Applicability Of SOAP Based Authentification For Distributed Project Teams

Predrag Pale, Jure Šimundić, Goran Živković, Branko Jeren
Faculty of Electrical Engineering and Computing, University of Zagreb
Address: Unska 3, Zagreb, Croatia
predrag.pale@fer.hr, jure.simundic@fer.hr, goran.zivkovic@lss.hr, branko.jeren@fer.hr

It is common for projects nowadays to have multidisciplinary teams whose members belong to different academic institutions world wide as well as to industry, government and NGOs.
Team members need access to computer and communication infrastructure, services and data with various levels of access privileges. They need access from various world wide locations to resources spread on different locations embedded in infrastructures belonging to different owners protected by numerous firewalls and other means.
The paper discusses applicability of SOAP for authentication and its practical advantages and drawbacks. Attention is paid to scalability, simplicity of use, maintainability of access rights, flexibility in changing team membership and especially to security issues.

I. Introduction

Only very simple or specific tasks can nowadays be performed by individuals. Majority of work is done in cooperation. Pairs, groups and teams collaborating in projects consist of individuals belonging not only to different professions, but also to different organizations and physical locations.

In their work and collaboration they simultaneously or sequentially use various resources: equipment, software applications, data and services. They do so in different ways, times and for different purposes. Those resources belong to different organizations and have different use policies applied to them depending of who is using them, when and for what purposes.

Thus the overall need of modern project teams is that every team member has readily available resources she or he needs, regardless of the current physical location of resource and user, regardless of who owns resource but always in accordance with use policy for that specific resource and that specific user.

As a consequence, a practical technical system is required which will identify users, authenticate them (make sure user is truly the person he claims to be) and authorize them for the use of the resource (determine which resource, when and how this user is permitted to use). Extended functionality of the system would offer logging of the use, too.

Such systems often come under the name AAI which stands for "Authentication and Authorization Infrastructure".

While various organizations and communities develop their AAIs, the real challenge arises when team members come from different communities which do not have a common AAI system.

This paper is addressing that problem in general. However, for the clarity of the text, an example of an academic project with team members from industry and government will be used.

II. Requirements

Team members will work on the project for a defined, limited time ranging from weeks to years. They originally belong to different organizations. Only their organizations can verify their identity.

Team members will need to use a variety of resources: communication infrastructure consisting of access equipment both wired and wireless; computing resources: computers (operating systems) and software applications; data and information: databases and web services; as well as services provided by computers and humans.

The level, intensity, timing and other properties of a resource usage need to be specifically defined for each user or user category. They need to be defined by the resource's owner.

Team members will access the resources from any participating organization or over the public networks, world wide.

The whole AAI should be able to operate on existing ICT infrastructures of participating organizations, linked either through private or public infrastructures, with as little changes as possible, if any.

III. The existing AAIs

One example of a practical, technical solution to inter-institutional AA requirements is AAI@EduHr, which stands for Authentication and Authorization Infrastructure of Science and Higher Education in Republic of Croatia. AAI@EduHr is a project brought up by SRCE (Computing Centre of Zagreb University) and CARNet (Croatian Academic and Research Network), under the financial support of Ministry of Science, Education and Sport, and now actively coordinated and maintained by SRCE. The AAI concept has emerged out of the need to provide each academic member, i.e. student and professor, with the simple, uniform and secure access to network resources on every scientific or higher education institution (college, institute, academy, etc.) that is part of the AAI@EduHr [1].

AAI@EduHr is connected with similar national AAI systems in Europe and in the world. AAI@EduHr is part of pan-European roaming system known as eduroam

(http://www.eduroam.org). *Eduroam* stands for Education Roaming, is a RADIUS-based infrastructure that uses 802.1X security technology to allow for inter-institutional roaming. Being part of eduroam allows users visiting another institution connected to eduroam to log on to the WLAN using the same credentials (username and password) the user would use if he were at his home institution. Depending on local policies at the visited institutions, eduroam participants may also have additional resources at their disposal [2.]. AAI@EduHr is also connected with eduGAIN (http://www.edugain.org)[1].

