Security Aspects for Large Scale Distributed Environments

The AutoBAHN use case

Giorgos Adam[1,2], Christos Bouras[1,2], Ioannis Kalligeros[1,2], Kostas Stamos[1,2,3], and Ioannis Zaoudis[1,2]

[1]Computer Technology Institute and Press "Diophantus", N. Kazantzaki Str, University Campus 26504, Rio Greece
[2]Computer Engineering and Informatics Dept., University of Patras
[3]Technological Educational Institute of Patra, Greece
{adam,stamos,bouras,zaoudis}@cti.gr, kallige@ceid.upatras.gr

***Abstract* — Automated Bandwidth Allocation across Heterogeneous Networks (AutoBAHN) is a tool under active development that supports a Bandwidth on Demand (BoD) service, intended to operate in a multi-domain environment using heterogeneous transmission technologies. The AutoBAHN system aims at providing a guaranteed capacity, connection-oriented service between two end points. Due to the level of access that the tool has to critical parts of the network, the importance of a trustworthy Authentication and Authorization Infrastructure (AAI) cannot be overestimated. This paper highlights the design and implementation for the Authentication and Authorization Infrastructure which is part of the AutoBAHN service and the decisions taken. The AAI is a service dedicated to enforce system security and to prevent unauthorized access and usage of resources. The BoD service modules may interact with AAI multiple times during a single request execution. After the initial authentication and authorisation check, the BoD system will apply additional, specific to BoD rules and policies to the request. The security mechanisms allow trustworthy operations in a multi-domain service without significant impact on performance.**

Keywords - Bandwidth on Demand; AAI; security; Quality of Service

I. Introduction

The GN3 European project [1] is a research project funded by the European Union and Europe's National Research and Education Networks (NRENs). It is a continuation of the previous GN2 project [19] and aims at building and supporting the next generation of the pan-European research and education network, which connects universities, institutions and other research and educational organizations around Europe and interconnects them to the rest of the Internet using high-speed backbone connections.

In the context of this project, a BoD service is being developed and the service is supported by the AutoBAHN tool. The AutoBAHN system is capable of provisioning circuits in heterogeneous, multi-domain environments that constitute the European academic and research space and allows for both immediate and advanced circuit reservations. The overall architecture of the AutoBAHN system, its goal and the network mechanisms it employs are thoroughly presented in [2]. This paper highlights the AAI architecture of the AutoBAHN service, the implementations challenges, the decisions taken and the basic security aspects and components of the AutoBAHN system.

AutoBAHN is using part of GÉANT's AA Framework [20] which addresses security issues for a number of different multi-domain network services in the GÉANT Service Area. This framework provides software developers with a common and flexible authentication and authorization solution to facilitate their software development process.

The rest of the paper is structured as follows: Section 2 describes the GN3 project while Section 3 presents the general architecture of the AutoBAHN system. In Section 4, we analyze how similar projects handled AA issues while Section 5 presents the general architecture related to authentication and authorization procedures. Section 6 describes the way that communication between system components can be considered secure. Section 7 presents some quantitative measurements and finally, Section 8 concludes the paper and presents future fields of this study.

II. GN3

Gigabit European Advanced Network Technology (GÉANT) is the main European multi-gigabit computer network for research and education purposes. It brings together over 400 participants from 32 NRENs, TERENA [21], DANTE [22], and over 20 subcontractors and third parties. It provides a dedicated, high capacity, 50,000 km data network that brings together 40 million users in research institutions across 40 countries, underpinning critical projects that would previously have been impossible without its capacity and reliability.

In the context of the GN3 project, a number of activities and services are prototyped and tested. Among them is AutoBAHN BoD service.

This BoD service is an end-to-end, point-to-point bidirectional connectivity service for data transport. It allows users to reserve bandwidth on demand between the participating end points. The data transport capacity dedicated to a connection can range from 1 Mbps up to 10 Gbps in steps of 1 Mbps. This service is offered collaboratively by GÉANT and a set of adjacent domains (NRENs or external partners) that adhere to the requirements of the service. These joint networks form a multi-domain area where the service is provided.

The service offers a high security level in the sense that the carried traffic is isolated from other traffic. It has to be noted that the traffic is isolated at logical layer and not necessarily at physical layer. This means that the core network will carry data from multiple users but there will be no “crosstalk” between the traffic streams.

