Expertise
and insight
for the future

Pauliina Salomäki

DesignIT User Access Management

Metropolia University of Applied Sciences

Bachelor of Engineering

Media Engineering

Bachelor's Thesis

31 May 2019

Author Title Number of Pages Date	Pauliina Salomäki DesignIT User Access Management 31 pages 31.5.2019
Degree	Bachelor of Engineering
Degree Programme	Media Engineering
Professional Major	Media Engineering
Instructors	Kari Salo, Principal Lecturer

The purpose of this thesis was to explore and propose different User Access Management (UAM) methods and solutions most suitable for a project website called ”DesignIT”. The website is a learning tool and aid for teachers and students to utilize during design related projects.

At the time of writing this report, the website does not provide any basic account management features such as resetting passwords or retrieving lost usernames, although the users must create accounts in order to use the tool. The administrators also have minimum control over these accounts.

In order to improve the overall user experience and offer the website administrators a way to manage the user accounts, this thesis proposes hypothetical and real UAM solutions to be implemented in the future.

To achieve the desired result for this thesis, a set of already existing user account management systems and methods were examined and compared in order to select the most fitting one for the website and to create models of some access management features the tool needs.

As a result, the website has a plan of UAM methods to implement should the administrators recognize the need for them. This thesis also argues the importance of UAM to justify the proposed solutions.

Keywords	access management, identity access management, identity management, user management, user access management

Tekijä Otsikko Sivumäärä Aika	Pauliina Salomäki DesignIT-sivuston käyttövaltuushallinta 31 sivua 31.5.2019
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Ammatillinen pääaine	Mediatekniikka
Ohjaaja	Yliopettaja Kari Salo

Opinnäytetyön tarkoituksena oli tutkia ja ehdottaa eri käyttövaltuushallinnan järjestelmiä ja menetelmiä käytettäväksi korkeakouluopiskelijoiden kansainvälisenä projektityönä luodulle verkkosivustolle nimeltä ”DesignIT”. Sivusto on luotu oppimistyökaluksi ja apuvälineeksi suunnitteluun liittyville kursseille ja projekteille sekä opettajien että opiskelijoiden käyttöön.

Insinöörityön tekemisen aikaan sivusto ei sisältänyt mitään käyttövaltuushallintaan liittyviä perusominaisuuksia, kuten salasanojen vaihtoa tai mahdollisuutta palauttaa kadotetut käyttäjätunnukset, vaikka käyttäjien tuleekin luoda tunnukset sivustoa käyttääkseen. Ylläpitäjillä ei myöskään ole juurikaan keinoja hallita käyttäjätunnuksia.

Sivuston käyttäjäkokemuksen parantamiseksi ja käyttäjähallinnan tarjoamiseksi ylläpitäjille insinöörityössä ehdotettiin sekä hypoteettisia että oikeita käyttövaltuushallinnan ratkaisuja, joita sivusto voi hyödyntää tulevaisuudessa.

Halutun lopputuloksen saamiseksi valittiin joukko olemassa olevia käyttövaltuushallinnan järjestelmiä ja menetelmiä tutkittavaksi ja verrattaviksi keskenään, jotta löydettiin sopivin vaihtoehto sivustolle. Menetelmät sisälsivät muun muassa käyttäjille luotuja salasananvaihdon ja tunnushallinnan keinoja, joista luotiin malliehdotuksia visuaalisten luonnosten avulla.

Tuloksena saatiin ehdotelma käyttövalmiista käyttövaltuushallinnallisista ratkaisuista käyttöönotettaviksi, mikäli sivuston ylläpitäjät pitävät niitä tarpeellisina. Insinöörityössä havaittiin, että käyttövaltuushallinnalliset ominaisuudet ovat tärkeitä sivuston käytettävyyden ja tietoturvan kannalta. Ehdotettujen menetelmien avulla käyttäjille turvataan heidän pääsynsä jatkuvuus sivustolle sekä parannetaan sivuston tietoturvaa kokonaisvaltaisesti.

Avainsanat	identiteetinhallinta, käyttäjähallinta, käyttövaltuushallinta, pääsynhallinta

Contents

List of Abbreviations and Key Concepts

Authentication	Confirming that a user is who they claim to be.
Authorization	Confirming that a user has the necessary permissions to access an area within an IT environment.
DDoS	Distributed Denial of Service attack. A malicious action to disrupt normal traffic flow to a website by sending requests in a rapid succession by using an automated bot.
Directory services	Specific type of tool that is used to manage access and rights.
ISAM	IBM Security Access Manager. An authentication and authorization solution for IT services, systems and applications.
IT	Information Technology. A technology field related to computer science and networks.
ITIL	Information Technology Infrastructure Library. A set of best practices for IT businesses to manage their IT services in the most efficient manner.
Sensitive information	Information that will cause harm to a person or a system if given access to and exploited by a malicious party.
SWOT	Strengths, Weaknesses, Opportunities Threats. An analysis method to examine a subject by listing and analyzing these four attributes of the matter.
TAM	Tivoli Access Manager. A user authentication and authorization solution developed by IBM.
UAM	User Access Management. Means for managing user accounts in a system.

User Directory	A database of user accounts in a certain service or website environment. Used to manage user accounts.
WAM	Web Access Management. Systems focused on providing identity and user management and security to web-based tools.

1 Introduction

The idea for this thesis was formed during working closely with the “DesignIT” project students and aiding them with the development of their website. While coming up with improvements along the process it became clear that the website does not include any user account management, i.e. the users or the administrators cannot manage or edit the user accounts that are needed in order to use the website. This inspired the study of creating a hypothetical user management solution that could be implemented in the future.

The ”DesignIT” website has been created for higher education students and teachers to utilize during designing projects and courses. It is an outcome of two years of planning, researching and creating a complementary learning tool to aid students to be more creative and productive, and to offer them a platform in which to visualize their ideas in a fun, gamified way. The official introduction of the website is seen below:

> The ”DesignIT” platform supports and promotes creativity! ”DesignIT” helps learners and users in general to execute and collect contextual data, analyze it and keep engagement alive through the gamified features. The platform can be used in mobile devices to allow smooth contextual data gathering. ”DesignIT” platform is especially suitable for project work where teams are solving wicked problems and need be creative.
>
> The tool has been designed and developed in the framework of the Erasmus+ project Design thinking in higher education for promoting human-centered innovation in business and society, 2017-1-EE01-KA203-034889. (”DesignIT”, 2019)

Access and user management solutions are vital for Information Technology (IT) services that have a digital user base. It is important to understand the value of user and identity access management in modern everyday services. The lack of basic user account management options such as resetting passwords greatly impairs the usability of the tool for the users in case they encounter problems with their user accounts (Ucisa 2019). In ”DesignIT” website, the administrators also have minimum control over the users and no visibility to the current user base.

The goal of this thesis is to research and narrow down possible ways to improve the ”DesignIT” website’s user management side, and plan a solution to be implemented in the future. This would ensure a smoother experience for the users, provide additional security and grant the tool’s administrators control and visibility of their user base. For learning tool such as ”DesignIT”, the management of user accounts does not need to be complicated since the accounts at hand contain only a few attributes to manage.

