Secure User-controlled Lightpath Provisioning with User-controlled Identity Management

Bob Hulsebosch, Robert de Groote and Martin Snijders

Telematica Instituut, PO Box 589,
7500 AN Enschede, The Netherlands
{Bob.Hulsebosch, Robert.deGroote, Martin.Snijders}@telin.nl

Abstract. To allow user applications to securely make use of various lightpath resources distributed across multiple domains in a user-friendly and privacy-preserving way requires identity management functionality. Identity and attribute information has to be provided by the user to allow for authorized access to these resources. An identity management framework can facilitate such information exchange. We describe an architecture and prototype that allows the user to setup an end-to-end lightpath that spans multiple network domains while being in control of the personal credentials he has to provide for that purpose. The architecture combines the user-controlled lightpath paradigm with novel user-centric identity management technology. This combination allows the user transparent and non-intrusive access to multiple services that are required for reservation and utilization of network resources in order to setup an end-to-end lightpath.

Keywords: user centric, identity management, federation, lightpath provisioning, network resources, trust

1 Introduction

In the user-controlled lightpath provisioning paradigm, end-users take the initiative to set up an optical peering connection. This peering connection must fulfill the end-user's needs (desired capacity, duration and starting time) and capabilities (available budget). End-users indicate through an application which network resources to allocate for an end-to-end lightpath. For instance, the Dynamic Resource Allocation Controller (DRAC) application allows the end-user to schedule and use optical end-to-end connections, i.e. lightpaths [1]. These lightpaths may exist within a single optical network service provider domain but may very well involve multiple providers in different domains as well. Typically, the network service providers offer the user a service that allows him/her to schedule network resources for lightpath provisioning.

Controlling and enforcing access to lightpath resources belonging to different owners is one of the challenges of user-managed lightpath provisioning. A critical requirement for end-to-end connection provisioning in this context is the existence of a certain amount of trust among the multiple independent stakeholders involved. Identity and related attribute information have to be exchanged to satisfy the trust

requirements and allow users to take control of and schedule optical network resources in collaborative domains. To allow user applications to make use of these network services that are distributed across multiple domains in a user-friendly way requires identity management functionality.

Identity management is concerned with controlling the pieces and types of information, i.e. attributes and identifiers, pertaining to a party that are (made) available to other parties. More concretely, it can be thought of as the processes/functions, protocols and policies used to establish, collect, interpret and access this information in a secure manner. User access to provider-offered network services has to be controlled and enforced and is facilitated by (federated) identity management. The identity provider plays an important role in any identity management framework. The identity provider is trusted by all parties in the federation and manages and links digital identities of the user. The identity provider can authenticate the user himself or delegate it to the authentication server that is authorative for that user.

Different identity management solutions exist nowadays that facilitate single sign-on and secure attribute exchange. Examples are SAML2.0 [2], Shibboleth [3], and WS-Federation [4]. These solutions are characterized as being identity provider centric, i.e. the identity provider controls the information flow, and can very well be used for secure lightpath provisioning [5]. Recent developments in the identity management arena, such as OpenID [6], Microsoft CardSpace [7] and Higgins [8], are much more user-centric and address ease-of-use and privacy protection among disparate business contexts. In these user-centric solutions the user is to a certain extent in control and at least aware of the information that is communicated to service providers. The use of such identity-centric identity management solutions for secure lightpath provisioning would be much more in line with the user-controlled paradigm and would therefore be preferred above the identity provider centric ones. In this paper we investigate if this assumption is true and if both paradigms can be combined into an overall user-centric architecture for secure lightpath provisioning.

The rest of this paper is organized as follows. Section 2 describes the concept of user-centric identity management and compares it with the identity provider centric model. Section 2 also briefly discusses and compares several user-centric identity management solutions. The architecture and prototype that combines user-centric identity management with user-controlled lightpath provisioning is presented in Section 3. This section discusses the underlying trust model and describes the single-domain case as well as the multiple-domain case. Finally, Section 4 concludes with a summary of our findings and indicates future steps for lightpath provisioning.

2 User centric identity management

User-centric identity management - also referred to as Personal Identity Frameworks or Identity 2.0 - focuses on user empowerment in sharing personal information and self-determination in establishing relationships with relying parties. User-centricity distinguishes itself from other notions of identity management by emphasizing that the user maintains control over ‘what, where, when, and to whom’ a user’s identity

attributes are released. The difference with the identity provider centric approach is shown in Fig. 1 below. Clearly, in the identity provider centric model the user is unaware of what identity information is communicated between the identity provider and the service provider also called relying party; the only thing the user has to do is to authenticate himself towards the identity provider. In the user-centric model the user is, besides an authentication session during e.g. the creation of an information card, also asked for consent regarding the identity provider to be used and the attributes to be communicated to the relying party by means of an information card.

