



DEGREE PROJECT IN COMPUTER SCIENCE AND ENGINEERING,
SECOND CYCLE, 30 CREDITS

STOCKHOLM, SWEDEN 2017

Design of a Federated Framework for Emergency Response

QASIM SARFRAZ

Examiner: Prof. Hannu Tenhunen

Supervisor: Prof. Björn Pehrson

MASTER IN SOFTWARE ENGINEERING OF

DISTRIBUTED SYSTEMS



**KTH ROYAL INSTITUTE OF TECHNOLOGY
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY**

Table of Contents

Table of Contents	2
Tables of Figures.....	5
Table of Abbreviations	6
Acknowledgments	8
Abstract	9
Chapter 1	10
Introduction	10
1. Motivation	10
2. Objective.....	10
3. Research Methodology.....	11
4. Contribution	11
5. Personal Motivation.....	11
6. Organization of this Thesis	12
Chapter 2	13
Stakeholders in Emergency Communication Services.....	13
1. Amateur Radio (AR)	13
2. Amateur Radio Operators (ARO).....	13
3. Role of ARO in Disaster	13
4. Stakeholders in Emergency Communication Services in Sweden	13
2.4.1 AMPRNet Sweden [www.amprnet.se]	14
2.4.2 Föreningen Sveriges Sändareamatörer [www.ssa.se]	15
2.4.3 Frivilliga Radioorganisationen [www.fro.se]	15
2.4.4 Local Radio Amateur Associations	15
2.4.5 Frivilliga Resursgrupperna [www.civil.se/frg/]	15
2.4.6 Microbit [www.microbit.se].....	16
5. User Group involved in Testing the Demonstration	16
6. User needs and Requirements	17
Chapter 3	18
Basics of Identity Management	18
1. Identity Management	18
2. Identity Provider (IdP).....	19

3.2.1	OpenID	20
3.2.2	Single Sign on (SSO)	21
3.2.3	Security Assertion Markup Language (SAML)	21
3.	Identity Federation (IdF)	22
4.	EduGAIN	23
3.4.1	How EduGain Works.....	23
5.	Identity Management System	24
6.	Discovery Service	25
7.	Authentication.....	25
8.	Web Authentication.....	26
3.8.1	Password-Based Authentication.....	26
3.8.2	Single Sign On, Authentication.....	27
3.8.3	Certificate-Based Authentication	29
3.8.4	Secure Socket Layer (SSL).....	33
9.	Authorization.....	33
3.9.1	Defining Authorization Groups	34
3.9.2	Defining ACL Matrix.....	35
10.	Service Provider (SP)	36
Chapter 4		38
Design and Implementation of Proposed Framework		38
1.	Design	38
4.1.1	AMPRemote: Secure remote operation/login to selected equipment	38
4.1.2	Device Used in Project.....	39
4.1.3	Framework Architecture	40
4.1.4	Authentication Mechanism.....	40
4.1.5	Authorization Mechanism.....	41
4.1.6	User Cases.....	41
2.	Implementation.....	42
4.2.1	Prerequisites	42
4.2.2	Identity Provider (AMPRID).....	43
4.2.3	Setup an Identity Federation for Emergency Response Organizations	43

4.2.4	Service Provider (AMPRemote)	44
4.2.5	Technologies	44
4.2.6	Architecture	45
4.2.7	Database	45
4.2.8	AMPRemote Usability Screenshots	46
4.2.8.11	Change	51
Chapter 5		53
Evaluation		53
1.	Comparison between Basic, Certificate and OAuh (AAI) Authentication and Authorization Infrastructures	54
Chapter 6		55
Conclusion and Future Work		55
1.	Future Work	55
References		56
Appendix 1: Installation of SSA Identity Provider (AMPRID)		61
1.	Get Ansible.....	61
2.	Clone or Download DevOps Repository	61
3.	Configure Host Inventory.....	62
4.	Configure Bootstrap	62
5.	Configure ldap-idp.yml / mysql-idp.yml.....	63
6.	Run the commands on Ansible	64
7.	Get SSL Certificate	64
8.	Configure IP Table	64
9.	Configure Attributes Resolver	64
10.	Configure Attribute Filter	65
11.	Configure IdP Properties	66
12.	Configure MySQL JDBC for Shibboleth IdP.....	66
13.	Configure JAAS DB Authenticator	66
14.	Customize Views.....	66
15.	Run Build.h.....	66
16.	Tomcat Configuration	67
17.	Joining IdP Federation.....	67

Appendix 2: Installation of SSA Service Provider (AMPRemote).....	68
1. Installation.....	68
2. SP Configuration.....	69

Tables of Figures

Figure 1: Earthquake in Pakistan [8].....	12
Figure 2: Missing people in earthquake [9]	12
Figure 3: SAML token example [31].....	19
Figure 4: Identity Provider (IdP).....	20
Figure 5: OpenID Model	20
Figure 6: Single Sign On.....	21
Figure 7 SAML Model	22
Figure 8: Identity Federation (IdF).....	22
Figure 9: EduGAIN [43].....	24
Figure 10: Identity Management.....	25
Figure 11: Basic Authentication Dialog	26
Figure 12: Custom Made Login.....	27
Figure 13: SSO Architecture	27
Figure 14: Apache server configuration file.....	28
Figure 15: Information Provided to SP	28
Figure 16: Trusted CA.....	30
Figure 17: Certificate Expiry.....	30
Figure 18: OSCP	31
Figure 19: Certificate Possession	32
Figure 20: Secure Socket Layer (SSL)	33
Figure 21: ACL or Authorization Control	34
Figure 22: Service Provider (SP).....	37
Figure 23: Sketch of AMPRemote.....	38
Figure 24: RRC-1258Mklls Setup [58].....	39
Figure 25: RRC-1258Mklls [25]	40
Figure 26: Proposed Framework Architecture.....	40
Figure 27: Authentication Sequence Diagram	40
Figure 28: Authorization Sequence Diagram	41
Figure 29: User A user login, change password and profile use case diagram.....	41
Figure 30: User B login, add and publish device use case diagram	41

Figure 31: User A check and send request for device usage use case diagram.....	42
Figure 32: User B check, approve or reject requests user case diagram	42
Figure 33; SP Architecture	45
Figure 34: Database Model.....	45
Figure 35; GrIDP Login Page.....	46
Figure 36: AMPRemote Login Page	46
Figure 37: Shibboleth Attribute Information	47
Figure 38: Home Page AMPRemote	48
Figure 39: My Owned devices.....	48
Figure 40: All Device Page	49
Figure 41: Request a device	49
Figure 42: Requests Page	49
Figure 43: Requested devices	50
Figure 44: Assigned to me devices	50
Figure 45: Assigned to others devices.....	50
Figure 46: Change Password.....	51
Figure 47: My Profile	51
Figure 48: Admin user management.....	52
Figure 49: Email sent to owner of device.....	52
Figure 50: Email sent to requester of the devices	52
Figure 51: AAROC/DevOps	62
Figure 52: GrIDP [28].....	67

Table of Abbreviations

AAIs	Authentication and Authorization Infrastructures
ACL	Access Control List
CA	Certificate Authority
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSS	Cascading Style Sheet
GrIDP	Grid Identity Pool
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IdF	Identity Federation
IdP	Identity Provider
IIS	Internet Information Services

JAAS	Java Authentication and Authorization Service
LDAP	Lightweight Directory Access Protocol
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SCIM	System for Cross-domain Identity Management
ShibD	Shibboleth Daemon
SP	Service Provider
SSA	Swedish Amateur Radio Society / Föreningen Sveriges Sändare Amatörer
SSL	Secure Socket Layer
SSO	Single Sign On
SSTC	Security Services Technical Committee
STS	Amateur Radio Operators
STS	Security Provider Service
SUNET	Swedish University Computer Network
SWAMID	Swedish Academic Identity Federation
WS-Federation	Web Service Federation
WWW	World Wide Web

Acknowledgments

This piece of work (research and implementation) is the result of thesis for my master degree in **Software Engineering of Distributed Systems (SEDS)** at **Royal Institute of Technology (KTH)** carried out for **Föreningen Sveriges Sändareamatörer (SSA)** and **AMPRNet**.

I am very thankful to **Prof. Björn Pehrson** who supervised me throughout the process and as well as examiner **Prof. Hannu Tenhunen** for giving me this chance to complete my master thesis.

I am also thankful to **Prof. Roberto Barbera**, **Dr. Bruce Becker**, **Mr. Marco Fargetta**, and **Mr. Awet Yamane** for their support and time.

I also acknowledge the courtesy of **SSA** to provide us with a special edition of the SSA Callbook.

And last but not the least my beloved wife **Selin** who made things easy for me during this process.

Qasim Sarfraz
2017-05-18

Abstract

This is a feasibility study exploring the potential of using advanced e-infrastructure mechanisms for federated identity management and service provisioning to support multi-organizational emergency response efforts. The mechanisms explored are primarily similar to the EduGAIN services developed and used by the national and regional research and education network communities with the objective to support international research collaboration. Such a service called AMPRemote has been developed and demonstrated is a service supporting radio amateurs to request access to remote HF-stations owned by other radio amateurs and the owners to grant access without sharing any sensitive information in a very secure environment. This could, for example, be useful in extraordinary situations when normal communication infrastructures are failing. The thesis includes needs and requirement analysis for a small core group of organizations involved in emergency response and a proposal for the design of a general emergency response management framework. The thesis also documents prototype implementations of an identity provider (AMPRID) and an experimental service (AMPRemote) used as a conceptual demonstration involving authentication and authorization of licensed amateur radio operators to access and operate radio transmission equipment requiring a license. The conclusions are positive and the primary stakeholders are using the results and recommendations for further development of other services based on this study.

Chapter 1

Introduction

This chapter will give you general overview of the thesis report, starting with the motivation behind this thesis work following by core objectives, research methodology used, and finally organizational flow of this thesis report.

1. Motivation

The organizations involved in emergency response are facing dynamic challenges during the time of emergency as well as during the normal practice sessions. One of the main challenge is coordination and collaboration of activities in multi-organizational emergency response, both internal and external level. Most of them are not aware of benefits of advanced e-infrastructure mechanisms. Those who are known the potential of using it, are not aware of security threats involved in e-infrastructure [1]. This is a feasibility study exploring the potential of using advanced e-infrastructure mechanisms for federated identity management and service provisioning to support multi-organizational emergency response efforts.

2. Objective

The general objective of this work is to explore the potential of using advanced e-infrastructure mechanisms to support multi-organizational emergency response efforts. An e-infrastructure includes computing and communication resources as well as data structures and collaboration tools supporting the stakeholders using it [1].

This study has been conducted in close cooperation with a small group of stakeholders involved in emergency response efforts. The study was suggested by one of the core stakeholders to support the development of a state of the art network exploiting advanced e-infrastructure mechanisms tailored to the use of network for emergency communication services. The stakeholders will be described in some detail in chapter 2.

The specific objectives/challenges include:

- Creating awareness among the stakeholders by initiating a needs and requirement analysis and demonstrating the potential of e-infrastructure technologies.
- Completing a first cycle of iterative systems design of an information system for multi-organizational collaborative emergency response efforts.
- Providing a recommendation for security solutions.

The mechanisms explored are primarily the EduGAIN [2] services offering a framework for federated identity management and service provisioning. EduGAIN is developed and used by the national and regional research and education network communities with the objective to support international research collaboration. The reasons for selecting this focus will be explained in the stakeholder analysis.

3. Research Methodology

The methodology used in the study is iterative systems design starting with a needs analysis as the basis for formulating system requirements for the systems design and implementation phase, followed by testing and evaluation and finally review and refinement of the needs and requirements for a next iteration until end-users and system developers agree that the needs are met. Meeting the needs of the end-users is the most important concern.

It is a well-documented truth that end-users in general have a hard time formulating needs of products or services that they know little about [3]. It is also well documented that development of new products or services can fail utterly due to developer's ignorance about user needs [4]. The introduction of new products and services have to be a dialogue between developers and users, especially when introducing systems that have the potential to affect legacy working procedures. This is part of the background for this study, to acquire a real-life experience of iterative systems design methods to get end-users involved in the design process. In this particular case, some of the stakeholders were aware of from the start that they need to strengthen their use of information and communication technologies beyond the walkie-talkie level that is currently the predominant tool used.

Since each iteration takes time, only one complete major iteration has been possible to accommodate within the time frame of this thesis project.

4. Contribution

The focus of this thesis project is the needs and requirements analysis and the design and implementation of an identity provider (IdP) [5] together with a simple sample service provider (SP) [6] for the involved stakeholder group.

The main contribution is the demonstration of how to provide a secure and efficient collaboration framework for organizations involved in emergency response efforts using a simple service selected by the stakeholders. The analysis includes proposals and recommendations guiding the end-users and the manufacturer of the devices used in this thesis project. The thesis also documents prototype implementations of an identity provider (AMPRID) and an experimental service (AMPRemote) used as a conceptual demonstration involving authentication and authorization of licensed amateur radio operators to access and operate radio transmission equipment requiring a license.

5. Personal Motivation

I have some personal motivation with this thesis project since my homeland Pakistan had been one of the victim of natural disasters (earthquake, flood and tsunami) quite many times. In

October 8, 2015, one of the recent biggest earthquake of the Pakistan's history had been occurred which has caused death over 100,000 people, approximately 138,000 people had been injured and over 3.5 million had rendered homeless. [7] This project gave me insight into the challenges faced by amateur radio domain in emergency response.



Figure 1: Earthquake in Pakistan [8]



Figure 2: Missing people in earthquake [9]

6. Organization of this Thesis

In chapter 2 we start with a stakeholder analysis and discuss the needs and requirement analysis for multi-party emergency response. Chapter 3 reviews terminologies and technologies used in our proposed system and puts the study into a larger context before focusing on the specific topic: how a federated environment like EduGAIN can be exploited for emergency management by facilitating sharing of resources and services between cooperating organizations. Chapter 4 contains the proposal for the design of a general emergency management framework together with an overview of the implementation and testing of the demonstration, while the implementation details are left to the appendices 1 and 2. Chapter 5 contains an evaluation of the demonstration while conclusions and future work are discussed in Chapter 6.

Chapter 2

Stakeholders in Emergency Communication Services

This chapter will highlight the stakeholders in emergency response services including organizations and manufacturers of the equipment used by these organizations. This chapter also sheds light on the users group involved in testing the demonstration and their needs and requirements.

1. Amateur Radio (AR)

Amateur radio is common radio broadcasting equipment but used by non-commercial amateur radio operators. It has many significant usages in science, industry and emergencies services. Research in amateur radio field resulted in many innovations in industry which really helped to improve economy, technology and saved many lives. Research and development (R&D) environment we get with amateur radio often not predicable in the labs. [10]

2. Amateur Radio Operators (ARO)

Amateur Radio Operators (ARO) are operators who operate their radios locally mostly licensed by the non-profit national organizations. They operate their radio in emergency and for non-commercial use to help emergency services and for the benefit of people affected by some disaster. During the disaster or emergencies ARO transmit messages to other amateur stations, these transmissions are not required any special permission from Federal Communication Commission (FCC). Many ARO do collaboration via communication groups devised by ARO. It may also allow to transmit messages by unlicensed individuals on behalf of licensed amateur radio operator. [11] Many ARO join local public amateur radio organizations as a volunteer. Those organizations help them to arrange meetings, drills, setup networks and other needed resources like documentation to transfer their equipment between countries.

3. Role of ARO in Disaster

During the disaster ARO operate their network for communication to provide assistance emergency services as well as private people affected by the disaster. In disaster, it is very common power outages and destruction of common communication infrastructure like telephone, cellular network and other dependent system like internet. [12]

4. Stakeholders in Emergency Communication Services in Sweden

In Sweden, each organization and each individual has a responsibility to act in emergency situations in order to save lives and property. On the national level, the authority assigned the default responsibility for issues concerning civil protection, public safety, emergency

management and civil defense in Sweden, as long as no other specific organization is given a dedicated mandate, is the Swedish Civil Contingencies Agency (MSB) [13]. MSB is responsible for identification and analysis of all sorts of risks, including formulation of mitigation strategies as well as contingency planning and operation. Unless this can be delegated to another organization, the 21 government county administrations as well as the 20 regional and 290 local commune administrations all have explicit responsibilities within their jurisdictions, and all have a security officer.

From a cost perspective, it is not reasonable to dimension the administrations to be able to manage all worst-case situation scenarios associated with small risks even if the expected costs are high. Instead, there are emergency plans for such scenarios, including checklists, education/training and exercises. These plans involve volunteers that can be called upon on short notice. There are a number of volunteer organizations with assigned responsibilities to provide trained volunteers with different areas of expertise. Some of the stakeholders in this thesis project are such organizations.