With ”DesignIT” being a web-based tool without a highly complex infrastructure behind it, the scope of this research does not need to delve deep into common IT service components such as networking or operation system environments.

Since this thesis only proposes an example solution and does not aim to create a fully functioning system to implement at the current state, there are no consequences to not having a solution ready for deployment at the end of the project. However, any possible challenges are taken into consideration in the process of this study.

Throughout this thesis, the ”DesignIT” website is referred to as the “website”, the “tool”, “the platform” or the “system“, depending on the subject matter at hand.

2 Current Situation

The website offers a very limited approach to any kind of Access Management at the current state. The website is openly accessible which means the registered users do not come from a specific supervised institutional or a company IT environment. In other words, the users do not need to be connected to an internal secure network connection at a university or at a company in which they would already have had to authenticate themselves by signing in with a username linked to the certain environment. The users are also not based in a certain country or a geographical location.

The users do not have to authenticate themselves or use any validation methods when creating their user accounts or logging in to the website. Authentication means an additional method for the system to ensure the user is a real person and not a “bot” that could harm the system by, for example, creating an infinite number or user accounts or logging in repeatedly so rapidly the website will be overloaded with requests. This type of action is called a DDoS (Distributed Denial of Service) attack that disrupts the normal data traffic to websites to disable them on purpose (Shakarian, Ruef and Shakarian, 2013: 13). A malicious party may also infest the system with a bug that pinpoints and exploits any flaws or vulnerabilities in the code and causes the site to crash.

A username, a password, a valid e-mail address and first and last names are the only required fields in the user registration process. Users can use their personal e-mail addresses from any provider to create an account. The email address has to be valid in order for the registration to succeed without generating an error message. A valid address must contain a minimum amount of characters before an at sign (@), followed by a domain, a dot (.) and a country code of two characters. However, in the website’s current state at the time of writing this thesis, the validation does not include verifying the address by any commonly used methods. An example method for email validation is checking if the domain server, that is the latter part of the email address, answers ping requests, i.e. it is online and can be connected to. (WebDigi 2009).

Below, Figures 1 and 2 show the website’s login and registration process.

Figure 1. Front page. Offers options either to log in with an existing account or to register to the website.

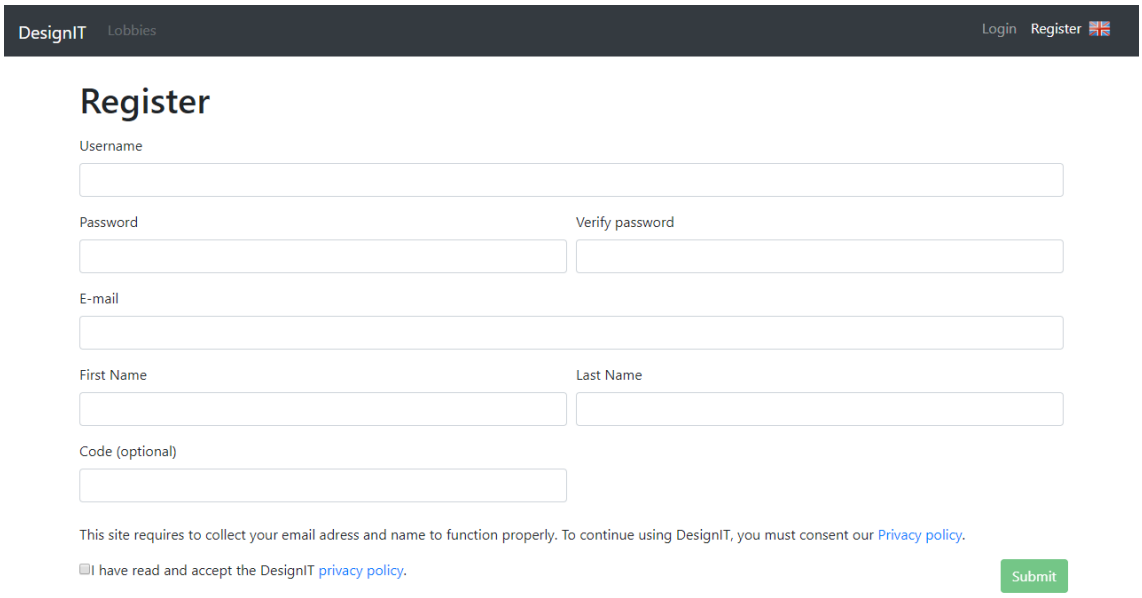

Figure 2. Registration page. All the required information for registration is shown here.

As seen in Figure 2, the registration form also includes an optional field for “Code”. The code is used to register immediately as a teacher.

Teacher accounts have extended rights in the tool. Teachers, that are called “Gamemasters” within the tool, can create the “Lobbies” which correlate to the whole course or the project that the students are partaking in. Into these lobbies the teacher creates “Challenges” that are certain tasks assigned to the students in order to

complete the course. The students join the Lobbies through a code provided by the course teacher, and form groups of 2-36 students that pick Challenges to complete as a group. Teachers set up the lobby and challenge settings by setting a maximum and minimum limits of participants, set start and finish dates for the challenges and come up with the challenges all together.

Teachers also help the teams with their challenges through a chat feature embedded into the tool, and pass or fail the challenges the teams have completed after reviewing them. Once a challenge is completed and approved by the teacher, the teams can move on to the next phase.

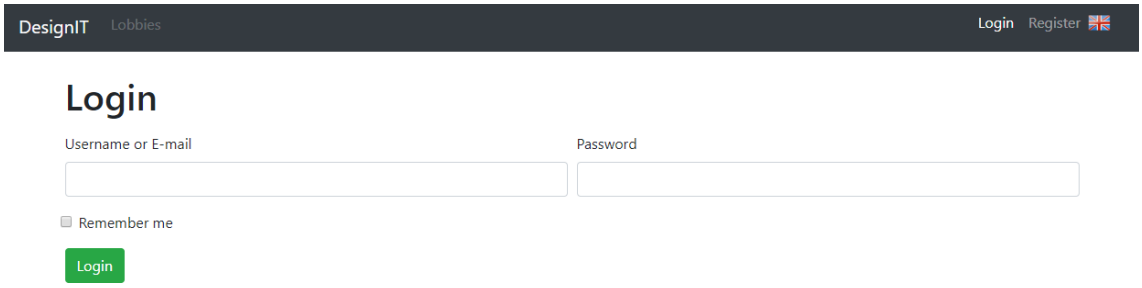

Figure 3. Login page. All current options at the login page are shown here.

At the time of writing this report, the website does not provide any account management options for the users such as resetting passwords, changing usernames or changing the e-mail addresses linked to the accounts. If a user forgets their password of username, the only way to regain access to the website and their project is to create a completely new account. As seen in Figure 3, the login page does not offer the choice of “Forgotten password?” often seen on login pages. Fortunately, the nature of the tool allows the users to re-join a group or a project as long as the maximum number of group members is not exceeded.

