperability, intelligent distributed systems, and the application of semantics to systems management. He has contributed to 3GPP, TMF, IETF, and OMA communications standards. He has a Ph.D. (2004) from Dublin City University. Prior to TCD he worked in the Ericsson network management research center, Ireland and several start-ups.

John Keeney is a research fellow with KDEG in the School of Computer Science and Statistics at TCD. His research focuses on the use of semantics in the management of autonomic adaptable systems, particularly networking and telecoms systems. He graduated from TCD in 1999 with an undergraduate degree in computer engineering. His Ph.D. in computer science, also from TCD, was completed in 2004. He has published in excess of 30 papers in significant journals, conferences, and workshops.
Hendrik Thomas studied Business Information Systems in Germany and won the best student award in 2005. Afterwards he worked as a research assistant for the Digital Mechanism and Gear Library and developed ontology-based retrieval tools. In 2007 he won the best paper award at the I-Society International Conference, USA. In 2008, he started his PhD in KDEG, Trinity College Dublin and is working on an ontology-based framework to improve reuse of ontology mappings. His research is within the SFI research project FAME. Since 2009 he continues his PhD in collaboration with Massey University in New Zealand.

Dave Lewis is a Research Lecturer with the Knowledge and Data Engineering Group (KDEG) in the School of Computer Science and Statistics of Trinity College, Dublin. He has 19 years R&D experience in academia and industry, with over 100 publications. His work encompasses the knowledge-driven engineering of open distributed systems for integrated Network and Service Management and for Autonomic Pervasive Computing and Communication systems.

Aidan Boran has 20 years research and development experience in the telecommunications industry. He has working on the development, integration and support of 2G and 3G mobile networks, focusing especially on network management software. In 1997, he joined Lucent Technologies to work with the 2G and 3G network management development group. In 2004 he began a research role in Bell Labs Ireland focusing on data and enterprise integration. He holds a BAI (1988) in engineering from Trinity College, Dublin. He is currently completing a PhD in Computer Science at Trinity College, Dublin focusing on the management of ontology-based information integration systems.

Declan O’Sullivan is director of the KDEG at TCD, and has over 20 years’ R&D experience in both industry and academia. He holds Ph.D., M.Sc., and B.A.(Mod.) degrees in computer science from TCD. His particular research interest is in knowledge driven approaches to achieving semantic interoperability, especially applied to network and service management in distributed networks. During his time in industry, he was involved in industry and fora such as TeleManagement Forum and Object Management Group (OMG). He has over 70 publications, and has contributed to several organizing and program committees in this field.