The main mean of providing and controlling each member's access right to a particular resource is over his or hers electronic identity. In other words, the electronic identity is a mean of achieving one's right within the framework of AAI@EduHr. Electronic identity represents a set of data related to each academic member that is used for AA purposes and that is stored in a specialized directory. The complete authority to manage those directories in a prescribed manner, is given to home institutions, i.e. to the institution which the addressed person is part of (as employee or enrolled student).

Access to network resources is established in three steps which involve *home institution*, *service provider institution* and the *access demanding end user*, all representing three basic communication subjects in the system of AAI@EduHr.

The access process goes as follows:

1. The end user submits her access credentials, i.e. user name and password, to the network access point of the institution at which he/she requires access.
2. The submitted credentials are then passed through intermediate services to his/her home institution, where they were created, issued and are being managed. Home institution authenticates the user and sends the result of authentication along with user's related authorization rights back to the service provider which placed the request.
3. Based on the received information, the service provider, i.e. the resource owner, makes the decision whether to grant the access to the user and about restricting that access to particular resources.

AAI@EduHr is founded on the technology of Web services, distributed LDAP directories, RADIUS servers and proxies, SOAP and SAML protocols along with associated technical solutions developed by SRCE [1].

IV. Used technologies

One of today's de facto standards in the field of AAA (Authentication, Authorization and Accounting) network requirements is RADIUS protocol, abbreviated from Remote Authentication Dial In User Service. RADIUS is a networking protocol that provides centralized Authentication, Authorization, and Accounting management for computers to connect and use network services. Authentication and Authorization characteristics in RADIUS are described in RFC 2865, while Accounting is described in RFC 2866 [3].

RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. It is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services through various types of network accessing points (Network Access Servers) such as dial-up servers, VPN servers, wireless access points, 802.1x compatible switches. These are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server. Additionally, the RADIUS standards support the use of RADIUS proxies. A RADIUS proxy is a computer that forwards RADIUS messages between RADIUS clients, RADIUS servers, and other RADIUS proxies (refer to Fig. 1).

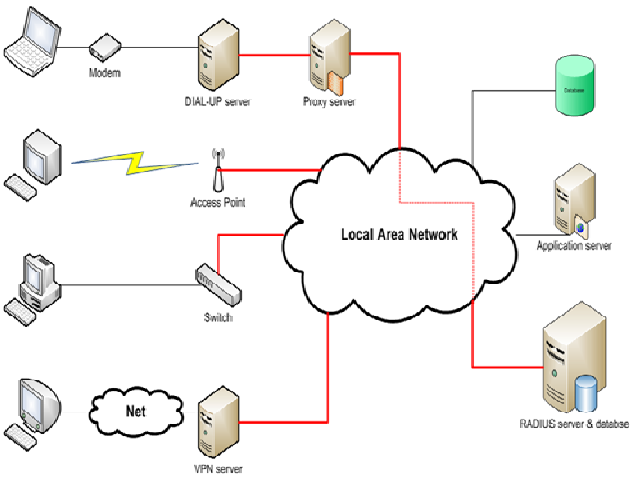

Fig.1. RADIUS protocol network components

A RADIUS client sends user credentials and connection parameter information in the form of a RADIUS Access Request message to a RADIUS server. The RADIUS server authenticates and authorizes the RADIUS client request, and sends back a RADIUS Access message response. RADIUS clients also send RADIUS accounting messages to RADIUS servers.

AAA process is shown in Fig. 2.

[1] eduGAIN enables sharing of identity data between federations, providing an interconnection layer to applications willing to provide inter-federation services over existing organizations and policies. It is part of GEANT project. The GÉANT network is the fast and reliable pan-European communications infrastructure serving Europe's research and education community.

