Centralized Approach for a Unified Wireless Network Access

Jan David Nose[1], Jaromir Likavec[2], Christian Bischof[3], and Arjan Kuijper[2,4(✉)]

[1] Fraunhofer-Gesellschaft e.V., Competence Center LAN, Darmstadt, Germany
[2] Fraunhofer Institut für Graphische Datenverarbeitung (IGD), Darmstadt, Germany
[3] Scientific Computing and University Computing Center, Technische Universität Darmstadt, Darmstadt, Germany
[4] GRIS, Technische Universität Darmstadt, Darmstadt, Germany
arjan.kuijper@igd.fraunhofer.de

Abstract. In this paper, a concept is presented that allows to deploy a unified wireless network access for all employees in organizations with heterogeneous network environments. It is designed to be easy to implement and to maintain. Also, it focuses on usability, removing the need for manual actions to obtain network access when roaming between locations. The concept has been tested in the Fraunhofer-Gesellschaft, and has proven to solve its requirements. It can be deployed with only a small team thanks to the reduced complexity in the branch locations, and it can also be maintained without much effort since ongoing manual tasks have been avoided. Since it is based on open standards, it can easily be customized to match the requirements of the individual organization, or be extended with future improvements. For research and education organizations it is particularly useful that this concept can be integrated with eduroam seamlessly. This allows not only the own employees to roam between locations, but also guests from other participating institutions.

1 Introduction and Motivation

The Fraunhofer-Gesellschaft is one of Europes largest research organizations with approximately 22,000 employees that work in over 60 different institutes. It has unique structure where its institutes operate almost independently, similar to autonomous enterprises [4–6]. This includes total control over the institutes network foundation, with only a few restrictions, which has led to a variety of network infrastructures with different vendors, concepts and technologies in use. Especially wireless networks differ due to financial reasons and, often in smaller institutes, a lack of expertise.

The technological advance of the last ten years has led to a rising number of mo-bile devices people work with. These devices rely on a wireless network, and play a more and more vital role in the workings of employees. For this reason enterprises should consider providing a reliable wireless network that can be used by employees.

S. Yamamoto (Ed.): HIMI 2015, Part I, LNCS 9172, pp. 547–559, 2015.
DOI: 10.1007/978-3-319-20612-7_52

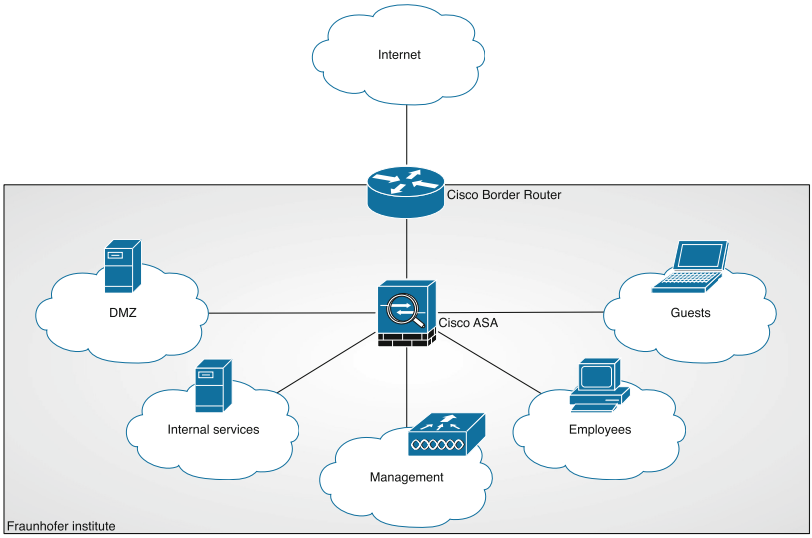

Fig. 1. Scheme of a generic network

Using the Fraunhofer-Gesellschaft as an example, this paper presents a concept how a unified wireless network access can be provided in institutions with multiple locations and heterogeneous network infrastructures. The solution must work independent of the local network infrastructure and it must not be vendor-dependent. To be applicable to research organizations and enterprises, it must also provide reasonable security for the users credentials.

Additionally, the concept is designed to be both easy to use and easy to maintain. The ease-of-use is important for acceptance by the employees, as well as for usability and productivity in general. The solution must be easy to maintain, since it should provide a unified access for all employees in all locations.