2.4.1 AMPRNet Sweden [[ww.amprnet.se](http://www.amprnet.se)]

AMPRNet Sweden is the core stakeholder in this project as well as the stakeholder suggesting and supporting this work. It is a non-profit association of local radio amateur organizations distributed all over Sweden and coordinates the operation of AMPRNet [14]. The AMPRNet network is a part of Internet based on a substantial IPv4 address space (44.0.0.0/8) allocated for experiments in the global radio amateur community in the infancy of Internet. This address space is managed by the non-profit organization Amateur Radio Digital Communication (ARDC) [15]. AMPRNet Sweden is an association managing and stimulating the use of the Swedish allocation 44.140.0.0/16. This address space is used by licensed Swedish radio amateurs to operate an independent, strictly non-commercial part of Internet. Besides being used for research, development, education and training, AMPRNet is meant to serve society in extraordinary situations when other alternatives are insufficient or non-existing, such as accidents or natural hazards. This objective has led to an agreement with SUNET [16], the Swedish university network, about Internet transit via their points of presence all over Sweden. The AMPRNet Sweden network consists of a number of Internet islands connected to Internet via SUNET. These islands are built using all sorts of links, wired or wireless, the latter mainly using license exempt and amateur radio spectrum. The services provided in the network include a broad range of dedicated radio amateur services as well as of services that are useful for organizations involved in extraordinary situations that may arise.

Although the needs in emergency situations include all sorts of communication, and voice communication via radio might be the single most important, AMPRNet focuses on data communication based on Internet technologies. Voice communication via radio walkie-talkie style without infrastructure as well as with infrastructure in terms of repeaters, seems to be a

well-established and mature traditional strength of the radio amateur community, while data communication in the sense of Internet seems still to have a lot of unexploited potential, beyond interconnection of repeaters for voice communication systems like Echo link [17], Internet Radio Linking Project (IRLP) [18] and others.

The AMPRNet planning process is currently in a needs and requirements analysis phase in which examples of e-infrastructure services need to be developed and discussed with key stakeholders. A few developments projects with the objectives to develop services that are useful in emergency response situations have recently started [19]. One of these projects is a follow up of this thesis project: to create a security framework for collaboration between organizations involved in emergency response based on the same mechanisms that are used in SUNET and other research and education networks.

2.4.2 Föreningen Sveriges Sändareamatörer [www.ssa.se]

SSA [20] organizes individual radio amateurs as well as their local associations. SSA maintains the official database of licensed amateur radio operators, the SSA Callbook [21]. By the courtesy of SSA, this database has been made available for the work described in this thesis to create an Identity Provider (IdP) used to authenticate and authorize individuals to get access to resources requiring such a license.

Many individual radio amateurs are also members of one or more of the organizations mentioned below.

2.4.3 Frivilliga Radioorganisationen [www.fro.se]

FRO [22] organizes training of volunteers in radio communication both for the military and civil defense. FRO has own radio resources that they may want to interconnect via AMPRNet.

2.4.4 Local Radio Amateur Associations

Many, but not all, radio amateurs are members of a local associations or “clubs” managing common resources and organizing a wide spectrum of training courses, including courses for getting an amateur license. Many local radio amateur associations are prepared to participate in emergency situations and also involved in providing communication services during athletic events of different sorts. These organizations are the members of AMPRNet Sweden and many of them actively involved in the development of the AMPRNet network.

2.4.5 Frivilliga Resursgrupperna [www.civil.se/frg/]

The voluntary resource groups are organized by the **Civil Defense organization** [23] to serve the regional and local communes, reporting to their security officer. FRG groups are potential end-users of services provided by AMPRNet.

A needs and requirements analysis for some basic services relevant in a couple of adopted emergency response scenarios is in progress involving twelve communes in the Stockholm region, FRGNORR [24]. Services that have been mentioned in an early phase of the needs analysis include

- Access to information (web access), e.g. documentation, guidelines, maps, etc.
- Voice and text-based cooperation tools, such as VoIP, chat and a ticket management system
- Secure remote operation/login to selected equipment, such as servers, communication infrastructure equipment, etc.
- Form filling, e.g. when recording evacuees in evacuation situations
- Data collection via sensor networks, e.g. weather data or other local environmental data

To facilitate the necessary dialogue between service developers and end-users, a few prototype services are being developed to concretize what is possible [19]

2.4.6 Microbit [www.microbit.se]

Microbit is a telecommunication systems developer/manufacturer producing the Remoterig equipment for remote control of HF radio stations via Internet that was selected by the stakeholders to demonstrate the potential of the services explored in this study [25]. Many radio stations have detachable front panels. Remoterig units are used to connect the front panel to the station via Internet. They are thus used in pairs, one unit at the location of the front panel and one unit at the location of the transceiver, which has to be close to the antenna. Examples of situations in which you want to do this is if the location from where you want to operate the radio does not allow deploying large enough antennas or is too noisy to operate from.

5. User Group involved in Testing the Demonstration

The user group selected for the demonstration includes AMPRid a few licensed amateur radio operators, for the following reasons:

- 1) The group has a strong track record for providing important communication services via radio, mainly voice, in emergency situations where other means of communication are insufficient.
- 2) The group is well defined since there is a maintained digital database available containing all its members SSA Callbook [26].
- 3) The group has access to, and operates, basic e-infrastructure resources, primarily different types of radio communication systems and networks, and to AMPRNet.

While the selected user group has more or less expert knowledge in the area of radio communication, its members are not necessarily knowledgeable in computing, computer communications and e-infrastructure-related technologies.

6. User needs and Requirements

After initial discussions with the stakeholders, it was decided that the analysis initially focus on the general security framework and do a first iteration including a simple service. Several of the prototype services discussed by the stakeholders above will require specific access rights and different sorts of authorization. A basic requirement is thus that users can be authenticated and authorized.

Since emergency management involves several different organizations that need to cooperate regarding information and communication services, a federated approach is proposed. This means that a common framework and common protocols are used by all organizations in the multi-stakeholder environment. Each organization contributes to the identity management by maintaining a database of their members and their authorizations to access services. Identity management thus includes authentication as well as authorization and access control.

A federated approach also means that each organization can act as a service provider (SP) of services they need and also authorize users of other organizations in the federation to use these services.

In order to avoid multiple username/password logins and thereby minimizing the risk for human errors in the security management process as well as the time spent by end-users on formal security management procedures, a single-sign-on concept (SSO) is proposed. SSO means that, once a user is authenticated, access is granted to all entities within the authorization of this user.

In next chapter, we will discuss standards and implementation platforms offering federated identity management, including both authentication, authorization and single sign on access control.

Chapter 3

Basics of Identity Management

In this chapter we will discuss concepts, technologies, and standards used in proposed systems design intended to meet the requirements discussed in the previous chapter. It will help the reader of this report to get deep understanding of core concepts like Identity Management, Identity provider, service provider, identity federation, disjunctive service and authentication and authorization within identity federated systems.

1. Identity Management

The starting point for identity management in a network environment is a digital identity. We will need an identity management system that can manage identities not only of people but also other kind of entities, such as organizations, software and hardware modules, data sets, etc.

A digital identity has to come in a form that facilitates authentication of the entity having that identity. Besides a unique name, the digital identity could include relevant attributes, such as a secret encrypted password or private key for a certificate. In the case of a human person, other relevant attributes could be age, gender, biometric parameters and a portrait, like in a passport.

The digital identity should also include attributes that can be used to specify authorizations given to the entity having that identity. In analogy, when stopped by the police a driving license can be used to prove the identity of the driver and also her/his authority to drive the car, a pilot license to fly an airplane, a radio operator license to operate a radio transmitter, a permission to access a certain sensitive set of protected data, etc.

Digital identities of people are often managed by organizations that have an interest in authenticating a specific group of users in order to provide services to them. It could be an association maintaining a list of members, a company maintaining a list of employees and/or customers, social media, a university having records of their staff, researchers, teachers and students, etc. To facilitate this identity management, the organizations set up an identity provider (IdP), that provides means for authorized parties to update the various attributes associated with an identity and answer queries regarding the authenticity and authority of an entity.

If people from different organizations often cooperate with colleagues at other institutions and they want also to use services provided by the institutions of their colleagues, there is a need for cross-authentication by forming an Identity federation (IdF). A set of organizations decide

to adopt a common policy based on mutual trust, a common technical standard for setting up an IdP and defined trust levels for involved procedures.

The standardization of identity management services and protocols are still in progress [27]. Although there seems to be a convergence, there are in practice several more or less similar solutions being used. Currently most commonly used standards include Security Assertion Markup Language (SAML), OAuth, OpenID Connect/Provider, (System for Cross-domain Identity Management) SCIM and Single Sign on (SSO) [28].

Swedish universities operate an IdP for their own staff and students and are all members of the SWAMID IdF [29]. Details regarding the IdF agreement is available on this [link](#).

AMPRNet Sweden considers the establishment of a similar IdF for members of the network of organizations involved in emergency response [19]. Since AMPRNet can be considered as an access network to SUNET, AMPRID has a bias towards adopting the same technical solutions as SWAMID, which means the solutions that are agreed internationally in EduGAIN.

2. Identity Provider (IdP)

An Identity Provider (IdP) is a system that creates, maintains and manages user's identity by some security token sharing mechanism [5]. It is often called Identity Assertion Provider. It works like an online service used to authenticate users who want to access resources often called Service Providers (SP). SP depend on these tokens to authenticate and authorize the users to use some services. SAML 2.0 [30] is widely used standard as in WS-Federation model IdP is a security provider service (STS). STS is authentication token service which plays significant role in identity management as it is used to authenticate and authorize the user's digital identity. A SAML assertion is a kind of security tokens, example token look like as below.

```
<saml2:Assertion xmlns:saml2="..." xmlns:ds="..." xmlns:xsi="...">
  <saml2:Subject>
    <saml2:NameID>
      ...
    </saml2:NameID>
    <saml2:SubjectConfirmation
      Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">
      <saml2:SubjectConfirmationData
        Address="192.168.0.1"
      </saml2:SubjectConfirmationData>
    </saml2:SubjectConfirmation>
    <saml2:SubjectConfirmation
      Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
      <saml2:SubjectConfirmationData
        xsi:type="saml2:KeyInfoConfirmationDataType">
        <ds:KeyInfo>
          <ds:KeyValue>...</ds:KeyValue>
        </ds:KeyInfo>
      </saml2:SubjectConfirmationData>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
</saml2:Assertion>
```

Figure 3: SAML token example [31]

There are many different IdP standards available as described below. We will be using only SAML.

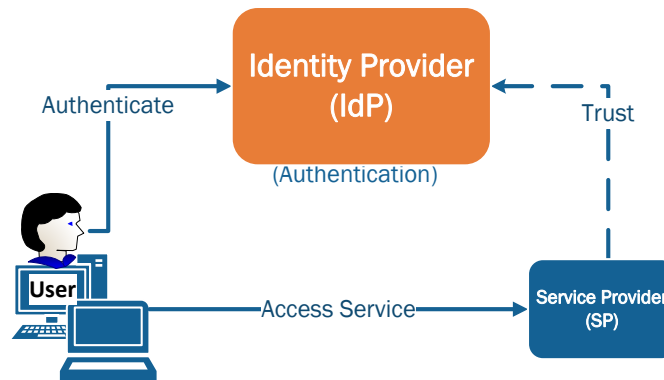


Figure 4: Identity Provider (IdP)

3.2.1 OpenID

OpenID (OID) is an open standard provided by non-profit organization called OpenID Foundation. It is based on decentralized protocol which allows users to authenticate by relying parties (service providers). User does not need to register on multiple sites and can log in on multiple unrelated sites using an existing account. [32] User can choose the information (name, email address or others) to associate with OpenID. Password is only shown to identity provider which confirm user's identity to the service used never sees password. Nobody owns OpenID since it is decentralized and anybody can choose to Many large organizations use an OpenID or become an OpenID provider. [33]

OpenID has been used by over one billion users and over fifty thousand websites worldwide. Many large organizations (including Google, Microsoft, Facebook, and Yahoo) accept OpenID. More details about organizations that use or support OpenID can be found on OpenID Foundation site. [34]

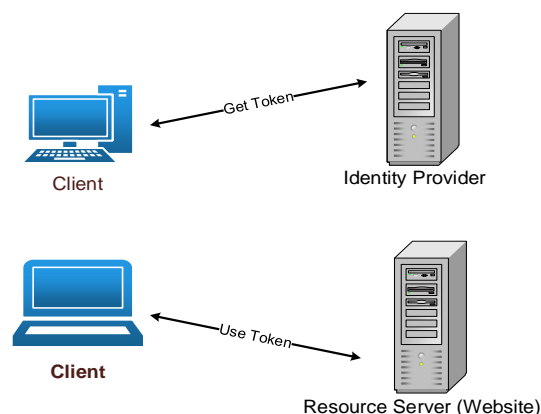


Figure 5: OpenID Model

3.2.2 Single Sign on (SSO)

System users and administrators are often facing complex interfaces when having to sign-in on different system multiple times, sometime with different user names and passwords. To solve the issue the Single Sign On (SSO) concept [35] was developed. The name refers to the idea that users need to authenticate only once to access all resources they are authorized to use. This not only saves time but also reduces the risk for human errors and system failures. [30]

To implement SSO, the Lightweight Directory Access Protocol (LDAP) is used by storing databases on servers. As user does single sign on to multiple systems, they also need to terminate the access on multiple systems. This term is called single sign off.

Single sign on can be configured in different ways [36]. The method adopted by EduGAIN is based on the Security Assertion Markup Language (SAML).

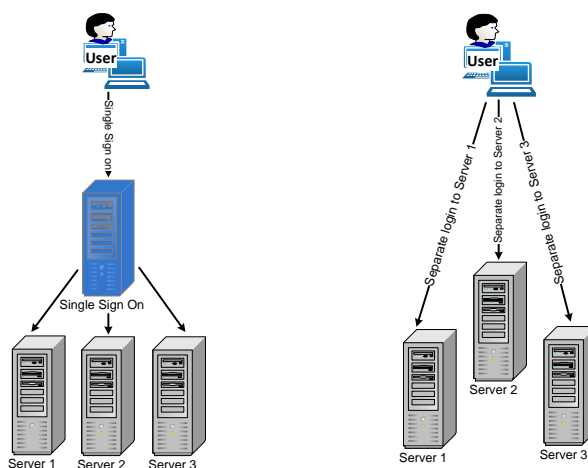


Figure 6: Single Sign On

3.2.3 Security Assertion Markup Language (SAML)

SAML, Security Assertion Markup Language, is an assertion-based framework using the XML data format for exchange of authentication communication between remote parties [37]. SAML is developed and maintained by the Security Services Technical Committee (SSTC) and open standardization consortium under the Organization for the Advancement of Structured Information Standards (OASIS) [38].

There are three parties in the SAML framework: 1) the Remote Party (User), 2) the Identity Provider and 3) the Service Provider, the parties exchange a token depending on the initiation scenario. As the name suggests, SAML allow remote parties to assert the identity, attributes and entitlements. It is flexible and easy to extend the open standard; it can be customized if needed. It includes full support for federated identity management [28].

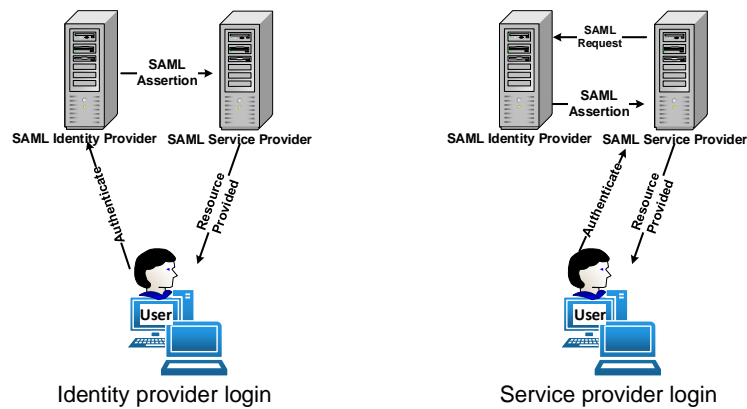


Figure 7 SAML Model

3. Identity Federation (IdF)

A federated identity in information technology is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems. An Identity Federation is form of group consisting of institutions and organizations that sign up to an agreed set of rules for information exchange to enable access to resources. Main purpose of the service is to build authentication and authorization infrastructure for a trusted environment so users can be identified digitally using single identity.

Federated identity management provides the way to manage identities by allowing an identity to establish the links between own identities to use for different services. It deals with user and user data security where user and system are within same network or domain. This approach helps to solve identity management challenges especially in a multi-organization environment [39].

Several technologies have been used for implementing federated identity management systems, including SAML, OAuth, OpenID, Security Tokens (Simple Web Tokens, JSON Web Tokens, and SAML Tokens), Web Service Specifications, Microsoft Azure Cloud Services, and Windows Identity Foundation [40]

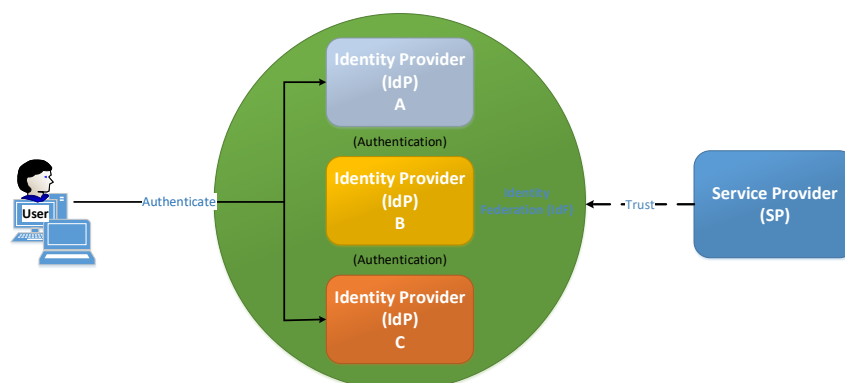


Figure 8: Identity Federation (IdF)

4. EduGAIN

EduGAIN is a service that interconnects several identity federations around the world. The main purpose of this service is to provide easy access to content, services and resources for global research and educational communities. It allows trustworthy exchange of information related to user identity, authentication and authorization via different identity federations infrastructure and provide framework for information to exchange [2].