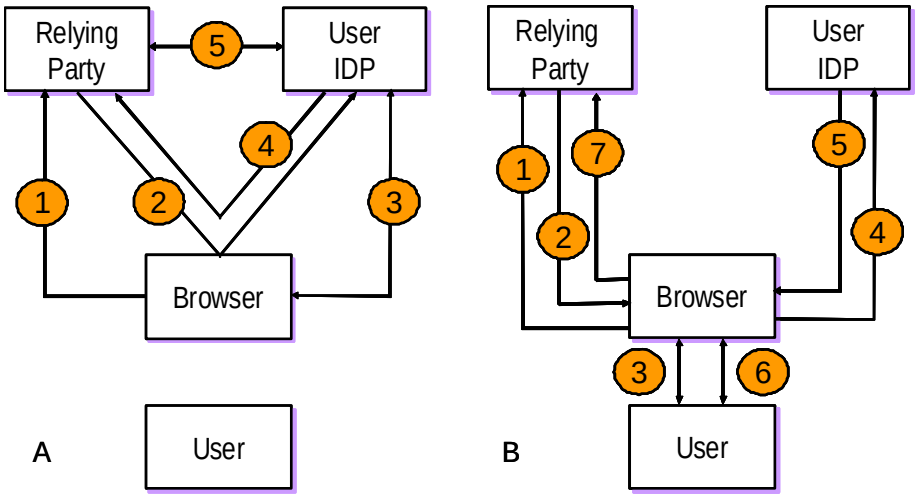

Fig. 1. Identity provider (IDP) centric (A) versus User-centric (B) identity management. The numbers reflect the sequence of the message flow.

Trust in user centric identity management still needs to be established. The relying party has to trust the user's identity provider. However, being in the credential exchange loop, the user can be made liable for the credentials he has provided thereby allowing for a more relaxed trust relationship between the relying party and the identity provider. On the other hand, the user is offered the means to control what credentials are exchanged with relying parties thereby guaranteeing his/her privacy.

The user-centric identity management approach thus allows the user to control the communication of personal credentials to relying parties. The primary approaches behind the user-centric model are identifier-based (such as OpenID) and information card (such as CardSpace) systems, plus other supporting standards and infrastructure components such as Higgins. The identifier OpenID protocol suffers from several drawbacks related to trust and privacy (i.e. sensitive to phishing attacks) making it less suitable to be used for business transactions [9]. Therefore the information card (infocard) approach adopted by CardSpace and Higgins seems best suitable for user-controlled lightpath provisioning as it offers more security, privacy and trust. Higgins should be preferred over MS CardSpace as it offers interoperability and therefore allows the use of both SAML and infocard-like solutions. The infocard approach also offers more security in the sense that phishing attacks that occur during the frequent

redirections of e.g. OpenID are prohibited. The infocard always ensures that the user is redirected to the right identity provider and not to a rogue one. The

In the next section we illustrate how infocard-based identity management solutions like CardSpace or Higgins may be used for user-controlled lightpath provisioning based on DRAC services that are used for optical network resource management in for instance the SURFnet6 network of the Dutch national research and educational network provider SURFnet [10].

3 User-controlled Lightpath Provisioning with infocards

This section describes an architecture for secure user-controlled lightpath provisioning by means of user-controlled identity management.

3.1 Scenario

The following scenario illustrates the scope of our work:

John is a surgeon and has his own personalized internet portal that provides links to recorded high-resolution videos of surgical operations. He uses these videos to learn how colleague surgeons tackle the operation or for educational purposes. The portal allows him to watch the videos at the hospital or at his private office. Prior to getting access to his portal John has to select an infocard from the Identity Selector application. John selects his self-issued 'Surgeon' card and gets access to his portal. Subsequently, he clicks on one of the videos he is interested in. Immediately the lightpath service is triggered informing John that a lightpath is required for the selected video and that more personal information is required to setup such a lightpath. For this purpose, John selects his 'DRAC' infocard and presents it to the lightpath service. Satisfied with the provided credentials, the lightpath service asks John when he wants to see the video. John wants to see it immediately. The lightpath service determines the most suitable lightpaths and asks John to select one. After having selected the shortest path, the DRAC services of the network providers constituting the lightpath are contacted by the lightpath service. A few seconds later the lightpath is provisioned and John is able to watch the video on his screen.