III. AutoBAHN BoD System

The AutoBAHN system is comprised by the Inter-Domain Manager (IDM), a module responsible for inter-domain operations of circuit reservation on behalf of a domain. This includes inter-domain communication, resource negotiations with adjacent domains, request handling and topology advertisements.

Furthermore, in order to build a real end-to-end circuit, the Domain Manager (DM) is another module that manages intra-domain resources. The IDM has an interface to the local DM from which it undertakes all intra-domain functions (abstracting the topology towards the IDM, scheduling and pre-reserving resources, monitoring etc.). This southbound interface of the IDM is the part of the AutoBAHN system that needs to be tailored to the domain-specific conditions.

In each domain, the data plane is controlled by the DM module using a range of techniques, including interfaces to the Network Management System (NMS), signaling protocols or network elements. As part of the AutoBAHN, a dedicated and independent Technology Proxy module allows the support of a range of technologies and vendors according to domain and global requirements.

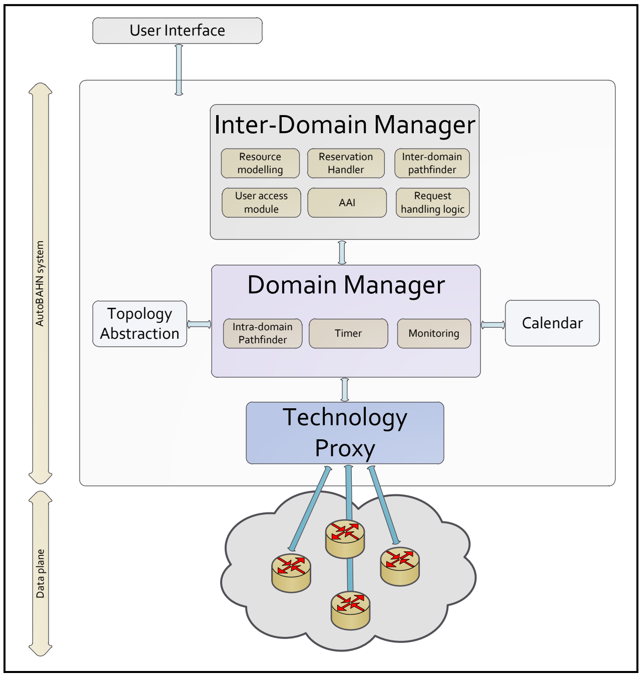

Figure 1. Basic architecture of AutoBAHN

The local NMS or service provisioning system, monitoring infrastructure, administration policies and security, may need to be adjusted for each networking domain making each Technology Proxy implementation and configuration unique. However, the design of the DM has been optimized to support modular deployment and leverage the management infrastructure already deployed in any domain.

The above set of modules is deployed in each domain (NREN) that participates in the BoD service. A web based graphical environment (WebGUI) is used as a centralized portal for user access to the whole set of deployed instances.

The above described architecture defines a multitude of communication interfaces that transfer sensitive information over the network. A potential security compromise (eaves dropping, message modification, unauthorized access, message replay) could have very important consequences as the system manages production networks. Furthermore, because of its distributed nature, the system needs a well-defined distributed authentication and authorization architecture as it spans a large number of independent administrative domains.

IV. Related Work

The AutoBAHN BoD system has been influenced by a number of other projects dealing with similar challenges for bandwidth on demand provisioning. In this section we present some of the most closely related ones, with an emphasis on their approach to AAI.

The Dynamic Resource Allocation across GMPLS Optical Networks (DRAGON) project [3] is also conducting research and developing technologies to enable dynamic provisioning of network resources on an inter-domain basis across heterogeneous network technologies. It mainly deals with GMPLS enabled domains and in a smaller scale compared to AutoBAHN. Regarding the AAI, the DRAGON project incorporates AAA policy into path computation, resource allocation and signaling functions. This requires high level associations of policy with users (or groups of users) as well as lower level associations of policy with actual network elements at a fidelity sufficient to implement meaningful policy based resource allocations. These two levels are loosely described as call control and connection control. Their approach is the synthesis of higher level AAA information into policy information which is associated with the Traffic Engineering (TE) resource level. They also utilize higher level AAA information to develop a set of policy rules. The TE policy data and the policy rules are used during path computation to incorporate AAA policy into provisioning operations. AAA policy decision can be combined with TE based provisioning decision [4].