EduGAIN provides a technical and policy framework to enable the exchange of trusted authentication and identity information across the borders of its member federations. Its goal is to extend the national Single Sign-On (Web SSO) to worldwide Web SSO, primarily for members of the research and education community. Service and Identity Providers, as well as their affiliated users are enabled to access each other's services via their national identity federations [41].

Major features include such as, trustworthy information exchange, improved security and user experience, cost reduction in development and service operations and enable service providers (SP) to expand their user base and identity providers to increase the number of available services to their users.

This service has been developed and provided by GEANT [42]. It is a major collaboration between European national research and education network (NREN) organizations and the European Union (EU). Main feature of EduGAIN is given below [2].

3.4.1 How EduGain Works

As shown in the figure below, EduGAIN interconnects the identity federations (IdF) which are group of institutions and organizations that sign up to an agreed set of policies for exchange of information about users and resources. These organizations use Authentication and Authorization Infrastructures (AAs) to build a trusted environment where users can be identified digitally [2].

The existence of multiple AAs and multiple identity federations makes it technically and administratively difficult when a user attempts to gain access to protected resources and services from other federations. The user must first be successfully authenticated by his/her home AA and then authorized by the visited service provider [2].

EduGAIN enables different AAs to interact securely. EduGAIN technology involves a "Metadata Service", which regularly retrieves and aggregates information from participating federations about services and identity providers, and makes this information available. EduGAIN coordinates necessary elements of the federations' technical infrastructure and provides a policy framework controlling the exchange of this information [2].

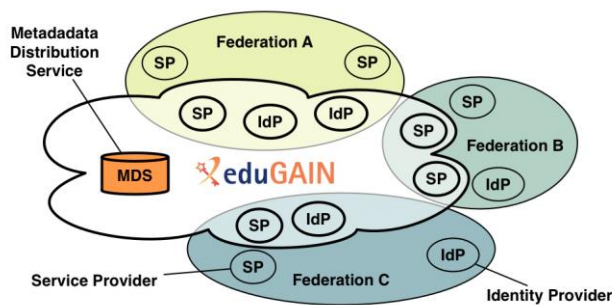


Figure 9: EduGAIN [43]

5. Identity Management System

To implement an identity management system, a number of players are involved. The key players being an Identity Provider (IdP), a service provider (SP) and remote parties of user groups (organizations, businesses or networks).

If the remote parties maintain digital identities for their users, it is often useful for them to agree with third parties on some sort of identification method for secure transaction.

Often it is a choice for the remote party to act as identity provider towards their own service provider. Identity provider (IdP) authenticates and authorizes to their own services. [44]

There is more than one way to accomplish authentication depending on what are the scale remote parties. The scale is usually defined in terms of a stakeholder level; individual, enterprise and government level. These stakeholders are often interested in the development of Identity management tools, systems and standards for effective usage and privacy protection of digital identities.

On the individual level, identities are important to facilitate enhanced and personalized user experience. They are used for social networking, blogging and any cyber networking is using web standard and web services.

On the enterprise level, businesses like Facebook, Google, PayPal, Yahoo and others, realized the need for identity data for their personalized services (advertisement, service offers for 3rd parties). They have adopted an open standard protocol for identity management called OpenID [45].

Government level organizations are usually acting as identity provider (IdP) and policy maker, which is very important for usage and protection of identities. Already major countries like Denmark, France and United Kingdom) started to adopt the SAML standard, Security Assertion Markup Language [30], on the national or local levels for various government services [36].

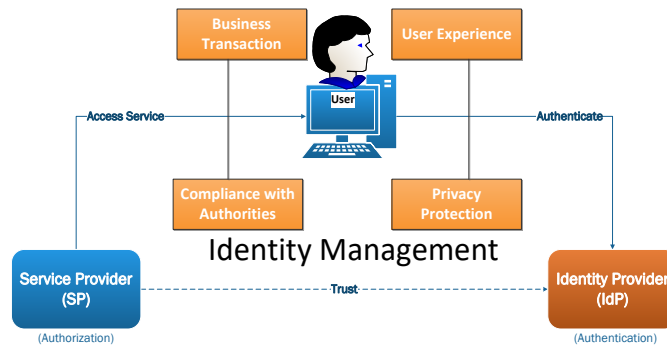


Figure 10: Identity Management

6. Discovery Service

A Discovery Service (DS) is a service that presents a standard interface for users to select their IdP from. A DS presents in some form, highly customizable, a set of identity providers (IdP) from which the user can choose. After the user makes a selection, the DS redirects the user to the SP, which then formulates the Authentication Request based on the user's selection [46].

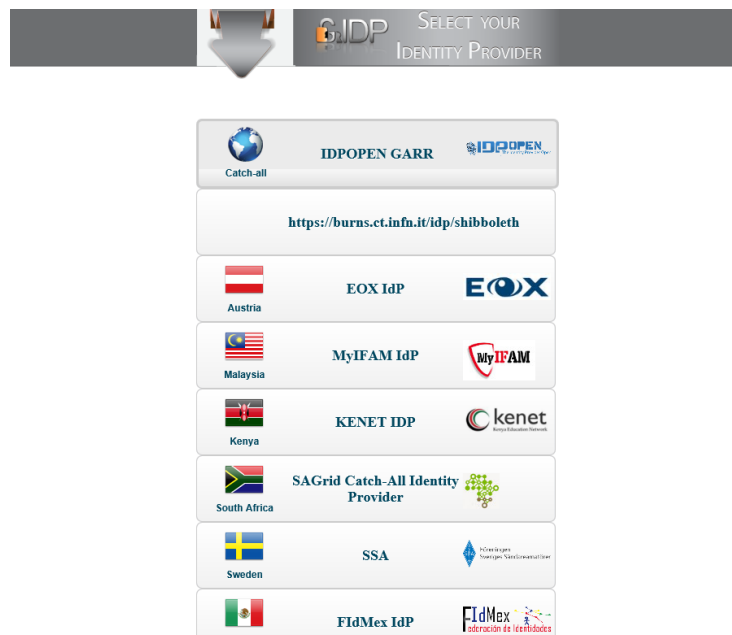


Figure 8: GridP Discover Service Interface

7. Authentication

Authentication is the process in which an individual, entity or service is verified. There are many types of authentication methods for example biometric, web-based and host-based authentication. The scope of this project is limited to web based authentications techniques.

8. Web Authentication

One of the most common and important uses of Internet is web browsing. There are many types of web sites, public and private. To protect private web sites, you need web authentication. Users access web sites via a small set of protocols, the most common being HTTP, which uses unencrypted text in the communication, and HTTPS, which adds a Secure Sockets Layer (SSL), a standard security technology for establishing an encrypted link between a server and a client.

Users send and receive requests via web browsers, such as Chrome, Firefox, Internet Explorer, Safari and others. The response content is rendered in some markup language, HTML, XML, JSON. Private web sites require some type of authentication mechanism to access. The most common web authentication methods are the following.

3.8.1 Password-Based Authentication

3.8.1.1 Basic Authentication

Basic authentication is user-name/password based. The user name and the password are given as input in the web browser and sent unencrypted as base64-encoded text. It is highly recommended to use HTTPS, since HTTP is unsecure and making it easy to capture and reuse the user name and password.

Web servers like Apache [47] and IIS [48] provide support for basic https-based authentication. The webmaster creates and decides the location of the password file. The information about authentication as well the location of password file and restricts the access to the web site content. Users wanting to access protected content via a web-browser are presented an authentication dialogue box as illustrated in figure below.

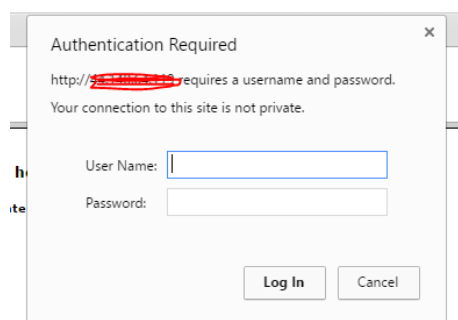


Figure 11: Basic Authentication Dialog

3.8.1.2 Custom Authentication

There are many web application programming languages (ASP.Net, PHP, Java) [49] which support custom authentication based on password by providing mechanism like cookies,

sessions and tokens. Password is usually saved in database in encrypted format. When user provides login's information is matched from database to authenticate the user. Some databases for example MySQL [50] provides customer Password function which is not possible to decrypt. You can create multiple layers of security and use custom made encryption for sensitive data. You can use custom made login interfaces you don't need to depend on browser default login dialog like in basic authentication.

The image shows a web form titled "Login to SSA Service Provider". It contains the following elements:

- A "Username" label above a text input field.
- A "Password" label above a password input field.
- A link "> Need Help?" to the right of the username field.
- A checkbox labeled "Don't Remember Login".
- A checkbox labeled "Clear prior granting of permission for release of your information to this service.".
- A red "Login" button at the bottom.

Figure 12: Custom Made Login

3.8.2 Single Sign On, Authentication

The concept of Single Sign On/Out (SSO) has been explained earlier. The most apparent benefits are user experience, security and resource savings. User can move effectively and securely between services without signing in multiple times as required in conventional login mechanisms. It is very secure as user's credentials are authentication by central SSO server and the actual services accessed by user don't need to store the user credential separately. Resources are also saved and services used by user does not need to have user storage instead relay on SSO server. User must be careful by sign out the session after each use, as once user is initially authenticated it can be misused for many services since SSO is enough for many resources.

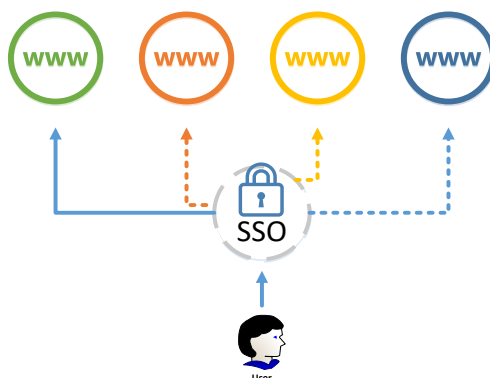


Figure 13: SSO Architecture

3.8.2.1 Implementation

After defining ACL, forcing the ACL is essential step so user can't have any unwanted access. There are many ways of implementation according to the needs of service provider who wants to authenticate and authorize the user on different services. I will just explain only those which are used in this project. We are using Shibboleth Identity Provider [51] which has shared module with Apache web server. To implement the ACL, we have to edit the following configurations tag in Apache site configuration file as shown in the figure below.

```

GNU nano 2.2.6 File: nodefault-ssl.conf
# alert of the client. This is 100% SSL/TLS standard compliant, but in
# practice often causes hanging connections with brain-dead browsers. Use
# this only for browsers where you know that their SSL implementation
# works correctly.
# Notice: Most problems of broken clients are also related to the HTTP
# Keep-alive facility, so you usually additionally want to disable
# Keep-alive for those clients, too. Use variable "nokeepalive" for this.
# Similarly, one has to force some clients to use HTTP/1.0 to workaround
# their broken HTTP/1.1 implementation. Use variables "downgrade-1.0" and
# "force-response-1.0" for this.
BrowserMatch "MSIE [2-6]" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
# MSIE 7 and newer should be able to use keepalive
BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown

<Location /api/>
AuthType shibboleth
ShibRequestSetting requireSession 1
require valid-user
</Location>

<Location /index.php>
AuthType shibboleth
ShibRequestSetting requireSession 1
require valid-user
</Location>

<Location /app/>
AuthType shibboleth

```

Figure 14: Apache server configuration file

3.8.2.2 After logging with SSO user gets information about mapped attributes as you can see in the figure below.

AMPRnet You are about to access the service:
SSA Service Provider of SSA
Description as provided by this service:
This service

Information to be Provided to Service	
eduPersonPrincipalName	qasims@sa0bxi.se
givenName	Qasim
groupName	Admin
mail	qasims@live.se
surname	Sarfraz
uid	qasims

The information above would be shared with the service if you proceed. Do you agree to release this information to the service every time you access it?

Select an information release consent duration:

Ask me again at next login
• I agree to send my information this time.

Ask me again if information to be provided to this service changes
• I agree that the same information will be sent automatically to this service in the future.

Do not ask me again
• I agree that **all** of my information will be released to **any** service.

This setting can be revoked at any time with the checkbox on the login page.

Figure 15: Information Provided to SP

3.8.2.3 Authentication Configuration Options in Shibboleth Identity Provider

Enabling the Module for Specific Content

```
<Location /private>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  Require valid-user
</Location>
```

Exclude a directory from authentication

```
<Location /public>
  AuthType Shibboleth
  ShibRequestSetting requireSession false
  Require shibboleth
</Location>
```

Enabling the Module Globally (Overrides other Authentication Rules)

```
<Location />
  AuthType shibboleth
  Require shibboleth
</Location>
```

3.8.3 Certificate-Based Authentication

Unlike in password-based authentication, you do not need a password when using certificate-based authentication. You rather use a certificate to authenticate in this method. It is more appropriate for more general Internet use. For a user who is making an Internet payment transaction, it is very important to know if the remote site is authentic or if the user risks exposing credit card information to an unwanted party. A public key certificate is the solution which provides a scalable and convenient mechanism for authentication issued by Certificate Authorities (CAs). Certificate based authentication is also used for non-Web services for example when connecting to remote devices and for electronic mail messages. A certificate is an association between an identity and a cryptographic key which consists of two pairs: a public key and a private key. As the names are suggesting, a public key can be distributed freely while the private key has to be kept secret. Most of the famous browsers (Internet Explorer, Chrome, Firefox) are installed with a collection of certificates that do not need to be validated if the certificate is from an authorized Certificate Authority (CA), such as VeriSign [52] or Comodo [53]. The most general form of rules and policies to validate certificates is called a Public Key Infrastructure (PKI) [54].

When your certificate needs to be authenticated, an authentication server will check the following:

3.8.3.1 Is certificate issue by a trusted CA?

The signing of certificate has two parts: First it must be signed correctly, otherwise it will be discarded. Secondly, the public key of the CA must be trusted for the purpose of authentication, otherwise it will be rejected. As you can see in the figure below, the certificate shown is signed correctly and issued for a specific domain, which ensures the identity of server.

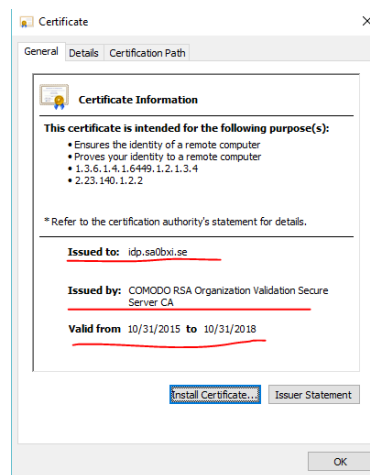


Figure 16: Trusted CA

3.8.3.2 Is certificate expired (checking valid from and valid to dates)?

The validity of the certificate is as important as a passport, driving license or radio operator license in real life. If the period of validity has expired, the authentication server will reject the certificate. In figure below you can see certificate dates.

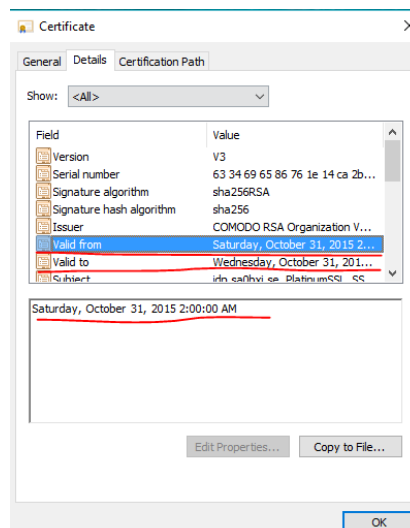


Figure 17: Certificate Expiry

3.8.3.3 Is certificate revoked?

Every certificate authority (CA) has maintained and published a list of revoked certificates. There are two main methods used by CA's for this purpose: The Certificate Revocation List (CRL) and the Online Certificate Status Protocol (OCSP). In the figure below, you can see the CA is using OCSP and there is information given to check the status.