Two cases can be identified in this scenario. One case that involves only a single network provider and thus a single DRAC-service and one case that involves multiple providers. In order to coordinate the lightpath provisioning efficiently we assume the existence of a so-called lightpath service. This lightpath service takes care of the discovery of DRAC-services, concatenating them into an end-to-end lightpath, scheduling, and provisioning of the lightpath. Before we describe the message flows of both cases in more detail we first present a high-level functional overview.

3.2 Trust model

The trust model for user-controlled lightpath provisioning is complex and by far not established yet. For single domain provisioning the network service provider can execute the authentication and authorization process himself. This solution becomes less manageable when a large group of users from different institutions are allowed access to lightpath resources and this is typically the case for many network service providers. A better approach is to share identity information that is stored and secured in one domain with other domains. In other words, identity information is made portable across contexts and institutional boundaries according to established policies that dictate, among other things, formats and options, as well as trust and privacy/sharing requirements. Such portability is usually realized by means of identity federation. The federation establishes trust between the network service providers and the users. The most ideal federation topology is represented by Fig. 2A.

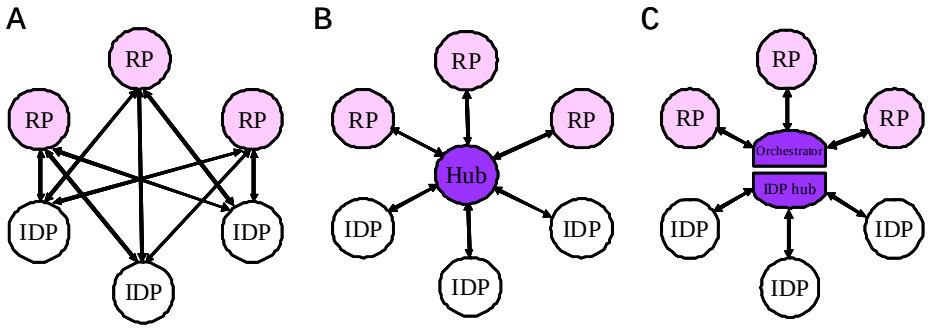

Fig. 2. Federated identity management topologies.

This topology assumes bilateral trust relationships between identity providers (IDPs) and Relying Parties (RPs). However, if the number of IDPs and RPs increases, and more importantly, if access to the services offered across all IDP-users is required, scalability issues are lurking. The introduction of a common platform or hub that is trusted by all parties is a solution to make the federation more scalable. The hub-model is illustrated in Fig. 2B.

The hub more or less becomes an identity broker that is trusted by all parties. The model implies, however, that there is less trust between the RPs and the IDPs. The RPs and the IDPs only have to trust the hub.

Besides federation of identity, lightpath provisioning also requires federation of network resources. In particular for the case of cross-domain lightpath provisioning. For cross-domain lightpath provisioning somehow the service providers constituting the end-to-end lightpath must be determined. Once they are discovered and contacted resources must be scheduled in such a way that all concatenated parts form, at the right time, a lightpath to a certain destination. This requires a lightpath orchestrator service that operates across and is trusted by multiple network service providers. Merging the orchestrator service with the federated identity hub results in a topology that is shown in Fig. 2C. We call the orchestrator service Lightpath Service.

Instead of a central orchestrator service an alternative hop-by-hop via routing-based mechanisms is imaginable for the establishment of a cross-domain lightpath [11]. This approach however results in fragile and long chains of trust between network service providers and hampers efficient identity exchange. Either all user information must be communicated between the network service providers or each of the providers individually must request the user's IDP for credentials. In a user-centric identity management scheme this will not work, i.e., the user will be bothered too much by all network service providers making the service too intrusive and unfriendly. Therefore the trust topology as depicted at the bottom of Fig. 2 will be used as the basis for our user-controlled lightpath provisioning by user-controlled identity federation architecture.

3.3 Architectural overview

Fig. 3 provides a high-level overview of the functional components that are needed for secure user-controlled lightpath provisioning with user-controlled identity management.

