Electronic Preprint for Journal of Information Processing Vol.24 No.4

Invited Paper

# Virtual Organization Platform Interoperability Provides the Long Tail an eScience Environment

Takeshi Nishimura[1] Eisaku Sakane[1] Kazutsuna Yamaji[1] Motonori Nakamura[1]
Kento Aida[1] Nate Klingenstein[2]

Received: April 5, 2016, Accepted: April 27, 2016

***Abstract:*** The core technology of eScience is the connection of distributed resources such that they appear as one virtual instance, enabling the collaborative research work on the Internet on that shared virtualized resource. eScience first embraced shared resources through support of "big science" in the Grid computing field. By contrast, emerging cloud services make high-end eScience infrastructure such as shared computing and disk resources affordable to common researchers. Though there are many such services to choose between, users always have to be authenticated as a researcher and authorized when they utilize services provided by a given collaboration. Effectively leveraging the world-wide deployment of academic identity federations may allow us to build a complete and coherent eScience environment more securely, easily, and scalably. One marked recent tendency in Identity Federation is to support virtual organization (VO), organizations composed of individuals principally domiciled at and authenticating against an organization but acting in a particular role within the virtual organization. A similar theme also emerged in Grid computing. However, all known current schemes have no common method for sharing VO information because every virtual organization is, today, largely bespoke, and these custom-built implementations take into account the principal needs of the federation and country and project where the VO emerged, leading each federation to employ different standards in integration with VO's and provision of information to VO's. This paper offers a historical perspective on VO technology, first by assessing its evolution in the Grid computing field followed by an analysis of progress in broader identity federation. Finally, potential evolutionary paths are divided into three natural categories, and we perform a technical and operational comparison of current VO technology and its capacity to meet these new use cases today and in envisioned futures. Reflecting how much development and operational costs are acceptable for each party concerned, two of these are considered preferred choices for the short-term and long-term transition to the unified, global VO platform.

***Keywords:*** virtual organization, group based access control, identity federation, Grid, SAML, authentication, authorization, eScience

## 1. Introduction

Japan's existing high-speed national research network, much like that of other countries, has facilitated the development of and widespread access to eScience environment. A typical example in eScience is the Grid, a somewhat ephemeral term representing virtualized and integrated computing resources, research data, experimental facilities, sensors, and human resources, and more, all generally shared over the Internet. The virtual organization (VO) is a core component of almost every Grid that has ever been realized, demonstrating its large scale relevance [1]. Access to virtualized research facilities and materials by research collaborators, sometimes from virtual organizations, can be made safer, easier and more scalable by lateral knowledge transfer and integration of a single sign-on (SSO) authentication mechanism, such as those deployed for shared web-based resources. This sort of mechanism has been independently developed, albeit with a much more limited scope, by Grid middleware functionalities themselves [2]. eScience environments have been utilized most actively in the fields collectively referred to as "big science," such as high energy physics, astronomy and biology [3], [10], [11]. However, world-wide deployment of academic identity federations [12] has the potential to make this same high-end infrastructure available to collaborations and subject matters that rarely receive the same level of funding and support, especially for computational resources. This is true not only for the most renowned scientists at the top research institutions in existing fields, but also up and coming scholars and new disciplines. Ubiquitous access to computational resources would be a crucial conduit for a meritocratic deepening of Japan's research efforts and subject matter expertise across numerous fields.

As detailed later in this paper, the academic communities in most countries operate identity federation using the SAML 2.0 standard [13], principally to grant access to web services. The SSO mechanisms implemented by the Grid and web-based identity federation both deliberately separate authentication from authorization, each of which can be implemented in a variety of places within identity systems [14]. Common use cases in web-based identity federation led naturally to the same conceptualization of VOs that powered the Grid, encouraging thoughts that this

[1] National Institute of Informatics, Chiyoda, Tokyo 101–8430, Japan
[2] Internet2, Washington DC 20036, USA

is the most common and useful basic representation in eScience. To support VOs in identity federation, the VO's infrastructure is typically operated independently from any institutional IdP. A service which is specifically designed for management of virtual organization users and their attributes is typically called as VO Platform. Many of the pioneering federations have developed and operated VO Platforms, but no single implementation has risen to the fore yet.

This has led to divergence in the current architecture of the VO Platforms in each identity federation, creating many problems, such as rendering services unable to share group membership or other VO-maintained attribute information with providers in other federations. Lack of any widely supported standard for expressing group membership across federations narrows its potential for worldwide research networks. SAML 2.0 secures communication between IdPs and SPs by means of metadata. The metadata is managed by each federation, enumerating valid keys, names, and endpoints, allowing providers to discard untrusted requests. In order to address these interoperation challenges that have arisen across federations, the concept of "inter-federation" involving wholesale exchange of metadata between domestic federations has gained mindshare. Consequently, presuming federation A and B have inter-federated, login using an IdP operated by federation A to a SP operated by federation B could be established without further administrative intervention. eduGAIN, which originally launched as an EU funded program is now the international inter-federation framework in the academic space [15]. If a similar framework to inter-federation could be adopted by VO platforms, it would strongly facilitate international research collaborations. However, in present circumstances, VO platforms in each country employ different names and semantics entirely, even for the most common use case of sending group information to SPs. Inter-federation of VO platforms may thus be considered a crucial requirement for maximum use of identity federation in eScience. This paper provides comparative survey results of the special characteristics of each VO platform and proposes potential paths towards a standard for user data exchange, intended to broaden and deepen access to eScience resources for everyone.

## 2. Basic Concepts and VO Overview

### 2.1 Dissociation of Authentication and Authorization

Various online services have been provided on the network since the early stage of the Internet, but the scope and scale of today's deployment is much larger, both technically and operationally. Every online service is offered from a different site. It is necessary for online services, which deal with information that may be personalized, such as email and file sharing to authenticate a user, i.e., to recognize who is the user, so that the online service can offer appropriate services for the user. In general practice today, a new account with a new password is issued directly to the user for authentication. This independent management of accounts by each service causes high operational costs, and invites security risks. A few examples follow:

* Operational costs involved with the issuance and management of user accounts are much higher. It is also inconvenient to the user, who may need not only to track all these accounts, but also to be able to select the right account for each service.
* An inconsistent level of trust, particularly at the baseline, for authentication and system security across different computational environments.

Complex operations are by definition expensive ones, and inconsistent security levels result in the lowest common denominator bringing the security of the entire implementation down to its level.

A first step towards the reduction of management costs and policy unification is sharing of account information (identity unification). LDAP implementation such as Active Directory are used widely as a source of unified identity within a single organization. These systems are fundamentally insufficient in terms of integration since authentication processing is done independently by each service.

