Using Identity Management and Secure DNS for Effective and Trusted User Controlled Light-Path Establishment


Telematica Instituut, P.O. Box 589, 7500AN Enschede, The Netherlands
Email: Bob.Hulsebosch@telin.nl

Abstract

This paper investigates and demonstrates the role of identity management as an integral part of the overall trust establishment mechanisms required for user-controlled end-to-end light-path provisioning. Within the scope of identity management, also lack of effective trust establishment procedures between the user’s identity provider and the optical network service providers hampers effective exchange of user identity information needed for authorizing the reservation and utilization of network resources. We show how secure DNS can help establishing trust between parties in different administrative domains, without any mutual prearrangement. This DNS approach enables the dynamic realization of secured communication channels in order to exchange identity-related information required for controlling the access to network resources.

1. Introduction

Advanced applications such as Grids are emerging that require more communication bandwidth than the traditional packet-switched Internet can provide today. This application driven bandwidth demand has led to the deployment of an increasing number of high-capacity optical networks that provide circuit-switched connectivity with a guaranteed quality of service. To operate these optical networks, intelligent methods of provisioning and control are required to enable greater flexibility of optical resource allocation and to reduce operational costs in setting up end-to-end light-paths spanning multiple domains.

Traditionally, end-to-end light-path connections have been set up via different network management technologies. So far, this process has been under control of the network operators, in the remaining of the paper referred to as Optical Network Service Providers (ONSPs). Recently there has been a liability shift moving the responsibility from the ONSP to the user. According to the new paradigm users reserve optical resources from a number of supplying ONSPs directly. In this way more effective management of light-path connections is possible [1]. It gives the user more control to find the light-path that best meets the needs of his application and budget. There have been efforts in the past to define customer based management protocols such as [2] and [3]. Similar network control plane management functionality is under development for optical networks as well [4, 5].

The user-controlled network paradigm, however, introduces trust issues between the user and the ONSP that did not exist before. Obviously, ONSPs will not allow just any user to reserve optical resources. As a main enabler of the overall trust, a solid authentication and authorization infrastructure is required to control the access to these resources. From an identity management perspective it is redundant and undesirable to expect users be known (i.e. have accounts) at all ONSPs on the path, as light-paths potentially cover multiple independent ONSPs. Moreover, the actual identity of the user will be irrelevant to the ONSP; more relevant are attributes like the role of the user or his membership to an organization or federation.

Trusted third parties can be used to authenticate and authorize users, typically based on the identities of the interacting entities. In Grid computing environments this is realized by a so-called Virtual Organization (VO) [6]. VOs serve specific communities like the high-energy physics, astronomers or bio-informatics [7]. For light-paths leveraging Grid middleware, the GLIF community may fulfill the VO role [8]. User institutions and ONSPs are somehow associated with a VO, i.e., both groups have a trust relation with it. Usually, this trust is based on membership and contractual agreements for the user institutions and ONSPs, respectively. While a VO-based, central authentication, authorization and accounting (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 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.

What is needed for inter-domain light-path creation is an identity management framework that allows for authenticated users to communicate identity related attributes in a mutually trusted and secure manner to ONSPs. Nowadays there exist several (standardized) identity management frameworks [9, 10, 11, 12, 13]. All these frameworks rely on federation of users and service providers, coordinated by so-called identity provider (IdP) components that are trusted by all parties. The IdPs manage and link digital identities of the user. The IdP can authenticate the user himself or delegate it to the authentication server that is authoritative for that user. Also, the IdP knows which attribute information service providers store regarding the user. The IdP may provide these attributes itself or direct interested parties to these attribute service providers in a controlled way. One of the greatest benefits of the mentioned identity management solutions is that they support Single Sign-On (SSO). SSO allows the user access to all resources where he has permission for after a single authentication action, without the need to enter multiple passwords. However, the absence of an a priori trust relationship between the ONSP and the IdP of individual users hampers the identity information exchange between them directly.

This contribution presents a framework whereby a VO supplies the necessary trust infrastructure for the ONSPs to rely on the provided user identities and attributes by the IdPs of users. The exact role of the VO in the secure and trusted exchange of identity credentials and attributes can be diverse. As mentioned above, turning the VO into a heavyweight central IdP is not desirable because it implies administration at the level of individual users. Administration at the level of organizations associated with the VO is preferable. In this paper we propose a lightweight VO that relates user IdPs and ONSPs in that they can cooperate (trust each other) within a VO framework. To this end, the VO accomplishes the task of a secure Domain Name System (DNS) tree administrator to establish trust between the user’s IdP and the ONSP dynamically for user controlled light-path provisioning. Adapting other lightweight roles for a VO is also possible, e.g., Certificate Authority and Relaying IdP. Refer to [14] for an evaluation of these lightweight VO roles.