2 Prerequisites

This chapter discusses the perquisites in the Fraunhofer-Gesellschaft, and where those apply to other institutions as well. The problems of current solutions are shown, and consequently requirements for a new solution are established.

2.1 Generic Network Design in an Institute

The highly independent nature of the Fraunhofer-Gesellschafts institutes has led to a wide variety of network designs. The following description introduces a very generic network design and indicated the differences that exist in comparison to the institutes actual networks (Fig. 1).

First, it must be not noted that all institutes operate a similar border router and the same firewall appliance. This enables the creation and use of site-to-site VPN connections, and the deployment of a unified security concept for the whole society.

The institutes network is divided into several subnets. The details vary, but normally a certain set of subnets exists in every institute. Those include a subnet for employees and departments, four for the DMZ, and one for guests. The subnet for employees has mostly total access to internal resources and the internet, while the guest network is restricted from accessing any internal resources, and often also restricted with regard to internet access.

The implementation of this network design differs between institutes, since they have different requirements and equipment. Most institutes operate equipment by Cisco Systems [3], but hardware by Juniper Networks [7] and Extreme Networks is also in use. But even if two institutes operate the same hardware, software versions and configurations diverge greatly. This results in a wide variety of computer networks, as design, hardware and software differ between institutes. As a result, solutions for a unified wireless network access, provided by network vendors, are not applicable, since they work only with a set of institutes.

Although the analysis above is specific for the Fraunhofer institutes, similar net-works are operated by universities and enterprises. It is not always possible to maintain a homogeneous network throughout an organization, which makes it impossible to rely on a solution provided by only one vendor of network equipment.

2.2 Existing Wireless Network Access Methods

Currently, no unified solution for a wireless network access for all employees exists in the Fraunhofer-Gesellschaft. Most institutes operate wireless networks that offer access to the employees of that specific institute, and some even provide wireless networks for guests. But the details differ greatly, which proves to be problematic, especially when institutes cooperate closely and employees travel a lot between them.

Typically, a guest has to request access to a wireless network from the local IT department, where ideally a unique, temporary account is created for the guest. Most times, the wireless network itself is not secured with a key, but the account credentials have to be entered into a Captive Portal in the users internet browser. This solution can very easily be deployed, requires no additional hardware, but has a lot of down-sides.

First of all, the process of how to request access differs from institute to institute, and is most often not standardized. This makes it difficult for employees visiting other institutes to gain internet access. Second, the wireless network is unsecured, allowing to capture a users traffic and analyze it if the user does not take additional security measures like using a Virtual Private Network (VPN). Often, users are not aware of this, and leave their connections unsecured. Especially in enterprises and research organizations, this poses as a security thread to the whole organization as sensitive information could be captures.

Third, mobile devices like smartphones do not offer comfortable interfaces to enter the credentials, especially if they are complex. This reduces usability, especially if the connection is disconnected regularly for security reasons, and the user has to reenter his credentials.

All in all, these restrictions often led to the employee choosing cellular networks over wireless local area networks, as they are easier to use with mobile devices, and do not require the effort to obtain and use temporary credentials. But cellular net-works are more expensive, provide less performance and are often unavailable inside buildings. This problem is not specific to the Fraunhofer-Gesellschaft.

In summary, the following problems or issues have to be solved by a new solution to provide an easy-to-use, truly unified wireless network access:

- In every institute a custom solution for wireless network access exists
- Manual actions by the IT department or the user are almost always necessary
- The guest network does not provide a satisfying user experience
- The guest network does not provide reasonable security

Analyzing these problems yields a set of requirements that are presented in the next section.

2.3 Requirements of a Unified Wireless Network Access

In the last section, the greatest problem with current solutions have been described. To solve those issues and to consider the technical distinctiveness of heterogeneous networks, the new solution needs to fulfill certain requirements. On the technical side, the concept must be applicable to all locations, which means it must be scalable and independent of vendor-specific technologies or protocols. Because the concept should be applicable to enterprises and research organizations, security is also an important concern. The necessary infrastructure must provide an adequate level of security for both the users credentials and traffic.

Additionally, the concept must be easy to implement and later on to maintain. The goal is to provide a unified access for all employees, which means that every location of an organization implements the solution and provides support for the local staff. Especially the maintenance and support requirements must be reduced to guarantee wide adaptation of the unified access method.

