Masaryk University
Faculty of Informatics

Integration of Masaryk University identities to Microsoft Office 365 cloud environment

Master's Thesis

Bc. Martin Čuchran

Brno, Spring 2017

Declaration

Hereby I declare that this paper is my original authorial work, which I have worked out on my own. All sources, references, and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Bc. Martin Čuchran

Advisor: Mgr. Kamil Malinka Ph.D.

Acknowledgement

I would like to thank my work advisor, Mgr. Kamil Malinka, Ph.D., for his patience, long term support and professional experience. I would also like to thank the whole team of Office 365 and identity management group on ICS for collaboration in questions of this master's thesis. Finally, I would like to especially thank my friends and my parents for their support during my whole studies.

Abstract

The aim of this thesis is to analyse, design and deploy Masaryk University authentication with required identities to Microsoft Office 365 cloud environment, regarding the current university environment and also to minimize the impact to common users of Masaryk University.

Keywords

Microsoft Azure, Active Directory, Microsoft Exchange Online, Microsoft Office 365, SimpleSAMLphp, Shibboleth, SAML, Identity management, Single sign-on, Microsoft Powershell, Microsoft Azure Active Directory Connect

Contents

1 Introduction

The age of information technologies and the orientation of business to services brings opportunities and challenges in the use of a cloud technologies. A collaboration is moved to the virtual environment and people are facing the need for faster and simpler information exchange. Masaryk University (MU) is an organization where the collaboration is required on daily basis. Therefore, there is a place for cloud platform such as a Microsoft Office 365 [5]. Office 365 is a group of cloud based applications providing the solution for collaboration and IT ground for the organization of teams. It has been introduced in 2011 and Masaryk University has adopted this cloud platform in 2013. In 2016, Office 365 was introduced in long-term focus of Masaryk University that led to the idea of identity and authentication integration.

The goal of this thesis is to provide a solution for integration of Masaryk University identities to Office 365 cloud, analyze unified authentication options in Office 365 and connect it to the production authentication system at MU. Main challenge is to look at the integration from global point of view, accept existence of existing cooperating systems, dependencies of the identities and create design in order to keep university concepts.

The thesis consists of two main parts. First part is oriented on unified authentication and its options in Office 365. The second part is oriented on the problem of an identity synchronization and the management regarding to the existing concepts.

Content of the thesis is written in nine chapters describing motivation, current environment, used technologies, analysis, design of integration, proof of concept implementation and finally the migration plan.

First chapter briefly introduces goal of the thesis and its structure.

The second chapter is devoted to the motivation and problem definition as main reasons for the thesis theme elaboration. Third chapter describes current environment of Masaryk University related to the topic of this thesis covering identities, information systems, Active Directory [7, 34] and Office 365.

Chapter four is devoted to technologies deployed in the production environment of Masaryk University and technologies designed to solve issues connected to the main goals of this thesis. It describes technologies recommended by the best practice and its advantages and disadvantages.

Chapter five covers analysis of issues and available options connected to the main goals of this thesis. It is related to the motivation and defined problems in the current environment.

Based on the analysis from chapter six, chapter seven is devoted to the design of solution covering synchronization of identities and MU unified authentication in cloud. As solution it is meant cooperation of existing components and implementation of the proof of concept. This design depicts data flow of identity attributes across existing and developed systems including required attributes and configuration of unified authentication.

Output of this chapter is used in proof of concept implementation described in chapter seven. This chapter describes implementation of Active Directory configuration changes, Office 365 configuration changes, configuration of Azure Active Directory Connect [11] and the implementation of Powershell Web Proxy. Output will be used for production deployment in the future.

Chapter eight describes migration plan and how to to minimize impact on common users of Office 365 service.