Section 2 outlines how DNS and its security extensions can be used for dynamically creating trust between the user’s IdP and the ONSP. Section 3 continues with a description of our implementation of an effective and trusted light-path establishment framework based on SAML identity management and Secure DNS technology. Section 4 evaluates and discusses the solution and implementation. Finally, in Section 5 we present some conclusions.

2. Secure DNS for identity management

DNS is used on the Internet to resolve the hostname of a node to an Internet Protocol address. With its security extensions called DNSsec, DNS can supply trusted cryptographic verification information along with DNS messages [15, 16, 17].

2.1. Applying DNSsec

We propose to use DNS for storing and locating IdP and ONSP certificates. The use of the security extensions of DNS guarantees the authenticity and integrity of these certificates towards requesting parties. The solution is as follows: DNSsec requires registration of a domain name for each VO (like, e.g., ‘astro-vo.org’). The VO shall manage this domain. The entries registered on this domain represent the institutions and ONSPs that are associated with the VO. The owner of ‘astro-vo.org’ shall ensure that it only lists the parties that adhere to the policies of the VO that have been agreed upon. If, for instance, ‘onsp.nl’ and ‘idp.nl’ are part of the ‘astro-vo.org’ identity management infrastructure, then the ‘astro-vo.org’ DNS should be able to securely resolve ‘onsp.nl.astro-vo.org’ and ‘idp.nl.astro-vo.org’ relationships. The DNS-entries for these domains should list a public key in order to be able to establish a secure connection between the involved IdPs, i.e. those of the users, and ONSPs. Hereby DNSsec guarantees that both the ONSP and IdP are associated with the same VO. Furthermore, DNSsec securely provides each party’s public keys to the other for establishing a secure channel between the ONSP and the IdP of the user. These two advances of DNSsec allow the ONSP and the IdP to trust each other and to securely communicate identity related information.

2.2. DNSsec and identity management

Figure 1 shows the stakeholders, their functional components, and the interactions between these
components during a light-path establishment session. The stakeholders are the VO, who administers a DNS tree, the user (who interacts through his application), the user’s IdP and attribute service provider, being all associated with the VO (i.e. registered in the DNS tree), and the contractual partners of the VO represented by the ONSPs, who on their turn are in charge of network resources and deploy network management and AAA functionality. In particular, the Network Management Controller (NMC) component of the ONSP plays an important role in the overall message flow. The NMC glues the identity and network management control planes together. The NMC provides a service that sets up the light-path through an interface to network management components in the network control plane. The NMC transforms the application light-path requests into a format that complies to different existing network management protocols [4, 5]. The NMC also has interfaces to the local AAA-servers for requesting authentication and authorization information, and to DNS resolvers for fetching IdP certificates.

This may lead to a slight complication in standard secure channel setup as described in Section 3.2. Furthermore, the certificates may be self-signed as they are only used to provide integrity protection and confidentiality. Actually, self-signed certificates are even preferred above certificates that are signed by recognized certificate authorities as the latter certificates may contradict with the DNSsec trust policy of the root.

The VO may want to classify its members on several grounds. There may for instance be Gold and Silver members depending on the contribution paid to the VO. The VO trusts the administrator of the IdP to locally set the right attributes for the right users.

2.3. Interactions

During light-path establishment, the following interactions, conforming to the message numbering depicted in Figure 1 may take place between the identified players and their functional components:

1. User authentication request. The user starts the application for setting up the light-path and authenticates towards the home IdP. The user uses the credentials that are known to the IdP of his institution for authentication. This allows the institution to control and assist the one who is allowed to setup light-paths. Typically a username / password combination like bob@idp.nl / ******** will be used. Also some information regarding the relevant VO must be entered (i.e. astro-vo.org, see below for an explanation). Prior to communicating username / password credentials to the IdP, the application needs to setup a secure channel with the IdP. In the absence of any prearranged security measures, an opportunistic approach can be taken [18, 19]. The IdP certificate that is to be used for setting up an opportunistically secured channel may be checked with a lookup in the DNSsec tree (see also section 3.2).

2. User authentication response. Upon successful authentication, the IdP will return a handle that contains a randomly generated number identifying the user at the IdP.

3. Light-path specification request. The application asks the user to enter light-path specific information like for instance destination, source and the time for the actual establishment of the path. If the institution of the user is a member of multiple VOs or if the application is not VO specific, the user is then asked to run his application in the context of a specific VO.