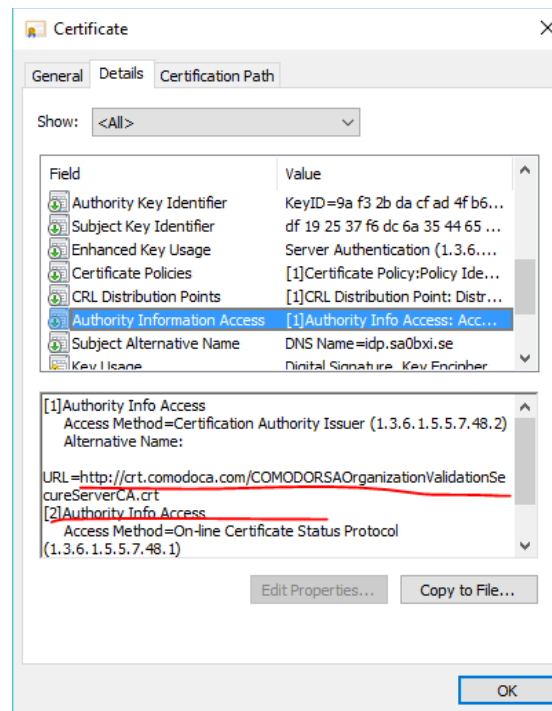


Figure 18: OCSP

3.8.3.4 Has the client proof of ownership/possession?

Certificate authentication will require the user to send some data using both encryption and decryption to demonstrate possession of both a public and private key. Success is proof of possession of the corresponding certificate. If data does not match, the authentication fails.

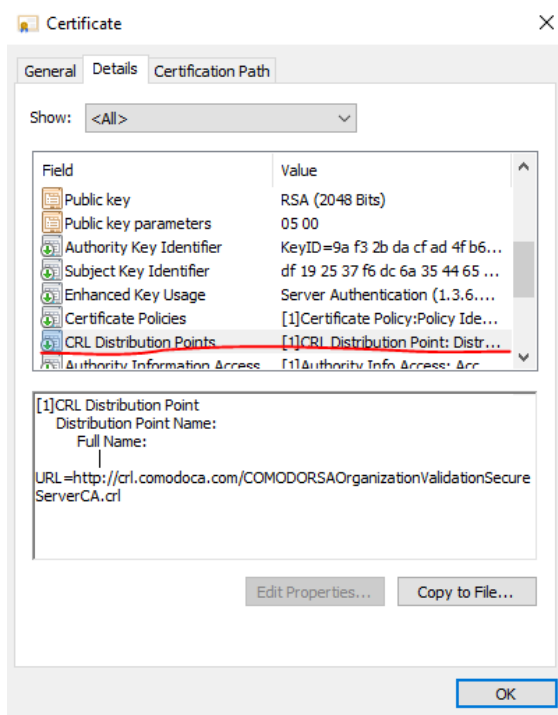
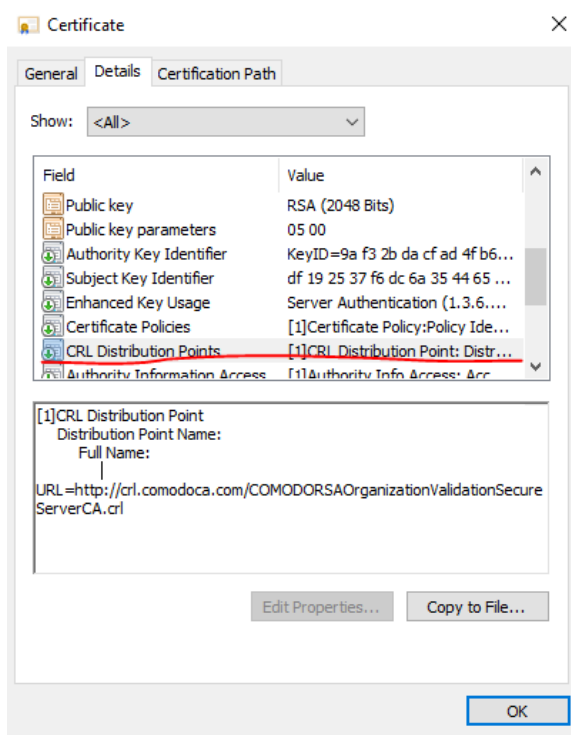


Figure 19: Certificate Possession

3.8.4 Secure Socket Layer (SSL)

SSL, as already mentioned earlier, is a protocol which uses an SSL certificate to authenticate. It is a security protocol for establishing an encrypted communication between client and server. Transport Socket Layer (TSL), which has evolved from SSL version 3.0, is becoming widely used. As shown in figure 15, the client and server handshake by identifying a cipher suite policy and initiate a session by identifying the information. In the next step, the client and the server exchange certificates. The certificate is validated upon reception and the server needs to be authenticated by its CA. In the next phase with certificate there will be server and client key exchange which authenticate each other side. SSL then allows sensitive information (credit card info, identity credentials and others) to be transmitted over Internet securely. [54]

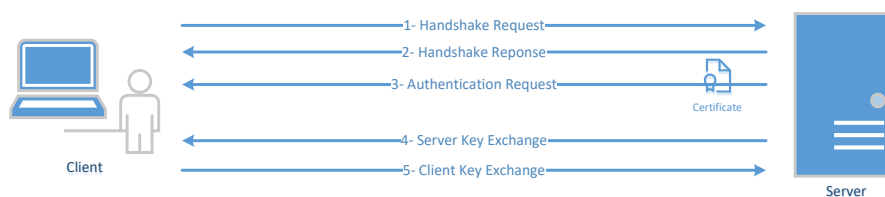


Figure 20: Secure Socket Layer (SSL)

9. Authorization

Authorization is often implemented as an Access Control List (ACL). An ACL resolves the right to access resources based on identity and policy. An ACL is often used as a security service in software applications. It helps in decision making, processes of determining and managing the subjects (users, devices or workflow) that should be granted access and the resources to which they should be granted access to. It also controls the methods and conditions of enforcement by which users are allowed to view, connect or consume resources. [55]

After authentication, a user wants to use the system features often protected by an ACL the authorization process will determine whether the user can access a certain feature or not. Authentication and authorization are working together. After authentication, the user get authorized to certain features of the system, for example changing the own password or user profile information. A user belonging to an administrator group, often has some additional authorization defined in ACL that a normal user does not have.

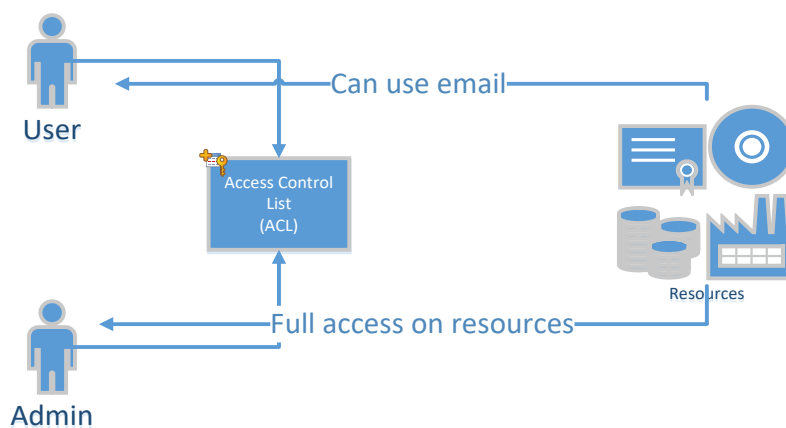


Figure 21: ACL or Authorization Control

There are three major parts in authorization mechanism.

- Defining Authorization Groups
- Defining ACL Matrix
- Authorization Implementation

3.9.1 Defining Authorization Groups

Most important thing in authorization mechanism is to define it affectively according to needs of users. A hierarchy can be helpful in defining authorization groups. Authorization can be defined many ways, for example a user can be member of multiple groups or can be member of higher level group which will includes all lower level.

3.9.1.1 Hierarchy levels

As you can see in Table 1 below, user Qasim belong to “Member” group has lowest level of access whereas Eric is a “Board” member has all access which includes “Admin” and “Member”.

Table 1: Hierarchy Levels

User	Group	Description	Level
Qasim	Member	A member	Limited
Johan	Admin	Admin can manage some users.	Limited, includes Member
Eric	Board	A board member can control all users.	Full access, includes Admin and Member

3.9.1.2 Multiple Levels

In multiple level a user can be member of one or more groups. As you can see in Table 2 below, Eric is a member of multiple groups “Member”, “Admin” and “Board”.

Table 2: Multiple Levels

User	Member	Admin	Board
Qasim	Yes	No	No
Johan	Yes	Yes	No
Eric	Yes	Yes	Yes

3.9.2 Defining ACL Matrix

After defining authorization's levels in Access control list (ACL) matrix, it is necessary step where actually we define what are the capabilities of a specific group. As you can see in Table 3 below is an example of group and their capabilities.

Table 3: Access Control Matrix (ACL)

Group	Publish Devices	Share Devices	Manage Users	Create Directories
Member	Yes	Yes	No	No
Admin	Yes	Yes	Yes	No
Board	Yes	Yes	Yes	Yes

3.9.2.1 Implementation

It has already been discussed in Authentication section [3.8.2.3](#).

3.9.2.2 Authorization Configuration Options in Shibboleth Identity Provider

Authentication only

```
<Location /DirectoryName/>
    AuthType shibboleth
    ShibRequireSession On
    Require shibboleth
</Location>
```

Optional authentication

```
<Location /DirectoryName/>
    AuthType shibboleth
    Require shibboleth
</Location>
```

Groups in file example

```
<Location /DirectoryName/>
    AuthType shibboleth
    ShibRequireSession On
    AuthGroupFile /var/www/secure/acl-group
    Require group 09ef
</Location>
```

Where /var/www/secure/ acl-group contains 09ef: Admin

Here is "OR" example If we want that user should be member Admin OR Board group

```
<Location /DirectoryName/>
    AuthType shibboleth
    ShibRequestSetting requireSession true
    Require shib-attr groupName Admin Board
</Location>
```

Here is "AND" example If we want user should be member Board AND Admin

```
<Location /DirectoryName/>
    AuthType shibboleth
    ShibRequestSetting requireSession true
    ShibRequireAll On
    Require shib-attr groupName Board Admin
</Location>
```

10. Service Provider (SP)

Service provider is often a generic term used in WS-federation model. It is often a web service which provided to principal users authenticated and authorized by a trusted identity provider (IdP). It can be application service, storage service or some internet service provider (ISP). In exchange of token security information is shared between identity provider (IdP) and service provider (SP).

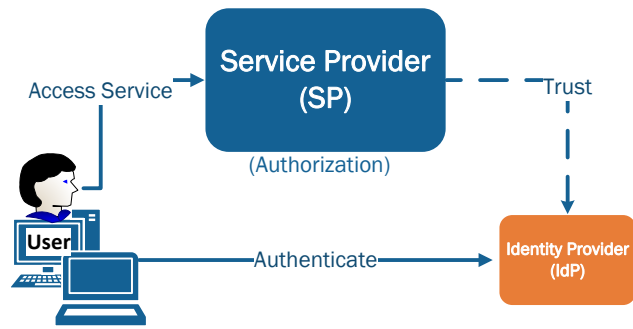


Figure 22: Service Provider (SP)

Chapter 4

Design and Implementation of Proposed Framework

In this chapter, we will explain the proposed federated framework's design and implementation, which mainly consists of identity provider (AMPRid) and a service provider (AMPRemote). For testing purposes, we coordinate with GrIDP [56] which is an identity federation for homeless identity providers. I will discuss conceptual design of the proposed solution in this chapter whereas complete technical details are given in Appendix 1 and 2 for AMPRid and AMPRemote respectively.

1. Design

AMPRid is basically implementation of standard Identity Provider so there is not much design of involved rather it more about technical implementation. As mentioned above technical implementation has been given in Appendix 1 for AMPRid. We will continue with the design of AMPRemote service.

4.1.1 AMPRemote: Secure remote operation/login to selected equipment

In this section, we will discuss the experimental service (SP) requested by the stakeholders as an example of what an e-infrastructure framework explored in this study makes possible.

The service allows licensed amateur radio operators to make requests to owners of remotely controlled radio stations to be authorized to use their equipment via a dedicated front end equipment. The front-end control panel of the radio station is connected to the back-end transceiver connected to the antenna via Internet using Remoterig (RRC) interfaces providing both Voice over IP (VoIP) channels and control signals from buttons and knobs.

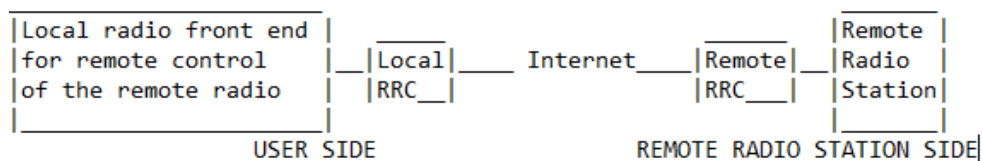


Figure 23: Sketch of AMPRemote

The procedure to manage requests is the following:

- The request to use a specific equipment is made to the SP.
- The SP authenticates the requesting operator via the IdP
- If the authentication is positive, the request is forwarded to the owner who can grant or deny it.

- If the request is granted, the necessary credentials are installed in the front-end unit of the requesting operator, who is also notified.

4.1.2 Device Used in Project

The Remoterig RRC-1258MkII (RRC) is mainly used in the thesis project implementation. RRC is a special device built for remote control of amateur radio stations via Internet by company called Microbit 2.0 AB [25]. RRC is simple, user friendly and cost effective way to connect remote radio station. RRC units are used in pairs, one is connected to radio (Radio-RRC) and other is connected to the control equipment (Control-RRC). A user does not need any computer for voice and data communication it can be done by two RRC units can be configured to work with most of the amateur radio stations. [57]



Figure 24: RRC-1258MkII Setup [58]

There are two ends of this communication one is called “Control” and another end is called “Remote”. Owner user saves the SIP Password of Remote side device in AMPRemote system when Requester user requests for usage, he uses Control side device is used to save password on it to connect to the Remote end as shown in the figure below.

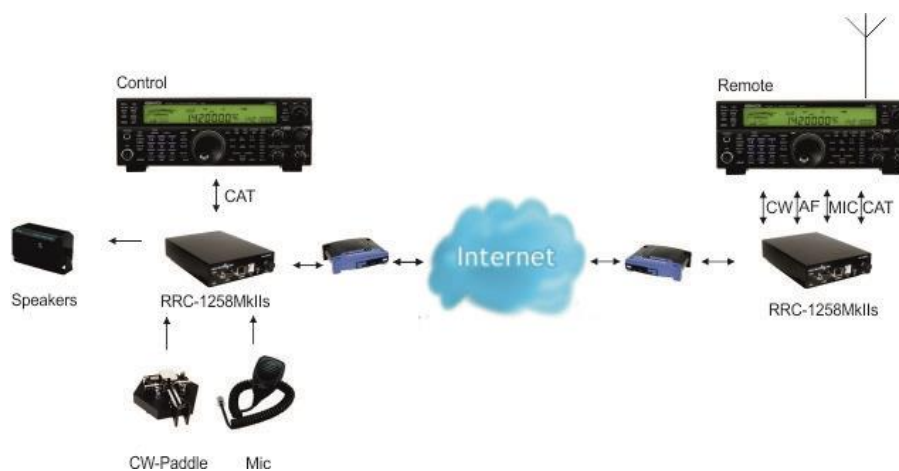


Figure 25: RRC-1258MkIIs [25]

4.1.3 Framework Architecture

In Framework architecture, you can see more clear communication flow.