OSCARS/BRUW project [5] which is another BoD service focuses on Layer 3 Multiprotocol Label Switching (L3 MPLS) QoS. Regarding AA, requests for inter-domain reservations are authenticated in the originating domain on the basis of an individual user and in the subsequent domains on the basis of the adjacent domain [6]. Users are authenticated and authorized for actions in their home domain and inter-domain authorization depends on the domains that participate. It also depends on the assurance that a request is coming from a trusted server in a trusted domain. Normally, all requests forwarded between domains are signed SOAP messages. The forwarded message adds the name of the originating user in case other domains wish to use that information for authorization or auditing. Currently, at the time of provisioning no further authentication is done. Provisioning is triggered by the time of the reservation. Once the provisioning has been completed, any traffic coming from the specified ingress router is able to use the requested bandwidth.

Moreover, the University of Amsterdam's Advanced Internet Research group has published a number of papers describing both the networking and the AAA issues for such a system [7][8][9]. They are using IETF's AAA Framework [10] and OASIS eXtensible Access Control Markup Language (XACML) Version 2 to describe policy, which is also followed by OSCARS for Authentication. They have also defined a Network Description Language, which is an RDF-based method to describe networks and to facilitate inter-domain interoperability [11].

V. AAI Architecture

AutoBAHN uses part of GÉANT's AA Framework which utilizes existing frameworks, industry standards and best practices in order to avoid re-inventing the wheel and to take advantage of its extensible design. It is Java-based, making use of Spring Security Framework, Crowd Integration library, OIOSAML java library and Maven.

In addition, we have developed our own architectural elements, such as our multi-domain user authorization which is described below, in order to bind and supplement the above technologies and meet our unique AAI requirements.

The current AA Framework implementation allows developers to make their own choice of Authentication Providers, User Attributes Providers and ACL services to use: the diagram below (Figure 2) shows the options offered to the service developers.

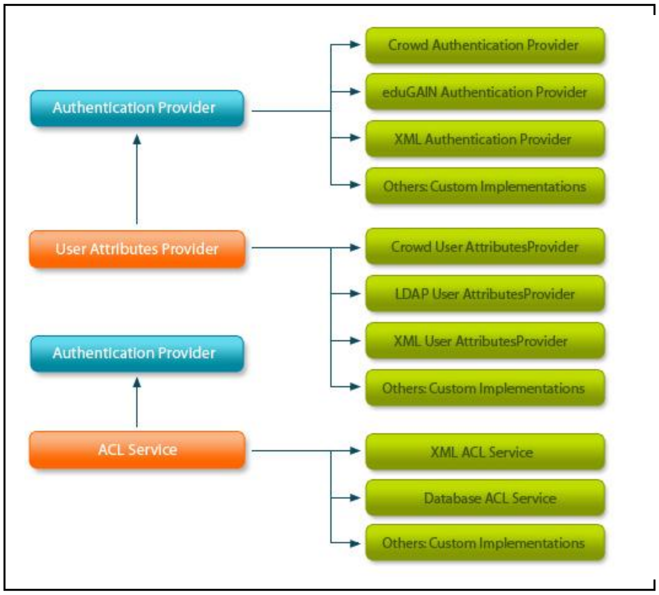
Authentication Provider
Crowd Authentication Provider
eduGAIN Authentication Provider
XML Authentication Provider
Others: Custom Implementations
User Attributes Provider
Crowd User AttributesProvider
LDAP User AttributesProvider
XML User AttributesProvider
Others: Custom Implementations
Authentication Provider
ACL Service
XML ACL Service
Database ACL Service
Others: Custom Implementations

Figure 2. The architecture of AA Framework [20]

AutoBAHN can be configured to use XML or Atlassian Crowd [15] for Authentication and User Attributes Provider. It can also support the existing eduGAIN [12] infrastructure for authentication and authorization. In addition, LDAP [14] or Relational Databases can be used as Authentication and User Attributes Providers. They also have the additional capability of supporting Access Control Lists for flexible definition of authorization policies.

A. *User Authentication*

The AutoBAHN system has been designed in such a way so that multiple authentication methods may be used, in a modular way. The authentication mechanism is based on the Spring Security Java framework [13] that provides advanced authentication, authorization and other security features for enterprise applications.