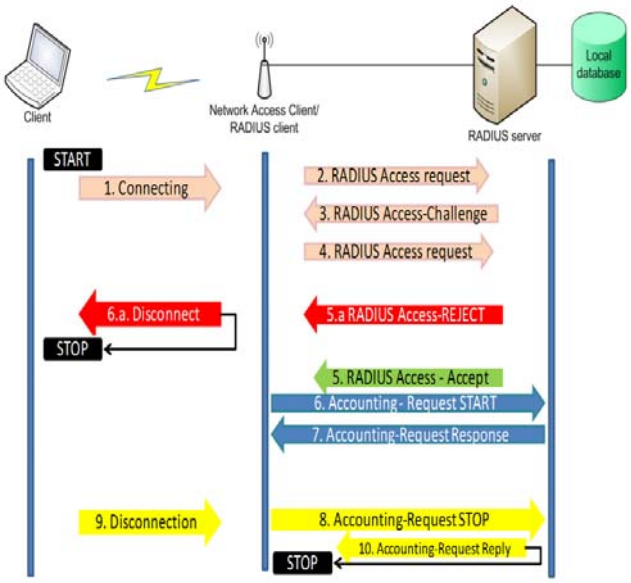

Fig.2. RADIUS AAA process

A RADIUS message consists of a RADIUS header and RADIUS attributes. Each RADIUS attribute specifies a piece of information about the connection attempt. For example, the list of attributes in the Access-Request message includes information about the user credentials and the parameters of the connection attempt. In contrast, the list of attributes in the Access-Accept message includes information about the type of connection that can be made, connection constraints, and any vendor-specified attributes (VSAs) [4].

To provide security for RADIUS messages, the RADIUS client and the RADIUS server are configured with a common shared secret in combination with MD5 hashing algorithm to encrypt the User-Password and other attributes such as Tunnel-Password (RFC 2868) and MS-CHAP-MPPE-Keys (RFC 2548). RADIUS support is nearly omni-present. Other remote authentication protocols such asTACACS and TACACS+, do not have consistent support from hardware vendors, whereas RADIUS is uniformly supported.

V. Including users from other communities

If looking for usable and present solution which would give scattered project members a simple and uniform access to network resources they are working with, AAI@EduHr would be an appropriate solution assuming that all the members are part of an academic community. Accessing various information and applications, database and other „online“ resources from a network outside of one's home network, poses no problem due to the AAI concept - all academic members can login with their user credentials from whatever (network/institutional) location they want, under the condition that the accessing location is registered within AAI@EduHr[2]. When it comes to the rest of the world, currently there are three regional eduroam confederations, in Europe, Asia-Pacific and the Americas (supported by Canada). In the United States of America the Internet2 working group FWNA (Federated Wireless Network Authentication) has started an initiative to create a RADIUS-hierarchy for higher education and to become eduroam participants.

It is a common occurrence among academic distributed teams to have a non-academic members associated to project who also need to be given an access to project resources. In most cases those associates come from commercial domain and by that have no identity within AAI@EduHr. Furthermore, if a team is composed of members coming from different countries, then the authorization attributes that are being passed between home and foreign location, must be uniformed in order to be interpretable on access–decision point.

This section explores whether AAI@EduHr can suit variable access requirements set by team members and if not, what would be the alternatives.

A. Solving AA requirements for non- academic team members

Assume there is a project team which consists of students and professors that come from two different colleges in two different cities. Also assume that on each college there are few external associates that come from business sector and that are involved in project. Participants must be able to login to both college networks and to use network resources only with their access credentials. In other words, further discussion analyzes the scenario where members demand access only to college networks and not to company networks that external associates belong to.

Due to fact that AAI@EduHr infrastructure only allows academic members to access network, non - academic members, hence associates, would not be able to access college resources. In order to understand proposed solutions, it is first necessary to explain how AAI@EduHr functions.

In AAI@EduHr every academic member is given his user name and password by his home AAI institution. These credentials allow him to authenticate himself on the network and to gain authorization rights. User name is a special identification mark formed in the way that AAI@EduHr proscribes as:

user_ID@home_institution_ID.country_code

User_ID represents user's unique identification name within his home database, *home_institution_ID* determines the AAI@EduHr institution that user belongs to while *country_code* specifies the country, e.g. *hr* for Croatia.