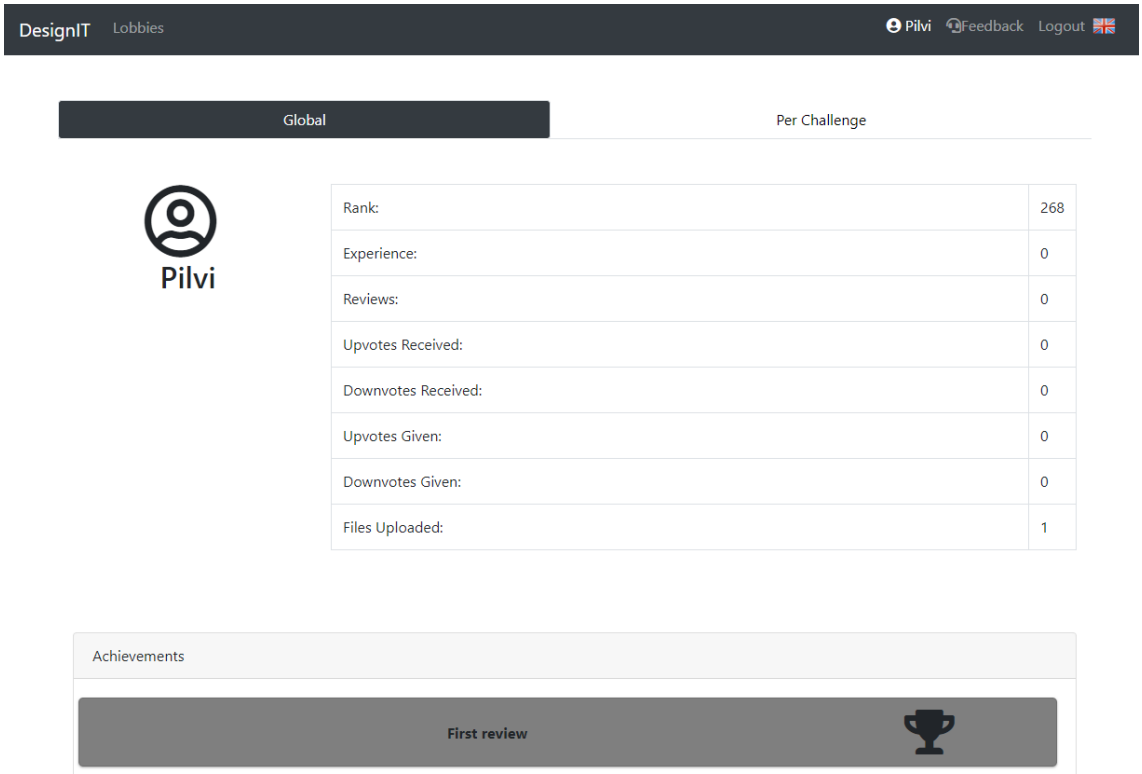

Figure 4. A user profile page.

As mentioned before, users have no control over their accounts nor their profiles. Only the site administrators can edit all users' usernames and their roles. Figure 4 demonstrates the whole extent of a user's profile page. Profiles display the user's username and a default picture, neither of which are changeable. The most important data seen here is the user statistics from using the tool. The page includes the points ("Rank") accumulated by the user, who in this case would be a student, along with a list of unlocked achievements. The points and the achievements are awarded by performing certain actions while using the tool. These statistics can be inspected "Globally", i.e. from all activities ever done by the user or "Per Challenge", which means activities done within certain "challenges" that are given out to the student groups by a project teacher.

There are no user directories, which are databases of the users and their user accounts. Therefore, the administrators of the tool do not have a register of the website's users or any method to manage their user accounts and passwords. In other words, the administrators do not know how many user accounts there actually are within the website.

3 Options and SWOT analysis

In this section, a selected three out of five already existing User Access Management solutions are examined and valuated in regards of which best suits the needs and specifications of the ”DesignIT” website. Each selected option is analyzed using a SWOT (strengths, weaknesses, opportunities, threats) analysis method to compare the pros and cons of each solution in order to choose the most suitable one for this study (Teece D.J. 2017: S1).

The five proposed solutions have been gathered from various online sources by searching for the most common modern UAM solutions and practices. The solutions gathered are Active Directory, Azure Directory Service, OAuth 2.0, Keystone (OpenStack) and Tivoli / ISAM. Out of these five options, Active Directory, OAuth 2.0 and Tivoli / ISAM are selected for further examination. Options Azure and Keystone are omitted due to the amount of unnecessary comparison for this particular research. However, they are mentioned here to provide a wider insight on different access management solutions in case any possible subsequent research is conducted on this subject.

3.1 Active Directory

Active Directory (AD) is a directory service product for Windows operating system environment developed by Microsoft. It is one of the most popular directory related solutions in IT world and has become a central part for many other Microsoft solutions.

Active Directory is a UAM solution to be used with Windows credentials, and requires a domain in which the user accounts are stored in. Users then login to Windows with these credentials, and after logging in they can access selected services directly without having to log in again due to a Single Sing-On (SSO) feature. This feature recognizes that the user has already authenticated themselves, and logs the user in automatically. (Clines S., Loughry M. 2008: Chapter 9)

Figures 5, 6 and 7 demonstrate how the AD is structured and how the user accounts are managed.

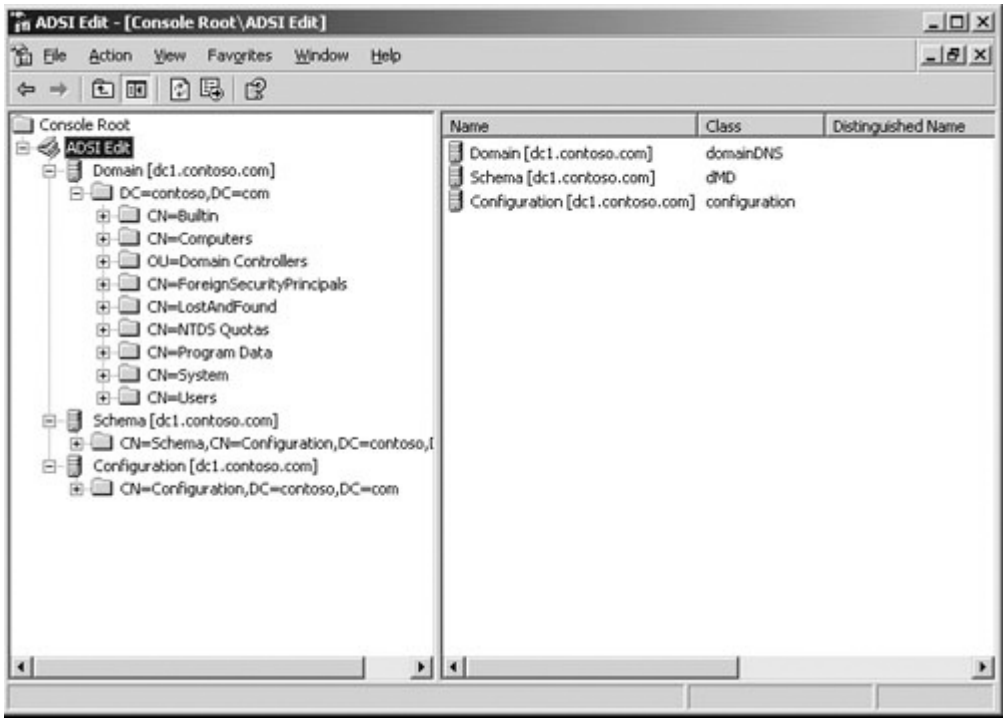

Figure 5. An example of Active Directory tree structure under domain “dc1.contoso.com” (Mulcare, Reimer 2003: Chapter 2).

