Centralized Digital Certificate Issuing System

Priya Gaonkar[1], Pranali Daruwale[2] , Prof Nagmani K.[3]

[1,2] Student, Computer Engineering, Shivajirao S. Jondhale College of Engineering, Maharashtra, India
[3] Professor, Dept. of Computer Engineering, Shivajirao S. Jondhale College of Engineering, Maharashtra, India

---***---

Abstract - *Eduroam is the world-wide standard Wireless LAN (WLAN) roaming system for educational institutions. In the present eduroam system, many institutions authenticate users by identification and password but, the demands for authentication by digital certificates are increasing for better protection and high security. There is a high complexity in the digital certificate issuing and distribution process at each organization can be a great problem. We have developed online sign-up system for authentication since manual ID distribution is imposing heavy burden to the institutional administrators in the current authentication system. In addition we can access a file only if we have digital certificate. The proposed systems are effective also for the disruption-tolerant authentication architecture, which realizes more stable and efficient eduroam system.*

***Key Words*: eduroam, wireless LAN roaming, digital certificate, online sign-up.**

1. INTRODUCTION

Many of the universities and research institutions today deploy campus wireless LAN (WLAN) system, and the students, staff and researchers are utilizing it in their day to day activities. The chances that the people in those institutions visit other institutions for conferences, collaborative research meetings, etc., have increased. Consequently, it is necessary for the users to be able to get network accesses at even visited sites. Eduroam is de-facto standard wireless LAN roaming system for research and educational institutes, enables a utilizer to access wireless network at the visiting institution with the personal account issued by his/her home institution.

Eduroam validate clients based on IEEE802.1X [2], which utilizes Extensible Authentication Protocol (EAP) [3]. EAP supports various types Authentication methods. Up until now in eduroam, PEAP and EAP-TTLS have been broadly utilized to acknowledge ID/password client verification. These days, the requests for verification by EAP-TLS [4] are expanding. In EAP-TLS, digital certificate are used for confirming user (terminals). Once a digital certificate has been introduced on the terminal, the client is liberated from re-writing ID/password even if the save credentials is incidentally lost, which is a typical circumstance with a few working frameworks. Accordingly, the ease of use can be enhanced exceptionally much.

1.1 Problem Statement

As eduroam signup process was manually, the students/faculties have to go through their respective registers to fill the pen paper based form and apply for the certificate. The details of the students are recorded manually. The administrator has to manually go through the registers to check the details of a particular student for in putting it into eduroam database. There was no automatic mechanism for automated generation of digital certificate. Whenever the administrator adds, updates or deletes a student, the basic details of the student is not updated accordingly in all other records related to that student.

1.2 Proposed System

In this paper we propose a Centralized Digital Certificate issuing System. We have developed online signup system to reduce the burden of the Institutional Administrator at every institution. The system will enable the end-users to sign-up and get on board easily. And user will also be able to access the required file. User can access this system through his/her mobile phone or Computer.

2. Centralized Digital Certificate Issuing System

Managing and issuing digital certificate at each institution impose a heavy labor for the institution. For realizing these system and introducing it to client user

Authentication by client certificates, a service that issues and manages digital certificates is needed. Regarding costs of operating Certificate Authority (CA), introducing CA at each institution is not practical. So we have deployed Centralized Digital Certificate issuing system for WLAN Roaming and can access a file after that.

2.1 System Working:

The below fig-1 shows process of Centralized Digital Certificate Issuing System. In the proposed system, we have introduced a web user interface. A user can ask for a digital certificate and download it on the interface. Furthermore we have introduced a function of accessing a file after getting a digital certificate.