The architecture of the authentication mechanism is based on a simple flow in which the main system components that are invoked during the authentication procedure are the Authentication Manager and the Authentication Provider. The user submits his credentials to the AutoBAHN Server and an Authentication Request is created at server-side. This request is sent to the Authentication Manager which is responsible for forwarding requests through a chain of Authentication Providers. The provider will request from the UserDetails Service to provide the granted authorities for this user. These authorities are later used during the Authorization phase. The Authentication Manager receives back the result of the described procedure and decides whether the authentication is successful or not.

TABLE I. Implementation Choices Available for Developers [20]

Provider	**Available choices**		
	Authentication Provider	***User Attributes Provider***	***ACL Services***
Attlasian Crowd	Yes	Yes	N.A.
eduGAIN	Yes	N.A.	N.A.
LDAP	Yes	Yes	N.A.
Relational Databases	Yes	Yes	Yes
XML	Yes	Yes	Yes

When a user connects to the graphical environment to submit a reservation request, his supplied credentials can be authenticated against the Authentication Provider which is currently used. The authorization mechanism is able to cooperate with interchangeable authentication modules as long as the authentication provider also supplies the necessary attributes that enable authorization decisions. As the eduGAIN scenario is the most complicated and interesting one, it will be described in more detail below.

In principle, when a user tries to access the AutoBAHN system, the user is redirected to the Single Sign-On (SSO) service of his/her federation. Then the user is authenticated through the federation software which sends the SSO response and SAML 2.0 authorization back to the AutoBAHN system. The response contains both authentication and authorization information as SAML 2.0

attributes. Finally, the AutoBAHN system checks the SSO response and SAML 2.0 attributes and responds to the user with a permission or denial to access the resources. The attributes that are transmitted are the following:

1) *Identifier*: A unique id of the user that wants to make a reservation. This could be either the name or the email of the user or a combination of both.
2) *Organization*: The organization/domain/federation of which the user is a member.
3) *Project Membership*: This attribute contains a specified value (e.g. AUTOBAHN) that demonstrates that this user is an authorized AutoBAHN user.
4) *Project Role*: This attribute offers granularity in terms of the subset of available actions that the user is allowed to perform and can contain values such as Service user, AutoBAHN administrator, etc.

The various project roles currently supported are:

1) *Service User*: People from e-science communities, other BoD systems, external client applications that become "service owners".
2) *Network Administrator*: People responsible for the data plane e.g., the underlying data network infrastructure.
3) *Autobahn Administrator*: People responsible for the control plane software.

In AutoBAHN system, the above attributes are considered to be equivalent of granted authorities meaning that based on the policy that is defined by the administrator, those attributes also define the appropriate jurisdictions and capabilities that a user can have during the usage of the system.

B. *Multi-domain User Authorization*

Authorization is the function of specifying whether a user has the access rights to perform an action on the system resources. AutoBAHN implements multi-domain user authorization, which means that the above procedure is done on every single Domain Manager.

After the authentication phase, the user is able to request access to the available resources. The authorization procedure takes place at the Domain Manager which determines whether the user is authorized to access the requested resource. This decision is based on the access policies that each DM has defined.

For operations that are decided along a multi-domain path (

Figure **3**), there are multiple Domain Managers. Thus, the decision has to be taken in every domain along the reservation path based on user attributes that have to be transmitted with the reservation request and mapped to the policies implemented by each domain.

As described earlier, the user attributes are retrieved during the authentication phase. These attributes are then forwarded to each domain of the reservation path at server-side. Before a request is examined by the system at each domain, the attributes are compared against the policy module to check whether the user has the required privileges. The policy is based on logical operations among the user attributes: identifier, organization, project membership and role.

Figure **3** shows the whole procedure for authentication and authorization when a user wants to create a service request. In Step 1, the user (through a web browser) tries to access the service submission interface and the request is intercepted by the eduGAIN filter.