But most importantly, the solution must be easy to use. The first reason for this is that it must compete with cellular networks which work out-of-the-box. The second reason is that with over 22,000 employees in case of the Fraunhofer-Gesellschaft, tens of thousands of devices need to be configured. This is simply not possible in a reasonable amount of time if either a complex configuration or regular reconfiguration is required. Ideally, devices need to be configured only once, without the need to touch them again to access the network. This would result in a user experience similar to cellular networks, with the benefit of more performance and less cost.

To summarize, the requirements for a unified wireless network access are:

- It must be scalable
- It must be vendor-independent
- It must provide reasonable security

– It must be easy to implement
– It must be easy to maintain
– It must be easy to use
– It should remove the need for manual actions

3 Potential Solutions

After establishing the requirements, three different approaches are presented that would solve the given problem.

3.1 Unsecured Guest Network

First, the aforementioned unsecured guest network is a viable solution. An open wireless network allows all guests to connect, and configured properly requires them to establish a VPN connection to secure their traffic. This solution is supported by all network equipment available, and requires almost no additional effort. But the usability is very low, because users must connect to a VPN gateway before they can use the internet. Besides introducing additional effort on the user, it also drains the battery life of mobile devices faster.

3.2 Vendor-specific Solutions

Second, vendor-specific solutions are available to connect at least the majority of locations. Designs suggested by major network manufacturers are based on the idea of one or two main locations, and a bunch of branch offices. Since the Fraunhofer institutes operate highly independent, and have different requirements than typical branch offices, this approach is difficult to implement, and cannot provide a truly unified wireless network access to all employees.

3.3 RADIUS Roaming Network

Third, a solution based on a RADIUS roaming network can be deployed. This roaming networks acts as an authentication backend for local wireless networks. RADIUS is a very widespread protocol, and is supported by every wireless network equipment available today. In combination with WPA2-Enterprise, a secure and vendor-independent wireless network can be provided. One example of an RADIUS roaming network is eduroam (http://eduroam.org, [10]), which allows members of research and education facilities to use the service worldwide. eduroam has an hierarchical infrastructure (Fig. 2), where different parties interact to provide the service together. On the lowest level, individual institutions provide two functionalities. First, they manage user credentials and operate an authentication server to authenticate those users, and second they operate an access network that allows users to access internet services once they authenticated successfully. The first role is called an Identity Provider, while the second role is called Service Provider.

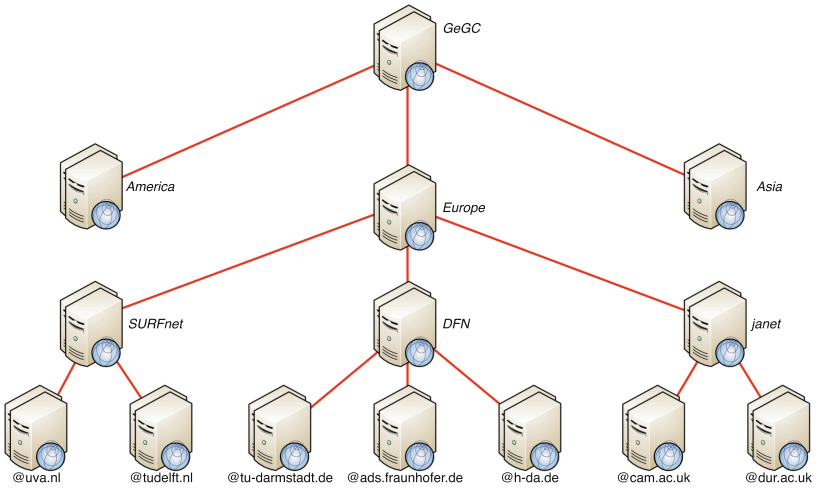

Fig. 2. Excerpt from eduroam hierarchy

Since RADIUS roaming networks are totally independent of vendors, and can be combined easily with secure wireless authentication methods, a solution based on such a network is the most appropriate choice for a unified wireless network access. eduroam proves that by providing network access to thousands of users worldwide.

4 Concept for a Unified Wireless Network Access

Looking back at the different solutions introduced in the last section, and the requirements summarized in the section before that, none of the presented solutions satisfy them all. But one does satisfy most of them, and that is the approach of a RADIUS roaming network. It is scalable, as shown during years of operation in eduroam, and it is vendor-independent, as it relies heavily on standardized technologies. However, it is not necessarily easy to implement in distributed environment. And although it is easy to use by the end-user, the administration is complex due to the high number of different components. The following section discusses how the concept of eduroam can be adapted for organizations like the Fraunhofer-Gesellschaft by reducing its complexity.