AD consists of numerous different partitions of a system which can easily be accessed through a logical tree structure seen in Figure 5. These components are stored under a certain domain. In this view there could be more domains if the structure has been designed so.

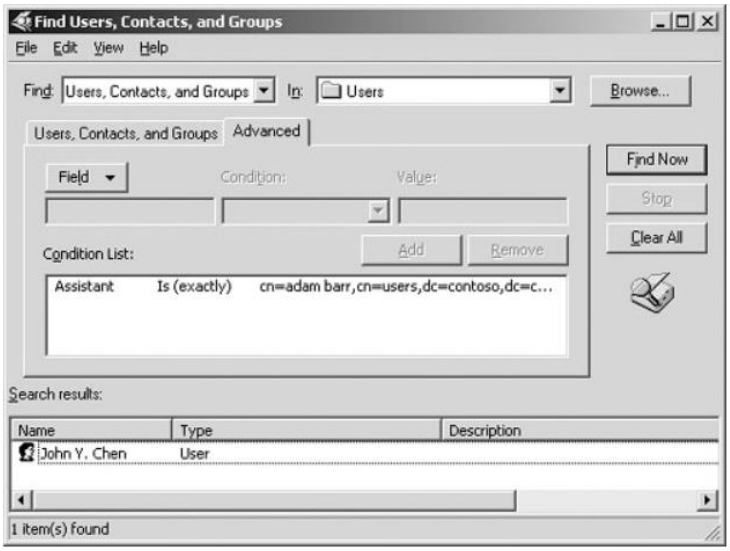

Figure 6. Search feature to find users or other in AD. (Mulcare, Reimer 2003: Chapter 10).

AD contains all data that has been input at the deployment phase of the service. The data, for example a user in Figure 6, can be found using a search function. By clicking on the search result, a window pops up containing all the details stored in this user account.

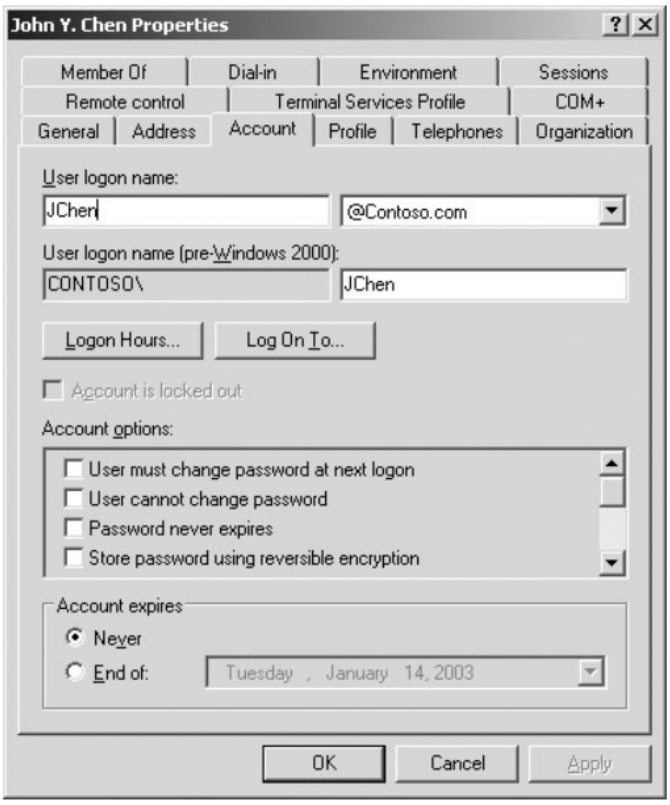

Figure 7. An example user account data in AD. (Mulcare, Reimer 2003: Chapter 10).

Figure 7 demonstrates some of the user account data that is stored in AD and shows some of the features for managing the user account. In “Account options” there are functions to make the user change their password at next logon, make the user unable to change their own password or make the password permanent. In addition to these, an administrator can also change the user account details and lock the account, if necessary.

AD is a vast database of users and other attributes and is not a preferred directory solution for simple applications or systems. (Clines S., Loughry M. 2008: Chapter 2)

Table 1. SWOT analysis on Active Directory.

Strengths	**Weaknesses**	**Opportunities**	**Threats**
Holds a substantial amount of data and attributes. Various ways to manage user accounts.	Cannot be implemented easily. Directed more for network resource managing.	Administrators could change the user passwords and deliver them to users as well as lock user accounts if needed.	Very large scale system. Requires a domain. Used with Windows credentials, not a web based solution.

The SWOT analysis in Table 1 is based on the basic handbook of AD provided by Clines and Loughry (2008).

3.2 OAuth 2.0

OAuth 2.0 is an industry-standard protocol for authorization that focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. This solution has been developed within the IETF OAuth Working Group. It has been used by social media platforms such as Twitter and Facebook. (OAuth 2.0 2019)

OAuth 2.0 works by adding more security into the login process by redirecting the user to an additional authorization step while logging into the system. By logging in via this step, the user is authorized by using access tokens. The login process is explained in the Figure 9. The additional step that is visible to the user is demonstrated in Figure 8 by using a mobile device login process on Facebook as an example provided by the OAuth 2.0 developer Parecki A. (2019).

Figure 8. An example of OAuth 2.0 login authorization process on Facebook on a mobile device (Parecki 2019).

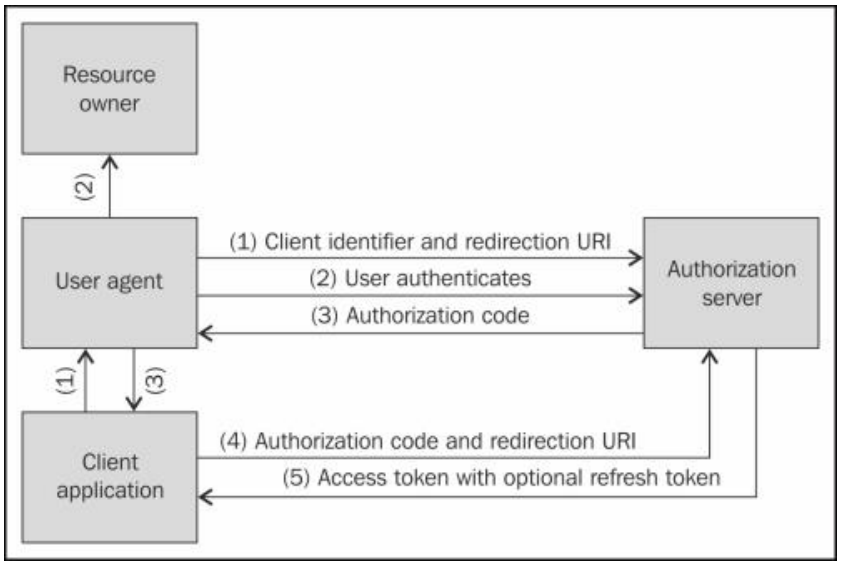

Figure 9. Workflow of authorizing user access in OAuth 2.0 (Spasovski 2013: Chapter 4).