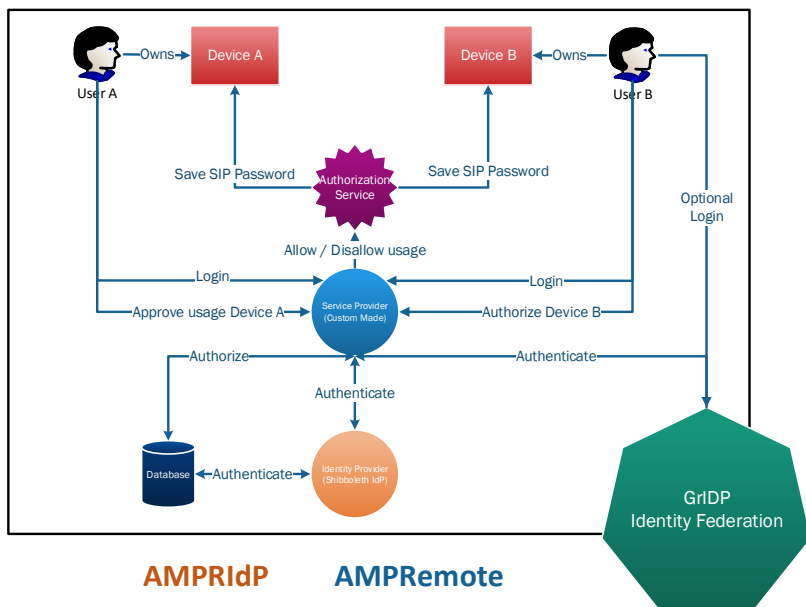


Figure 26: Proposed Framework Architecture

4.1.4 Authentication Mechanism

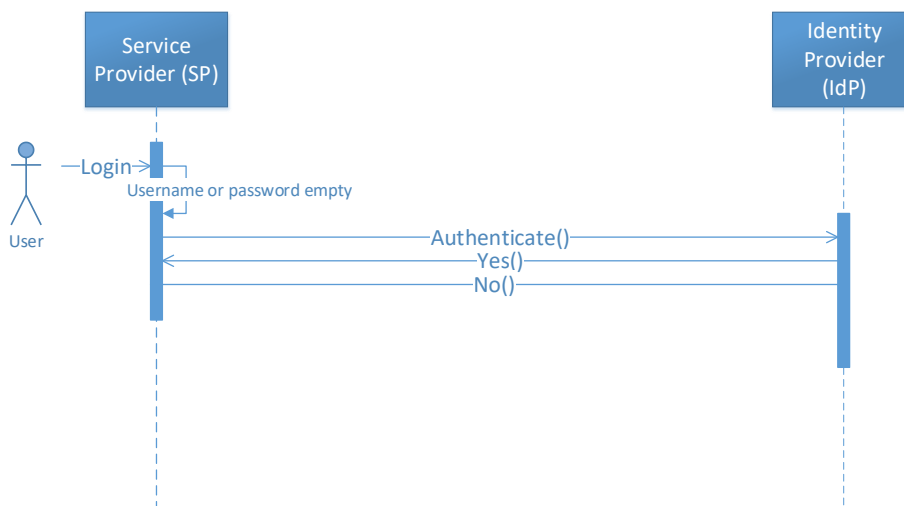


Figure 27: Authentication Sequence Diagram

4.1.5 Authorization Mechanism

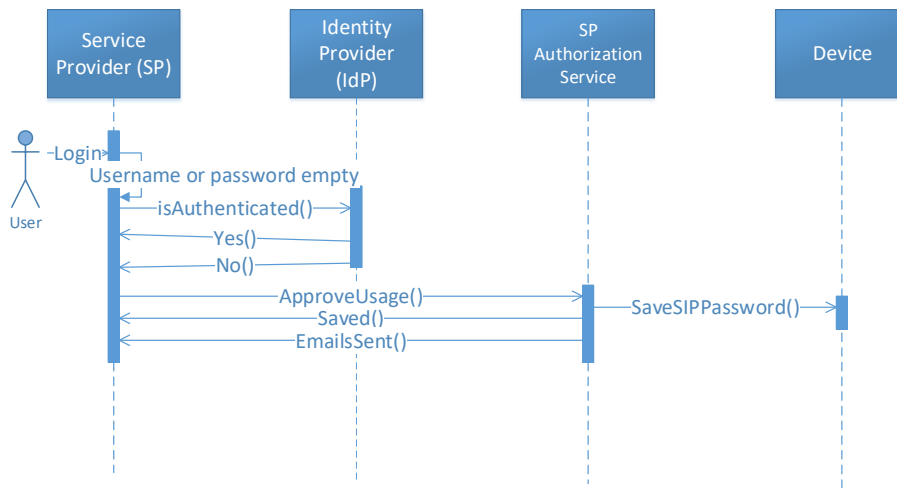


Figure 28: Authorization Sequence Diagram

4.1.6 User Cases

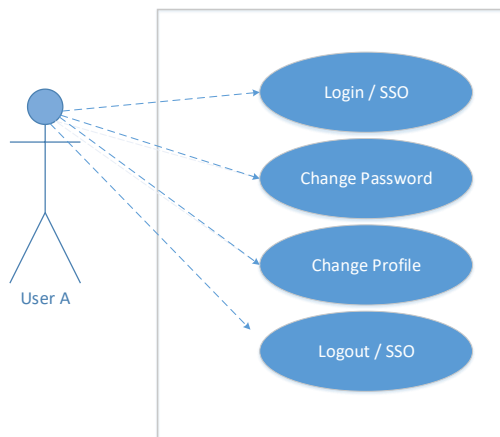


Figure 29: User A user login, change password and profile use case diagram

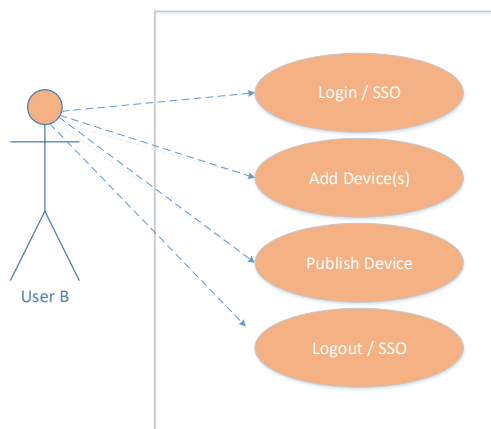


Figure 30: User B login, add and publish device use case diagram

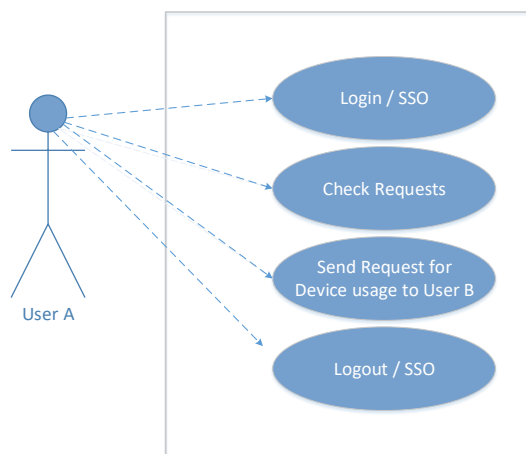


Figure 31: User A check and send request for device usage use case diagram

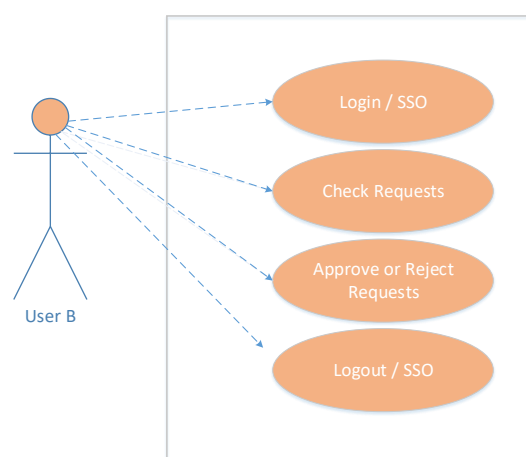


Figure 32: User B check, approve or reject requests user case diagram

2. Implementation

The implementation of a demonstration includes the Identity Provider (AMPRid) and the Service Provider (AMPRemote) offering secure authorization of licensed operators to use remotely controlled radio stations. The details of the implementation procedure are provided in Appendix 1 and Appendix 2 respectively. We will here focus on the principles.

After discussing the prerequisites for the implementation and demonstration, we will discuss the IdP and SP separately.

4.2.1 Prerequisites

There were a number of prerequisites/challenges defined by the stakeholders:

- The demonstration, including IdP and SP, was to be implemented in a Linux environment. A virtual machine running Ubuntu 12.04 Linux was provided on a VM-server hosted at NUNOC. The intention is to use the URL `idp.ssa.se`. During the test

phase, another domain was used and is currently still idp.sa0bxi.se. A temporary Comodo certificate was used in the development phase.

- The SSA Callbook, i.e. the national records of licensed radio amateurs kept by SSA, one of the stakeholders, is implemented as a MySQL database. The tools to be used for implementation of an IdP were originally built for using LDAP, which lead to some complications to sort out.
- To take advantage of an opportunity to demonstrate how an IdP could join an Identity Federation, the DevOps solution from Africa-Arabia Regional Operations Centre (AAROC) was to be used [59]. This solution had, however, so far been tested on an Ubuntu platform, which lead to multiple iterations.
- The Remoterig Device (RRC) [58] selected by the stakeholders in this project to facilitate remote operations of radio stations over Internet currently only supports basic non-SSL authentication offering limited security. In a discussion, the manufacturer responded that a more elaborate certificate-based solution will be developed only when demanded by customers. Some of the end-users were, however, not aware of, or ignored, the risks and consequences of leaving their devices insecure.

4.2.2 Identity Provider (AMPRID)

To setup an identity provider you need to install couple of software in sequence, the sequence in many cases is important to configure the IdP properly. To make this process automated we can use some kind of automation tool, in our project we are using Ansible [60]. Ansible uses a language called YAML [61] which is used to write playbooks are simple human readable commands. More details about these playbooks are given in appendices.

Such a playbooks repository called DevOps [62] to setup an IdP is maintained by Africa-Arabia Regional Operations Centre (AAROC) [63] in collaboration with Catania Science Gateway [64].

SSA maintains the member's database, we have generated initial secure random passwords. which the users are prompted to change at their first login.

The IdP has been added to the GrIDP IdF [56] for demonstration purposes.

4.2.3 Setup an Identity Federation for Emergency Response Organizations

To setup an Identity federation for the organizations participating in emergency response, each organization needs to implement an identity provider (IdP). One of the organization can act as identity pool so all other organizations can join identity federation to provide home to their identity provider (IdP). After being part of identity federation these organizations will be listed in discover service [46] as shown in figure. GrIDP is identity pool and SSA being partner identity provider (IdP) is part of identity federation (IdF) which is visible in discovery service. To be part

of identity federation, identity provider (IdP) organization needs to follow the terms and conditions of identity federation (IdF) and share the metadata of its identity provider (IdP) which will be added to IdF metadata file. More details about metadata is given IdP appendix.

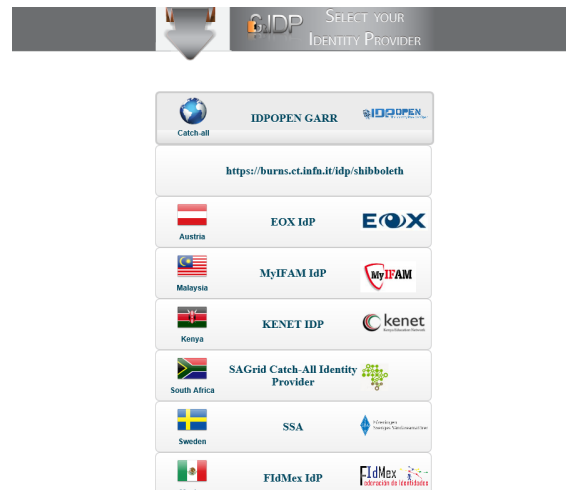


Figure 1: GrIDP Discover Service Interface

4.2.4 Service Provider (AMPRemote)

The AMPRemote Service Provider is a custom-made portal for owners and users of remotely controlled radio stations to authorize/request authorization for the usage of Remoterig-supported radio stations. The Remoterig units have a built-in web page offering access via a web browser. It is protected by basic HTTP authentication as explained in a previous section. Due to the lack of a secure standard interface, we have tailored an as secure as possible solution following the guidelines from The Open Web Application Security Project (OWASP) Authentication cheat sheet [38]. The SP authorization service is sending sensitive information (device login and SIP Password) only on Transport Socket Layer (TLS) as recommended by OWASP. Complete setup details can be found in SP appendix.

As discussed above, this should be regarded as a temporary solution.

4.2.5 Technologies

AMPRemote service provider is a web application built with PHP as back-end Web API [65] and front-end is developed with HTML 5 and Angular JS. PHP is open source lower overhead secure language suitable for all kind of web applications. HTML 5 and Angular JavaScript is very suitable for client side as it is cross browser supported.

4.2.6 Architecture

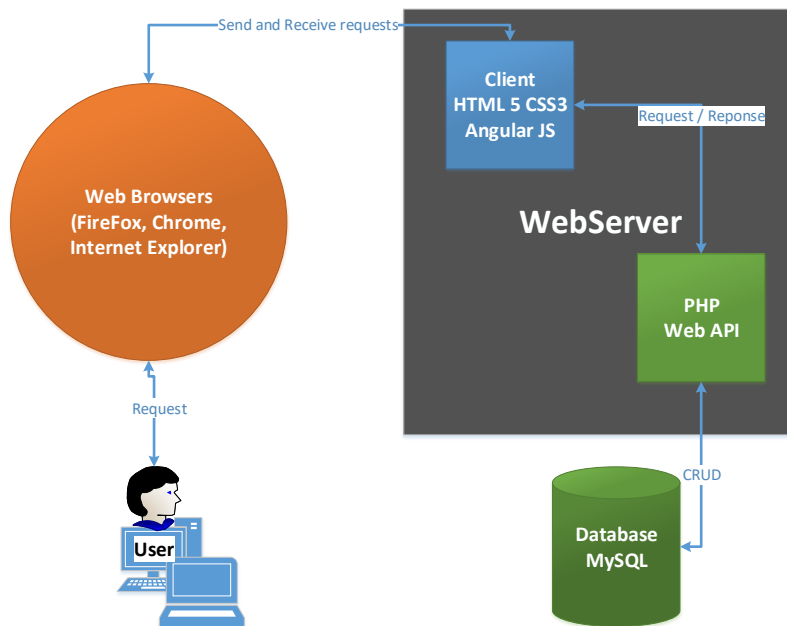


Figure 33; SP Architecture

4.2.7 Database

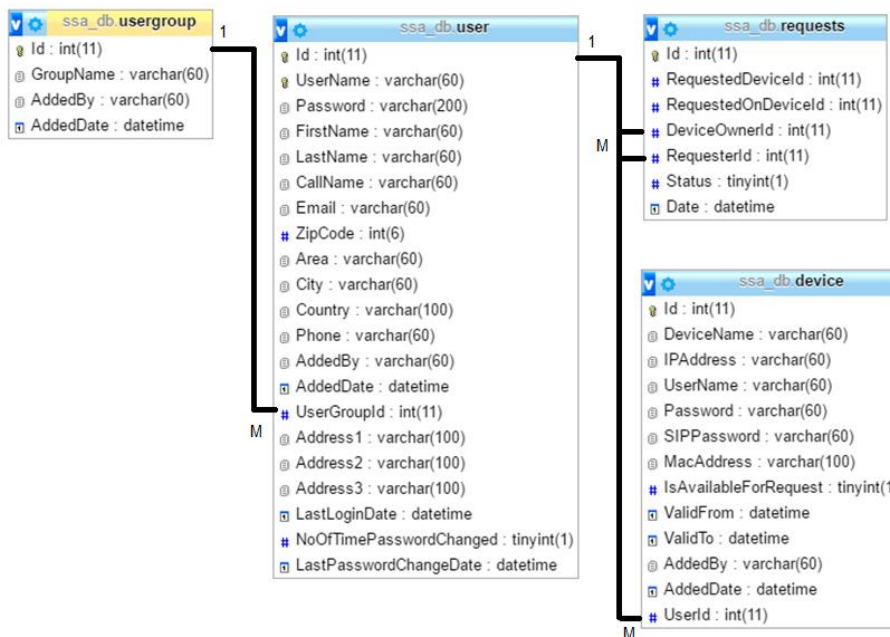


Figure 34: Database Model

4.2.8 AMPRemote Usability Screenshots

As I mentioned some use cases scenarios in use cases section, here we can see some real screen shoots for some for some those.

4.2.8.1 GrIDP Discovery Page

You can access AMPRemote service provider (SP) on this [link](#). Below is the image of GrIDP discovery service. SSA is included in it.

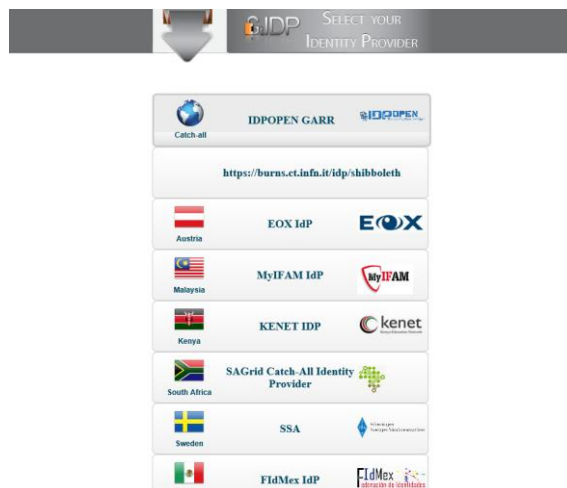


Figure 35; GrIDP Login Page

4.2.8.2 Login

AMPRemid authentication login page. Upon false login information, user will get error message.

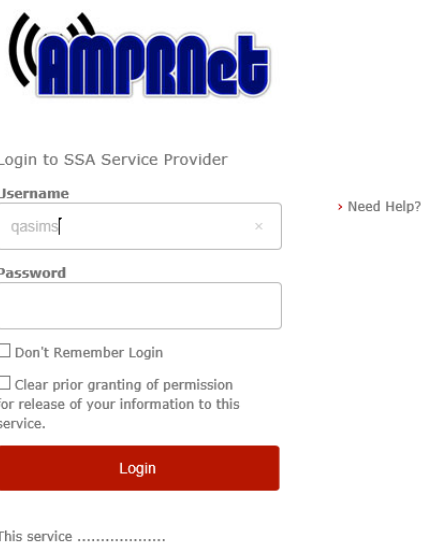


Figure 36: AMPRemote Login Page

4.2.8.3 Information Provided Confirmation

These are Shibboleth IdP default attributes used in IdP which were configured in attribute resolver file in IdP configuration. User can choose to send the information on this page, always or reject it.

You are about to access the service:
SSA Service Provider of SSA
 Description as provided by this service:
 This service

Information to be Provided to Service	
eduPersonPrincipalName	qasims@sa0bxi.se
givenName	Qasim
groupName	Admin
mail	qasims@live.se
surname	Sarfraz
uid	qasims

The information above would be shared with the service if you proceed. Do you agree to release this information to the service every time you access it?