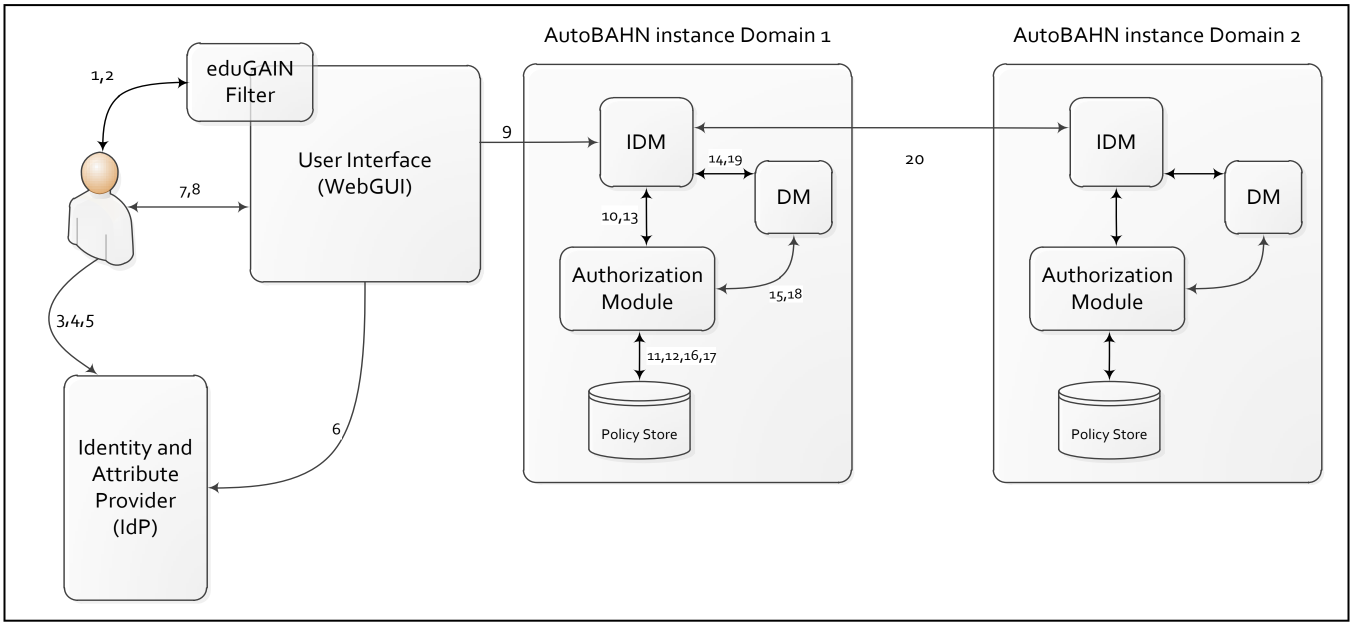

Figure 3. The user creates a reservation between different domains

The eduGAIN filter redirects the user to his local AAI (Step 2). The user's web browser sends an http request to the IdP server (Step 3). The IdP server sends to the web browser a page to authenticate the user and the user submits his credentials to the IdP server (Steps 4 and 5). The IdP server redirects the user to the WebGUI request page, and associated attributes are also sent (Step 6). The user fills in necessary parameters and submits the service request which may bundle multiple circuit reservation requests (Steps 7 and 8). The WebGUI forwards the service request and user attributes to the initiating IDM (Step 9).

The IDM deals with each reservation in the service separately. For the first reservation, it forwards the user attributes and reservation parameters to the AuthR module and the AuthR module constructs a policy evaluation query (Steps 10 and 11). The query is checked against the existing policies stored in the Policy Store and the AuthR module returns an answer (Steps 12 and 13). Assuming the response allows such a request, the IDM forwards it to the DM for intra-domain checking (Step 14). The DM calculates possible paths and forwards the reservation parameters to the AuthR module (Step 15). The AuthR module constructs a policy evaluation query and the query is checked against the existing policies stored in the Policy Store (Steps 16 and 17). The AuthR module returns an answer and the DM replies to the IDM about the feasibility of the reservation (Steps 18 and 19). The IDM forwards the request and the user attributes to the next domain along the path for further processing (Step 20) and finally, this process is repeated for all domains until the first reservation request has been evaluated. If a service request contains more than one reservation, this process is repeated for all reservations within this service request.

VI. TRUSTED AND SECURE COMMUNICATION BETWEEN SYSTEM COMPONENTS

To ensure a secure and trusted communication between system components, WS-Security standard [23] is used in addition with Edugain PKI infrastructure [24].

WS-Security (Web Services Security, short WSS) is a flexible and feature-rich extension to SOAP to apply security to web services. It is a member of the WS-* family of web service specifications and was published by OASIS.