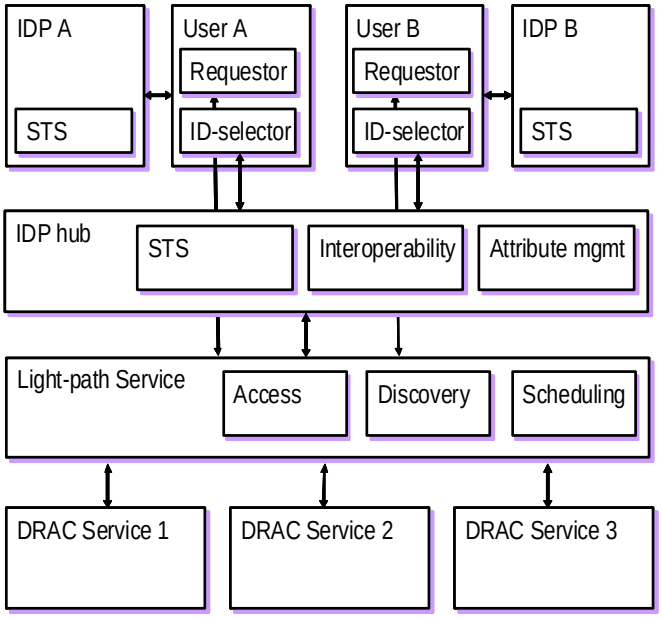

Fig. 3. High-level functional overview.

The user, interacting through the identity selector on the service requester (a client application running on a client system), may have identities issued by one or more identity providers. Each such digital identity of the user is represented by an infocard that the identity selector on the service requester system can process. An infocard endows the identity selector with the ability to request and obtain security tokens from

the corresponding identity provider when the user selects that digital identity for use in a given interaction context. For instance, the infocard presented to the Portal will differ from that presented to the DRAC services.

At the IPD side, either self-issued or managed identity providers are available that run a Security Token Service (STS) to which a requester or target service (Portal or Lightpath Service) can submit security token requests. The STS can issue security tokens containing the requested claims after the requester has provided suitable proof of authentication as required by the identity provider's security policy. According to our scenario the user's IDP will provide tokens for accessing the video portal whereas the IDP-hub will provide tokens for accessing the Lightpath Service.

The architecture supports both single- and multi-domain lightpath scenarios. It assumes a Lightpath Service that act as an orchestrator service towards multiple network service providers that use a DRAC-service for their network management. The Lightpath Service collects relevant information regarding lightpath provisioning across multiple DRAC service providers and thereby operates on a meta-level. This relevant information is related to accessing, discovery and scheduling of lightpaths. The architecture furthermore assumes that the Lightpath Service is trusted by the network service providers. The Lightpath Service interacts with the IDP-hub that represents the federation of the user's IDPs.

The Lightpath Service offers, on behalf of all network service providers, a common policy that must be fulfilled prior to getting access to its services. This policy is established under mutual agreement of all members of the federation. This implies that a user only once has to authenticate himself towards the Lightpath Service and consequently has access to all DRAC services in the federation.

The IDP hub is trusted by the network service providers and collects user identity claims from the user IDPs. These claims are converted into tokens via its secure token service. The tokens are presented to the Lightpath Service that uses them to enforce user access. Additionally, the IDP-hub may provide identity interoperability functions as different user IDPs may use different identity management standards and products. Furthermore, it may play a role in attribute management aspects related to for instance semantic and syntactic mapping of attributes or it may add several attributes/claims to the token such as federation membership status (e.g. gold – silver –bronze).

3.4 Cross domain provisioning

Being the most complex case we start with cross-domain lightpath provisioning. In that case, multiple DRAC-services constitute the end-to-end lightpath and multiple lightpath requests have to be made. To simplify the scenarios studies here, we assume that all DRAC-service providers act in the same federation. This implies that we may also assume that there is a common policy for each user in the federation. In other words, the federation likely will define and make obligatory such a common policy for all its DRAC-service providers. In that case, a single infocard would be sufficient to serve all the DRAC-service providers in the federation. The Lightpath Service is the most likely candidate to enforce this policy and to receive the infocard. Offering the Lightpath Service an infocard allows the user access to its services. The user then indirectly, i.e. via the Lightpath Service, obtains access to the network resources of

the individual DRAC-service providers. The corresponding message flow is shown in Fig. 4. We assume that the user has already entered the portal via username/password authentication or via the use of a self-issued infocard.