A second step may be taken by sharing the results of authentication rather than the credentials needed to directly authenticate the user, which dissociates authentication and authorization from one another and eliminates the need for one common authentication mechanism. Authentication is used to identify a user, while authorization gives proper access rights to resources for the user once authentication is complete and the formerly unknown user is associated with a known digital identity. In the field of identity federation and Grid, system architecture has been designed based on this concept of dissociation of authentication and authorization. A strong relationship of mutual trust between the entity responsible for authentication and the entity responsible for authorization based upon that authentication result is crucial to allowing this dissociation of authentication and authorization. PKI and other asymmetric cryptographic technology is often used for the relationship.

More seamless cooperation becomes possible by combining multiple services if user identity is shared among services. Especially for Grids providing data processing services that involve various resources on the network, having a common identifier by which to refer to the user is particularly important. It is also important when mashing up distinct smaller, atomic services to realize combined service. Such use cases are becoming widespread in eScience deployment, leading to chaotic innovation.

Sharing account management and authentication processing is realistic in an environment where it's possible to unify operational criteria, particularly if there is a hierarchical structure. Any solution should be suitable for any enterprise which manages systems and accounts in a unified way as a single organization, including universities. The quality of credential issuance and subsequent authentication, typically referred to categorically as a "level of assurance," or LoA, is important when issuing new accounts, modifying existing accounts, and allowing previously anonymous users to associate themselves with a known account, e.g., authentication. It's generally reasonable to expect a user identified by an organization for services in use by that organization to have been better credentialed and authenticated than a user from an irrelevant organization, but quantifying this is difficult and standards have not made clear distinction easy. Where a single organization is responsible for both the services and the identities in use,

a high level of reliability and consistency is generally achievable.

Use of cloud-based services has been spreading rapidly in recent years. Identity federation has been an engine underpinning this transition, especially when a common identifier is available to different cloud services for a single user at an organization. As cloud services are becoming more important, so too are those identity services required to leverage cloud services to the fullest extent possible. Public cloud services now offer a competitive alternative to Grid environments run by universities, and these public cloud services are now grappling with the same identity management challenges that have manifested themselves in academia for years. Truly enabling these services will require building a consistent-yet-distributed system with multiple independent entities responsible for providing services and identities, all within a mesh-like framework.

### 2.2 Group-based Access Management

A typical service offers a collaborative environment for multiple users rather than any single user acting in isolation. There are many services that are intended to be accessible only to a discrete subset of the entire authenticated user base, making common access controls necessary to efficiently enable them. Such services are popularly desired in laboratory and joint research activities.

Sharing a single account and password across an entire group is one mechanism by which group access has been achieved. It has multiple drawbacks: when a member leaves, distribution of a new password to users becomes required. The process to refresh group password is much troublesome and consciousness of security in password management often becomes thin as ambiguous responsibility for resource management emerges and access credentials protect nothing but common resources. This places no constraints on where or how groups form, for better and for worse, nor any limitation on the management of the group. Group members are sometimes given an interface by which they can manage their information; an administrator within the group may manage membership in other cases; or, an administrator wholly outside the group may responsible. This ad-hoc approach to group membership management and credentialing often contrasts starkly with contractual requirements and the need to carefully audit and control access to sensitive or limited resources.

One countermeasure is implementation of an additional mechanism to audit access by group members using individual identities. This offers some advantages in that each user does not have to remember a password for group access and leaks of passwords become less catastrophic.

### 2.3 VO Management

One rational conceptual approach to identity management is to consider the user's authenticating organization, such as the university to which they belong, the ultimate authority for that user population. However, there are many groups involved in that extend beyond the boundaries of a single organization, such as research collaborations that span multiple universities. VOs allow users to be grouped somewhat independently of any ultimate authenticating authority, though this depends on use case. Cross-organizational use cases are pervasive enough that an identity management system which does not presume it operates within the context of a single organization is necessary to solve the problem generally.

Various frameworks have been proposed and implemented for VO management. Grids and general identity federations alike both have typical distributed service environments in deployed practice that dissociate authentication and authorization, and the essential model in use by each is largely the same. Differences in implementations are encountered not based on whether an identity system was built for the Grid or not, but more in terms of the architecture of the identity management system (distributed or centralized), protocols used, data quality controls, provisioning policies for personal information protection, etc. Evidence for both this consistency and these points of divergence is presented in detail in the next two sections, covering traditional Grid-based VO architecture and identity federation-based VO architecture.

## 3. Application of VO Concepts in Grid Environment

### 3.1 VOs in Grid Environments

Grid computing enables the dynamic sharing of resources regardless of their geographic and political distribution, as end user demand and resource policy are the primary drivers of access. The key concept in today's dynamic resource sharing is the VO [1] because it's the granularity at which access management is generally performed. VOs may be conceived of around user communities, organizations, or resources, and they are typically focused, specific collaborative teams operating towards common goals. For example, in the high energy physics research community, researchers distributed all over the world require high computational power and large storage capacity to analyze the huge amount of experimental data generated by particle accelerators. Empirical experience demonstrates that virtual organizations typically emerge in response to challenges that exceed, in some manner, the scale a single organization can effectively manage [3].

### 3.2 VO Management in Grid Environments

Authentication and authorization are fundamental concepts for actually rendering and enforcing access control requirements. Grid Security Infrastructure (GSI) is now a de-facto standard for authentication for grid computing. GSI is implemented using a public key infrastructure (PKI) [2], [4]. There is more variety in authorization approaches, likely reflecting a wider variety in authorization requirements than authentication requirements for key use cases. Most of these approaches are object-oriented, representing resources and users or other agents that need access to the resources. Representation and expression of authority is a common need which is often rooted in a primary authority that can make and record actual and specific decisions. A sampling of authorization model implementations follows:

**grid-mapfile**

The authorization model in Globus Toolkit is best represented by the grid-mapfile and associated mechanism [2], [5]. A grid-mapfile associates the Distinguished Name in a digital certificate, typically tied to authentication, with a local account name at a resource, e.g., a UNIX local account. The user's local account name

is registered in the grid-mapfile, allowing for the mapped user to act using that local account.

**VOMS**

Virtual Organization Membership Service (VOMS) is an implementation of the authorization model originally developed by the European DataGrid (EDG) [6]. Before VOMS was developed, EDG had been registering authorization information in repositories managed by each virtual organization in LDAP directories specific to that virtual organization. Resource providers (RPs) would query the LDAP server to generate grid-mapfile representations of user bases for the services that they operate. This authorization is capable of expressing only basic Booleans and relations; thus, it has not been able to represent a series of key user attributes, such as roles, subgroups, and other categorizations that vary by deployment and discipline.