The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats such as SAML, Kerberos, and X.509. Its main focus is the use of XML Signature, XML Encryption and XML Timestamp to provide end-to-end security and in our case all three options are available for use.

WS-Security makes heavy use of public/private key cryptography [16]. With public key cryptography, a user has a pair of public and private keys. A central problem for use of public-key cryptography is confidence (ideally proof) that a public key is correct, belongs to the person or entity claimed (i.e., is 'authentic') and has not been tampered with or replaced by a malicious third party. The usual approach to this problem is to use a public-key infrastructure (PKI) in which one or more third parties, known as certificate authorities, certifies ownership of key pairs.

AutoBAHN makes use of eduGAIN PKI for validating the identity of the components. The trust establishment process is enabled by means of using TLS connections for each eduGAIN interaction and including XML-Sig digital signatures for the appropriate protocol elements and assertions.

eduGAIN inter-component trust is based on X.509 certificates. It is rooted at a set of Certification Authorities (CA) created and maintained within the project. This set will be referred to as the eduGAIN truststore and all AutoBAHN components accept any of the CAs contained by the truststore as valid roots of trust. CAs in the eduGAIN truststore conform to the eduGAIN Certificate Policy, a document defining the rules and procedures agreed by the eduGAIN participants to rely on digital public certificates issued to the components of the infrastructure.

At least one of these CAs will be specifically established and run by the project. This root CA is referred as the eduGAINCA. The self-signed certificate of the eduGAINCA is the minimum content of the eduGAIN truststore.

A. PKI Structure

The structure of the eduGAIN PKI is shown in Figure 4. Each CA inside the eduGAIN truststore (shown as "Acc CA" in the figure) is accredited to issue certificates for components in a particular branch of the eduGAIN component identifier namespace (shown as "CId" in the figure). Certificates for components outside these branches are under the eduGAIN CA. The eduGAINCA issues certificates only to other CAs and these subordinated CAs will in turn be responsible for issuing certificates to the individual components. The eduGAIN infrastructure provides at least one of these subordinated CAs, known as the eduGAINSCA.

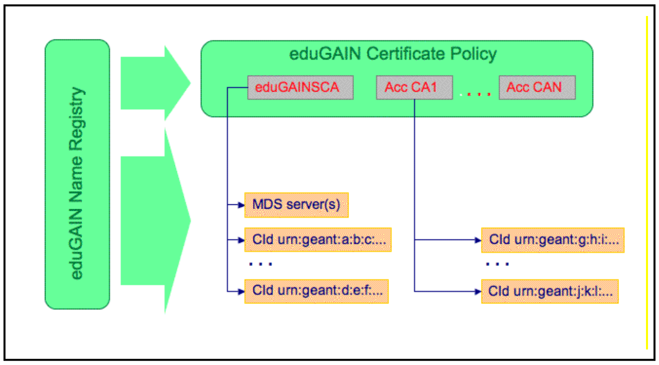

Figure 4. eduGAIN PKI Structure

The eduGAINSCA is able to provide a set of separately managed Registration Authorities (RA), according to the management procedures of the different eduGAIN namespaces under its responsibility.

B. *Trust Validation Procedure*

Trust validation is performed by eduGAIN components according to a two-step procedure:

1. The received certificate shall be evaluated to check whether the whole trust path correctly resolves to the eduGAIN root of trust.

2. The eduGAIN component identifier contained in the Subject Alternate Name extension of the received certificate shall be evaluated against the metadata available for this interaction. It must match with the component identifier as stored in these metadata.

A failure in any of the verifications above causes a rejection of the requested operation with a TrustError result. This procedure implies that for a proper trust evaluation, all metadata exchange through the MDS must contain the eduGAIN component identifiers applicable in each case.

Unless otherwise specified in the corresponding profile, all connections between any two eduGAIN components uses TLS and perform two-way certificate validation (both initiator and responder) according to the above procedures.

Validation of the certificates associated with XML Signatures follow the procedures described above.

In principle, when the client module wants to communicate with another module (the resource), it sends its request to the required resource along with its X.509 certificate signed by eduGAIN CA. The resource authenticates the client by validating its certificate using eduGAIN API. The certificate contains identification information that allows the resource to authenticate only designated clients.

The detailed procedure in the context of the AutoBAHN system for the trusted communication between AutoBAHN modules is as followed.