On every institution within AAI@EduHr there is local RADIUS server set together adjoint LDAP directory which it uses to authenticate local users and to read their access rights. Once the user submits request to access institution

[2] Only scientific and higher education institutions are allowed to register according to AAI@EduHr Organization Rulebook.

network that is not his home one, local RADIUS server reads *home_institution_ID* part of the user name realm which tells it that the user is not in his local database (because he belongs to other institution) and that authentication must be taken to user's home RADIUS server. RADIUS packet is then send to root/top RADIUS server in charge for *country_code* domain. Root RADIUS server acts as proxy which knows how to reach user's home RADIUS server which he sends/proxies packet to. User's home RADIUS server receives the RADIUS Access Request message, checks the user against the data stored in his local LDAP directory and sends the answer back the same way as it was received - over root RADIUS proxy. If accepted, that message also contains the list of user's authorization rights read from LDAP which will be used to make access decision on the originating network. Process is illustrated on Fig. 3.

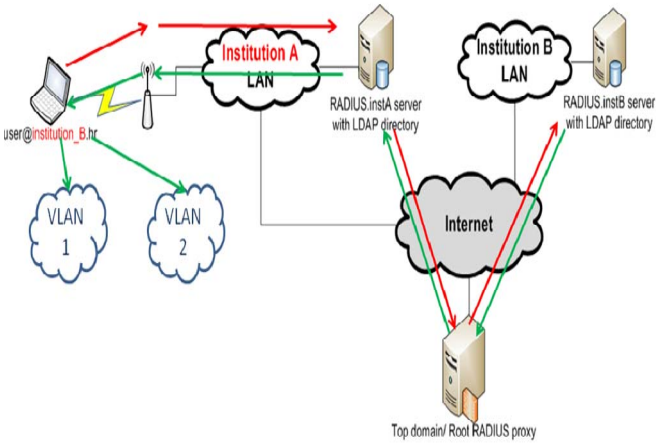

Fig.3. Authentication and authorization in AAI@EduHr

In case that non-academic members demand network access, problem would be that users have no identity anywhere within AAI@EduHr. Solution for that might be in creating their identity on colleges they cooperate with by entering them into LDAP directories. But this solution entails few problems. First of all, temporarily adjoint members would have to receive an attribute that marks them as external associates, i.e. as outsiders and by that they would become separated from the rest of academic community. For now, AAI@EduHr does not provide that kind of attributes. Furthermore, it is important to ensure and to regulate a voucher for those members meaning that system must somehow mark the person responsible for that particular associates entered into the system. That also requires new attributes. Assuming that in a year, there are several distributed projects on colleges, ongoing adding and removal of adjoint associates becomes extremely impractical. It becomes also impracticable due to fact that mostly just one or two persons are responsible and authorized to manage LDAP directory, so needing them to process and manage so many associates would be a problem. Another reason lies in rigorous security policy that demands high level of authorization for entering certain data so the pledge for the non-academic member would not be easily feasible.

Due to above stated reasons, solution for the AA problem is further explored. One possible solution would be to delegate the AA request of external members to their home company servers which would be a consistent solution with the one that exists in AAI@EduHr - that is, users are being authenticated at their home institutions. In order to accomplish this procedure, RADIUS server at the institution on which network access is demanded, should be configured to send every non-AAI@EduHr traffic somewhere else in the network and not to root RADIUS server. That is, if the user is *user1@company1.country_code* then send that request to Company1's RADIUS server or if the user is *user2@company2.country_code* then send it to Company2's RADIUS server. But doing so, there would still remain the necessity to access local RADIUS configuration for every single extern associate in order to tell the server where to send those kinds of RADIUS requests and also how to process the incoming RADIUS replies. Furthermore, this would also require the external queried server to undergo the similar configuration changes.

In order to avoid any short-termed changes made to local RADIUS server or its database, an additional RADIUS server could be set up and connected to the main RADIUS server of local institution network (refer to Fig. 4). New server would be subordinated to the main one. The reason for introducing this server is that it could be more often and quite easier accessed and reconfigured for the project purposes.