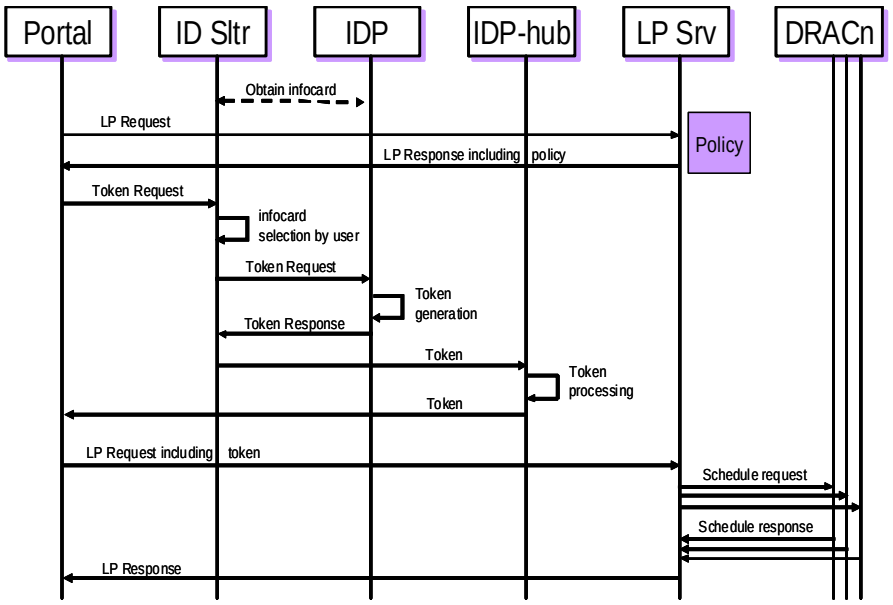

Fig. 4. Message flow for nDRAC services that trust the Lightpath Service and the IDP-hub. The IDP-hub is trusted by the user IDPs.

The message flow starts with the creation of an infocard. This out-of-band process is done via the IDP of the user and in cooperation with the IDP-hub. For instance, the infocard may be created and downloaded during a first time visit at the Lightpath Service. During the creation process the user has to authenticate himself towards his IDP. After all, the user's IDP knows best how to authenticate the user and typically stores user attributes or knows where to find them. Being part of the federation, both the IDP and the IDP-hub know and trust each other and thus can securely exchange security tokens with each other.

Note that the infocard is not the security token; it represents the token issuance relationship that the user has with the IDP and indirectly with the IDP-hub. In order to provide some assurance to the user that an infocard was indeed issued by the IDP, the infocard should carry inside a digitally signed envelope (i.e. enveloping signature) signed by the IDP. Additionally, to meet the Lightpath Service policy requirements, the token is signed by the IDP-hub as well. After all, the Lightpath Service Provider only trusts the IDP-hub and not the user's IDP.

The Lightpath Service receiving a request for a lightpath specifies in its policy what kind of identity information is required in order to access and use its service. The policy also specifies the IDP-hub that it trusts, i.e. is part of the federation. This allows the identity selector service to present the right infocards to the user. Once the user has selected an infocard it will be presented to the IDP and a token will be

requested. The IDP creates a token with the token service and returns it to the identity selector service. Subsequently, the latter forwards the token to the IDP-hub for further processing. The IDP-hub could add additional federation-specific attributes such as membership status (Gold – Silver – Bronze) to the token or it could convert the token into a SAML authentication and attribute requests format that is desired by the Lightpath Service. Here the use of Higgins shows added-value compared to MS CardSpace. The Higgins-enabled IDP-hub and identity selector are able to talk infocards as well as SAML towards each other. After processing, the new token will be signed by the IDP-hub and returned to the identity selector service. The identity selector service on its turn sends it to the Lightpath Service. If the received token contains the proper credentials, the user will be granted access and can specify his lightpath requirements. The Lightpath Service will then try to find possible lightpaths that meet the specification. For this purpose the Lightpath Service needs to access the different DRAC differences that constitute the end-to-end lightpath. It will use the token for this purpose as well.

Prior to sending the token to the DRAC-service provider, it will be encrypted with the DRAC-service provider's public key. This is done for multiple DRAC-service providers. The token grants the Lightpath Service access to network resource information available at the different DRAC-service providers allowing it to calculate lightpaths after the user has specified the desired lightpath via the Lightpath Service GUI (see Fig. 5). The possible lightpaths are shown via the GUI to the user who selects the most suitable one. The Lightpath Service then schedules the selected lightpath resources in the DRAC-services. This scheduling ultimately results in the provisioning of the lightpath. Note that during the whole process of lightpath provisioning the user only has to present infocards, he doesn't need to authenticate himself once.