1) The AutoBAHN module that wants to communicate (client) must have a certificate so no interaction for credentials is needed. The X.509 certificate is issued by a Certificate Authority (CA) subordinated to one of the eduGAIN roots of trust.
2) The client module sends its request and the certificate to the resource.
3) The resource module performs trust validation by checking that the whole trust path of the certificate correctly resolves to the root(s) of trust defined by eduGAIN.
4) The resource checks that the client module is allowed to access it.
5) The resource provides the requested answer to the client module.

VII. Quantitative Measurements

In order to verify the scalability of the system, we have taken some quantitative measurements using Apache JMeter [25] as benchmarking tool. The test scenario specified the submission of 200 requests in time frame of 50 seconds resulting in 4 requests per second. The following graph presents the response time against the number of active threads. The lines refer to various steps during the submission of a reservation request in Client Portal.

The response time peaks at 330 milliseconds when the greatest number of requests is being processed.

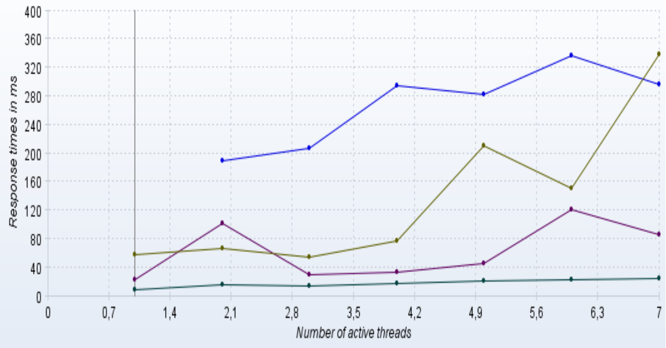

Figure 5. Response Time vs Active Threads

VIII. Conclusions and Future Work

In this paper, we presented an Authorization and Authentication Infrastructure that is used in AutoBAHN project to ensure a secure and trusted communication among its components.

AutoBAHN is considered a distributed system since each NREN deploys an instance based on their specific network technology and their needs in general. Because of that, it was important to emphasize in multi-domain user authorization ensuring that this communication is secured by WS-Security specification.

Also, a strong advantage of AutoBAHN's authentication and authorization mechanism compared to approaches of similar projects is the fact that it can support third party providers such as LDAP or Atlassian Crowd increasing the flexibility and the interoperability of the project. Furthermore, the AA process takes place in each single domain that is involved to a reservation path making the allocation of network resources more secure and robust. It's not a one-time procedure that takes place only in the originating domain.

AutoBAHN is designed in a highly scalable manner based on modules that perform specific tasks and communicate with one another. AuthR module handles AA tasks and then communicates with local DM, which later on sends the appropriate messages through the IDM to the rest of the AutoBAHN instances. This separation allows for a more convenient administration of the AAI in order to keep it up to date by adopting latest technology standards.

Currently AutoBAHN has been deployed in 6 NRENs creating a pan-european bandwidth on demand service. Several more NRENs have expressed interest or are already in the process of joining the service. This service is currently fully operable and being offered to NREN staff and clients.

The main lesson learnt was that the utilization of existing frameworks and open standards enabled us to implement our own custom AAI solution for a complex multi-domain environment and at the same time ensure extensibility and flexibility. In addition, due to the importance of the security mechanisms to the operation of the service, we consider it

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-209-7

essential that the specification of the AAI architecture needs to be an integral part of the system design from the start.

Next step is the full integration of the latest AA Infrastructure that is a result of SA2/Task5 Common Framework efforts [17]. The WS-Security standard is based on WSS4J, a well-known and commonly used Java library for securing Web Services. In our case, we can additionally use AA Framework's two way SSL communication as an extra security layer above WS-Security, which is based on X.509 certificates that are issued by eduPKI CA, the next-generation CA of GÉANT's project [18].

ACKNOWLEDGMENT

The authors would like to acknowledge the contribution of their GN3 partners and especially the JRA2 Task 2 and SA2 Task 5 groups.

REFERENCES

[1] "GN3 European Project," [Online]. Available: http://www.geant.net/pages/home.aspx. [retrieved: June, 2012]

[2] M. Campanella, R. Krzywania, V. Reijs, A. Sevasti, K. Stamos, C. Tziouvaras, and D. Wilson, "Bandwidth on Demand Services for European Research and Education Networks," in 1st IEEE International Workshop on Bandwidth on Demand, San Francisco (USA), pp. 65-72, 2006.