From here, the user is redirected back to the website after a successful login. By this method, the user is thoroughly authorized leaving minimum risks for unwanted access to the tool by third parties.

Table 2. SWOT analysis on OAuth 2.0.

Strengths	**Weaknesses**	**Opportunities**	**Threats**
Simple to implement. Implementable on a web based solution.	API keys and access tokens are vulnerable. URL redirection can get intercepted.	Can be user from a mobile device.	API keys and access tokens can be stolen and exploited.

The characteristics seen in Table 2, and all of the attributes of OAuth 2.0 are comprehensively explained in official OAuth 2.0 instructional videos by Parecki (2019).

3.3 IBM Tivoli Access Manager (TAM)

IBM Tivoli Access Manager (TAM) also known as IBM Security Access Manager (ISAM) is an authentication and authorization solution for corporate web services, operating systems, and existing applications. (Wikipedia 2019)

As high level description of the solution, TAM consists of two core components: a user registry and an authorization service. The latter includes an authorization database and an authorization engine that handles the login requests. The requests are sent to the authorization service for evaluation and upon approving the request, a resource manager within the system then allows access to the resource content protected by the TAM system. Figure 10 demonstrates the system architecture. (IBM Redbooks 2005)

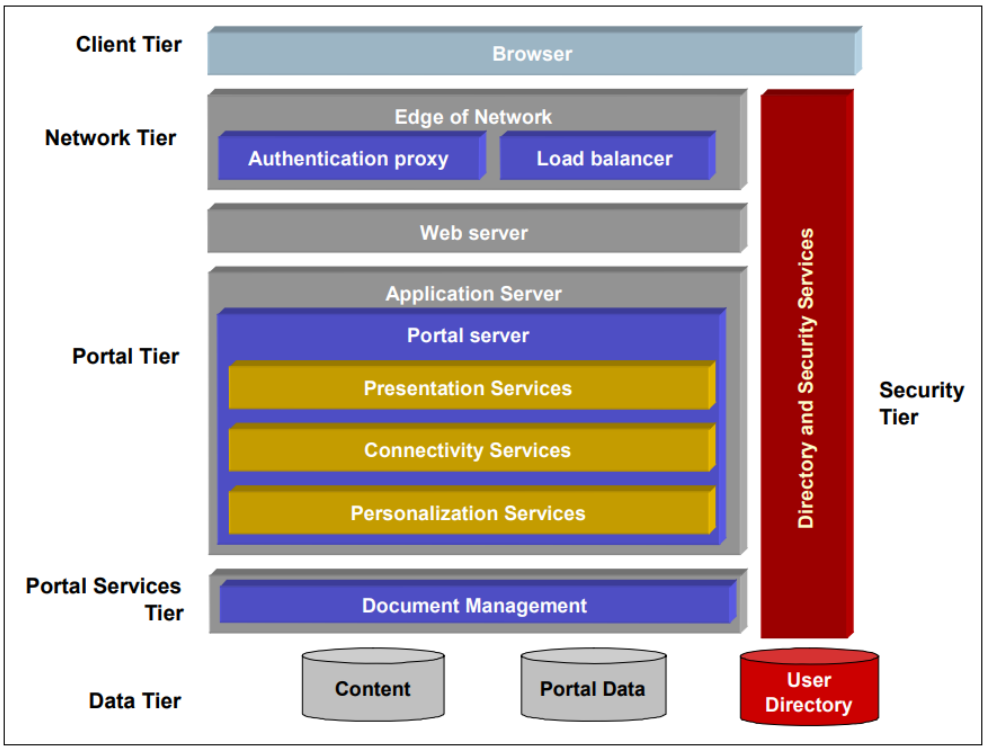

Figure 10. High level graph of TAM architecture logical components (IBM Redbooks 2005: 23).

As seen from Figure 10, TAM is a complex system that comprises of multiple tiers on many platforms. It is best suitable for a system that needs management in all the levels demonstrated above. For DesignIT, an additional portal or content database are not needed, since it is a web-based solution. More attributes are briefly listed in Table 3.

Table 3. SWOT analysis on TAM. (IBM Redbooks 2005)

Strengths	Weaknesses	Opportunities	Threats
Security through user registry and an authorization service. A complete system for UAM and content protection.	Costly due to being a complete system, in comparison to other examined solutions.	Automated user access management.	Large scale. Directed towards corporate web services, i.e. more complex solution than this research is looking for.

4 Proposed Solutions for “DesignIT”

From the previously examined and compared UAM solutions, the one selected to improve “DesignIT” tool’s access management processes is OAuth 2.0. Justification for this solution to be proposed is disclosed in the next chapter.

4.1 Why OAuth 2.0

OAuth 2.0 improves the security in accessing the ”DesignIT” website without overcomplicating the administrative side of the platform or lessening the usability of the tool from the users’ perspective. As it functions as a Web Access Management (WAM) (Poza, D. 2018) compatible solution, it is the easiest to implement and to integrate into the platform. Additional benefit for “DesignIT” is the fact that OAuth 2.0 can also be used to authorize logins from mobile devices, which is a majorly important feature of the “Design IT” tool. It also minimizes the workload the other solutions would possibly cause in order to bring into use.

4.2 Other UAM improvements for ”DesignIT”

The main thing users need with most user accounts is the possibility to retrieve their forgotten passwords and usernames. Usually, this is automated by following a link to a form in which the user types the email address linked with their account. If the email address has a match in the system, the form then retrieves user data linked to this address, and sends the username, if asked for, and a link to a password reset page with an accompanying message to the user. If the email address has not been registered into the website, this process will not succeed. Below is a proposed flow for this within the ”DesignIT” website.

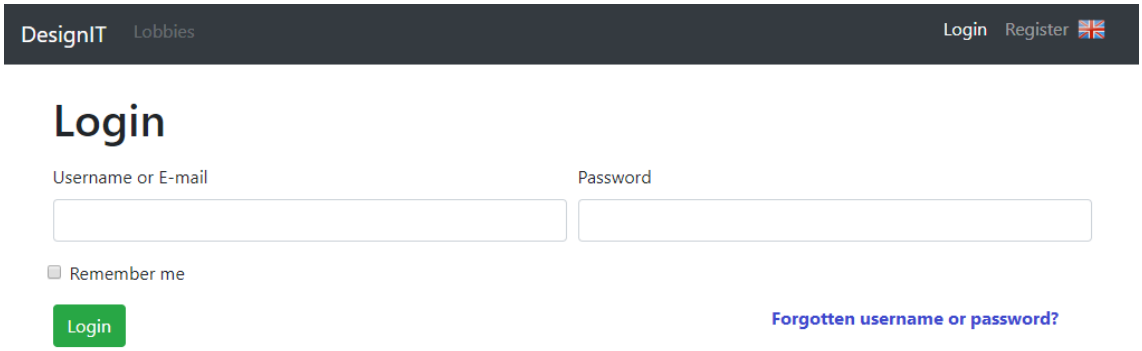

Figure 11. Login page with the feature for retrieving passwords and usernames added.