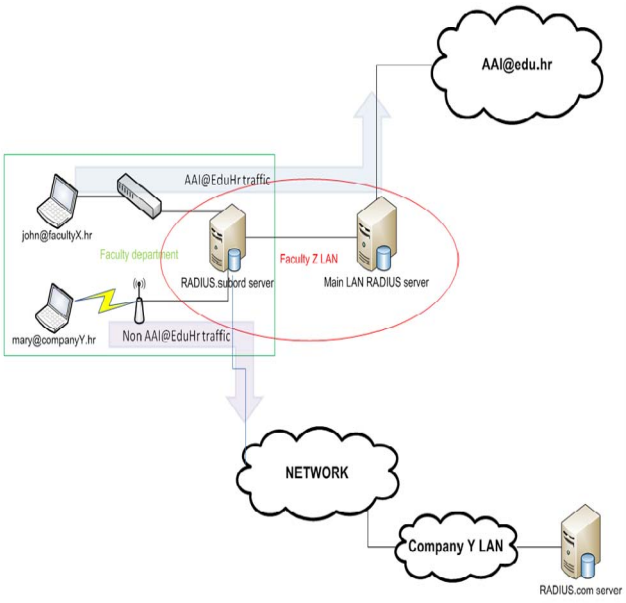

Fig.4. AA schema with main and subordinated RADIUS servers

The AA mechanism for AAI@EduHr registered users would be to send their access request to main RADIUS server which would handle the AA process further as previously explained. For all the other users, the options would be either to enter them locally in auxiliary RADIUS

LDAP directory or to configure subordinated server to send those request in the network. Finally, main RADIUS server must be configured to grant access to network for all users that were successfully authenticated and authorized by subordinated RADIUS servers.

If every institution department sets up its own RADIUS server, it would mean that the total amount of inputs and changes made to one server or its database would be less than inputs that would have to be made on one main RAIDUS server for the whole institution. Also the changes made to main RADIUS server would be smaller and more permanent since it they would involve handling requests from few specified subordinated servers.

This solution, however, brings up one major security issue and that is, main RAIDUS server would have to grant access on blind for the external user which is huge security risk and most probably would be rejected by those in charge for institution network security.

B. Authorization atribute inconsistency among foreign AAI participants

As mentioned before, AAI@EduHr is connected with similar national AAI systems in Europe and in the world. AAI@EduHr is part of pan-European roaming system known as eduroam (http://www.eduroam.org) and is connected with eduGAIN system also. In having case that distributed project members come from different countries which belong to one of those systems, the authentication process will take steps as explained before - through national RADIUS proxies, but the problem here lies within uncoordinated attributes on international level. In AAI@EduHr, attributes that clearly separate students from professors do not exist - students are only recognized by the expiry date of their study. This would mean, for example, that the student from Norway and professor from France would be authorized with the same rights on faculty in Croatia - they would be granted the access to network resources in the way that is settled for that kind of users (users that can authenticate but whose authorization attributes are not interpretable).

All together, the amount of administrational and technical management together with changes that security policy would require is too big for the activities which are perhaps not so intensive and ongoing for the institutions that is distributed projects. Having distributed project activities with members outside academic domain could not be easily managed within AAI@EduHr unless the infrastructure is reorganized. Thereby AAI@EduHr does not offer flexible, scalable and uniform solution that supports stated requirements of distributed teams in case they consist of foreign members or external associates from commercial domain.

C. Reorganizing AAI@EduHr infrastrucutre

Solution to mixed distributed teams could be in setting AAI@*new_domain*.country_code where *new_domain* part of realm could be commercial, government, industrial, etc. This would mean that project participants could be a part of different domains in which they would have their electronic identity and the root RADIUS server would have to know how to reach every domain with home RADIUS servers on it. In other words, it is evident that on the highest level there should be a mechanism able to resolute participants coming from different domain and to route AA traffic upon that.

In next section, a new solution for distributed project teams apart from AAI@EduHr will be suggested.

VI. Overlaying on existing communication infrastructures

Although the existing national infrastructure could not be generally used for distributed projects, basic principles upon which AAI@EduHr resides could be the starting point in suggesting new approaches. This would mean next:

1. On every remote location or institution whose members are part of distributed project team, a RADIUS server should be placed with its corresponding database.
2. All RADIUS servers are connected with each other or they are connected to main RADIUS proxy which knows how to reach every other one.
3. Users are being authenticated by their home institution with the transfer of authorization rights to the network on which they ask for access.