Select an information release consent duration:

Ask me again at next login

- I agree to send my information this time.

Ask me again if information to be provided to this service changes

- I agree that the same information will be sent automatically to this service in the future.

Do not ask me again

- I agree that **all** of my information will be released to **any** service.

This setting can be revoked at any time with the checkbox on the login page.

Figure 37: Shibboleth Attribute Information

4.2.8.4 Home Page

Below is home page of SSA service provider (SP). User can logout, update own information like password and other profile information. On the left side, there is collapsible menu, depending on the rights of the user will see number of menu options. In the right panel user, will see highlight, for example number of requests available to approve, how many devices user has been added and others.

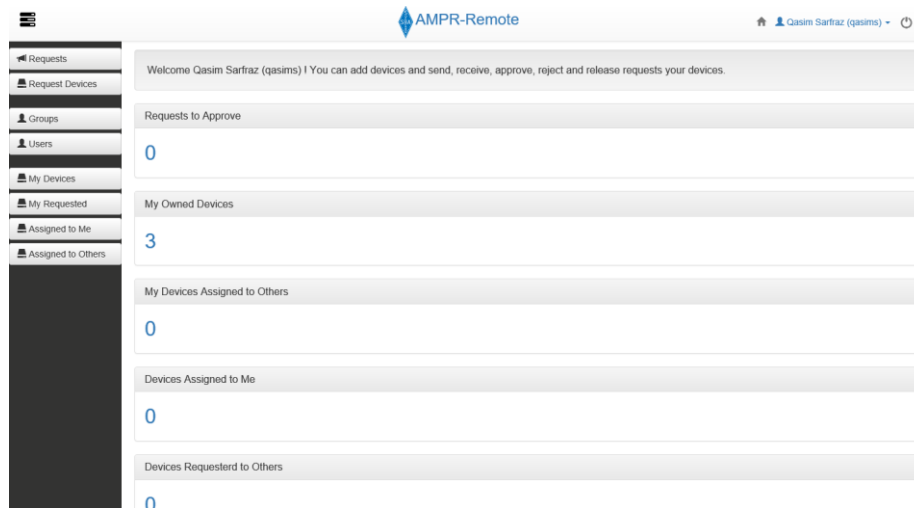
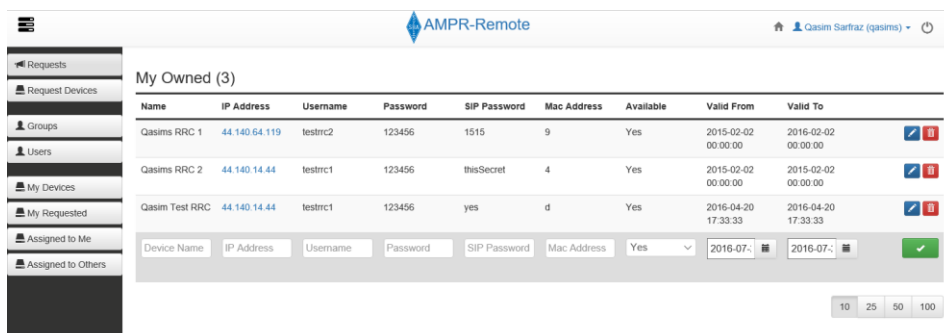


Figure 38: Home Page AMPRemote

4.2.8.5 Register Own Device

To use this service user must register a device for that user needs on My Owned menu and fill up the form. Number of fields are required (name, IP address, username, password, sip password). User also choose device availability, if device is not available it will not show in Request Devices page and no user can send usage request.



Name	IP Address	Username	Password	SIP Password	Mac Address	Available	Valid From	Valid To
Qasims RRC 1	44.140.64.119	testrc2	123456	1515	9	Yes	2015-02-02 00:00:00	2016-02-02 00:00:00
Qasims RRC 2	44.140.14.44	testrc1	123456	thisSecret	4	Yes	2015-02-02 00:00:00	2015-02-02 00:00:00
Qasim Test RRC	44.140.14.44	testrc1	123456	yes	d	Yes	2016-04-20 17:33:33	2016-04-20 17:33:33

Figure 39: My Owned devices

4.2.8.6 Request Page

If user clicks on Request Devices page will see list of all devices available for request from other users. User can see device name and name of the owner. User can send a request to owner of device for usage.

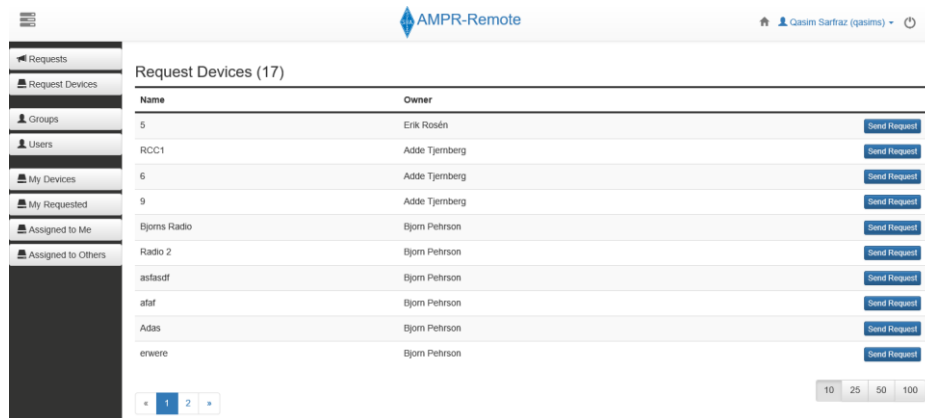


Figure 40: All Device Page

If user clicks on Send Request button system will show a dialog box where user is required to choose own device from which he wants send request and save SIP password on it. User is required to register device in order to see in this list otherwise user will get a message “Please add a device to send request from”. After pressing Send button a request will be sent to owner to approve or reject.

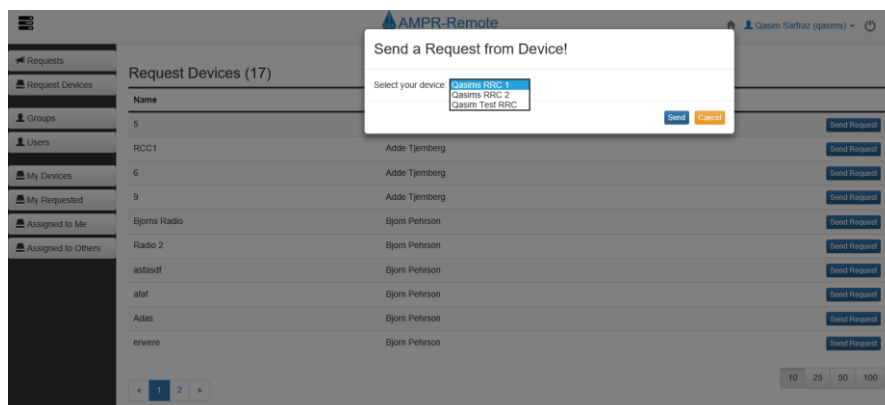


Figure 41: Request a device

4.2.8.7 Requests

If user clicks on Requests menu will see list of user’s owned devices requested by the other users. As an owner of the device user can approve or reject the request.

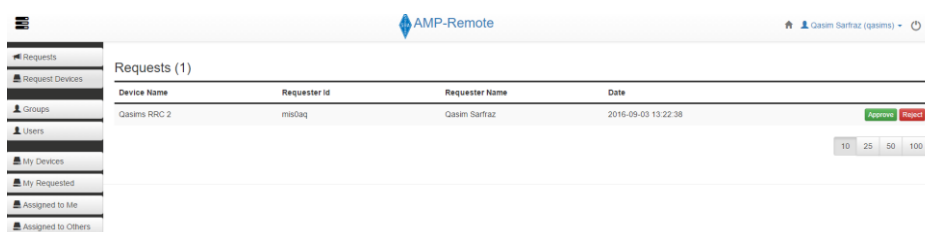
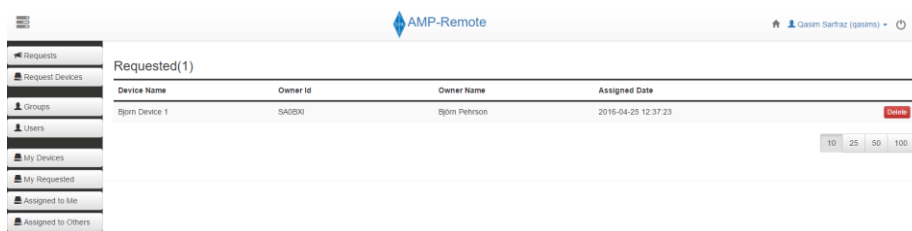


Figure 42: Requests Page

4.2.8.8 Requested

Requested page is very similar like Requests but here user will see list of requested devices to others by himself and not approved or rejected yet. User can delete a request already sent to another user by clicking on Delete button.

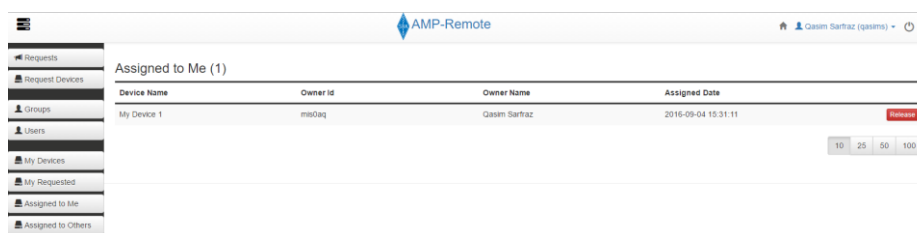


Device Name	Owner Id	Owner Name	Assigned Date
Bjorn Device 1	SAGBM	Bjorn Pehrson	2016-04-25 12:37:23

Figure 43: Requested devices

4.2.8.9 Assigned to Me

It is very similar like Requested page but it lists of device user requested and approved. User can release device when it is not needed another more.

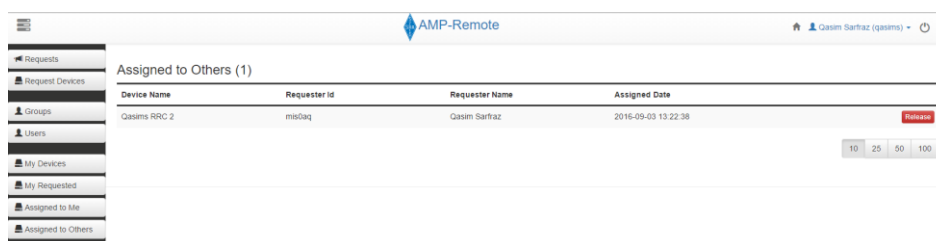


Device Name	Owner Id	Owner Name	Assigned Date
My Device 1	msoaq	Qasim Sarfraz	2016-09-04 15:31:11

Figure 44: Assigned to me devices

4.2.8.10 Assigned to Others

It is list of user's owned devices assigned to others which are approved already by user. User can release a device anytime it is needed by clicking on Delete button.



Device Name	Requester Id	Requester Name	Assigned Date
Qasims RRC 2	msoaq	Qasim Sarfraz	2016-09-03 13:22:38

Figure 45: Assigned to others devices

4.2.8.11 Change Password

On first login user, will be forced to change password. Afterword user can click on arrow on profile icon on right side and choose change password from menu. User must follow the password strength constraints mentioned on password change form. For example, 8 characters long length of password.

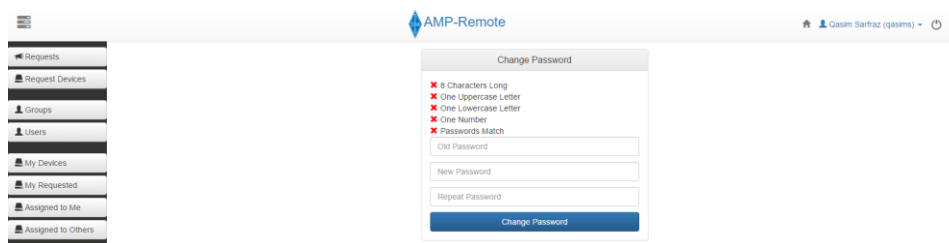


Figure 46: Change Password

4.2.8.12 My Profile

User can click on arrow on profile icon on right side and choose My Profile from menu to change profile information for example, address and contact.

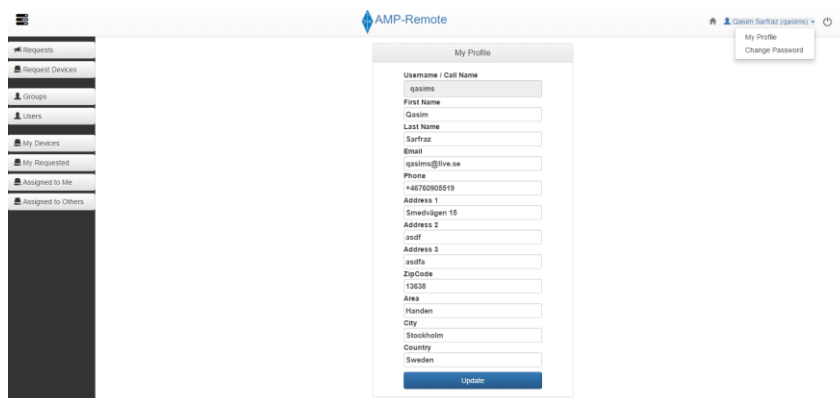


Figure 47: My Profile

4.2.8.13 User Group and Users

If user belong to admin group will see two extra menus Groups and Users, user can create, update or delete user groups and users. Right now, there are two default groups available, Member and Admin.

The screenshot shows the AMPR-Remote user management interface. The page title is "Users (13796)". There is a search bar for "Search by username". Below the search bar is a table with columns: Group, Username, Password, First Name, Last Name, Email, Phone, Address, ZipCode, Area, and Country. The table contains three rows of user data.

Group	Username	Password	First Name	Last Name	Email	Phone	Address	ZipCode	Area	Country
Admin	qasims	*****	Qasim	Sarfraz	qasims@live.se	+46700905519		13038	Härnösand	Sweden
Member	bjorn	*****	Bjorn	Peterson	bjornson@kth.s	+46737087980		19042	Märsta	Sweden
Member	adde	*****	Adde	Tjernberg	adde@jernberg			0		Sweden

Figure 48: Admin user management

4.2.8.14 Sending Email Confirmation

Upon approving a request, Requester and Owner both will get an email confirmation as shown below.

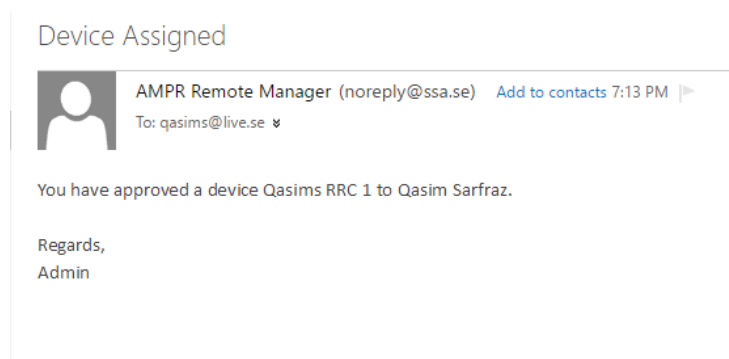


Figure 49: Email sent to owner of device

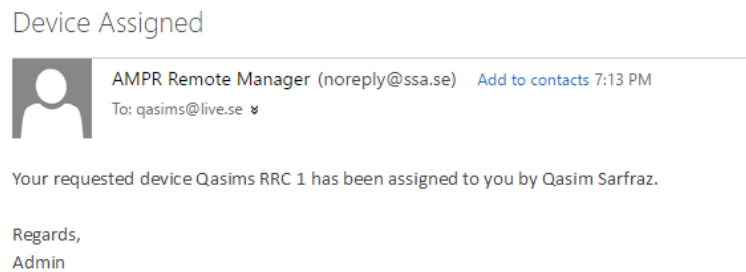


Figure 50: Email sent to requester of the devices

Chapter 5

Evaluation

The Catania Science Gateway framework and the EduGAIN certificate-based SSO framework for authentication and authorization are good choices as the basis for a collaborative Information System managing emergency response efforts. The AMPRID service based on the SSA Callbook records of licensed operators maintained by SSA is a sustainable solution. The stakeholders should go ahead and stimulate other stakeholders in collaborative emergency response efforts to establish their own IdP services and join the Emergency Response Identity Federation.

Proposed solution has been demonstrated at the annual meeting 2016 of SSA, participant in the presentation were mostly users and stake-holders of the system and they confirmed that the system meets their needs and requirements as mentioned in chapter 2. Many have appreciated the device management functionality in AMPRemote since many of them owned more than one RRC equipment but they were having difficulty to manage their devices sensitive information. One particular question for if AMPRemote can handle multi manufacturer devices which is not the case right now, mainly for two reasons one, most of the SSA members are using devices from same manufacturer as mentioned above in chapter 2 and the second it is out of the scope of this thesis.

After discussion with the people we get to know after the demo they were more aware of potential security threats in using radio equipment without proper security measures, which eventually fulfilled one of our objective of this thesis.