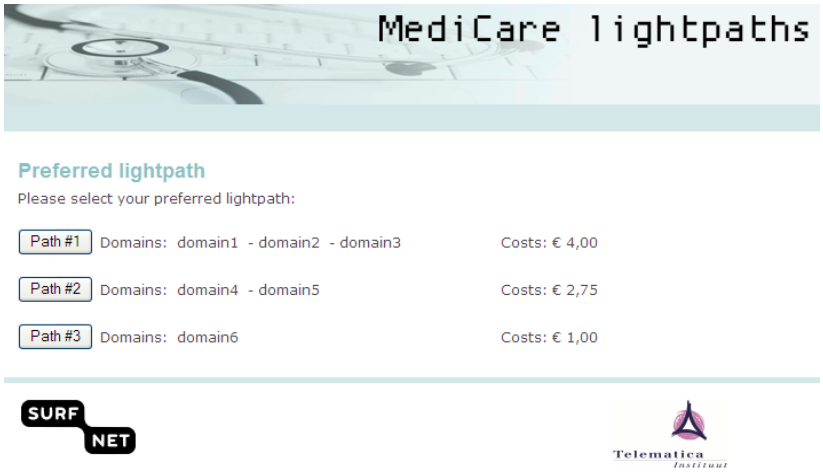

Fig. 5. Lightpath selection in the Lightpath Service GUI.

3.5 Single domain provisioning

In case a user requires an end-to-end lightpath inside a single network domain, e.g. the SURFnet6 optical network, the message flow shown in Fig. 4 is applicable as well. The added value of the Lightpath Service becomes negligible in this scenario; functionality-wise the Lightpath Service collapses with the DRAC service at the network provider.

3.6 Implementation

The goal of our implementation effort is to demonstrate and validate the role of user-centric identity management in user-controlled lightpath establishment. The above-mentioned scenario motivated us to build a medical video portal application that could benefit from user-controlled lightpaths, allowing high definition video material to be streamed without delays from and to locations preferred by the user. The video portal and the Lightpath Service it leverages operate in different administrative domains. This requires the user to authenticate twice – once to the video portal, and once to the Lightpath Service. The whole system is implemented and relies heavily on the Higgins Open Source Identity Framework [12]. The IDP is an extension of Higgins' STS IDP, both the portal and IDP-hub are web applications implemented in Java. All components run in an Apache Tomcat web server.

Several WS-* implementations are used during the whole process. WS-MetadataExchange is used by the Identity Selector to obtain the policy from the IDP/STS and by the Portal to retrieve the policy from the Lightpath service. The policies issued by the Lightpath Service and IDP/STS are specified using WS-SecurityPolicy. Policies inform the Portal that the Lightpath Service requires a SAML token from the STS of the IDP and that such a token must contain a claim with the membership status of the requestor, and inform the identity selector of e.g. the required authentication method. WS-Trust is used by the identity selector in order to obtain a security token from the IDP/STS.

The identity selector used in our implementation is the standard Microsoft CardSpace card selector that comes along newer versions of Microsoft Windows. The card selector is triggered by simple policy objects embedded in an HTML page. A simple mechanism is in place to bootstrap WS-SecurityPolicy policies into these embedded objects so that they can be intercepted by the card selector.

The Lightpath Service is developed in Java. All GUI widgets are Java Swing controls. The application acts as a wizard, leading the user from authentication, to specifying lightpath request parameters, viewing available lightpaths, and finally reserving a chosen lightpath. The GUIs of the Lightpath Service, including the CardSpace login button, and the identity selector are shown in Fig. 6 and Fig. 7, respectively.

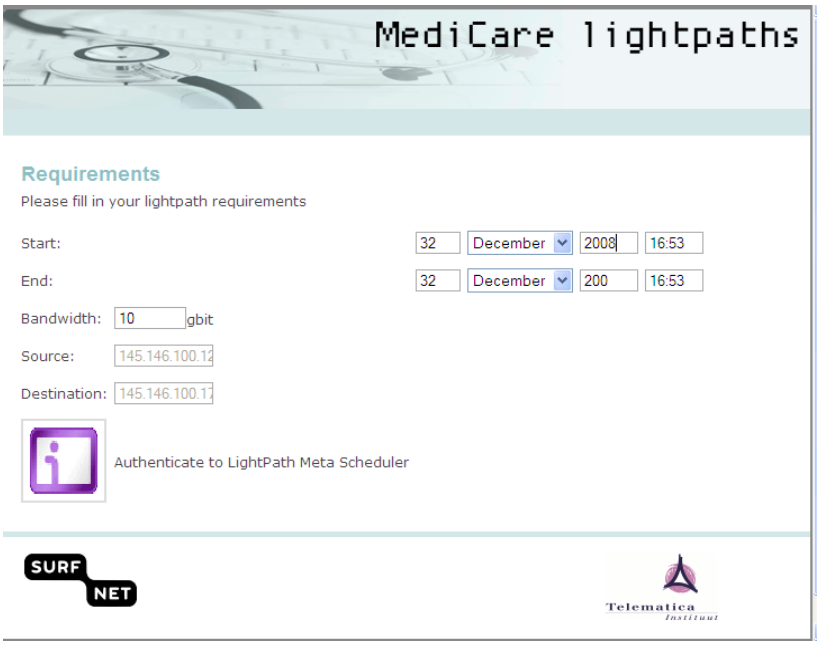

Fig. 6. Lightpath Service GUI.