4. Light-path specification reply. After the user enters the details, the application determines the ONSPs that are required to create a light-path to the destination source. How this is exactly done is beyond

Prior to light-path establishment, registration with the VO has to be done. Both the user institutions and ONSPs that have an association with a certain VO must register and publish their certificates in the tree that is administered by that VO. As the tree is DNSsec enabled, this means that the VO signs all DNS traffic. The parties that obtain information from the DNS tree can use this VO-signature as a trust reference.

Notice that we require that the certificates published in the DNS tree are not VO specific, i.e. the same certificate can be published in multiple VO DNS trees.

Figure 1: Stakeholders and their interactions for light-path establishment.
the scope of this work. We assume however that the user is in full control of the light-path provisioning; there is no delegation to for instance an ONSP.

5. The user application sends a request for light-path reservation to the NMC of each of the ONSPs. The request includes the IdP user-related handle, the IdP identifier, the VO identifier and the light-path details such as source, destination, capacity, and usage time. Prior to this request, similar to the way described in the first step, an opportunistic encrypted request exchange is required between the application and the NMC. The certificate of the NMC that is used for this purpose is verified by the application via DNS resolving.

6. Based upon the VO and IdP information in the request, the ONSP resolves the IdP certificate (using a DNS CERT record) from the VO DNS tree (Step 7). The IdP can use the certificate to publish the location of the IdP service. Alternatively, the IdP could list a DNS SRV-record stating the location of the IdP service. The latter solution offers more flexibility as it allows for independent changes of the IdP certificate or IdP service location.

8. The public key in the IdP server certificate is used by the ONSP to setup a secure (i.e. TLS) channel with the IdP. A mutual authenticated channel is needed and for this purpose, the ONSP communicates its VO identifier (onsp.nl.astro-vo.org) to the IdP. Based upon this information, the IdP is able to fetch the ONSP certificate from the VO DNS tree and compare it to the one used for the established secure channel. If both certificates match, the IdP has verified that the ONSP is associated with the VO and can be trusted to send identity related information for resource reservation. The ONSP can request identity-related information, e.g., attributes, using the handle that was obtained in Step 2 and represents the user. See section 3.2 for a more detailed description of setting up a mutual authenticated opportunistic communication channel.

9. The handle allows the IdP to verify the authentication status of the user and to collect other information, i.e. attributes, that belong to this user, e.g. Gold membership (Step 10).

11. An authentication and attribute assertion (e.g. complying with the SAML 1.1 specification) is returned to the ONSP.

12. ONSP NMC forwards the assertion to the ONSP AAA-server and requests an authorization assertion.

13. The AAA-server determines, based upon the assertion and its own policies, whether or not to grant the user (application) access to resources as stated in request. The outcome is returned to the NMC. This approach differs from the approach taken by Gommans et al. [20] were the AAA server communicates with network management control plane services.

14. In case of a positive outcome the NMC forwards the initial light-path request to the vendor specific optical network management component.

15. The optical network management stack makes the reservation.

16. The user application receives a light-path response including a confirmation of the light-path reservation (e.g. in the form of a token). The token authorizes the user to use the reserved light-path in due time.

We note that other message sequences are possible as well. Due to the immaturity of the technology and services, it is unclear at the moment, which sequence is best to follow.

3. Implementation

The goal of our implementation effort is to demonstrate and validate the role of identity management and DNSsec in user-controlled light-path establishment.

3.1. Identity Management

This section describes our implementation of a SAML 1.1 identity management framework.

3.1.1. Stakeholder components

The User IdP is based on the SourceId SAML1.1 Toolkit [21]. This toolkit consists of a workflow engine (configured to process the SAML1.1 protocol), a servlet layer (exposes the workflow unit to a distributed environment), and a demo IdP (a simple web application with a small set of example users and a web browser user interface).

The NMC of the ONSP is a J2EE web application. It exposes an interface that receives so-called “LightpathRequest” messages and will return “LightpathResponse” messages. It uses SOAP conversational message exchange in a similar way as the SAML protocols do. The light-path related messages are expressed according to a dedicated language called Light-Path Markup Language (LPML).

3.1.2. Collaborations between stakeholders

The collaboration between the application and the IdP is a proprietary protocol. The user authenticates with the IdP through the application and the application receives a “handle”, representing the authenticated user during this session, and a SAML1.1 response containing an authentication statement and other information about the authentication process.