Login session starts from Figure 11. In case the user has forgotten their username or password, they click on the link under the password field. From this link, they are directed to the retrieval form seen in Figure 12.

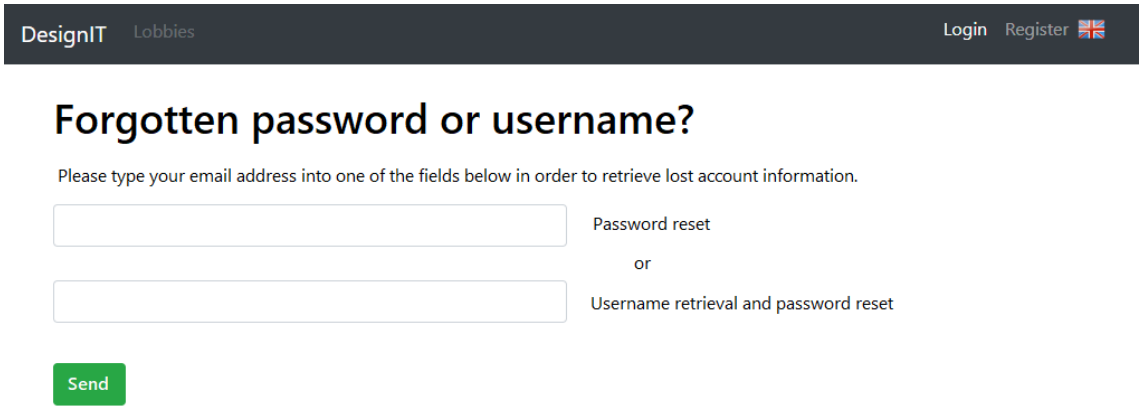

Figure 12. A suggested account information retrieval page.

User then inputs their email address into one of two fields depending on what information is being retrieved. In case the email address is not found from the system, the page generates an error message seen in in Figure 13. If the email address has been registered into the website, the information is sent successfully to the user and the form shows this in Figure 14.

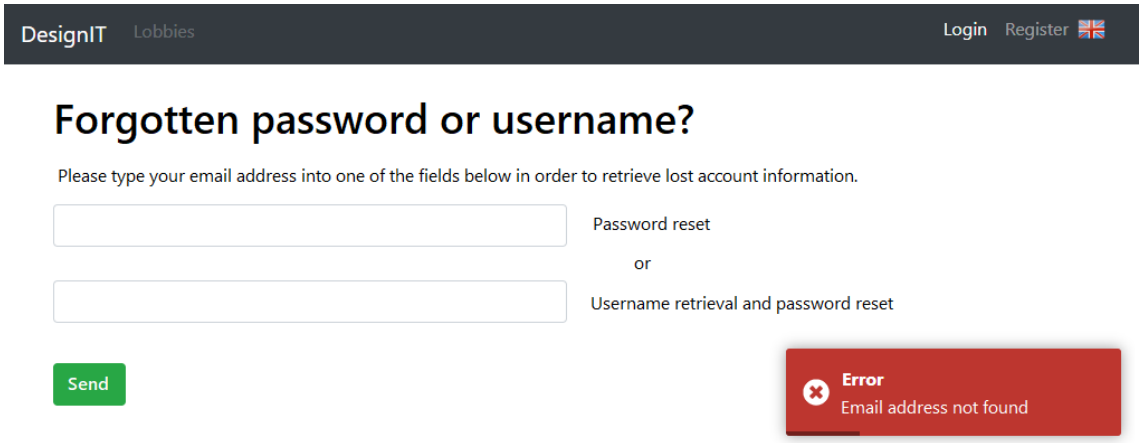

Figure 13. Error for incorrect email address while retrieving password or username.

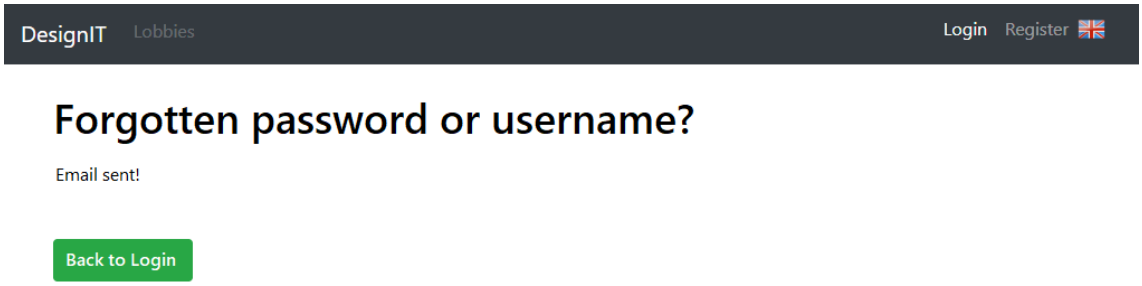

Figure 14. Successful retrieval request.

From there, the user has to find the email sent by the website and follow the instructions. A suggestion for the cover letter sent by the system to the user:

> *Hello "First name",*
>
> *You recently requested a new password and/or a retrieval of Your DesignIT username. Your username is "Username". For password reset, please follow the link below. The link is valid for the next 48 hours.*
>
> ***Reset password** (link to password reset form)*
>
> *In case this request was not sent by You, please contact our support at (support email address) for any questions, or ignore this message.*
>
> *Thank You,*
> *DesignIT*
> *(support email)*
> *("DesignIT" logo and link to the website)*

When the user follows the link in the email, they are directed to a page for resetting their password as seen in Figure 15. The form asks for the new password twice and states the minimum password requirements. These requirements are also hypothetical at this point, since the registration form does not include these while creating the initial password. Adding minimum password requirements would greatly improve the safety of using the website, since a complex password minimizes the risks of a third party guessing the password and gaining access to the website wrongfully (Technics Publications 2018).

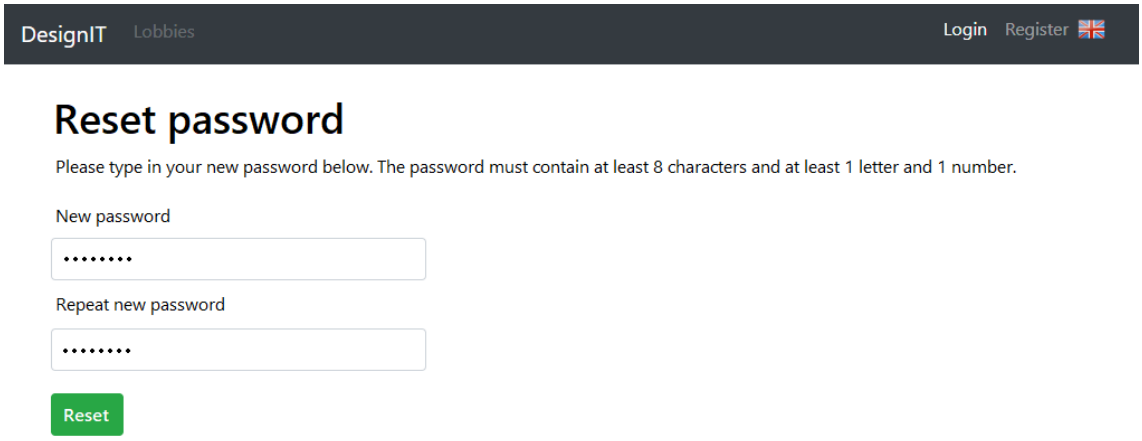

Figure 15. Password reset form suggestion.