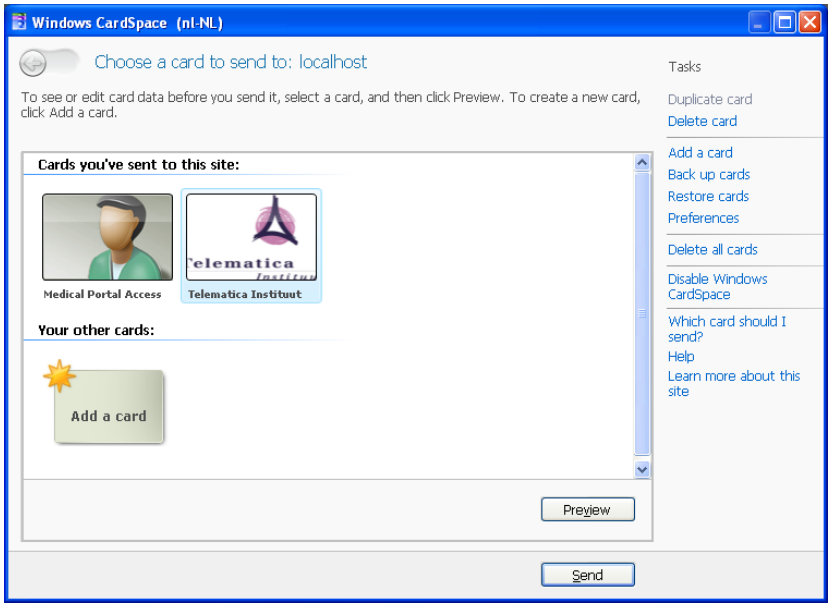

Fig. 7. Identity Selector GUI.

4 Related work

The use of identity management solutions for lightpath establishment is not new. An identity provider centric solution is presented in [5]. DNS and its security extensions (DNSsec) are used to guarantee trust between the involved parties. We have proposed a user centric alternative to offer the user better insight in the communication of his personal information among those parties. The DNSsec approach can very well be combined with user centric identity management for dynamic trust establishment between the parties involved for lightpath setup.

In section 3.2 we already mentioned that the hop-by-hop approach for secure lightpath provisioning, as described by Gommans at al. [12], is not very suitable for user centric identity management. In this model authentication and authorization is communicated between the authentication, authorization and accounting (AAA) servers of the different network providers without any user involvement. The advantage of the model, however, is that there is little reliance on central or coordinating entities in the network whereas we rely on a central identity hub and Lightpath Service orchestrator. A similar, approach for user-controlled lightpath provisioning is described in [13]. In this paper a policy restricted signaling architecture is proposed that allows users to reserve lightpaths over multiple domains whilst ensuring that management rules of each domain are enforced. Again, the user is offered little means for controlling the release of his personal information in order to get access to network resources.

GRID-based solutions typically rely on a Virtual Organization (VO) that enforces centralized access to distributed resources [14]. While such a VO-based, central AAA approach is straightforward and intuitive, it becomes impractical to administer as soon as VOs expand into distributed multi-institutional collaborations, VO memberships change dynamically, and user rights vary on a periodic basis or per user's role in an organization. Obviously, it is impractical and does not scalable for the VO itself to store and manage all the identities and corresponding attributes. Such identity-related information could better be stored and managed by the registered members themselves, allowing the VO to only administer at the organizational level. User centric identity management provides this functionality.

5 Discussion and conclusions

We have presented an overall security architecture that combines secure and trustworthy user-controlled provisioning of lightpaths with user-centric identity management.

Though the user wants to be in control of the dissemination of his personal credentials, too much consent works counter productive. Straightforward implementation of user-centric identity management solutions is therefore not going to work as multiple services have to be provided with credentials. From a user's point of view it is not friendly to submit an infocard to each requesting network service provider that is part of the end-to-end lightpath. We foresee, however, the existence of a meta-service that facilitates the user in setting up lightpaths across multiple network

service providers. Such a meta-service is trusted by all parties that besides providing basic functionality as service discovery and scheduling also takes care of access control. The latter implies that the user only once has to provide an infocard to this meta-service, called Lightpath Service, prior to getting access to multiple network service providers. Furthermore, an IDP-hub seems, from a scalability point of view, required to orchestrate the provisioning of identity information towards the Lightpath Service. The IDP-hub federates the IDPs of the users. Given the heterogeneity of identity management solutions it is best to turn this IDP into some kind of identity meta-system that is capable of interworking with the different identity management flavors. Higgins for instance provides such a meta-system.