VOMS improved the flexibility and scalability of the authorization mechanism. As part of authentication bootstrapping into VOMS, a user's attributes are stored in a relational database. A user obtains a shorter-lived, so-called "proxy certificate", which directly contains attribute information represented as Fully Qualified Attribute Name (FQAN) inserted in the extension field of an X.509 certificate. An RP authorizes the user by simply interrogating the contents of the presented proxy certificate. While VOMS allows an RP to define finer-grained policies for authorization, it also generally leads to significant operational complexity. Currently, VOMS as an implementation is maintained by the Italian National Institute for Nuclear Physics (INFN) [7].

**CAS**

The Community Authorization Service (CAS), developed by the Globus Alliance, addresses flexibility requirements in a similar way to VOMS [8]. In the CAS implementation, a user's attributes are stored in the CAS server and inserted in the extension field of a proxy certificate. A key conceptual difference is that a CAS server authorizes the user to access resources, while the RP retains the right and responsibility of authorizing user access in the VOMS model. CAS was implemented as a web service in Globus Toolkit Version 3. Development stalled there and looks unlikely to accelerate, particularly since the most current Globus Toolkit, Version 5, does not support web services at all.

**PERMIS**

Privilege and Role Management Infrastructure Standards Validation (PERMIS) is a more ornate authorization model implementation that follows the principles of Role Based Access Control (RBAC) [9]. Attribute authorities in PERMIS are often independent and issue attributes that associate a role with a user. An application determines authorization based on the attributes and governs access to resources accordingly. While early implementations of PERMIS required an X.509 attribute certificate, similar to proxy certificates but with a longer lifetime and a presumed focus on attributes alongside the DN, the latest version does not require usage of certificates. The latest version also supports expression of policy in plain XML and the use of SAML attribute assertions to convey user data.

## 4. Application of VO Concepts in Identity Federation

The introduction of identity federation at this point in this review mirrors its chronological rise in deployment, which typically followed the rollout of most Grid middlewares. Identity federation itself provides a trust framework for the exchange of authentication results and, optionally, user attributes, between multiple identity providers (IdPs) and multiple service providers (SPs). Identity federation has entered global use with some consistency, but mainly only in academia. Most use SAML as their primary protocol.

As of December 2015, 61 academic identity federations were operated at a production level [12]. The Japanese identity federation serving our domestic research and education community is named GakuNin, and it has been in operation since 2010 [16]. While the widest adoption of the technology to date has been in North America and Europe, there has been attention from other parts of the globe, most notably South America and Southeast Asia.

Authentication is performed by an IdP, each of which is typically independently owned and operated by an academic institution. Services are generally not capable of directly authenticating users themselves: instead, if an SP requires user authentication, it will issue a request to an IdP. After successful authentication of the user by the IdP, and in some failure states, an authentication result is returned alongside any requisite user attributes. SPs utilize the attributes in authorization processes such as access control for web-based resources. In this model, user information is generally expected to be managed solely by the identity source, e.g., universities in today's deployments. Commonly available attributes describe a user's organizational and departmental names, usernames, email addresses, and so on. GakuNin has defined 18 different kinds of attributes [17].

The operation of each IdP by academic institutions generally results in implicit benefits in identity proofing since the user and university are likely to ascribe considerably higher value to credentials that control access to more resources, particularly those that are personalized. There has been running tension between the use of identity federation to power services that are purely focused on research and academia and others that serve the academic community in a variety of ways, often commercial.

### 4.1 Common Features of VOs in Identity Federation

Since user authentication and data storage is highly distributed in identity federation, VOs have evolved to suit the technology by consisting primarily of a set of user identifiers that spans multiple authorities, analogous to a sort of distributed grid-mapfile. A set of user identifiers can be generally informally interpreted as the canonical list of members of a VO. A VO Platform (VOP) provides a system to manage VOs in this sort of highly distributed environment through the local creation, representation, and maintenance of VOs, typically simply through addition or removal of members. The set of identity providers that may be used with a given VOP typically matches or is a subset of an identity federation, but this isn't universal. Some VOPs support free-range

identity providers with more open registration policies, while others with strict security needs typically cater only to a few IdPs chosen specifically by the VOP operator.

VOPs rely on user identifiers asserted by IdPs, which means the VOP will often be acting in an SP role directly. By contrast, the VOP is typically directly responsible for conveying information about the VO and its membership to end SPs that are associated directly with shared resources. VOPs will often offer a variety of these mechanisms in parallel to provide this information to SPs. For example, a joint research project may be managed by a VO using a VOP to share a research dataset and to exchange comments about relevant academic topics.

Expression of VO membership and permissions is done in a wide variety of ways, including pushed data, pulled data, and reassertion of data. Mechanical authorization in this model, consisting mostly of enforcing access control checks on supplied data, is generally performed by those destination SPs as well. We examine detailed protocols and methods for conveying VO information to SPs in today's theory and practice in this section, while the following section proposes alternatives to today's protocols and methods.

The capacity of educational organizations to own and operate identity providers is widely variable. A practical delineation of duty has emerged between user vetting, often occurring out of band or ahead of time, and real-time access management. Identity proofing and other formal processes associated with user registration and management in virtually all cases should be and are performed by the organization directly. The more mechanical work of answering requests for authentication or queries for user data is more readily outsourced to a third party organization when this is desired.

Some users that have no access to any live identity provider may be directly supported by VOPs as self-registered local accounts or through the use of identity providers that provide a reasonably consistent identity check without themselves vetting the initial registration. In this instance, the VO or VOP may be directly thought of as the vetting authority.

### 4.2 VO Platforms in Identity Federation

Many VOPs are operated in production infrastructures that are actively used. In this section, we survey existing VOPs.

**Figure 1** depicts the common architecture of existing VOPs. Each VOP consists of three components, an authentication component, a management component, and a provision component. The authentication component receives assertions and user identifiers from IdPs to recognize the users. The management component provides the user interface to manage VOs on the VOP, e.g., addition and deletion of VO members by a VO owner. The provision component provides VO information to the relevant SPs. For example, some VOP can provide information about VOs which the accessing user belongs to, so SPs can control the access based on that information.