The framework is also good for service provisioning. The different stakeholders can harmonize and add services that can be agreed upon as common tools. Those will make the tools easier to use and minimize the risk for human errors by simplifying the security procedures.

Regarding the specific service used for demonstration, AMPRemote, as mentioned above, security in the communication between the service provider authorization service and the devices to be used can be improved. After discussing with the RRC manufacturer, we got the impression that they are thinking of updating the security of existing devices as most users are not informed enough to demand it themselves. It was not possible to test different authentication methods for AMPRemote in this study. We do, however, still have some recommendations for the manufacturer if they plan to upgrade the security in their future products. First and foremost, we recommend a certificate based authentication it is quite secure but complex to implement, secondly, we recommend using OAuth 2.0 as API, as it is a really secure protocol being used by Google and Facebook, Twitter and Microsoft as well.

1. Comparison between Basic, Certificate and OAuh (AAI)

Authentication and Authorization Infrastructures

Features	Basic AAI	Certificate Based AAI	OAuth AAI
Deploy / Implement	Easy to deploy / Implement	Complex to implement	Easy to implement
Administration	Easy to administrate	Complex to administrate	Easy to implement
Required Password	Yes	No	No
Required HTTPS	No	Yes	Yes
Reliability	Unsecure without HTTPS	Issue from CA	Well known for security

Chapter 6

Conclusion and Future Work

The purpose of this work has been to demonstrate the benefits of using EduGAIN functionality, especially federated single sign on authentication and authorization services, to facilitate cooperation between different volunteer groups involved in emergency management. The user group selected for this demonstration was licensed amateur radio operators, for several reasons, including: 1) the group has a strong track record for providing important communication services via radio, mainly voice, in emergency situations where other means of communication are insufficient, 2) it is well defined since there is a maintained digital data base available containing all its members and 3) the group is in the process of establishing AMPRNet as a resource for Emergency Response and has plans for developing more services that could fit into the same framework.

All members of the group are, however, not necessarily knowledgeable in more advanced computing, computer communications and e-infrastructure-related technologies. As pointed out earlier, it is a well-documented truth that users have a hard time making a needs analysis involving products or services that they know little about. It is also well documented that development of new products or services can fail utterly due to developer ignorance about user needs. The dialogue is crucial for success.

The results of this study were demonstrated, and gained considerable interest, at the annual meeting 2016 of SSA in April 2016 and at a training event of FRGNORR in October 2016. Discussions are under way to integrate the services developed in a larger context, including setting up identity providers for FRG in the FRGNORR communes and developing a single-sign-on emergency management portal with relevant services.

1. Future Work

Other services that are mentioned will be presented elsewhere, include AMPRoam [19], a service offering radio amateurs Internet access via all Wi-Fi access points deployed in AMPRNet and AMPRoar [14], an Open Access Repository offering high visibility publication of different sorts of documents, such as experiment reports, software, data files, hardware designs, etc. The upload procedure supports simple assignment of a license regulating how the documents can be used from the spectrum of Creative Commons licenses.

A mobile access point/gateway/pocket server is being setup in another project [66]. AMPRid and federated framework design also can be useful to connect different organization together.

References

- [1] The EU Framework Programme for Research and Innovation, "e-infrastructures," The EU Framework Programme for Research and Innovation, [Online]. Available: <https://ec.europa.eu/programmes/horizon2020/en/h2020-section/e-infrastructures>. [Använd 01 01 2016].
- [2] GÉANT, "About eduGAIN," GEANT.ORG, [Online]. Available: http://www.geant.org/Services/Trust_identity_and_security/eduGAIN/Pages/About-eduGAIN.aspx. [Använd 01 01 2016].
- [3] L. Macaulay, "Cooperation in understanding user needs and requirements," *ScienceDirect*, vol. 8, nr 2, pp. 155-165, 2000.
- [4] N. B. Martin Maguire, "User requirements analysis," Kluwer Academic Publishers., Montreal, Canada, 2002.
- [5] MIT Information Systems & Technology, "The Knowledge Base," MIT, [Online]. Available: [http://kb.mit.edu/confluence/display/glossary/IdP+\(Identity+Provider\)](http://kb.mit.edu/confluence/display/glossary/IdP+(Identity+Provider)). [Använd 23 06 2016].
- [6] MIT Information Systems & Technology, "SP (Service Provider)," MIT, [Online]. Available: <http://kb.mit.edu/confluence/display/glossary/SP+%28Service+Provider%29>. [Använd 01 01 2016].
- [7] Wikipedia, "2005 Kashmir earthquake," Wikipedia.org, [Online]. Available: https://en.wikipedia.org/wiki/2005_Kashmir_earthquake. [Använd 25 06 2016].
- [8] BBC, "Kashmir earthquake: Broken city, broken promises," BBC.com, [Online]. Available: <http://www.bbc.com/news/world-asia-34464815>. [Använd 25 06 2016].
- [9] People.com.cn, "Thousands feared dead after quake jolts south Asia," People.com.cn, [Online]. Available: http://en.people.cn/200510/09/eng20051009_213394.html. [Använd 25 06 2016].
- [10] S. Suri, "Amateur radio in emergency communications advanced digital communication network," i *In Proceedings of the 1st International Conference on Wireless Technologies for Humanitarian Relief (ACWR '11)*. ACM, New York, NY, USA, 29-29, 2011.
- [11] Federal Communications Commission, "AMATEUR RADIO SERVICES," Federal Communications Commission, [Online]. Available: http://wireless.fcc.gov/services/index.htm?job=service_home&&id=amateur. [Använd 12 12 2016].
- [12] ARRL, "Amateur Radio Emergency Service," ARRL.org, [Online]. Available: <http://www.arrl.org/amateur-radio-emergency-communication>. [Använd 03 03 2016].
- [13] Myndigheten för samhällsskydd och beredskap, "Om MSB," MSB, [Online]. Available: <https://www.msb.se/sv/Om-MSB/>. [Använd 01 11 2016].
- [14] AMPRNet.se, "Projekt," [Online]. Available: <http://amprnet.se/projekt.html>. [Använd 01 06 2016].

- [15] Amateur Radio Digital Communications, "Amateur Radio Digital Communications - Home," AMPR.org, [Online]. Available: <https://www.ampr.org/>.
- [16] SUNET, "Sunet - About Us," SUNET, [Online]. Available: <https://www.sunet.se/about-sunet/>. [Använd 01 01 2016].
- [17] EchoLink, "Introducing EchoLink," EchoLink.org, [Online]. Available: <http://www.echolink.org/>. [Använd 01 11 2016].
- [18] The Internet Radio Linking Project, "The Internet Radio Linking Project," IRPL.net, [Online]. Available: <http://www.irpl.net/>. [Använd 01 11 2016].
- [19] Sweden - AMPR, "AMPRoam," se.AMPR.org, [Online]. Available: <http://se.ampr.org/amproam.html>. [Använd 01 08 2016].
- [20] Sändareamatörer, Föreningen Sveriges, "Om SSA," SSA.se, [Online]. Available: <http://www.ssa.se/ssa/om-ssa/>. [Använd 12 06 2016].
- [21] Föreningen Sveriges Sändareamatörer, "SSA - SM Callbook," SSA.se, [Online]. Available: <http://www.ssa.se/sm-callbook/>. [Använd 01 01 2016].
- [22] Frivilliga Radioorganisationen, "Om FRO," Frivilliga Radioorganisationen, [Online]. Available: <https://fro.se/om-fro>. [Använd 01 11 2016].
- [23] Civilförsvarsförbundet, "Om Oss," Civilförsvarsförbundet, [Online]. Available: <http://www.civil.se/om-oss/>. [Använd 01 11 2016].
- [24] Frivilliga resursgruppen, "FRG - Home," Frivilliga resursgruppen (FRG), [Online]. Available: <http://www.frgnorr.se/>. [Använd 01 11 2016].
- [25] Remoterig, "Microbit 2.0 AB - RRC-1258MkII TS-590 Twin," Remoterig.org, [Online]. Available: http://www.remoterig.com/wp/?page_id=2456. [Använd 19 07 2016].
- [26] Föreningen Sveriges Sändareamatörer, "SM Callbook," SSA.se, [Online]. Available: <http://www.ssa.se/sm-callbook/>. [Använd 01 11 2016].
- [27] International Organization for Standardization, "ISO/IEC 24760-1, ITU-T Y.2720," ISO.org, [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:57914:en>. [Använd 01 11 2016].
- [28] SAML XML.org, "About Saml," SAML XML.org, [Online]. Available: <http://saml.xml.org/about-saml>. [Använd 03 05 2016].
- [29] SWEDISH ACADEMIC IDENTITY FEDERATION, "SWEDISH ACADEMIC IDENTITY FEDERATION," SUNET.SE, [Online]. Available: <https://www.sunet.se/swamid/>. [Använd 01 06 2016].
- [30] SAML.XML.org, "SAML Specifications," SAML.XML.org, [Online]. Available: <http://saml.xml.org/saml-specifications>. [Använd 02 06 2016].

- [31] C. K. A. N. P. H.-B. C. M. Ronald Monzillo, "Web Services Security SAML Token Profile Version 1.1.1," OASIS Standard, 2012.
- [32] P. Siriwardena, "OpenID Connect," i *Advanced API Security Securing APIs with OAuth 2.0*, Berkeley : Apress , 2014, p. 248.
- [33] OpenID, "What is OpenID," OpenID, [Online]. Available: <http://openid.net/get-an-openid/what-is-openid/>. [Använd 02 05 2016].
- [34] OpenID.Net, "Sponsoring Members," OpenID.net, [Online]. Available: <http://openid.net/foundation/sponsoring-members/>. [Använd 02 05 2016].
- [35] Sign-On, Open Group - Single, "Single Sign-On," [Online]. Available: <http://www.opengroup.org/security/sso/>. [Använd 03 05 2016].
- [36] SAML.XML.org, "List of organizations using SAML," SAML.XML.org, [Online]. Available: <http://saml.xml.org/wiki/list-of-organizations-using-saml>. [Använd 02 05 2016].
- [37] P. Siriwardena, "SECURITY ASSERTION MARKUP LANGUAGE (SAML)," i *Advanced API Security Securing APIs with OAuth 2.0, OpenID Connect, JWS, and JWE*, Berkeley: Apress, 2014, p. 248.
- [38] Open Web Application Security Project, "Authentication Cheat Sheet," OWASP.org, [Online]. Available: https://www.owasp.org/index.php/Authentication_Cheat_Sheet. [Använd 01 08 2016].
- [39] SAML.XML.org, "Federated identity," [Online]. Available: <http://saml.xml.org/federated-identity>. [Använd 01 05 2016].
- [40] D. Rountree, *Federated Identity Primer*, Newnes, 2012.
- [41] R. S. (. L.-1. T. L. L. Hämmerle (SWITCH/GN4-1), "Comparison of Authentication and Authorisation Infrastructures for Research," GEANT Limited on behalf of the GN4-1 project, 2016.
- [42] GEANT, "GEANT - About," GEANT.org, [Online]. Available: <http://www.geant.org/About>. [Använd 01 01 2016].
- [43] eduGAIN, "About eduGAIN," [Online]. Available: http://services.geant.net/edugain/About_eduGAIN/Pages/Home.aspx. [Använd 15 07 2016].
- [44] N. Mörnesten, "Providing Identification Services to External Entities using SAML," KTH, Stockholm, 2011.
- [45] OpenID.net, "Sponsoring Members," OpenID, [Online]. Available: <http://openid.net/foundation/sponsoring-members/>. [Använd 01 01 2016].
- [46] Shibboleth.net, "IdP Discovery," [Online]. Available: <https://wiki.shibboleth.net/confluence/display/CONCEPT/IdPDiscovery>. [Använd 01 01 2014].
- [47] THE APACHE SOFTWARE FOUNDATION, "Apache - Home," Apache.org, [Online]. Available: <https://www.apache.org/>. [Använd 01 11 2016].

- [48] Microsoft, "Internet Information Services (IIS)," Microsoft, [Online]. Available: [https://msdn.microsoft.com/en-us/library/ee532514\(v=vs.90\).aspx](https://msdn.microsoft.com/en-us/library/ee532514(v=vs.90).aspx). [Använd 01 11 2016].
- [49] Wikipedia, "List of programming languages," Wikipedia.org, [Online]. Available: https://en.wikipedia.org/wiki/List_of_programming_languages. [Använd 06 06 2016].
- [50] MySQL, "Why MySQL," [Online]. Available: <https://www.mysql.com/why-mysql/>. [Använd 06 06 2016].
- [51] Shibboleth Identity Provider, "Shibboleth Identity Provider," Shibboleth, [Online]. Available: <https://shibboleth.net/products/identity-provider.html>. [Använd 14 12 2016].
- [52] Verisign, "Home," Verisign, [Online]. Available: <https://www.verisign.com/?dmn=www.verisign.se>. [Använd 01 11 2016].
- [53] Comodo, "SSL Certificate by Comodo," Comodo, [Online]. Available: https://ssl.comodo.com/?track=8252&s_track=7639#_ga=1.167024059.427763852.1478948667. [Använd 01 11 2016].
- [54] H. Bidgoli, Handbook of Computer Networks: Distributed Networks, Network Planning Control, Management, and New Trends and Applications, Copyright © 2008 John Wiley & Sons, Inc., 2008.
- [55] Open Web Application Security Project, "Access Control," OWASP.org, [Online]. Available: <https://www.owasp.org/index.php/Authorization>. [Använd 01 08 2016].
- [56] Grid Identity Pool (GrIDP), "GrIDP - About," gridp.garr.it, [Online]. Available: <https://gridp.garr.it/>. [Använd 01 01 2016].
- [57] Remoterig, "RRC-1258 MkII(s) User Manual," [Online]. Available: http://www.remoterig.com/downloads/RemoteRig_RRC1258-MkII_Users_manual.pdf. [Använd 19 07 2016].
- [58] Remoterig, "RRC - Microbit 2.0 AB," Remoterig.com, [Online]. Available: <http://www.remoterig.com/wp/?s=rrc>. [Använd 19 07 2016].
- [59] AAROC DevOps, "AAROC Ansible LDAP role release," [Online]. Available: <https://zenodo.org/record/11914#.WODn7zt95aQ>. [Använd 11 11 2016].
- [60] Ansible, "HOW ANSIBLE WORKS," Ansible.com, [Online]. Available: <https://www.ansible.com/how-ansible-works>. [Använd 17 07 2016].
- [61] Ansible, "YAML Syntax," Ansible.com, [Online]. Available: <http://docs.ansible.com/ansible/YAMLSyntax.html>. [Använd 01 01 2016].
- [62] Africa Grid, "DevOps Pre-release v0.0.3," africa-grid.org, [Online]. Available: <http://www.africa-grid.org/devops/2014/10/24/DevOps-v0-0-3-Release/>. [Använd 15 07 2016].
- [63] Africa-Arabia Regional Operations Centre (AAROC) , "We are the Africa-Arabia Regional Operations Centre," africa-grid.org, [Online]. Available: <http://www.africa-grid.org/AAROC/>. [Använd 01 08 2016].

- [64] Catania Science Gateway, "Catania Science Gateway - About," catania-science-gateways.it, [Online]. Available: <http://www.catania-science-gateways.it/about>. [Använd 01 08 2016].
- [65] Wikipedia, "Application Programming Interface," Wikipedia.org, [Online]. Available: https://en.wikipedia.org/wiki/Application_programming_interface. [Använd 06 06 2016].
- [66] AMPRNET, "Mobil accesspunkt/gateway/fickserver med stöd för fränkopplad drift," AMPRNET.se, [Online]. Available: <http://amprnet.se/fickservern.html>. [Använd 03 03 2017].
- [67] "What is a CSR (Certificate Signing Request)?," SSL Shopper, [Online]. Available: <https://www.sslshopper.com/what-is-a-csr-certificate-signing-request.html>. [Använd 07 19 2016].
- [68] "JAASAuthnConfiguration," Shibboleth Wiki, [Online]. Available: <https://wiki.shibboleth.net/confluence/display/IDP30/JAASAuthnConfiguration>. [Använd 20 07 2016].
- [69] S. S. Provider, "Shibboleth Service Provider," Shibboleth, [Online]. Available: <https://shibboleth.net/products/service-provider.html>. [Använd 14 01 2016].
- [70] AMPRNet, "Welcome to the AMPRNet Portal," AMPRNet, [Online]. Available: <https://portal.ampr.org/index.php>. [Använd 01 11 2016].
- [71] Un Multimedia, "Searching for Missing After Pakistan Earthquake," unmultimedia.org, [Online]. Available: <http://www.unmultimedia.org/s/photo/detail/100/0100032.html>. [Använd 25 06 2016].

Appendix 1: Installation of SSA Identity Provider (AMPRID)

The SSA IdP (AMPRID) has been setup in a virtual machine running Ubuntu 14.04.4 LTS on a virtual machine server hosted by NUNOC. It is accessed via the web at idp.sa0bxi.se. The setup involves the following steps.