With an increasingly more prominent role and use of web services in lightpath provisioning federating them becomes important: lightpath services need to talk to DRAC services in a secure and trusted manner. Besides lightpath specific information, identity information is required as well for authorization. However, federated web services communication not always occurs via the browser and thus without the knowledge of the user. Somehow the user must be informed about the usage of identity information by federated web services. The current user-centric identity management solutions, however, do not support this functionality. It is therefore questionable if today's user-centric identity management will flourish in service oriented architectures. The challenge is to find solutions that allow the user some control of the release of his personal information in federated web services environments without being too intrusive. Delegation models might provide a solution for such environments and might be worth for further future investigation. For instance, the Lightpath Service could be authorized by the user, via its IDP, to contact and access certain DRAC service providers. Already, the MS Geneva Framework, that comprises amongst others MS Cardspace, provides functionality for such delegation [15]. Alternatively, the applicability of Dynamic SAML due to its flexibility and scalability benefits regarding trust could be considered as well [16].

Lack of IDPs that generate trustworthy tokens is another drawback of current user centric-identity management solutions. The entity controlling the hub could very well become a provider of such a secure token service for lightpath provisioning (or for service access in general). Furthermore, the user's infocards are all stored on a single PC thereby hampering the user in setting up lightpaths from another device. Future research could therefore also focus on making infocards accessible from any device, anytime, and anywhere. They should move along with the user.

Acknowledgments. The work described in this paper was conducted in the GigaPort Next Generation research program, sponsored by the Dutch government and coordinated by SURFnet.

References

1. Nortel. Application Brief: Dynamic Resource Allocation Controller (DRAC), 2006.
2. OASIS Security Assertion Markup Language (SAML) 2.0, March 2005, see http://saml.xml.org/saml-specifications#samlv20.
3. Shibboleth project website: http://shibboleth.internet2.edu/.

4. WS-Federation Language, Version 1.1, 2006, Lockhart, H. et al., see http://www.ibm.com/developerworks/library/specification/ws-fed/.
5. Hulsebosch, R.J., Bargh, M.S. Fennema, P.H., Zandbelt, J.F., Snijders, M., Eertink, E.H.: Using Identity Management and Secure DNS for Effective and Trusted User-controlled Lightpath Establishment, International Conference on Networking and Services ICNS 2006, July 16-19, 2006 - Silicon Valley, USA, Marriott Hotel, Santa Clara.
6. OpenID, see http://openid.net/.
7. MS Cardspace, see http://msdn.microsoft.com/en-us/netframework/aa663320.aspx.
8. Higgins, see http://www.eclipse.org/higgins/.
9. Bournez, C., Bichsel, P.: First Report on Standardisation and Interoperability - Overview and Analysis of Open Source Initiatives, Combined deliverable: Merger of D3.3.1 and D3.4.1, FP7 EU Primelife project, 30 May 2008.
10. Van der Pol, R., Dijkstra, F.: Network and Capacity Planning in SURFnet6, submitted to TNC2009.
11. Gommans, L., Dijkstra, F., de Laat, C. Tall, A., Wan, A., van Oudenaarde, B., Lavian, T. Monga, I., Travostino, F.: Applications Drive Secure Lightpath Creation across Heterogeneous Domains. In IEEE Communications Magazine, Optical Control Planes for Grid Networks: Opportunities, Challenges and the Vision, volume: 44, issue: 3, March 2006, pp. 100-106.
12. Higgins Open Source Identity Framework 2008, see http://www.eclipse.org/higgins.
13. Truong, D.L., Cherkaoui, O., Elbiaze, H., Rico, N., Aboulhamid, M.: A Policy-based approach for user-controlled Lightpath Provisioning. IFIP/IEEE NOMS, pp. 859-872, April 2004.
14. Foster, I., Kesselman, C.: The Grid 2: Blueprint for a New Computing Infrastructure, November 2003, Morgan Kaufmann Publishers.
15. Brown, K., Mani, S.: Microsoft Code Name “Geneva” Framework Whitepaper for Developers, 2008.
16. Harding, P., Johansson, L., Klingenstein, N.: Dynamic Security Assertion Markup Language: Simplifying Single Sign-On. In: IEEE Security & Privacy, Volume 6, Issue 2, pp. 83-85, March-April 2008.