Perun [18] was originally developed for authentication and authorization for a Czech Grid named MetaCentrum. In addition to federated identities, Perun supports social identities such as Google Accounts and Facebook Connect. VO information may

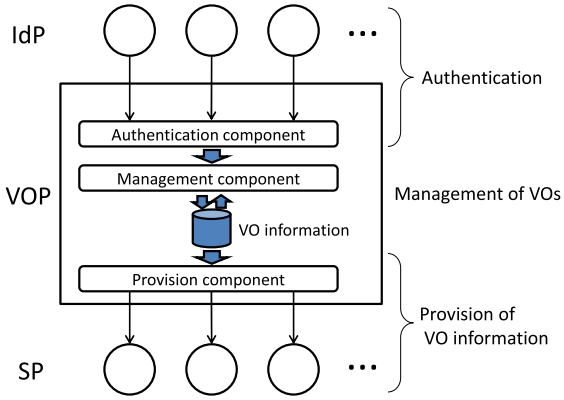



**Fig. 1** Common architecture of VO platform.

be supplied to services either in the pushed identity assertion or through a back-channel query to an LDAP directory. Since this mechanism is somewhat unique, it's exhaustively described later in this study. The primary instance of Perun is operated by CESNET, but there are instances in other deployments using the same software.

COmanage [10] is a VOP developed by Internet2 in the U.S. Its focus is on efficient collaboration among members of a VO, bundling many services that may be useful to a VO alongside baseline identity management. LIGO [19] actively uses COmanage as a VO. There is no instance operated by any federation. Instead, LIGO operates COmanage as a dedicated VOP for users of LIGO and related VOs. A complex and flexible registration workflow can be configured by each VO. Users can join the VO through that workflow. The most basic example would be the presentation of a web-based form that is presented upon interception of unauthenticated access to prompt for authentication at trusted sources and recognize authenticated users, typically leading to review and approval of the user by an administrator.

GakuNin mAP [20] is developed and operated for VO management by NII for research services built on Japan's GakuNin federation. For users who do not belong to any IdP, GakuNin mAP supports a so-called OpenIdP [21], a basic identity provider that allows for self-registration. GakuNin mAP is designed to primarily supply VO information to SPs by means of SAML 2.0 Attribute Query that is executed after the initial authentication, allowing the VO to administer additional attributes without imposing requirements on the rest of the workflow. Additionally, originally in support of services like associated email lists, GakuNin mAP also supports VOOT, a basic protocol that is able to provide data sets about multiple users to a single service, such as a complete list of a group's membership.

Since VO infrastructure is invariant in its essential function while powering workflows that are themselves highly variable, many other implementations have emerged. There are countless examples, but prominent additions to the above list of VOPs are HEXAA [27], OpenConext [28]/SURFconext [29], and Switch GMT [30]/SWITCHtoolbox [31], all of which are operated by various federations in various countries [32].

REMS [11] was not developed specifically as a VOP, but it is a system specialized for authorization to research datasets such as genome data and biobanks. Workflow can be completely

customized from application to approval. Each resource has zero or more approvers and zero or more reviewers. They may each be involved in the workflow, and approvers can approve specific changes. Approved users then access SPs directly, which query REMS themselves to verify that the user is indeed approved for any intended actions. REMS supports SAML 2.0 attribute queries for user data, but it can also proxy user attributes and authentication received from an IdP, flattening the user representation and the identity model for applications when desired. The interface and workflow make it an attractive selection as a VOP despite having been developed primarily for other use cases.

Grouper [22] was principally designed specifically for group management by organizations that internally delegate portions of their identity management infrastructure, such as to the organizational units of universities. Grouper itself may also be repurposed as a VOP if it is configured to support many IdPs for authentication. The full set of groups within a Grouper instance may be thought of as a tree of identity information that is typically expressed through LDAP group membership. Extensive customization is possible and extension is intended, allowing for the integration of diverse data sources. User provisioning is another key part of Grouper, propagating changes in group membership out to systems that act as primary interfaces, much like Perun.

### 4.3 Interfaces between VO Platforms and SPs

The survey of implementations above is necessarily brief, but it touched upon multiple different mechanisms by which data can be ultimately provided to services. Multiple mechanisms are often supported in tandem by a single implementation, and this list is not exhaustive, but the most widely adopted mechanisms are described in order of popularity.

1. SAML 2.0 attribute queries
2. IdP proxying
3. VOOT
4. LDAP
5. Perun's push mechanism

SAML 2.0 defines attribute queries in the core specification and similar protocols offer similar features. In common practice, the SP makes a query containing an identifier supplied by an organizational IdP that will be recognized by the VOP, and the VOP responds with a set of VO-managed attributes and identifiers that tag the user with additional information, such as resource access privileges. This approach is preferred by many deployers because it offers the best privacy protection for users, requiring services to have a trust relationship and an identifier in hand before issuing any successful query, and ensures that data only resides at authoritative sources, incurring the incidental benefits of fresher data, superior trust, and auditability. On the other hand, since queries are issued in the context of specific users, it's generally impossible for the SP to use this mechanism to retrieve a complete list of members of a particular VO. The generic identity management term for the VOP's role in this arrangement is "attribute authority" (AA).

Shibboleth [23] is most widely-used SAML implementation in identity federation, particularly in academia. The Shibboleth SP has a basic mechanism for issuing subsequent SAML 2.0 attribute queries after an initial payload of user data is received, here called "SimpleAggregation." This process depends on the SP having received a user identifier like eduPersonPrincipalName [24] from the initial identity source that will be recognized by the AA that answers the attribute query. Regardless of the outcome of the query, all the information that is received from all identity sources is flattened into a single representation for applications. This is in keeping with Shibboleth's general implementation philosophy of abstracting identity processes from the application itself, so in general, the application doesn't need to be further modified beyond the initial externalization of these identity processes, which is necessary to leverage identity federation in general.

IdP proxying is not conceptually bound to any single protocol, though it is in practice often also based on SAML. IdP proxying retrieves VO information via the user agent and the Web Browser SSO Profile, by far the most common way for SAML to be deployed, instead of a direct attribute query. Mechanically, an SP requests authentication of a VOP as if it were an IdP. The VOP then effectively relays that request by issuing its own request for user authentication to the primary IdP. The VOP receives some user identity information from the source IdP that is then concatenated with VO specific information maintained locally, completing a representation of the user that can be passed to services in a single payload. That payload is delivered by the user's web browser in the penultimate step. Since the user's browser is the intermediary in this mechanism, no SP can retrieve VO information using this interface without the user's involvement. As the user is the vector for data transport, direct communication between services is not necessary, and the proxy represents a single auditing point, this mechanism is actually more amenable in practice to highly secured digital environments than direct attribute queries.