2 Motivation

Identity management is part of every organization. Based on the size of an organization, it can consist of simple notes or large interconnected systems. In these days with large interest in information technologies and automatization of processes, a lot of identity management systems exist [4]. System of identities on Masaryk University is complicated. University identity is used in very heterogeneous environment and is very dynamic. Changes in academic membership are made on daily basis. Students start or finish their studies, change their study programs. Dynamic changes are also part of access management and often need to be reflected in connected systems as well. These changes made academic environment interesting. Academic environment also includes world wide collaboration, which creates need of identity linking and accessing from different systems. Considering the fact, we are trying to deploy full Office 365 (O365) service to Masaryk University, we have the motivation to appropriately connect university identity and implement part of new Masaryk University identity concept which is currently in development. In case of Office 365 service we must also consider the fact of existing instance of this service at Masaryk University.

Management of identities in Microsoft cloud environment, which includes Office 365, is just a small piece in more complex architecture of Masaryk University identity management. Because of that, this piece must perfectly fit into larger architecture, which includes lot of existing systems and defined processes. Following section describes selected problems that solution created by this thesis will solve.

2.1 Problem definition

Use of Office 365 as a collaboration platform regarding university concepts requires implementation of a system that is able to synchronize identities from Masaryk university intranet systems, where university identity of every employee and student is created, to Microsoft Azure Active Directory [6, 32] (AAD) and connected applications, where identity must be stored and managed for cloud purposes. An example of this situation is user mailbox. Creation of user mailbox re-

quires valid identity in cloud environment. Considering unified authentication, synchronization of key attributes of identity is required. On the other hand, collaboration as is designed in Office 365 requires group management reflecting actual situation such as categorization based on project or course membership. This approach requires synchronization of mentioned information to cloud environment as well. Masaryk University identity management system manages employee and student personal user accounts, groups of user accounts, groups of specific resources and roles in these resources. This solution, including Office 365, comes with problems, which need to be identified and resolved. The main problems of the identity synchronization in our case are:

- Synchronization speed of thousands identities
- Straggle identities across Masaryk University intranet systems
- Performance limitations of cloud interfaces
- Licensing
- Specific relations between identities

Masaryk University environment involves tens of thousands of identities, which need to be managed and synchronized to cloud environment. Every day, there are changes made on some identities in one of intranet systems. These changes need to be evaluated and provisioned across other university systems. Best case scenario, it means to synchronize changes in real time or specific amount of accepted time.

Main changes of the user identity may be done in one of two main information systems. These systems are IS MU[1] and INET MU[2]. Changes in groups or group membership are made in these systems either, or it may be done by some other external systems. For other external systems we consider intranet systems operated by faculties or other economic centers on Masaryk University with independent management. All created changes must be evaluated and provisioned to connected systems. In our case, it includes synchronization of changes

1. https://is.muni.cz
2. https://inet.muni.cz

to Microsoft cloud environment via specific interfaces. Microsoft cloud environment interfaces are accessible over following communication technologies:

- Microsoft Powershell remoting [3]
- Microsoft Graph API [4]
- Microsoft web interface - Grafical User Interface [5]

Microsoft cloud applies several limitations in their communication protocols. Limitations may affect number of concurrent connections, number of called queries or functionality.

Synchronization of identities includes creation of user accounts. We need to evaluate user competency and correctly assign licenses to this user objects regarding the Microsoft licensing policy [19] and signed agreements. Because of Microsoft licensing model which distinguishes employees, students, alumni, and these competencies can overlay, operation of license association may be nontrivial from identity management point of view.

To sum up, this thesis must cover integration of Office 365 required changes to MU identity management and solve some performance issues. Following sections cover description of current environment and technologies that will help create appropriate solution to reach the final goal of this thesis.

3. Microsoft Powershell remoting is an implementation of remote calls via SOAP web service in Microsoft environment
4. Microsoft Graph API is unified REST API for Microsoft online services
5. https://portal.office.com

3 Current environment

Following the motivation, defined problems and the main goal of this thesis, this chapter describes following parts of current Masaryk University environment:

- Masaryk University Identity
- Identity and Access management system
- Information systems - IS MU [1], INET MU [2]
- Active Directory
- Microsoft Office 365

Description of the mentioned parts of the environment depicts current and final state of system components. Final state is designed regarding the concepts at Masaryk University.