The collaboration between the application and the ONSP involves a request-response protocol. The light-path request from the application to a NMC contains the handle of the user among other relevant
information. The request and response messages are expressed in LPML and sent via SOAP over HTTP. The collaboration between the ONSP NMC and the IdP is a 100% SAML1.1 compatible message exchange. The NMC of the ONSP sends a SAML1.1 request containing an Authentication Query and an Attribute Query to the SOAP endpoint of the IdP.

3.1.3. Libraries
Various libraries have been developed to realize the collaborations mentioned above. All libraries use the open source XmlBeans utility [22].

3.2. DNSsec for Transport Layer Security
This section describes how our Java based implementation uses DNS and DNSsec [16, 17, 23] for establishing secure channels between the stakeholders.

3.2.1. Certificate Resolving
Our prototype resolves party identifiers (such as idp.nl.vo.org or onsp.nl.vo.org) to certificates associated with those parties. One possible way of resolving party identifiers to certificates in a secure way is by using DNSsec as a federation mechanism but other trusted channels may also provide similar functionality (e.g. secure databases, a secure file system, a trusted telephone book on the web). For resolving identifiers to certificates through DNS or DNSsec we implemented a DNS Resolver. The resolver uses the DNSjava [24] library for constructing and sending the actual queries that conform to the DNS protocol. Because the DNSjava library does not provide secure DNS resolver functionality, it must be configured to use a DNSsec resolver running in a trusted environment to achieve DNSsec functionality.

3.2.2. Secure Transport
The resolver provides us with a certificate including a public key that can be used to encrypt traffic to the remote party. We implemented the IETF Transport Layer Security protocol (TLS) [25] that is a secure protocol using encryption over TCP connections.

3.2.3. Customized Handshake
There is a slight complication in using TLS with client authentication (e.g. the IdP authenticating the ONSP). Since the server party, i.e. the IdP, does not know or trust the client party, i.e., the ONSP, the server party wants to verify the client party through the trusted VO channel. The client party’s VO identifier is needed to resolve the client certificate, so this VO identifier needs to be sent to the server. Since this identifier must contain a reference to a VO, the option of encoding it in the client certificate is not desirable. This would require the client to have a certificate for each VO that it is associated with. We would rather like to use the same client certificate across multiple VOs because it ultimately points to one and the same party. Therefore we need to send at least the VO identifier separately from the certificate. Moreover, sending a convenient client identifier may also be easier to deal with (i.e. suited towards DNS) than the Distinguished Name that is typically found in X.509 certificates not bound to a specific host. To that purpose we have extended the TLS handshake with a custom step: The client socket checks the TLS server certificate against the certificate that was retrieved from a certificate resolver (e.g. DNSsec). The server socket initially accepts the client certificate, expects a peer name and VO name as the first thing that is sent by the client and retrieves the client’s certificate from a certificate resolver. That certificate is compared to the one that was used to setup the TLS connection.

3.2.4. Extending TLS
This paragraph describes the usage of certificate resolvers (i.e. the DNSsec resolver) and "extended” TLS for establishing secure channels between the different stakeholder components in our prototype.

Between the application and IdP, the server authentication is done on TLS level by comparing the server certificate against the one in the VO DNSsec tree. This channel does not use client (user) authentication on TLS level since a proprietary user authentication step is performed on application level as described in section 3.1.2.

The channel between the ONSP NMC and the IdP uses full-blown “extended” TLS with both peers verifying certificates through DNSsec. The IdP server certificate is compared with the IdP certificate in the VO DNSsec tree. ONSP client authentication is done through TLS client certificates that are checked afterwards in the VO DNSsec tree.

Between the application and the ONSP NMC the server authentication is similar to the one in the User-IdP channel. Client authentication is done on application level through a handle that is generated by the identity management framework. This handle is used by the NMC of the ONSP for user authentication.

3.3. AAA and Network Control
Our NMC offers two more interfaces for communication with AAA-services and management services in the network control plane, respectively.

The authorization attributes for the ONSP service are fetched from the user’s IdP, but the policy that defines what effects these attributes have, is preferably implemented outside of the NMC in an external dedicated authorization server. So far, in our prototype, authorization rules have been implemented in the NMC itself. In the near future we plan to replace this by a call to an external AAA-server. A generic API using LPML has been defined to control optical
switches through the NMC (see section 3.1). The NMC translates LPML requests to vendor specific messages on a (possibly proprietary) switch management interface that controls the actual switch hardware.

3.4. Light-Path Application

The light-path application is developed in Java. All GUI widgets are Java Swing controls. The application acts as a wizard, leading the user from authentication, to specifying light-path request parameters, viewing available light-paths, and finally reserving a light-path.