VOOT [25] is a protocol specifically designed for the VOP use case. It can retrieve a complete representation of group membership in either of the two conceptual directions: a list of groups of which a user is a member and a complete enumeration of a group's membership. In order to use VOOT as the interface between a VOP and an SP, the SP should implement VOOT client functionality, whereas the VOP should implement VOOT server functionality. VOOT itself has not yet been formally standardized in any standards body, but it is based on popular standards such as OpenSocial or SCIM. Unfortunately, this depends on the VOOT version.

LDAP [26] was not primarily intended for use that crosses organizations, but it is still often used to retrieve the same two views of group membership that VOOT provides. In order to use LDAP as the interface between the VOP and an SP, the SP should implement LDAP client functionality, whereas the VOP should implement LDAP server functionality. with the major difference between VOOT and LDAP is that LDAP has no singular widely accepted way to represent user identifiers or enforce access controls on data viewership. LDAP interfaces presuppose strong trust between SPs and the LDAP server itself, often explicitly through service accounts.

Perun's push mechanism is very different from the other interfaces in that the provisioning of information to applications is triggered by changes in the VO itself rather than user activity,

such as the association of a new member with a VO. The VOP generates configuration directives specific to each SP and places them in a file as expected by an application, which is itself relayed to the SP automatically. This mechanism can be applied to non-web protocols since there are no presumptions about client behavior or capacity. For example, it would be possible for secure shell (SSH) access to a server to be managed using Perun's push mechanism, which is very difficult to accomplish with any other widely deployed approach. Applications must carefully and deliberately reload local configuration files to ensure fresh user data since those files are effectively managed directly by the VOP. Another advantage inherent to this method is that the SP implementation does not have to contain any VOP-specific code, often allowing existing naive implementations to be used without further modification.

## 5. Proposed Methods for VOP Integration

From a user's standpoint, virtual organizations appear to be very tightly associated with service providers. Stepping back and viewing the problem orthogonally, today's VOPs appear less like an integrated platform for many VOs and many services, but rather a remote and ad-hoc management mechanism for specific resources. Some resources are only available through use of a specific VOP, making it more of a bottleneck for access by the long tail than an enabler of it.

The first step towards integration of VOPs is a somewhat unrelated precondition: it is necessary that all VOPs recognize the same set of IdPs in order for a VOP to recognize any user in any VO on other VOPs. Since each existing VOP currently recognizes a different set of IdPs, as mentioned in the previous section, it is possible that a VOP cannot recognize some members of VOs on other VOPs. In this way, IdP recognition is only half of the puzzle; relevant SPs must also support the same set of IdPs in order to coordinate and cooperate with the VOP.

eduGAIN, an emerging international inter-federation framework for research and education, may be part of the solution to this problem. As of December in 2015, 37 federations have formally joined eduGAIN, in the process enabling possible mutual connection between 1486 IdPs and 1025 SPs throughout the world [15]. This presents challenges for VOPs principally in policy, administration, and interface design, weighed against the overwhelming benefit of a larger and more distributed user base to draw from.

The most that the authors realistically expect from the eduGAIN integration process is greater homogeneity in terms of which providers in academia will communicate with other providers in academia. It should be noted that only user identifiers and some user data are interoperable among those VOPs and SPs by eduGAIN. VOP-managed VO information such as group membership is not interoperable without deeper VOP integration.

At a minimum, a VO will need to be assigned some form of identifier that a VOP can use to uniquely identify a VO. This would typically be done by establishment of a namespace for VO IDs and assignment of namespaces to VOPs for further partition and assignment to individual VOs.

Beyond those basics, we propose three candidate methods for deeper VOP integration. We explore each method in the following subsections.

1. Protocol standardization
2. VOP proxy
3. VO information sharing among VOPs

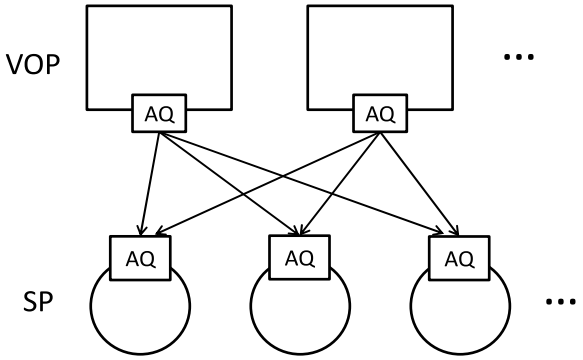



**Fig. 2** Method 1: Protocol standardization.

### 5.1 Protocol Standardization

The most immediate integration problem stems from the wide variety of integrations, invoking the old saw that the nice thing about standards is that there are so many to choose from. As a result, an SP today generally has to support a distinct mode of interoperation with each VOP, as illustrated by the five different interfaces described in Section 4.3. If there were a widely adopted, standardized interface for relying services to interrogate VOPs, then services would be able to identify all VOs in the local universe. It is not necessary that any protocol be adopted as an international standard to achieve progress, but an agreement between interested parties is fundamental.

**Figure 2** depicts VOPs and SPs interacting through a hypothetical standardized protocol that is based on SAML 2.0 attribute queries because it's the most widely deployed of the current solutions. AQ denotes support for an attribute query profile for virtual organizations. Because all VOPs would then be able to ensure they at least speak the lingua franca protocol, any SP could issue queries to any VOP and retrieve VO information as governed by use cases and policies needed to protect services.

As mentioned in Section 4.3, each of the existing interfaces has its own merit and set of examples, and standardization on any single mechanism may impinge the deployment scope of other mechanisms that are better suited to other problem spaces. For example, if we were to adopt SAML 2.0 attribute queries as the only standard interface for interaction between SPs and VOPs, user privacy would be well protected. However, it would be impossible to retrieve lists of all VO membership, leaving important use cases like mailing list services in a precarious situation, dependent on every user's express and active involvement to flesh out a set. While the inconvenience is unfortunate, the greater problem is that this is nonsensical to the users themselves, making the solution unpalatable for deployment.