3.1 Masaryk University identity and access management

Identities of Masaryk University are straggled into several systems that made this environment extremely heterogeneous. Such systems include information systems IS MU, INET MU, UCN Active Directory and other internal systems which can be found at faculties and are managed by independent groups. This situation requires to create unified concept of identities and access management at Masaryk University. This concept specifies source of identities, services and components responsible for managing access, identity changes and propagation of these information to the services that are used by individuals.

---

1. IS MU is information system of Masaryk University. It currently hosts numerous applications utilized for managing study-related records, e-learning tools and those facilitating communication inside the University
2. INET MU is information system of Masaryk University. The purpose of the system is to enable access to data stored in MU university-wide databases, primarily in the integrated database of human resources, wages, and economical data operated by the ICS MU

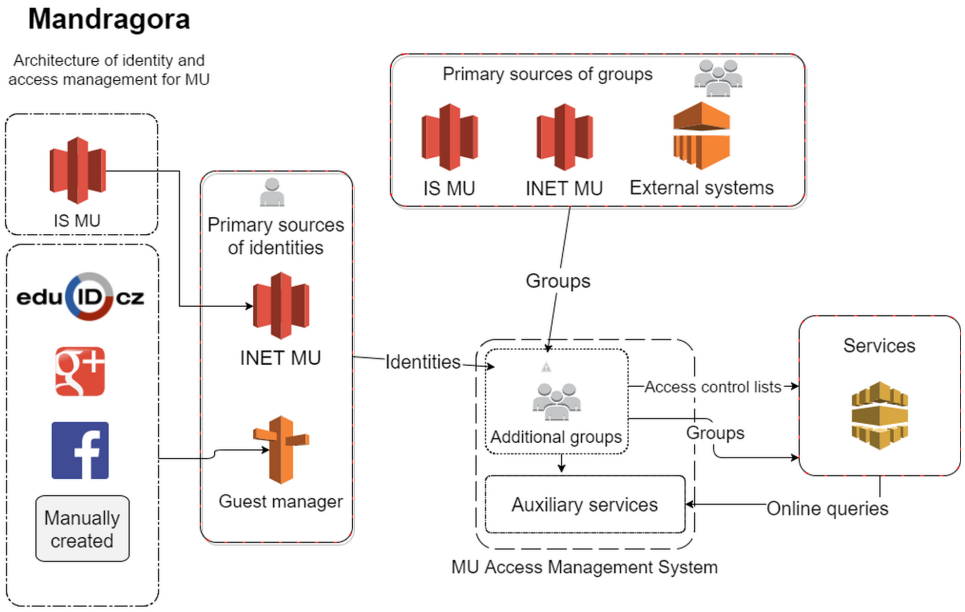

Figure 3.1: Architecture of identity and access management at Masaryk University [3, 20]

Identity management system role in current state is provided by INET MU and IS MU itself and component called AccountManager. AccountManager is an application connected directly to databases of INET MU and IS MU. It obtains data from these databases and based on statically defined rules creates information about changes on identities which need to be provisioned to connected services. One of this service is Microsoft Active Directory *ucn.muni.cz*. AccountManager also mediates an interface for creating guest identities. Problem of current solution is that documentation of AccountManager is obsolete as system itself which prevents any change been made to existing rules.

Target state will be covered by system, which is partially implemented and simultaneously used. It will solve problems of AccountManager. It is called Perun [14, 20]. Perun is identity and access management system and is a part of the Mandragora project [3, 20] at Masaryk University, covering field of identity management. Perun ensures implementation of identity management concept of Masaryk Univer-

sity regarding all new requirements. It can be extended using connectors to specific data sources and data outputs.

Figure 3.1 describes identity concept where IS MU and INET MU with connected components are considered to be the primary source of identities. External systems can be used as source of guest identities. These identities may be added with group relationship from internal and external systems. All gathered information and dependencies are properly evaluated and provisioned to connected services. Single point of identity evaluation enables better management of identity and access to university resources. Goal of this thesis is to consider Microsoft Office 365 as one of the connected services and implement required changes.