4.1 Introduction

Analyzing the roles defined by eduroam for the operation of the service, it becomes clear that the operation of an Identity Provider is more complex than that of a Service Provider. The reason for this is that most organizations and institutes already operate wireless access networks, which can easily be extended to provide access to roaming users. But managing user credentials and providing authentication endpoints can be much more difficult in large and distributed organizations.

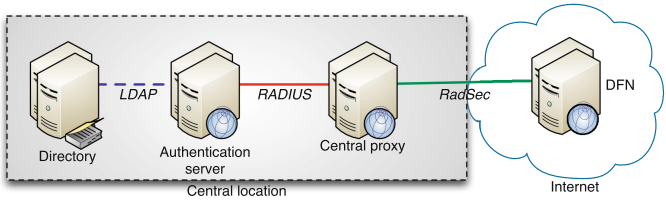

Fig. 3. Infrastructure of centralized IdP

The logical consequence is that to reduce the efforts required to deploy a unified wireless network access, it is necessary to reduce the complexity of the authentication solution. Therefore, we propose a design where one Identity Provider is responsible for the whole organization, while the single locations only provide the access networks. This approach requires a centralized authentication service, though. Figure 3 shows the central authentication infrastructure with its components and connections. The following section more clearly defines the role of the central authentication service.

4.2 Design

In this section, the different components of the concept are discussed. To achieve the goal of easy implementation and maintenance, the concept splits the responsibilities in a centralized authentication service and local service providers.

Centralized Authentication Service. The centralized authentication service consists of several components that need to be deployed and maintained. First, a user database has to exist that can be used to authenticate users. To provide network access to all employees, this requires that every user has an account in the central database. Depending on the deployment, this can either be an already existing account that is also used for other services, or a new account solely for this purpose. While the second option introduces additional over-head in managing a second account, it provides additional security benefits as the account credentials cannot be used to authenticate against other services of the organization.

Second, an authentication server is required. It must support authentication via the RADIUS protocol, and to secure the users credentials should require that authentications use the Extensible Authentication Protocol (EAP, [1]) with encryption of the users credentials. Due to the number of possible configurations and combinations regarding EAP, the secure configuration of an authentication server requires a lot of knowledge, which is one reason that is implementation and operation should be centralized. Not all locations may have the expertise to provide a secure configuration of an authentication server, especially when compatibility with a lot of client operating systems is required.

By reducing the number of authentication servers, ideally to only one central cluster, the required amount of effort to deploy a unified wireless network access

is reduced significantly. Furthermore, a small team can be trained to handle the issues that arise during operation, which reduces response times to support requests and allows for a more stable usage. Especially with EAP methods with encryption, the local IT departments are no longer able to support their users with regard to authentication failures. Since all information is hidden from the network devices, and is only available at the authentication server, support requests must be directed at the maintainers of this server. This in return provides an even greater benefit to the locations, as the overhead of grating network access is fully outsourced and centralized.

Centralizing the authentication service has some additional benefits:

- The service can be used from day one by all employees in range of an access net-work.
- Focusing all efforts on a central service allows to deploy greater redundancy and achieve higher availability than it would have been possible if every location need-ed their own infrastructure.
- Since the locations only need to provide a wireless access network, the solution can be deployed very rapidly in many locations at once. This allows to scale the unified access very quickly over the whole organization.

Decentralized Service Provider. The responsibility of a service provider is to operate a wireless access network that users can connect to. Since most locations today already operate wireless networks, adding another one is no difficult task. Configuring it to communicate with the central authentication server can be more difficult, though. Experience has shown that several issues exist with the operation of wireless access networks with WPA2-Enterprise configurations. While the solution is very secure in terms of data layer encryption and privacy of user credentials, configuring such a network on a mobile device can be complex due to the large number of configuration parameters. In the operation of eduroam, for example, we have observed a high number of authentication requests that is spawned regularly by misconfigured clients, which try to reconnect constantly independently of the authentication servers response to the first request.