One could envision variations on this approach that build from a small set of protocols rather than any one model of the five enumerated. Doing so would increase VOP functionality at the cost of increased implementation complexity for some VOPs that do

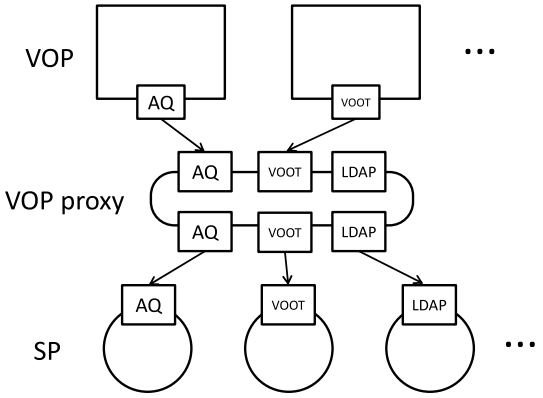



**Fig. 3** Method 2: VOP Proxy.

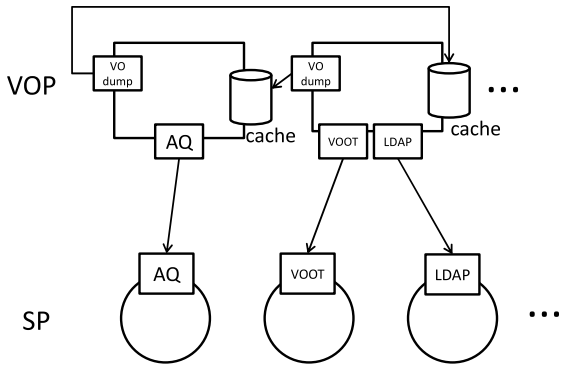



**Fig. 4** Method 3: VO information sharing among VOPs.

not support the subset of the chosen protocols.

In any case, some services would need to be re-architected: those that were built upon models that were not selected for standardization. Transition costs are better measured in terms of adoption rates rather than in terms of deadlines or financial incentives.

### 5.2 VOP Proxy

Another practical method for integration would be a VOP proxy. In this method, a single large proxy service would act as an intermediary between VOPs and SPs. This universal hub could support much greater variety in protocols and interface mechanisms, perhaps many of those detailed in this study. Especially given differences between protocols in widespread use, one of the key benefits of this sort of a proxy approach would be protocol translation, which could be done consistently in the proxy itself. The proxy further simplifies matters for VOPs and SPs by aggregating services and identity sources, offering flexibility to both VOPs and SPs in terms of the granularity on which they choose to define and represent themselves. Furthermore, a VOP proxy could send a query to all VOPs, merge the results, and send those results back to the SP, offering a nuanced querying functionality that is not possible in more distributed systems.

**Figure 3** depicts VOPs and SPs interacting through a VOP proxy. The VOP proxy is placed between VOPs and SPs, and it translates queries from SPs. For example, when an SP sends a query to VOP proxy using SAML 2.0 attribute query, the proxy sends it to the first VOP that supports SAML 2.0 attribute query as it is. On the other hand, the second VOP does not support SAML 2.0 attribute query but supports VOOT, so the proxy translates the query into VOOT protocol and sends it to the VOP. All responses from VOPs are collected and are sent back to the SP.

SPs would need to be reconfigured to trust and utilize the VOP proxy rather than directly communicating with VOPs.

The VOP proxy may encounter challenges in protocol translation for a VOP if the VOP only supports limited protocols. For example, if one VOP only supports SAML 2.0 attribute queries, then VOOT queries and LDAP queries could not be satisfied by any amount of magic mapping because such queries are simply not possible using SAML 2.0 attribute queries. As a result, all VOPs would need to be extended to support what would be considered a minimal set of general protocols.

The minimal set could be further reduced by limiting the use cases and protocols formally supported by the VOP proxy service, but only at the expense of limiting the protocols and features that SPs would be able to expect of VOPs.

As a direct result of these considerations, the implementation cost of a VOP proxy would depend principally on two factors: the number of protocols SPs can use, and the number of protocols that the VOPs support. Fewer protocols would be less expensive but come at the cost of reduced functionality that would not satisfy certain use cases.

### 5.3 VO Information Sharing among VOPs

The third integration approach that we consider is direct implementation of a mechanism to replicate and share VO information across VOPs. Through these means, VOPs would be able to appear as a more integrated and singular platform by offering consistent access to the same data set through the same mechanisms. There would be no need to implement any new entity or reformulate SP configurations because each SP is already connected to a VOP and it is the VOPs that are changing, existing interfaces and implementations will often be usable by applications without modification.

**Figure 4** depicts SPs interacting VOPs modified by this method. Each VOP has been modified to have a cache that contains information of VOs on other VOPs. The cache is updated periodically through the dedicated protocol. The dedicated protocol is denoted by "VO dump." Each SP could send queries to a VOP as before. Because the VOP aggregates VO information on its own and VO information on the cache, the SP could obtain necessary information of all VOs on all VOPs.

This comes at the inevitable cost of heavy changes to VOP implementations. VOPs must be extended to cache VO information from other VOPs. A dedicated protocol would also be necessary to communicate VO information between VOPs. We believe that the VOOT protocol, if standardized, would provide sufficient functionality for inter-VOP communications. Any VOP could periodically query other VOPs for updated information about VOs that are managed at a given VOP using the VOOT protocol. VOPs would need to be able to authenticate one another directly to provide trusted collaboration.

A variation on this method would use real-time queries between VOPs instead of caching. This invokes the familiar old trade-off between data freshness and bandwidth – computational,

**Table 1** Comparison of three integration methods.

| | | Protocol std. | | VOP Proxy | | | VO Sharing | |
|---|---|---|---|---|---|---|---|---|
| | | VOP op | SP op | VOP op | P op | SP op | VOP op | SP op |
| Cost | Pre impl. | C | C | A | C | B | C | A |
| | Pre nego. | C | C | A | A | A | B | A |
| | Post | A | A | A | C | A | C | A |
| Scalability | | A | | C | | | A | |

network, and otherwise – required.

In support of this approach, we introduce the concept of a VO having a "home VOP". Each VO would have one home VOP where the VO could be managed. Information about that VO as supplied by other VOPs would be no more than a mere cache, which may help to avoid namespace collision. There are open questions around VOs that could be managed in parallel by multiple applications and VOPs. Construction of a trust and namespace model to make this realistically possible is very difficult, but the use cases are very compelling.

The home VOP concept can be applied in other integration methods as well. A VO could be assigned a principal VOP in which it operates and that is considered its authority.

Each SP could also be assigned a home VOP. That VOP would serve as the main and first responder to queries from the SP. From the perspective of the VO, such a network of VOPs would abstract away the constraint of tight integration with an SP. From the perspective of the SP, the network would enable it to recognize all VOs regardless of their home VOPs.

### 5.4 Comparison of the Three Integration Methods

We compare the three integration methods in terms of cost and scalability. The cost can be divided multiple ways: into implementation cost and negotiation cost, cost of integration and cost of maintaining that integration, and cost to VOP operators and cost to SP operators.

**Table 1** shows the results of this comparison. Columns denote proposed integration methods and who is responsible for expenses. "VOP op" denotes VOP operators. "SP op" denotes SP operators. "P op" denotes hypothetical implementers and operators of a VOP proxy.