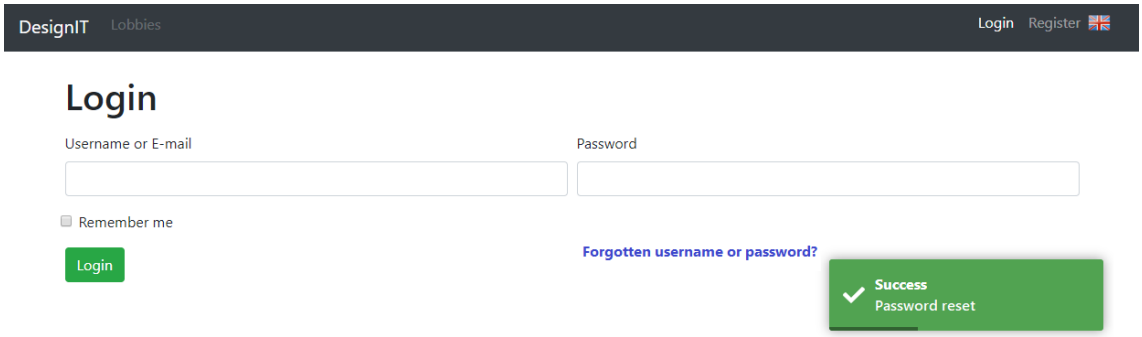

Figure 16. Successful password reset. The user is redirected to Login page.

In case the new password follows the minimum requirements, the user is redirected back to Login page from which they can now log in with the new password, as seen in Figure 16. A pop-up message informs the user that the password has now been reset. For additional safety and confirmation, the system could also send the user an email confirming that the password has been reset. As already proposed in cover letter before, the user could again be instructed to contact ”DesignIT” support team in case

they suspect someone else has tried to or has already reset their account's password without their consent.

In addition, there could also be a feature for the users to request changes to their user account roles. In a situation where the user, be it teacher or a student, wants to either downgrade of upgrade their role and not lose their original account, a request form could be added to the user profile page or to a completely new page at the navigation bar titled "Request". A case example to prove a need like this would be a situation where the current course teacher becomes obstructed to continue supervising and managing the course and needs a substitute in order for the course and the challenges to be finished on time. With a request form, the current teacher could request a student user to be promoted to a teacher, or a "gamemaster" in "DesignIT" terms, or the student could send this inquiry in case the teacher is unable to.

The simplest way to implement this would be to have the request form send a message to the administrators support email for the admins to perform the role change by hand, and afterwards confirming the role change to both parties by email. On the other hand, having a fully automated role change would remove the need for administrator input in most cases. Here automation would mean a process where the system checks that the requester is a user with a role high enough to be authorized to perform this change, and the role would be changed almost instantly. In "DesignIT" user environment there are currently only two roles, so a teacher would have this authorization by default. Both the student and the teacher would then receive an automated email confirming that the role change has succeeded, and the student would log into the website as a teacher at the next login.

If a teacher role should be revoked from a user, these two suggested processes would work the same, but backwards. As mentioned above, a user with a student role would not be able to revoke teacher roles automatically by lacking the correct authorization to do so.

5 Maintenance

As IT services in general, access management solutions are also maintained throughout the service's lifecycle. With proper maintenance, the risks of causing system vulnerabilities and usability issues are minimized. This can be achieved by following the guidelines of existing IT industry protocols and best practices defined by the ITIL (Information Technology Infrastructure Library) framework, for example. ITIL is "not a standard in the formal sense but a framework which is a source of good practice in service management." (Griffiths R., Lawes A., Brewster E., Sansbury J. 2016).

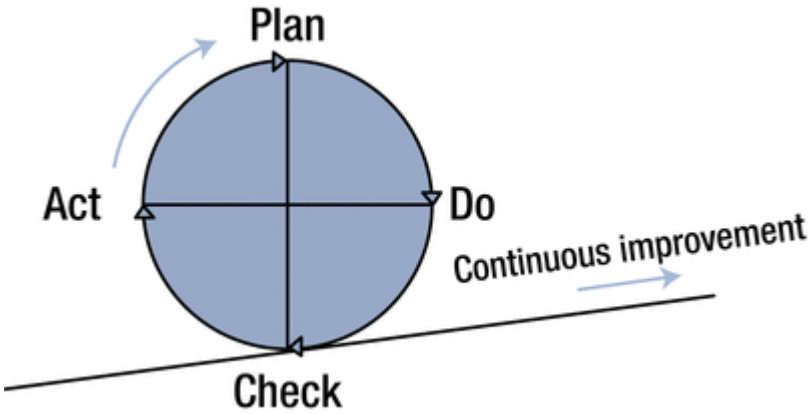

Figure 17. Deming's PDCA cycle. (2016).

By following these guidelines, the service providers have a good baseline for maintaining their solutions and keeping their services continuous. Figure 17 demonstrates one commonly used method called the "PDCA cycle". This idea and set of actions seen in the figure can be utilized during initial planning of an IT service, and during planning the continuum of a service. (Kaiser, A. K. 2016)

A proper IT service maintenance requires many aspects to consider in order to sustain a good IT service. Some of these aspects are discussed in the following chapter from the access management point of view. "DesignIT" website's future and maintenance is being examined on its own in the second subchapter.

5.1 UAM and IT solution lifecycles in general

The lifespan of one user access management solution per system might be short due to constant advancements in the IT industry, for example in regards of security and usability aspects. In addition to that, an IT service must meet the users' expectations and take into account of what people in general have been accustomed to by (presumably) using digital services daily, and what they would expect from a good modern IT service.

Cyber security related solutions must keep up with continuously evolving threats, which also applies to access management services since access management exists to prevent unwanted admissions and to ensure a safe environment for all the users and for the system itself. Certainly, for functionality and security reasons it is in the best interest of providers to follow the latest and best practices in the IT industry. Competent service providers should upkeep their services according to these said best practices by updating their software regularly, offering patches to fix vulnerabilities, having a recovery plan and strategy to detect threats. (Sakr, Zomaya 2018: B6) If not, they risk making their system vulnerable to cyber-attacks and might impair the usability of the system for best user management processes. (Campo, Dransfeld, Heuer 2017: 62)

By harnessing the best possible solutions for User Access Management, the user-friendliness of the service also greatly improves if the user account related actions happen naturally and smoothly from the users' front end, and if the users have minimal needs to contact an administrative person regarding their accounts. (The Evolution of Identity and Access Management 2019)

5.2 ”DesignIT” and UAM

As the ”DesignIT” website is still under development at the time of writing this thesis, the aspect of Identity and User Access Management has not yet become a vital part of the website due to focus on the overall functionality of the tool. However, the creators of the website have started to extend the complexity of handling and managing the user identities and accounts on the administrative side and researching methods to improve the users' possibilities to manage their own accounts.

Consulted on May 24th, 2019, the creators confirmed that they have requested an email address for the project from their supervising university. A project mailbox will enhance basic user management features such as sending a confirmation message to a registered user's valid email address after the registration and enabling the users to reset their forgotten passwords or usernames.