4. Evaluation and Discussion

This section examines the effectiveness of applying identity management and DNSsec technology for user-controlled light-path establishment. Furthermore it verifies whether essential requirements are met.

4.1. Effectiveness

The introduction of identity management technology for cross-domain light-path establishment allows users to share identity information in a controlled and transparent way. Pre-registered accounts at all network providers are not needed anymore and the desired SSO functionality is obtained almost for free.

The definition of the NMC component abstracts AAA and light-path application specific functionality from the network control plane management services. It allows for clear control plane services that are dedicated to resource scheduling only.

The use of DNS resolver functionality in the application allows for transparent localization of the home IdP service of the user. Relatively intrusive localization services, like the ‘Where Are You From’ (WAYF) used in Shibboleth, are not needed [26]. This WAYF-bottleneck is now shifted to the VO that the user’s organization is associated with (e.g. is member of). In other words, a service is needed that allows the user to express the effective VO that he is operating under. Since applications will be most of the time VO-specific, the DNS information regarding the VO can be provided by the application as well.

DNSsec allows the home IdP of the user to directly communicate with any VO-associated ONSP via a secure channel without interference of the VO in the communication of identity and attribute information, offered via e.g. SAML 1.1. This direct relationship may be more effective compared to for instance the alternative relaying VO solution direction where the VO acts as a man in the middle that may become a potential bottleneck [14].

Furthermore, DNSsec enables the creation of secure communication channels between two peers that are initially strangers, i.e. the user’s IdP and the ONSP. This is done dynamically without any bilateral prearranged security measures. Authentication of both peers is achieved through key distribution in DNS, leveraging upon the authentication of the DNS in DNSsec (see also ref. [19]). Note that this security does not come for free and is associated with additional computational costs in the network. Besides its usefulness for opportunistic encryption, other applications for DNSsec to dynamically establish trust relationships between two parties are to our knowledge barely addressed in the literature. Two other related sources have been found. There is a strong overlap with the proposed solution described in [27]. Here DNSsec is combined with RADIUS authentication for dynamic trust establishment between domains. In [28], DNSsec is used to securely fetch information from DNS. The fact that DNSsec has just recently been standardized may be the cause for its limited deployment.

4.2. Requirements

Our proposed identity framework fulfills a number of high-level requirements. First of all, the framework preserves the distributed identity character. Secure authentication and attribute exchange is facilitated over multiple domains. Authentication is performed in the user’s home domain, where the user is best known. The solution framework is also flexible with respect to the number of attributes to communicate and the authentication method to use. User authorization can, irrespective of the true identity of the user, be granted based on VO membership affiliation and attributes provided by the IdP. As a consequence, the ONSP doesn’t have to deploy user authentication solutions.

Secondly, the IdP guarantees the privacy of the user towards the identity consumers, i.e., ONSPs. The ONSP doesn’t know the true identity of the user; only is assured of the user’s affiliation to a certain VO and his/her several relevant attributes (e.g. Gold member). Access control management to user attributes remains an issue. In particular if the number of ONSPs in the VO is large. The user must specify which ONSP has access to what attributes. This is more complex as the user often does not know beforehand which ONSPs will ask for attributes.

Thirdly, due to the low profile of the VO in the light-path establishment process and its simple DNS administrative task, the solution seems economically viable from a scalability and functional perspective.

Finally, standard technologies like SAML, TLS and DNS are used to successfully implement the solution.
5. Conclusions

The success of user-controlled light-path establishment depends heavily on how securely, effectively, and transparently identity data flows across the stakeholders. But managing identity data is extremely challenging, because of the proliferation of distributed identity data stores and the lack of trust between their owners and the identity consumers.

Identity management alone is not enough however. Identity and attribute information must be shared between the user and the ONSP which may have no initial trust relationship with each other and may typically reside in different administrative or security domains. We therefore introduce a trusted third party, i.e., the VO, to offer the necessary trust to provide for effective identity and attribute exchange between the user’s IdP and the ONSPs that constitute the required light-path. The VO can, in the role of a DNS tree administrator, effectively use the security extensions of DNS to dynamically create a direct trust relationship between the ONSPs and the user’s IdP. DNS also allows the ONSP to discover the proper IdP. DNSsec furthermore guarantees correctness of DNS records and can be used as a safe certificate store. The use of all other basic DNS advantages like caching, replication, and priorities increases even more the integrity of the communication between the user’s IdP and the ONSP. This makes the DNSsec solution interesting for the VO from a business and administrative viewpoint.

6. Acknowledgement

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

7. References