1. Get Ansible

To setup an identity provider server in Linux environment you need some automation tool which automate the all process installations. We are using Ansible which is a fantastic tool can be downloaded from <https://www.ansible.com/get-started>. After installing Ansible there are some settings required in “ansible.cfg” file located in main directory. It is also recommended to create Ansible vault at this step as it is needed in next steps, please see detail in this page http://docs.ansible.com/ansible/playbooks_vault.html

What is Ansible?

Ansible is a radically simple IT automation engine that automates cloud provisioning, configuration management, application deployment, intra-service orchestration, and many other IT needs. It uses no agents and no additional custom security infrastructure, so it's easy to deploy and most importantly, it uses a very simple language (YAML, in the form of Ansible Playbooks) that allow you to describe your automation jobs in a way that approaches plain English [60].

2. Clone or Download DevOps Repository

Download or clone a copy of below repository <https://github.com/AAROC/DevOps> preferably in “/etc/ansible/” folder on your Linux machine.

What is DevOps?

DevOps is a paradigm in the IT services and applications world which assumes a far greater communication between those developing services and those who operate them. There are a lot of interpretations of just what DevOps is, and if you ask the internet, you'll get a lot of discordant answers. Here's just one of many opinions of what it means: Let us consider the context of African e-Infrastructure, in the particular case of the Africa-Arabia Regional Operations Centre [63]. For more detail please read the page:

<http://www.africa-grid.org/devops/2014/10/24/DevOps-v0-0-3-Release/>

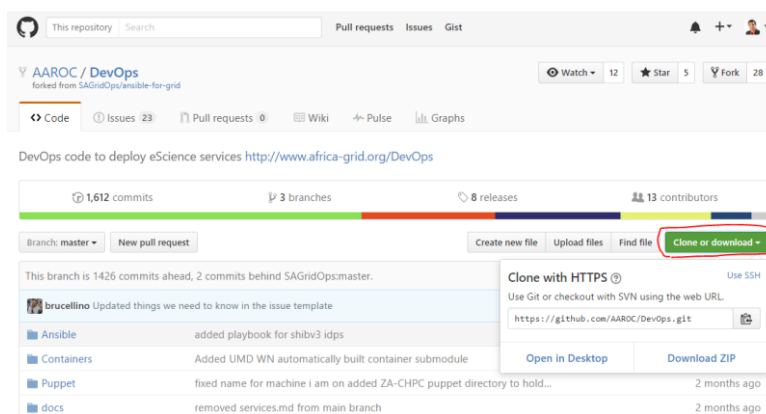


Figure 51: AAROC/DevOps

3. Configure Host Inventory

In this step, you need to create Inventory for hosts given example as below. In cloned repository, there is folder called “/etc/ansible/DevOps/Ansible/inventories” if you have multiple inventories you can place under it.

LDAP-servers and Shibboleth-Idps are default attributes, you can mention host name(s) under it to include in your inventory. Host name can be IP address or hostname like www.hostname.com. You can read installation instruction on this page:

<https://github.com/AAROC/DevOps/wiki/idp-ldap-playbook>

```
[ldap-servers]
#idp.se.ampr.org needs_certificate=true ansible_user=bruce
idp.sa0bxi.se needs_certificate=true ansible_user=qasim

[shibboleth-idps]
#idp.se.ampr.org needs_certificate=true min_jvm_size=1024m ansible_user=bruce
idp.sa0bxi.se needs_certificate=true min_jvm_size=1024m ansible_user=qasim
[identity-ssa:children]
ldap-servers
shibboleth-idps

[Debian-servers:children]
identity-ssa
```

4. Configure Bootstrap

Here we can customize “bootstrap.yml” as given below according to our need.

```
# This is the bootstrap play for AAROC machines.
- name: bootstrap the machines
  hosts: all
  become: true
  roles:
# we don't need become here, because bootstrap is designed to run as root.
  - bootstrap
```

```

pre_tasks:
- name: debug
  debug: var=site_name
- name: Send Slack Message
  slack:
    domain: africa-arabia-roc.slack.com
    token: sBWZXBHgua6QqSnj6QDw9bFE
    msg: "Starting bootstrap on {{ inventory_hostname }} at {{ site_name }}"
    channel: "#devops-bootstrap"
    username: "Ansible on {{ inventory_hostname }}"
    #icon_url: "http://www.example.com/some-image-file.png"
    link_names: 1
    parse: 'full'
  tags:
    - slack
post_tasks:
- name: Send notification message via Slack
  slack:
    domain: africa-arabia-roc.slack.com
    token: sBWZXBHgua6QqSnj6QDw9bFE
    msg: "bootstrap on {{ inventory_hostname }} has run at {{ site_name }}"
    channel: "#devops-bootstrap"
    username: "Ansible on {{ inventory_hostname }}"
    #icon_url: "http://www.example.com/some-image-file.png"
    link_names: 1
    parse: 'full'
  tags:
    - slack

```

5. Configure ldap-idp.yml / mysql-idp.yml

In above mentioned repository, there is file called “idp-ldap.yml” if you are setting up an identity provider using Lightweight Directory Access Protocol (LDAP) as back-end for user management you can customize the file according to your identity provider configuration.

I have used MySQL which means I have removed some roles like LDAP and other and customized this file according to my requirement as given below.

```

- hosts: idp.sa0bxi.se
  name: Configure Shibboleth Identity Provider
  environment:
    JAVA_HOME: /usr/lib/jvm/default-java
  pre_tasks:
    - name: Install pip
      become: yes
      apt: name='python-pip' update_cache=yes

    - name: Update pip
      become: yes
      pip: name='pip' state=latest

    - name: Install pexpect
      become: yes
      pip: name='pexpect' state=latest

```

```
roles:
  - osct.shibboleth-idp-v3
```

6. Run the commands on Ansible

After above all steps are completed you can run these commands on Linux terminal. This will install most of the roles like Shibboleth-IdP, LDAP, Tomcat and others. It will ask Ansible vault pass together with root user password.

- `ansible-playbook -k -u root --ask-vault-pass /etc/ansible/bootstrap.yml`
- `ansible-playbook -k -u root --ask-vault-pass /etc/ansible/idp-ldap.yml`

7. Get SSL Certificate

To get Secure Socket Layer (SSL) certificate from any SSL authority certificate signing request (CSR) is needed.

What is Certificate Signing Request (CSR)

CSR is encrypted text which is generated on the server that will be used by certificate authority to create SSL certificate. It has some public information including organization name, domain name, locality, country. It also includes public key which include in certificate later on [67]. On following link, there is detailed information about how to generate CSR.

<https://www.instantssl.com/ssl-certificate-support/csr-generation/java-ssl-certificate.html>

You can get free trail SSL certificate from <https://ssl.comodo.com/free-ssl-certificate.php>.

8. Configure IP Table

This step can be skipped if using two different machines for IdP and SP. In my case I am using same machine for IdP and SP. All HTTP requests must be forward to HTTPS for secure communication to do that HTTP default port 80 needs to forward on HTTPS default port 443 for SP and IdP is using port 443 which is going be forward on port 8443.

- `sudo iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 443`
- `sudo iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8443`
- `sudo sh -c "iptables-save > /etc/iptables.rules"`
- `sudo apt-get install iptables-persistent`

More details can be found on following link:

<https://wiki.jenkins-ci.org/display/JENKINS/Running+Jenkins+on+Port+80+or+443+using+iptables>

9. Configure Attributes Resolver

Attributes and LDAP need to configure in this step, in my case I am not using LDAP rather MySQL database connector needs to be configured in attribute resolver file found in this path `"/opt/shibboleth-idp/conf/attribute-resolver.xml"`.

Attributes

```

<!-- Schema: Core schema attributes-->
<resolver:AttributeDefinition xsi:type="ad:Simple" id="uid" sourceAttribute$
  <resolver:Dependency ref="mySIS" />
  <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:di$
  <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:0.9$
</resolver:AttributeDefinition>

<resolver:AttributeDefinition xsi:type="ad:Simple" id="mail" sourceAttribut$
  <resolver:Dependency ref="mySIS" />
  <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:di$
  <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:0.9$
</resolver:AttributeDefinition>

```

Database

```

<!-- Example Static Connector -->
<!-- Example Relational Database Connector -->
  <resolver:DataConnector id="mySIS" xsi:type="dc:RelationalDatabase">
    <dc:ApplicationManagedConnection jdbcDriver="com.mysql.jdbc.Driver"
      jdbcURL="jdbc:mysql://localhost/ssa_db"
      jdbcUserName="myUserName"
      jdbcPassword="XXXXXX" />

    <dc:QueryTemplate>
      <![CDATA[
        SELECT * FROM user WHERE UserName = '$resolutionContext.principal'
      ]]>
    </dc:QueryTemplate>
  </resolver:DataConnector>

```

10. Configure Attribute Filter

Attribute filter needs to be configured to define what attributed should be available in exchange information between IdP and SP. Attribute filter file found in path “/opt/shibboleth-idp/conf/attribute-filter.xml”.

```

<AttributeFilterPolicyGroup id="ShibbolethFilterPolicy"
  xmlns="urn:mace:shibboleth:2.0:afp"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:mace:shibboleth:2.0:afp
http://shibboleth.net/schema/idp/shibboleth-afp.xsd">
  <AttributeFilterPolicy id="global">
    <PolicyRequirementRule xsi:type="ANY" />
    <AttributeRule attributeID="eduPersonPrincipalName">
      <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="uid">
      <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="mail">
      <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="surname">
      <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="givenName">
      <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
  </AttributeFilterPolicy>
</AttributeFilterPolicyGroup>

```

11. Configure IdP Properties

There are general properties which need to configure like IdP path, cookies and others in file found in path “/opt/shibboleth-idp/conf/idp.properties” example mentioned below, reset is as default.

```
# Set the entityID of the IdP
idp.entityID= https://idp.sa0bxi.se/idp/shibboleth
# Set the scope used in the attribute resolver for scoped attributes
idp.scope= sa0bxi.se
# General cookie properties (maxAge only applies to persistent cookies)
idp.cookie.secure = true
#idp.cookie.httpOnly = true
idp.cookie.domain = idp.sa0bxi.se
#idp.cookie.path =
#idp.cookie.maxAge = 31536000
```

12. Configure MySQL JDBC for Shibboleth IdP

In this project, MySQL has been used instead of LDAP was not suitable for our project. To configure MySQL as backend for Shibboleth IdP, MySQL JDBC drivers called Connector/J is needed which can be downloaded from this link

<https://dev.mysql.com/downloads/connector/j/>. After download, it need to copy to “/opt/shibboleth-idp/bin/lib”

13. Configure JAAS DB Authenticator

Java Authentication and Authorization Service (JAAS) is an authentication mechanism Shibboleth has provided support for using JAAS as a back-end for the password authentication login flow [68]. We have searched a lot about JAAS plugin for Shibboleth IdP V3 but could not find any readymade solution. I did collaboration with [Marco Fargetta](#) from Catania Italy and during that we have been successfully customized a JAAS plugin for MySQL for Shibboleth IdP V3 from an old plugin code. JAAS4DB jar file need to copy in path “/opt/shibboleth-idp/webapp/WEB-INF/lib”.

Plugin is available for reuse on GitHub <https://github.com/AAROC/tagish-jaas>.

14. Customize Views

Shibboleth IdP has default graphical user interface (GUI), You can customize it according to your requirements. You can find front-end page (login, logout, password and others) in “/opt/shibboleth-idp/views”.

15. Run Build.h

Above steps have updated the original java file (Idp.war) for Shibboleth IdP to use MySQL as backend data storage. The file “Idp.war in “/opt/shibboleth-idp/war” needs to update. There is

build file available in “/opt/shibboleth-idp/bin” needs to run so new “idp.war” file can be compiled according to above changes. It is very important step if missed will not able to see changes on Shibboleth IdP.

16. Tomcat Configuration

To run Shibboleth IdP properly, SSL certificate is required to configure with it, following is tomcat configuration file available in “/opt/tomcat/conf/server.xml”. Path for key store file and password for the key store is required which was created while CSR generation in previous step. You need to restart tomcat after below configurations.

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
SSLImplementation="edu.internet2.middleware.security.tomcat6.DelegateToApplicationJSSEImplementation" scheme="https" SSLEnabled="true"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" clientAuth="false" keystoreFile="path_to_keystore" keystorePass='some_password' />
```

17. Joining IdP Federation

This step can be skipped if setting up an independent IdP. For test purposes SSA IdP and SP joins Grid Identity Pool (GrIDP).

Grid Identity Pool (GrIDP)

Grid Identity Pool (GrIDP) is an identity federation is a cross domain/cross border identity federation. It is spanning on multiple continents to simplify, facilities and promote the use and the adoption of shared electronic research services and resources across the world. It is two main goals as follows. [28]

- A home to IdP and SP which is not yet member of any national federation
- To provide authentication services for users not member of any IdP.

GrIDP provides several core services such as a "catch-all" IdP for home-less users, an IdP matching social identities and a multi federation discovery service. The discovery service of GrIDP can also be used by SPs of one or more of the following identity federations CAFe, CARSI, COFRE,eduGAIN, EduIDM, GRNET, IDEM, RCTSAAI, SIR and SWAMID. [28] For more detail please read the page <https://gridp.garr.it/>



Figure 52: GrIDP [28]

Metadata

To be part of any identity federation IdP owner needs to provide metadata to identity federation and also needs to configure the path in “/opt/shibboleth-idp/conf/metadata-provider.xml”. Metadata is available in “/opt/shibboleth-idp/metadata/”. Example metadata is available on this link:

<https://idpopen.garr.it/metadata/idp-metadata.xml>.

```
<MetadataProvider id="gridp-test" xsi:type="FileBackedHTTPMetadataProvider"
metadataURL="https://gridp.garr.it/metadata/gridp-test.xml"
backingFile="{idp.home}/metadata/gridp-test.xml">
</MetadataProvider>
```

Appendix 2: Installation of SSA Service Provider (AMPRemote)

1. Installation

If you run “idp-ldap.yml” given in the repository as mentioned in steps above, it will install most of the roles and software (shibboleth IdP, LDAP and others) itself.

To host service provider (SP) portal on the same machine we need to install Apache, PHP and MySQL you can install these by following commands.

```
sudo apt-get update
```

1. Install Apache

```
sudo apt-get install apache2
```

2. Install MySQL

```
sudo apt-get install mysql-server libapache2-mod-auth-mysql php5-mysql
```

3. Install PHP

```
sudo apt-get install php5 libapache2-mod-php5 php5-mcrypt
sudo service apache2 restart
```

More details can be found on this page:

<https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-ubuntu>.

2. SP Configuration

There are many ways to configure SP with IdP in this project the most common method, Shibboleth SP [69] has been used. For this purpose, Shibboleth SP Daemon needs to install.

Shibboleth SP Daemon

Shibboleth Daemon (ShibD) is process which processes all SAML assertions together with Apache. Apache has module called “mod_shibd” for it, which sends assertions to ShibD process. ShibD and mod_shibd are two difference processes need to install for SAML Web SSO.

Following are the steps to configure Shibboleth SP Daemon.

1. Install ShibD

Run following command to install Shibboleth Daemon.

```
sudo apt-get install libapache2-mod-shib2
```

2. Configure ShibD

To configure ShibD metadata needs to configure according you IdP entities. You need configure “/etc/shibboleth/attribute-map.xml” and attribute-map.xml if you have defined attributes other than default in IdP configurations.

3. Define Metadata

To make it work with identity federation you can need to describe your own metadata for your SP. You can generate it with tool that comes with Shibboleth SP package by running following command.

```
shib-metagen -c /etc/ssl/certs/yourcertificate.crt -h yourhost.yourdomain > /etc/shibboleth/yourSP-metadata.xml
```

4. Copy Certificate Fie in Shibboleth Directory

SSL certificate needs to copy in path “/etc/shibboleth/”.

5. Setup Apache for Shibboleth

First you need to enable Shibboleth’s Apache module by running following command.

```
a2enmod shib2
```

After this step, you need to edit apache default site configuration file which is located on path “/etc/apache2/sites-available/default-ssl.conf”.

Below is example configurations snippet used.

```
<Location /api/>
    AuthType shibboleth
```

```

        ShibRequestSetting requireSession 1
        require valid-user
    </Location>
    <Location /index.php>
        AuthType shibboleth
        ShibRequestSetting requireSession 1
        require valid-user
    </Location>
    <Location /app/>
        AuthType shibboleth
        ShibRequestSetting requireSession 1
        require valid-user
    </Location>

```

6. SSL Certificate

With above step, you have to add SSL certificate path in apache config.

```

SSLCertificateKeyFile "/path/my.key"
SSLCertificateFile    "/path/certs.pem"

```

7. Restart ShibD

This is very important step after above configurations you have to restart ShibD and Apache by using following commands.

- `sudo /etc/init.d/shibd restart`
- `sudo service apache2 restart`

8. Access Attributes in Application

Below is example how to access shibbolized attributes.

```

<html>
<body>
<?php
echo "Hello world !";
// Do we have any variables defined in attribute map
if (isset($_SERVER['eppn'])){
echo 'Hello ' . $_SERVER['cn'] . ' from ' . $_SERVER['o'] ;
}
// or any attributes starting with Shib-
else {
echo 'You are unknown !';
}
?>
</body>
</html>

```

If you need more details can be found this page <http://federation.belnet.be/?q=node/24>

TRITA-ICT-EX-2017:41