There has also been plans to implement a profile editing page for the users. The page will include the ability to change the linked email address if needed. Consequently, there will be an additional need to verify the email address again by the project mailbox mentioned before. (Panagiotopoulos 2019)

The importance of exterminating user accounts after they are no longer used depends on the user base growth rate and the whole "DesignIT" website's life expectancy. In case the website will be a short-term project with no plans for long-term upkeep, there might not be a need for deleting or disabling the accounts for now. Although, this is a standard phase of user accounts' lifecycle (ITIL), and would help keep the size of the user database at a reasonable level for the best functionality of the website. Getting rid of stagnant user accounts will likewise improve the secureness of the website, so that an abandoned user account equipped with a possible easy-to-guess password does not get picked out and exploited by malicious parties in order to gain unauthorized access to the website and its contents.

6 Conclusion

The objective of this thesis was to explore and suggest user account and access management methods to be implemented by a learning tool website called ”DesignIT”. As a result of examining and comparing five different UAM methods, the most suitable one for this purpose was selected along with creating hypothetical account management features for the website. These results were presented with an approach to encourage the website developers into harnessing them into use after this research.

Although being only a suggested improvement, the importance of concentrating on user access and account management aspects have been argued throughout this thesis by showing how much the user access management (UAM) could be improved. The study has also demonstrated what lacking these properties can cause in means of security and usability.

In case the outcome does not meet the requirements of the website in the future, this study now exists as a reference point to be utilized by possible consequent researches. The biggest limitation for this research was the fact that ”DesignIT” website is still well under construction at the time of writing this thesis, and the proposals do not answer a high priority need within the tool at the moment.

For a follow-up research, the foremost thing to focus on would be the thorough investigation on how to implement these proposed solutions and improvements in practice.

References

”DesignIT” website (2019) [online]. URL: https://DesignIT.e-ce.uth.gr/#/. Accessed 22 May 2019.

Erasmus +, EU (2019) About DesignIT Project [online]. URL: https://projectDesignIT.eu/. Accessed 22 May 2019.

Ucisa (2019) ITIL – A guide to access management [online]. URL: http://www.ucisa.ac.uk/search.aspx?cx=008281077274678676179%3Ayulrfklwima&cof=FORID%3A11&q=access&sa.x=0&sa.y=0. Accessed 22 May 2019.

Shakarian P., Ruef A., Shakarian J. (2013) Introduction to Cyber-Warfare : A Multidisciplinary Approach [online]. URL: https://ebookcentral.proquest.com/lib/metropolia-ebooks/detail.action?docID=1115159&query=ddos. Accessed 24 May 2019.

WebDigi (2009) How to check if an email address exists without sending an email? [online article]. URL: https://www.webdigi.co.uk/blog/2009/how-to-check-if-an-email-address-exists-without-sending-an-email/. Accessed 30 May 2019.

Teece D.J. (2017) SWOT Analysis, in Augier M., Teece D. (eds.) The Palgrave Encyclopedia of Strategic Management. Palgrave Macmillan, London [online]. URL: https://link-springer-com.ezproxy.metropolia.fi/referenceworkentry/10.1057/978-1-349-94848-2_285-1. Accessed 28 May 2019.

Poza, D. (2018) The Difference Between Web Access Management and Identity Management [online blog]. URL: https://auth0.com/blog/the-difference-between-wam-and-idm/. Accessed 28 May 2019.

Clines S., Loughry M. (2008) Active Directory for Dummies [online]. John Wiley & Sons Inc. URL: https://ebookcentral.proquest.com/lib/metropolia-ebooks/reader.action?docID=353374&query=active%2Bdirectory. Accessed 30 May 2019.

Mulcare M., Reimer S. (2003) Active Directory® for Microsoft® Windows® Server 2003 Technical Reference [online]. URL: https://learning.oreilly.com/library/view/active-directory-for/0735615772/ch02s02.html. Accessed 30 May 2019.

OAuth 2.0 website (2019) [online]. https://oauth.net/2/. Accessed 29 May 2019.

Parecki A. (2019) OAuth Access Tokens Explained [online video]. URL: https://oauth.net/videos/. Accessed 29 May 2019.

Parecki A. (2019) OAuth All the Things! What is OAuth 2.0? [online video]. URL: https://oauth.net/videos/. Accessed 29 May 2019.

Parecki A. (2019) OAuth 2 Simplified [online article]. URL: https://aaronparecki.com/oauth-2-simplified/#web-server-apps. Accessed 30 May 2019.

Spasovski M. (2013) OAuth 2.0 Identity and Access Management Patterns [online]. URL: https://learning.oreilly.com/library/view/oauth-20-identity/9781783285594/. Accessed 30 May 2019.

Martinelli S., Nash H., Topol B. (2015) Identity, Authentication, and Access Management in OpenStack [online]. O'Reilly Media Inc 2015. URL: https://learning.oreilly.com/library/view/identity-authentication-and/9781491941249/ch01.html. Accessed on 29 May 2019.

Wikipedia (2019) IBM Tivoli Access Manager [online]. URL: https://en.wikipedia.org/wiki/IBM_Tivoli_Access_Manager. Accessed 30 May 2019.

IBM Redbooks (2005) Identity and Access Management Solutions Using WebSphere Portal V5.1, Tivoli Identity Manager V4.5.1, and Tivoli Access Manager V5.1 [online]. URL: https://ebookcentral.proquest.com/lib/metropolia-ebooks/detail.action?docID=3306546&query=access%2Bmanagement. Accessed 22 May 2019.

Voulgaris, Z. (2018) Passwords and Entropy and their role in Cybersecurity [online video]. Technics Publications. URL: https://learning.oreilly.com/videos/passwords-and-entropy/9781634623612. Accessed 29 May 2019.

Griffiths R., Lawes A., Brewster E., Sansbury J. (2016) IT Service Management - Support for your ITSM Foundation exam [online]. URL: https://learning.oreilly.com/library/view/it-service-management/9781780173184/14_ch01.xhtml. Accessed 29 May 2019.

Kaiser, A. K. (2016) Become ITIL Foundation Certified in 7 Days: Learning ITIL Made Simple with Real-life Examples [online]. URL: https://learning.oreilly.com/library/view/become-itil-foundation/9781484221648/. Accessed May 30 2019.

Sakr S., Zomaya A. (2018) Encyclopedia of Big Data Technologies [online]. URL: https://link-springer-com.ezproxy.metropolia.fi/referencework/10.1007/978-3-319-63962-8. Accessed 24 May 2019.

Campo M., Dransfeld H., Heuer F. (2018) Endpoint Security, in Abolhassan F. (ed) Cyber Security. Simply. Make it Happen [online]. URL: https://link-springer-com.ezproxy.metropolia.fi/book/10.1007/978-3-319-46529-6#about. Accessed 25 May 2019.

Identity Management Institute (2019) The Evolution of Identity and Access Management [online]. URL: https://www.identitymanagementinstitute.org/the-evolution-of-identity-and-access-management/. Accessed 25 May 2019.

Panagiotopoulos, S. (2019). Email to Panagiotopoulos, S., 24 May