While it would technically suffice to install a central RADIUS server, against which the local wireless infrastructures authenticate directly, several risks exist with regard to this design in large deployments, the greatest being overloading the central authentication server. Especially in the context of roaming networks like eduroam, a huge performance improvement can be achieved if faulty requests are discarded or rejected before ever reaching the authentication server.

For this reason, a local RADIUS proxy is deployed. Its only purpose is to accept authentication requests from the local wireless infrastructure, and forward valid re-quests while rejecting faulty ones. This allows to greatly reduce the load on the central authentications servers, introduce load balancing and save bandwidth. The configuration of the server is identical for all its instances, so it is very easy to deploy and manage it using modern DevOps tools.

Deploying a local proxy has two additional benefits. First, it abstracts from the local infrastructure, and provides a single communication gateway. This makes it easy to configure firewall rules and secure the traffic between authentication server and institute. This is especially true since second, the local proxy provides an extensible connection to the authentication server. Independent of the location and its equipment, the connection between the authentication and proxy servers can be secured with state of the art technology without having to deal with restrictions by the local networking equipment.

Overall, in large deployments outweigh the benefits of this solution the additional cost of deploying and maintaining the local proxy. Using this approach, the deployment of the unified wireless network access is reduced to the deployment of the local proxy, and the configuration of a wireless access network.

Connecting Proxy and Authentication Server. Since the locations are most likely distributed, untrusted networks like the internet have to be used to communicate between them. This requires that additional security measures are taken to secure the privacy of RADIUS traffic, which is by its nature unencrypted.

The first solution would be to establish a VPN connection between the location and the main office, and tunnel all RADIUS traffic through it. A VPN link is most likely already established between the locations to encrypt sensitive traffic, which makes this approach very easy to deploy.

Alternatively, the protocol RadSec can be used. It is an extension of RADIUS, and used TCP and TLS to establish stateful, encrypted connections between RADIUS servers [11]. In case both sides support RadSec, no additional components are required to secure the traffic, which makes this a viable alternative to VPN in same cases

5 Implementation

The concept proposed in this paper has been implemented by the Fraunhofer-Gesellschaft as its unified wireless network access for roaming employees, and by connecting to the eduroam roaming network, even for guests from other research or education organizations [2,8]. Full details can be found in [9]. The field test provided valuable information about the assumptions made when designing the solution, and allowed to verify that the requirements where met. Figure 4 visualizes the final infrastructure. The following section discusses both the implementation and the operation of this field test.

5.1 Discussion of the Implementation

As a requirement, the implementation must be easy. Although this is generally true, a differentiation can be made between the implementation of the central and distributed parts of the concept. Since the separation of Identity Provider and Service Provider resulted in only a single authentication infrastructure, not

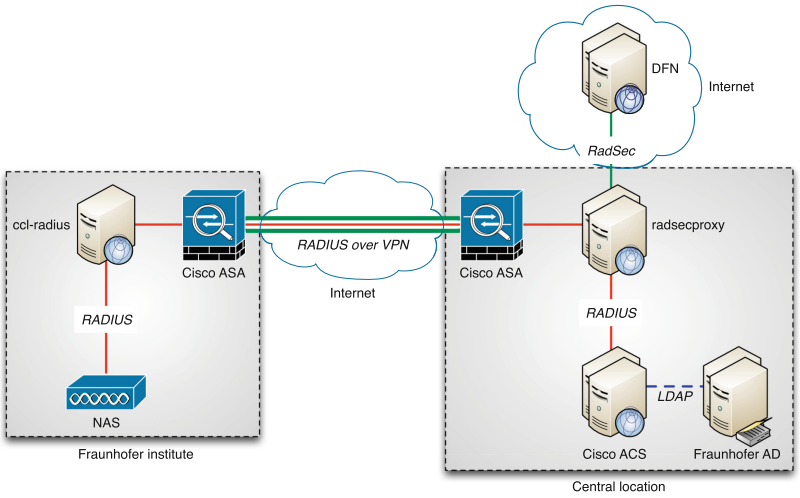

Fig. 4. Final infrastructure

maintained by the local IT department, the cost to implement the solution at the different locations weighs more than the cost to deploy the centralized authentication service.