In other to provide AA for the user, it is necessary that RADIUS packet reaches RADIUS server on remote location. But since the RADIUS server is in this case a part of college or company network, it is most likely protected with strong firewall protection which would deny passage of the packet inside the network to the server. One solution to this problem would be to drill a hole in the firewall but in most cases such action would not be feasible due to strong security policies conducted in companies and institutions. Thereby a new approach should be found, one that offers sure passage through firewall in order to reach the server behind it. SOAP protocol offers that solution.

SOAP protocol (Simple Object Access Protocol) is application level protocol used for the exchange of XML messages between applications on remote computers. Its most often use is for RPCs (Remote Procedure Call). Present Internet is full with proxies and firewalls which allow only HTTP based traffic. By putting SOAP above HTTP in network architecture, SOAP messages are encapsulated into HTTP payload and SOAP packets can easily travel through every network that allows HTTP, mostly what all do. Other advantages of using SOAP are its invariance from platforms, operating system and programming language in which the application that uses it is written. These properties reside on XML that is used as the formatting language. Any program interprets SOAP could be used to connect with SOAP. SOAP protocol is described in RFC 3288.

SOAP message (refer to Fig. 5) consists of few parts:

- **Envelope** that is obligatory since it identifies XML document as SOAP message. It uses xmlns:soap namespace and it always has the value set to http://www.w3.org/2001/12/soap-envelope. The required

SOAP Envelope element is the root element of a SOAP message.

- **Header** that is dispensable and which carries information regarding the intendancy of the message, transfer identifier and message originator and receiver data. The optional SOAP Header element contains application-specific information (like authentication, payment, etc) about the SOAP message.
- **Message body** that is obligatory and that contains the actual SOAP message intended for the ultimate endpoint. Immediate child elements of the SOAP Body element may be namespace-qualified. It carries tags that are defined by the calling method. This part of SOAP message also carries information about errors that have occurred. The SOAP Fault element holds errors and status information for a SOAP message.

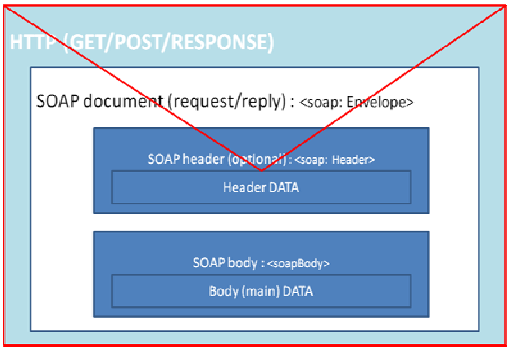

Fig. 5. SOAP message

Since SOAP protocol would be used for carrying confidential data, i.e. user credentials, throughout network, security issues must be address. User credentials (user name and password must) be protected during the transfer. SOAP header gives flexible space to expand SOAP message in respect to security mechanism that might be incorporated. Although RFC 3288 does not address these issues, according to [5], SOAP header could be supplemented with these elements: encryption elements, digital signing elements and authorization elements.

W3C recommends the use of SecTags (Security Tags) as part of unique name space with the URI designation http://schemas.xmlsoap.org/soap/security/. There for, three security tags related to above suggested header additions would be <Encryption>, <Signature> and <Authorization>.

VII. Suggested solution

The authentication process that uses SOAP suggestions could take the following steps:

1. When accessing the network, the user is being authenticated against the local database. In case the user is not on his home network, RADIUS server delegates authentication of user to his home institution RADIUS server which has him stored in its local database.

2. In order to achieve this, RADIUS server passes user credentials to some external program placed on the same server. That program is able to generate SOAP message with user credentials and send it over HTTP through network towards RADIUS proxy or directly to addressed RADIUS server. Home institution/network could be read out from user name in a way similar or the same that exists with AAI@EduHr (user_ID@institution_ID.country_code).

3. When addressed network server receives HTTP packet, it decapsulates the packet, gets user information and authenticates the user against its local database. The result of authentication along with user authorization rights are send back to originator. The answer is sent back also as SOAP (over HTTP protocol) in order to pass through firewall on originator side.