The row "Pre impl." denotes the cost of implementation that must be performed before baseline functionality associated with the mechanism is realized. It includes VOP proxy implementation expenses and various modifications to or extension of existing implementation that SPs and VOPs would need.

The row "Pre nego." denotes negotiation cost, i.e., whether the parties concerned have to talk to adopt some decision prior to any VOP integration. These costs are derived from both the protocol adopted for SPs to retrieve VO information from VOPs and the protocol to share VO information among VOPs.

"Post" denotes operational costs that would be incurred after successful VOP integration. Generally, integration is more expensive than singular or isolated deployment.

"Scalability" denotes whether we envision the integration method would work at large scale in an environment composed of many SPs, IdPs and VOPs. "A" denotes it should work well, while "C" denotes anticipated problems at large scale.

In the cost rows, "C" indicates the cost is heavy in comparison to other methods, whereas "A" indicates minimal expense.

The first method, protocol standardization, involves great negotiation cost principally because VOP operators and SP operators would need to be involved in extensive collaboration and standardization work to define a consistent set of protocols. Some implementation cost would also be necessarily incurred. If an SP depends on a specific legacy protocol, or more particularly a feature of a legacy protocol which is not adopted in a new standard, it could be forced to modify its implementation. Also, the VOP implementation also itself may need to be modified for similar reasons.

Special mention of Perun's identity provisioning mechanism is warranted. If some similar mechanism for pushing identity data is not widely adopted, there will be a resultant increased implementation cost for SPs that could otherwise depend on the push mechanism. This is because all of the other options assume significantly less deep integration with the application itself. Adoption of such a mechanism would, by contrast, increase implementation costs for VOPs based on other technologies.

We would envision little additional operational cost resulting after VOP integration except for the inevitability of bugs and bug fixes in new implementation and protocols.

The second method, VOP proxying, places a service as an intermediary between VOPs and SPs. Columns in this table show implementation, negotiation, and operational costs for a VOP proxy with a presumption that no protocol standardization takes place. There is no negotiation cost between VOPs and SPs. Instead, there is a heavy implementation cost for the VOP proxy itself because it must support all the protocols any VOP supports. Each SP must change the configuration of the destination of queries, as indicated by use of the grade "B."

A VOP proxy would also involve operational costs, as it is a new online service that would need to have very high availability. This implicitly includes additional implementation costs for the VOP proxy operator to handle changes in integration with any given SP or VOP.

The third method, VO sharing, does not require any SP modification or negotiation. It requires negotiation between a few of the parties involved, principally between VOP operators, as depicted using the grade "B." All VOPs would need new functionality to share VO information.

There is additional operational cost for VOPs after VOP integration resulting from the simple fact that they will be managing more varied information about more VOs than before.

From the perspective of scalability, VOP proxying has an apparent problem in the centralization of query processing from SPs at the VOP proxy. Decentralization and technical approaches to remediation can achieve the availability necessary, but with associated operational costs.

Through the above comparison, we conclude that VO sharing would be the most cost-effective approach from a short-term

perspective where SPs and SP operators are the organizations with the most influence. On the other hand, from a long-term perspective, protocol standardization offers the distinct benefit of the lowest operational cost after VOP integration. Of course it presumes that the all involved parties can agree on the eventually negotiated solution.

## 6. Concluding Remarks

Virtual organization support has become a very important theme for identity federations around the world in recent years. Even as the deployment of academic identity federations becomes worldwide and inter-federated, VO management platforms remain stuck within the political boundaries of national federations. Truly inter-federated VOs are crucial for getting maximum value out of identity federation for eScience, particularly for organizations and individuals in that long tail who historically have not been able to fully participate.

We provided a historical perspective on VO technology in the Grid computing field followed by comparative survey results of the special characteristics of each VO platform. Our assessment revealed that today's implementations, even where conceptually very similar, vary widely in practical terms amongst VOPs.

Finally, we proposed three applicable methods for integration of VO platforms. We also reflected on how much development cost and operational cost are acceptable for each party concerned, and our results indicate specific preferred approaches for short-term and long-term development towards a virtually unified VO platform.

### References


[1] Foster, I., Kesselman, C. and Tuecke, S.: The Anatomy of the Grid: Enabling Scalable Virtual Organizations, *International Journal of High Performance Computing Applications*, Vol.15, No.3, pp.200–222 (online), DOI: 10.1177/109434200101500302 (2001).

[2] Butler, R., Welch, V., Engert, D., Foster, I., Tuecke, S., Volmer, J. and Kesselman, C.: A national-scale authentication infrastructure, *Computer*, Vol.33, No.12, pp.60–66 (online), DOI: 10.1109/2.889094 (2000).

[3] Chervenak, A., Foster, I., Kesselman, C., Salisbury, C. and Tuecke, S.: The Data Grid: Towards an Architecture for the Distributed Management and Analysis of Large Scientific Datasets, *Journal of Network and Computer Applications*, Vol.23, No.3, pp.187–200 (online), DOI: http://dx.doi.org/10.1006/jnca.2000.0110 (2000).

[4] The Globus Security Team: Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective, Globus Alliance (online), available from ⟨http://toolkit.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf⟩ (accessed 2015-11-01).

[5] The Globus Security Team: GT 6.0 GSI C Security: Key Concepts, Globus Alliance (online), available from ⟨http://toolkit.globus.org/toolkit/docs/6.0/gsic/key/index.html⟩ (accessed 2015-11-01).

[6] Alfieri, R., Cecchini, R., Ciaschini, V., dell'Agnello, L., Frohner, K., Lrentey, K. and Spataro, F.: From gripmap-file to VOMS: managing authorization in a Grid environment, *Future Generation Computer Systems*, Vol.21, No.4, pp.549–558 (2005).

[7] Ceccanti, A., Giacomini, F. and Vianello, E.: VOMS home, The Italian National Institute for Nuclear Physics (online), available from ⟨http://italiangrid.github.io/voms/index.html⟩ (accessed 2015-11-01).

[8] Pearlman, L., Welch, V., Foster, I., Kesselman, C. and Tuecke, S.: The Community Authorization Service: Status and Future, arXiv:cs/0306082 (2003).

[9] Chadwick, D., Zhao, G., Otenko, S., Laborde, R., Su, L. and Nguyen, T.A.: PERMIS: A modular authorization infrastructure, *Concurrency And Computation: Practice And Experience*, Vol.20, No.11, pp.1341–1357 (online), DOI: 10.1002/cpe.1313 (2008).

[10] Flanagan, H. et al.: Enabling efficient electronic collaboration between LIGO and other astronomy communities using federated identity and COmanage, *Proc. SPIE 8451, Software and Cyberinfrastructure for Astronomy II*, *84511H* (online), DOI: 10.1117/12.925713 (2012).