The implementation of the distributed part is very straight forward. Since wireless networks are almost always already available, it is easy to add another one as the wireless access network employees and guests can use. This leaves the installation of the local RADIUS proxy as the biggest hurdle. Since its configuration is the same for every installation, this proxy can very easily be deployed automatically with the help of automation tools. Depending on the form of communication between the sites, additional firewall rules need to be configured, which concludes the implementation of the solution in a branch (Fig. 5). The implementation of the centralized authentication solution is more complex, as it has more dependencies. Also, it is unique to the organization. For the Fraunhofer-Gesellschaft, a user database already existed, which reduced the required effort to the deployment of an authentication server.

In summary, the deployment of this solution can be done in very little time after the necessary preparations have been made. The reason for this is the easy implementation of the role of Service Provider, which helps tremendously to reduce the overall effort to provide a unified network access to all employees.

5.2 Discussion of the Operation

Several requirements concerned the operation of the new concept, especially the ease of use and the removal of manual actions. For the operation of the service, two phases can be identified. First, an initial configuration must be performed to enable a device to use the service. Second, the device can use the service without interaction. For every stage the compliance with the requirements is analyzed separately.

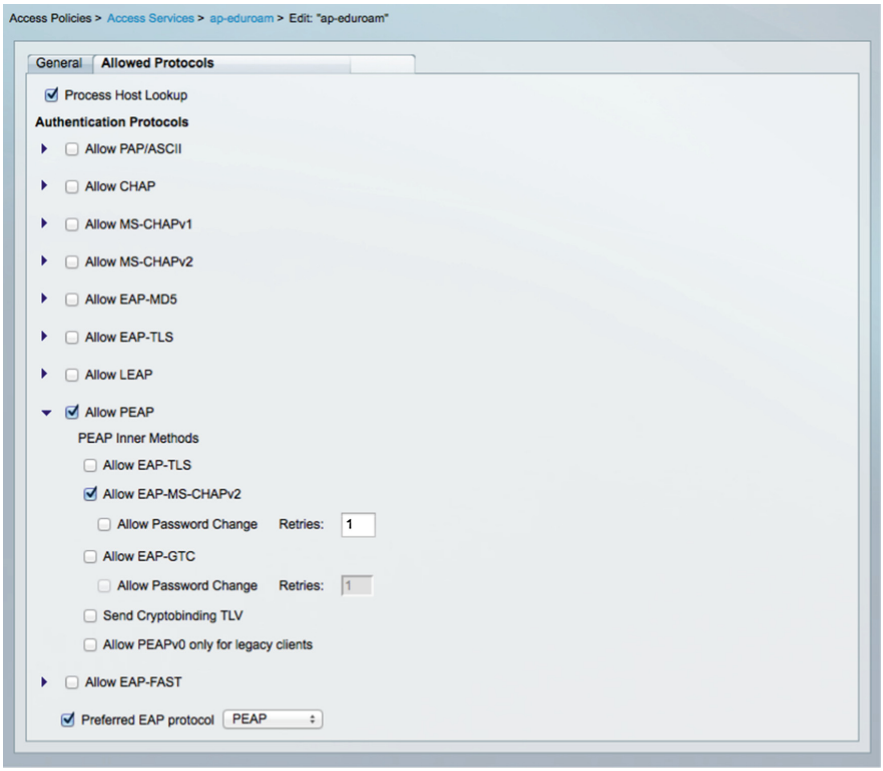

Fig. 5. Configuration of authentication types

In the first phase, the initial configuration, manual interaction is necessary. The employee needs at least the documentation of how to configure his device, and often requires assistance to perform all tasks required. And, as the configuration of advanced parameters is required, for example the EAP type, it does not fulfill the re-quirement to be easy. Those problems can only be partially addressed by the introduction of automated configuration tools. But since the configuration has to be done only once, and the solution provides strong security, the additional effort is worth it.

In comparison to the current solutions for guest access, the new concept provides great benefits to the local IT departments. The amount of manual interactions is significantly reduced and the service can be used more easily, for example without a captive portal. Furthermore, the local IT department can rely on the support of the central team to troubleshoot and solve problems that arise, in contrast to their own solutions for which they are responsible themselves.

6 Conclusions

With the introduction of a RADIUS roaming network, and the implementation of eduroam specifically, the defined goals are met. Additionally, the separation

of Identity Provider and Service Provider singlehandly fulfills several requirements. First of all, it provides great scalability, as the deployment of the role of Service Provider can be done with less effort than the establishment of an Identity Provider requires. Second, it enables an easy implementation of the concept in the institutes, again due to removing the need for distributed authentication servers. Third, since eduroam is based on open standards and protocols, it is vendor-independent, and last but not least it only requires an initial configuration, thus reducing the need for manual actions by all participants.