4. The same program that has sent SOAP access request packet across the network, waits for the answer. Upon receiving SOAP access reply packet, it reads the result and pass it back to RADIUS server which instructs network access server whether to grant or deny access to user.

Hence, on every network there should be local RADIUS server that is able to communicate with external program in order to accomplish the AA requirements. That external program would take the user credentials from RADIUS server, generate SOAP message and send it across the network and wait for answer. Upon receiving the answer, it should be able to decapsulate the packet and retrieve the answer which would subsequently pass over to RADIUS server telling the server whether the user has been successfully authenticated or not.

The whole procedure is illustrated in Fig. 6.

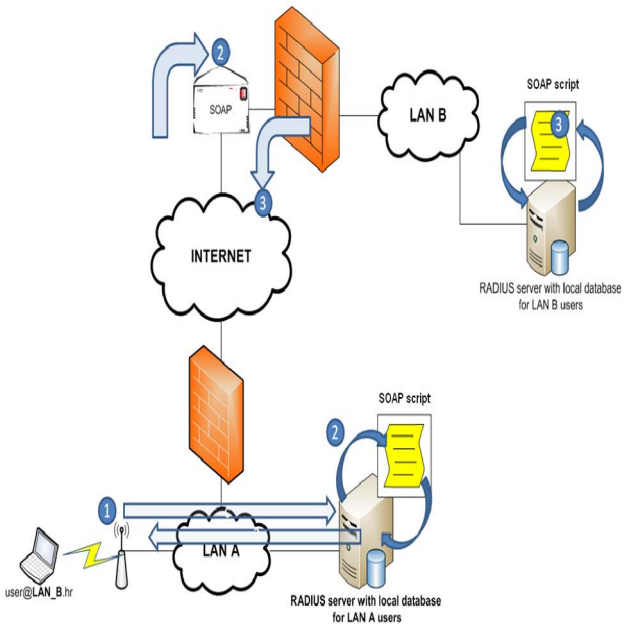

Fig. 6. AA over RADIUS server and external server-side program

VIII. Conclusion

When it comes to providing distributed project members with an access to network which they do not administratively belong to, existing solutions such as AAI@EduHr or eduroam and eduGAIN academic infrastructures do not meet the necessary requirements. This regards authentication of non-academic members that, for example, may be associates on the project from commercial network domain as it regards attribute inconsistencies present on international level in the process of authenticating foreign members. Nevertheless, AAI@EduHr and eduroam are promising foundation for new solutions. An upgrade would be required which would involve the forming of new domains such as commercial, industrial, government besides the current academic one. In such a scenario all root RADIUS servers would know how to reach every domain with home RADIUS servers on it for AA requests. Another approach to the problem would be to set up RADIUS servers on each network location of involved project participants where the server would communicate with the external program placed on the server in order to authenticate and authorize users over SOAP protocol. SOAP protocol offers assured package transfer through network firewalls and its advantages include its invariance from platforms, operating system and programming language in which the application that uses it is written. Since the user credentials are carried in SOAP message across the network and represent confidential data that must be secured, SOAP security tags offer extensible mean of protecting the message under way. SOAP protocol provides complete transparency and integration without the need to change security policy of the infrastructure upon which it resides.

REFERENCES

[1.] Miroslav M., Regulation book AAI@EduHr, June 11th 2008, *Pravilnik o ustroju autentikacijske i autorizacijske infrastructure znanosti i visokog obrazovanja u Republici Hrvatskoj - AAI@EduHr*, http://www.aaiedu.hr/docs/AAI@EduHr-pravilnik-ver1.3.1.pdf, January 28th 2010.

[2.] Eduroam, http://www.eduroam.org/, , January 28th 2010

[3.] Group of authors by IETF,RFC 2865, July 28th 2006, *Remote Authentication Dial In User Service (RADIUS)*, http://www.ietf.org/rfc/rfc2865.txt, January 30th 2010.

[4.] Wikipedia, RADIUS, March 27th 2009, http://en.wikipedia.org/wiki/RADIUS, January 30th 2010.

[5.] Satoshi H. and Hiroshi M., SOAP Security Extensions, November 8th 2000, http://www.trl.ibm.com/projects/xml/soap/wp/wp.html, Februrary 5th