[11] Linden, M., Nyrönen, T. and Lappalainen, I.: Resource Entitlement Management System, TNC 2013 Innovating Together, *The 29th Trans European Research and Education Networking Conference*, pp.1–12 (2013).

[12] REFEDS (Research and Education Federations): Federations, available from ⟨https://refeds.org/federations⟩ (accessed 2015-11-01).

[13] Cantor, S., Kemp, J., Philpott, R. and Maler, E. (Eds.): Security Assertion Markup Language (SAML) V2.0 (Mar. 2005), available from ⟨http://saml.xml.org/saml-specifications⟩.

[14] Clercq, J.D.: Single sign-on architectures, *Proc. InfraSec 2002*, *LNCS*, Vol.2437, pp.40–58 (2002).

[15] GÉANT: GÉANT Services - eduGAIN, available from ⟨http://services.geant.net/edugain/Pages/Home.aspx⟩ (accessed 2015-11-01).

[16] GakuNin: Academic Access Management Federation in Japan, available from ⟨https://www.gakunin.jp/En-fed/⟩ (accessed 2015-11-01).

[17] GakuNin: System Administration Standards for the GakuNin（Ver. 2.0), available from ⟨http://id.nii.ac.jp/1149/00000219/⟩ (accessed 2015-11-01).

[18] Procházka, M., Licehammer, S. and Matyska, L.: Perun – Modern Approach for User and Service Management, Michal, *IST-Africa Conference Proceedings*, pp.1–11 (2014).

[19] Abbott, B. et al.: LIGO: the Laser Interferometer Gravitational-Wave Observatory, *Rep. Prog. Phys*, Vol.72, No.076901 (2009).

[20] Nishimura, T. et al.: Group Management System for Federated Identities with Flow Control of Membership Information by Subjects, *Computer Software and Applications Conference Workshops* (*COMPSACW*), *2012 IEEE 36th Annual*, pp.94–99 (online), DOI: 10.1109/COMPSACW.2012.27 (2012).

[21] OpenIdP (NII): available from ⟨https://openidp.nii.ac.jp/?lang=en⟩.

[22] Internet2: Grouper (online), available from ⟨http://www.internet2.edu/products-services/trust-identity-middleware/grouper/⟩ (accessed 2015-11-01).

[23] Shibboleth Consortium, available from ⟨https://shibboleth.net/⟩ (accessed 2015-11-01).

[24] Internet2: eduPerson & eduOrg, available from ⟨http://www.internet2.edu/products-services/trust-identity-middleware/eduperson-eduorg/⟩ (accessed 2015-11-01).

[25] GÉANT: VOOT 2.0 (online), available from ⟨http://openvoot.org/⟩ (accessed 2015-11-01).

[26] Sermersheim, J. (Ed.): Lightweight Directory Access Protocol (LDAP): The Protocol, RFC 4511, available from ⟨https://www.ietf.org/rfc/rfc4511.txt⟩.

[27] HEXAA (HiEd eXternal AA), available from ⟨http://www.hexaa.eu⟩.

[28] OpenConext, available from ⟨https://www.openconext.org/⟩.

[29] SURFconext, available from ⟨https://www.surf.nl/en/services-and-products/surfconext/index.html⟩.

[30] Hämmerle, L.: SWITCH Group Management Tool (online), available from ⟨https://www.switch.ch/aai/downloads/AAIgmt_documentation.pdf⟩ (accessed 2015-11-01).

[31] SWITCHtoolbox, available from ⟨https://www.switch.ch/services/toolbox/⟩.

[32] Florio, L. et al.: Deliverable D14.1 (DJ3.0.1) Report on the Achievements and Recommendations for any Future Work (Identity and Trust Technologies for GÉANT Services) (online), available from ⟨http://geant3plus.archive.geant.net/Resources/Media_Library/Documents/D14-1_DJ3-0-1_Report-on-the-achievements-and-recommendations-for-any-future-work.pdf⟩ (accessed 2015-11-01).

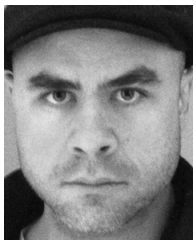

**Takeshi Nishimura** graduated from the University of Tokyo, Japan, where he received his B.Sc. and M.Sc. degrees in information science in 1996 and 1998, respectively. From 2001, he was a research associate at the University of Tokyo. Since 2009, he is a project researcher at National Institute of Informatics, Japan. His research interests are authentication and authorization for federated identity, identity federation management and public key infrastructure (PKI).

**Eisaku Sakane** received his Dr.Sci. from Osaka City University in 2003. He joined Osaka University and became a specially appointed assistant professor at the Cybermedia Center in 2006. He is now an associate professor (by special appointment) at National Institute of Informatics from 2009.

**Kazutsuna Yamaji** was received his Ph.D. degree in Systems and Information Engineering from the Toyohashi University of Technology, Japan, in 2000. Currently he is an associate professor at the National Institute of Informatics (NII), Japan. His primary research interests include modeling and developing trusted e-science space in order to share and reuse research materials.

**Motonori Nakamura** graduated from Kyoto University, Japan, where he received his B.E., M.E. and Ph.D. degrees in engineering in 1989, 1991 and 1996, respectively. From 1994, he was an assistant professor at Ritsumeikan University. From 1995, he was an associate professor at Kyoto University. Currently he is a professor at National Institute of Informatics, Japan (NII). His research interests are message transport network systems, network communications and Identity & Access Management. He is a member of IEEE, ISOC, IEICE and JSSST.

**Kento Aida** received his Dr.Eng. degree in electrical engineering from Waseda University in 1997. He became a research associate at Waseda University in 1992. He joined Tokyo Institute of Technology and became a research scientist at the Department of Mathematical and Computing Sciences in 1997, an assistant professor at the Department of Computational Intelligence and Systems Science in 1999, and an associate professor at the Department of Information Processing in 2003. He is now a professor in National Institute of Informatics from 2007. He was also a researcher at PRESTO in Japan Science and Technology Agency (JST) from 2001 through 2005, and a research scholar at the Information and Computer Sciences Department in University of Hawai'i in 2007.



**Nate Klingenstein** has been working on federated identity since the inception of the field, around 1999. Starting as a technical writer with Internet2, he gradually achieved greater professional successes, now a Senior IAM Systems Engineer at the University of Utah. He was one of the principals responsible for the creation of Shibboleth, and served as documentation and outreach lead for years. Nate was also co-chair of the SSTC, the SAML standards committee, for 5 years.