[3] F. Leung, J. Flidr, C. Tracy, X. Yang, T. Lehman, B. Jabbari, D. Riley, and J. Sobieski, "The DRAGON Project and Application Specific Topologies," in Broadnets, San Jose, California, USA, pp. 1-10, 2006.

[4] Xi Yang, Tom Lehman, Chris Tracy, Jerry Sobieski, Shujia Gong, Payam Torab, and Bijan Jabbari, "Policy-Based Resource Management and Service Provisioning in GMPLS Networks", IEEE INFOCOM, pp. 1-12, 2006

[5] C. Guok, "ESnet On-Demand Secure Circuits and Advance Reservation System (OSCARS)," in Internet2 Joint Techs Workshop, Salt Lake City, Utah, 2005.

[6] Chin Guok, Robertson, D., Thompson M., Lee J., Tierney B., and Johnston W. "Intra and Interdomain Circuit Provisioning Using the OSCARS Reservation System", Broadband Communications, Networks and Systems, pp. 1-8, 2006. BROADNETS 2006. 3rd International Conference

[7] L. Gommans, C. de Laat, and R. Meijer, "Token based path authorization at interconnection points between hybrid networks aind a lambda grid," in Proceedings of IEEE GRIDNETS 2005

[8] L Gommans B van Oudenaarde F Dijkstra, C. de Laat, T. Lavian I Monga, A Taal F Travostino, and A Wan "Applications drive secure lightpath creation across heterogeneous domains,' IEEE Communications Magazine, vol. 44, no. 3, pp. 100-106, 2006.

[9] Y Demchenko, L. Gommans, C. de Laat, A. Tokmakoff, and R. van Buren, "Policy based access control in dynamic Grid-based collaborative environment," in International Symposium on Collaborative Technologies and Systems, pp. 64-73, 2006.

[10] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, and D. Spence, "AAA authorization framework," IETF RFC 2904, Aug. 2000.

[11] J.J van der Ham, F. Dijkstra, F. Travostino, H.M.A. Andree, and C.T.A.M de Laat "Using RDF to describe nfetworks"' iGrid 2005 special issue, Future Generation Computer Systems, vol. 22, no. 8, pp. 862-867, 2006.

[12] "Deliverable DJ5.2.3,3: Best Practice Guide - AAI Cookbook - Third Edition", [Online]. Available: http://www.geant2.net/upload/pdf/GN2-08-130-DJ5-2-3-3_eduGAIN_AAI_CookBook-1.pdf [retrieved: June, 2012]

[13] "Spring Security Framework," [Online]. Available: http://static.springsource.org/spring-security/site/ [retrieved: June, 2012].

[14] "LDAP," [Online]. Available: http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol [retrieved: June, 2012].

[15] "Crowd," [Online]. Available: http://www.atlassian.com/software/crowd/ [retrieved: June, 2012].

[16] "Public Key Cryptography," [Online]. Available: http://en.wikipedia.org/wiki/Public-key_cryptography [retrieved: June, 2012].

[17] G. Forge, "GÉANT AA Framework," [Online]. Available: https://forge.geant.net/forge/display/AAI/Home [retrieved: June, 2012].

[18] "eduPKI", [Online]. Available: http://www.geant.net/SERVICES/ENDUSERAPPLICATIONSERVICES/Pages/eduPKI.aspx [retrieved: June, 2012].

[19] "GN2 Project", [Online]. Available: http://www.geant2.net/ [retrieved: June, 2012]

[20] "GEANT AA Framework", [Online]. Available: http://www.geant.net/Services/NetworkPerformanceServices/Pages/GEANT_Framework.aspx [retrieved: June, 2012]

[21] "TERENA", [Online]. Available: http://www.terena.org/ [retrieved: June, 2012]

[22] "DANTE", [Online]. Available: http://www.dante.net/ [retrieved: June, 2012]

[23] "WS-Security", [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss [retrieved: June, 2012]

[24] "eduPKI", [Online]. Available: http://www.geant.net/Services/UserAccessAndApplications/Pages/eduPKI.aspx [retrieved: June, 2012]

[25] "Apache JMeter" , [Online]. Available: http://jmeter.apache.org/index.html [retrieved: June, 2012]