Participating in eduroam has some additional advantages. For the employees, it means that they can obtain Internet access even outside of the Fraunhofer-Gesellschaft, for example in universities and other research institutions. Additionally, tools are constantly developed or advanced to provide the user of eduroam with help and information, with eduroam CAT being just one example. For the administration, eduroam provides the benefit that it is constantly improved, and its security and stability are researched by many different organizations. The introduction of RadSec and Dynamic Discovery are only two examples of this process. Those efforts, for both users and administrators, could not have been made by the Fraunhofer-Gesellschaft itself, if it had implemented its own roaming network.

Within the given restrictions and requirements, the implementation of eduroam in the Fraunhofer- Gesellschaft is the best approach to a unified wireless network access. It fulfills the requirements, and meets the goal to provide a reliable network access which can be used satisfactorily by all employees. As the service is based on open standards, it can be adjusted later on to support different authentication types or user directories, if the need arises. This, and its modular design, provide a great platform to operate the service even if requirements change in the next years. Looking at the years of operation, the next section proposes possible improvements and changes to the concept, followed by an outlook on future enhancements to eduroam.

References

1. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.: Extensible Authentication Protocol (EAP). RFC 3748 (Proposed Standard), June 2004. http://www.ietf.org/rfc/rfc3748.txt, updated by RFC 5247
2. Aderhold, A., Wilkosinska, K., Corsini, M., Jung, Y., Graf, H., Kuijper, A.: The common implementation framework as service – towards novel applications for streamlined presentation of 3D content on the web. In: Marcus, A. (ed.) DUXU 2014, Part II. LNCS, vol. 8518, pp. 3–14. Springer, Heidelberg (2014)
3. Cisco Systems Inc.: Installation and Upgrade Guide for Cisco Secure Access Control System 5.4, August 2013. http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/installation/guide/csacs_book.html. Accessed 11 December 2013
4. Grosse-Puppendahl, T., Herber, S., Wimmer, R., Englert, F., Beck, S., von Wilmsdorff, J., Wichert, R., Kuijper, A.: Capacitive near-field communication for ubiquitous interaction and perception. In: ACM UbiComp 2014, pp. 231–242 (2014). http://doi.acm.org/10.1145/2632048.2632053

5. Grosse-Puppendahl, T.A., Berghoefer, Y., Braun, A., Wimmer, R., Kuijper, A.: Opencapsense: A rapid prototyping toolkit for pervasive interaction using capacitive sensing. In: 2013 IEEE PerCom, pp. 152–159 (2013). http://doi.ieeecomputersociety.org/10.1109/PerCom.2013.6526726
6. Grosse-Puppendahl, T.A., Braun, A., Kamieth, F., Kuijper, A.: Swiss-cheese extended: an object recognition method for ubiquitous interfaces based on capacitive proximity sensing. In: 2013 ACM SIGCHI Conference on Human Factors in Computing Systems, CHI 2013, pp. 1401–1410 (2013). http://doi.acm.org/10.1145/2470654.2466186
7. Juniper Networks Inc.: Juniper Networks Horizontal Campus Validated Design Guide, May 2012. http://www.juniper.net/us/en/local/pdf/design-guides/jnpr-horizontal-campus-validated-design.pdf. Accessed 10 December 2013
8. Limper, M., Jung, Y., Behr, J., Sturm, T., Franke, T., Schwenk, K., Kuijper, A.: Fast and progressive loading of binary encoded declarative 3D web content. IEEE Comput. Graphics Appl. **33**(5), 26–36 (2013). http://dx.doi.org/10.1109/MCG.2013.52
9. Nose, J.D.: Centralized approach for a site independent wireless network access. Technical report, Department of Computer Science, TU Darmstadt (2013)
10. Wierenga, K., Winter, S., Wolniewicz, T.: The eduroam architecture for network roaming, July 2013. http://tools.ietf.org/html/draft-wierenga-ietf-eduroam. Accessed 10 December 2013
11. Winter, S., McCauley, M., Venaas, S., Wierenga, K.: Transport Layer Security (TLS) Encryption for RADIUS. RFC 6614 (Experimental), May 2012. http://www.ietf.org/rfc/rfc6614.txt