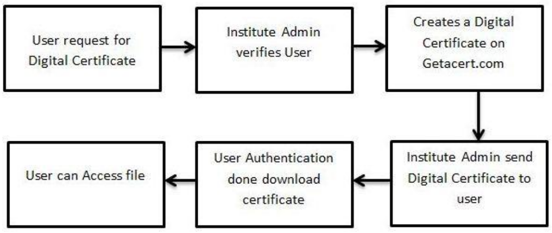

User request for Digital Certificate
Institute Admin verifies User
Creates a Digital Certificate on Getacert.com
Institute Admin send Digital Certificate to user
User Authentication done download certificate
User can Access file

Fig 1: Block Diagram of Centralized Digital Certificate Issuing System

In this system if a new user visits this system, user will have to get registered to the system. Then the user will have to sign up thorough credentials and will be verified by verification process (One Time Password). The entire user's information is stored in database. The Institute Administrator will login into the system using his credentials. Later, admin will receive list of students who have requested for digital certificate, update of digital certificate and requested for accessing a file. First the user is checked in the database; if the user is found in the database then admin will proceed to user's request for creating a digital certificate. Digital Certificate is done OpenSSL [6] in our system. User downloads certificate at its end in browser. When the user download digital certificate he will be validated through OTP (One Time Password) after that digital certificate will be downloaded.

[5] The below fig-2 shows how user will download and install digital certificate at user end. User will have to go through different process according to terminal. On can install digital certificate by following steps shown on screen. To install certificate on Android there some complex steps.

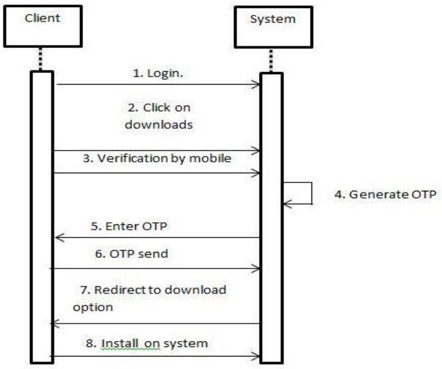
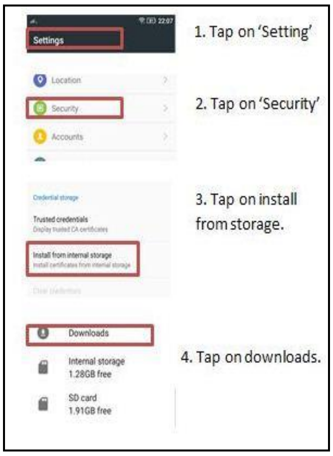


Fig 2 Installing Digital Certificate on Pc



1. Tap on 'Setting'

2. Tap on 'Security'

3. Tap on install from storage.

4. Tap on downloads.

Fig 3: Installing certificate on Android

2.2 Accessing a file

Here in this system after receiving digital certificate user will able access a file for that user clicks on Authenticate user option there he/she will able download file.

3. CONCLUSIONS

We have developed a centralized digital certificate issuing system based for online sign-up system to reduce the burden to the institutional administrators. Using the certificate based authentication instead of ID/password-based one is considered effective in improving both the usability and the stability of eduroam. The Project entitled "Centralized digital certificate issuing system" has been developed and satisfies all proposed requirements. The system will be highly scalable and user friendly. Almost all the system requirements will be met. This system will help in managing sign-up system and reduce time requirement. The features and the functionality of the current system can also be applied to Portable computing devices and operating systems like Android OS, iOS, Windows OS etc.

ACKNOWLEDGEMENT

We are thankful to this institute to channelize our skills and encourage us to work together with cooperation and co-ordination .We would like to thank our project guide Prof. Nagmani K. for her encouragement and tremendous guidance throughout the making of this project.

REFERENCES

[1] L. Florio and K.Wierenga, "Eduroam, providing mobility for roaming users," *Proceeding of EUNIS*, 2005.

[2] P. Congdon, B. Aboba, A. Smith, G. Zorn and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines," IETF RFC3580, September 2003.

[3] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H.Levkowetz, Ed., "Extensible Authentication Protocol (EAP)," IETF RFC3748, June 2004.

[4] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz,Ed., "Extensible Authentication Protocol (EAP),"IETF RFC3748, June 2004.

[5] [IEEE Paper] Tomo NIIZUMA and hideaki GOTO Centralized Online Sign-up and Client Certificate Issuing System for eduroam" 2014 IEEE 38th Annual International Computers, Software and Applications Conference Workshops.

[6] OpenSSL, https://www.openssl.org/