3.2 Active Directory ucn.muni.cz

Masaryk University operates Microsoft Active Directory with domain name *ucn.muni.cz*. In current state Active Directory provides storage and authentication of active identities, groups and other network objects such as computers. It also provides access to stored information via standard LDAP [21] protocol for other LDAP based services. Identities are provisioned to Active Directory by AccountManager, where Active Directory plays the role of service. Active Directory has role of identity attributes source for MU unified authentication based on SAML [15] or ODATA [16] protocols.

3.3 MU Office 365

Microsoft Office 365 is one of the services that is available for users of Masaryk University. Office 365 is software as a service product primarily focused on team collaboration. This product offers applications for shared web space, email communication, instant messaging, planning of work and others. Masaryk University is using tenant named *ucnmuni* with Education license plan assigned. License agreement allows assign access to online applications to all employees, students and alumni of university.

Current environment provides two types of user accounts that correspond to their mailboxes. Type is distinguished by its e-mail address as follows:

- <uco>@mail.muni.cz
- <uco>@ucn.muni.cz

Microsoft Office 365 is not the first solution for e-mail communication at Masaryk University. Some users are using other e-mail solutions from historical reasons. Other e-mail solutions are often not provided centralized. Because of that, all user accounts in Office 365 are not created with fully configured mailbox. For these reasons, unified concept of e-mails at Masaryk University was created. Concept of unified e-mails defines two types of e-mail for all members of MU:

- <uco>@mail.muni.cz - hosted in IS MU
- <uco>@muni.cz - hosted in Office 365

Current state of university Office 365 tenant did not require synchronization of all users to cloud environment because the account in Office 365 was optional. Regarding the new concept of identities and e-mails, all users must have account created in Microsoft Office 365 including synchronization of changes.

New solution of integration of Masaryk university identities to Office 365 must include new technologies to improve inappropriate configuration of current environment state. Next chapter will describe technologies with possibility of use in this field and their advantages.

4 Technologies

Management, evaluation and synchronization of a large amount of identities presented at Masaryk University to Office 365 regarding the best practice and security policy of MU require the use of specific technologies. This chapter describes main technologies that are possible to use during designing the final integration solution. Selected technologies may be suitable for different parts of final solution:

- SimpleSAMLphp [8]
- Shibboleth [9]
- Active Directory
- Azure Active Directory
- Office 365
- Active Directory Federation Services [10]
- Azure Active Directory Connect
- Powershell [12, 31]
- Network load balancing [13]

4.1 SimpleSAMLphp

SimpleSAMLphp is application written in native PHP language. The main focus of the application is made on the support for the following protocols:

- SAML 2.0 as a Service Provider (SP)
- SAML 2.0 as an Identity Provider (IdP)

Advantage of SimpleSAMLphp is in its support for other identity protocols and frameworks, such as Shibboleth 1.3, A-Select [22], CAS [23], OpenID [24], WS Federation [25] or OAuth [26]. It can be also

easily extended by developing own modules. SimpleSAMLphp uses memcache session handler which allows scale pretty well. Memcache is used for replication layer that allows unlimited number of SimpleSAMLphp front-ends work with back-end matrix of memcache servers. Replication and load balancing can be used.

Another advantage of SimpleSAMLphp is in its simple configuration based on PHP programing language and better deployment options in cluster environment. For the main disadvantage we can consider the missing support of ECP extention of SAML protocol. Masaryk University operates one clustered instance of SimpleSAMLphp for purpose of MU unified authentication.

4.2 Shibboleth

Shibboleth is an application that offers capability of web single sign-on across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner. The Shibboleth implements widely used federated identity standard SAML, to provide a federated single sign-on and attributed exchange framework. A user authenticates with his or her organizational credentials and the identity provider passes the identity information necessary to the service provider to enable an authorization.

Shibboleth is used as identity provider for active authentication requests. Active authentication request uses extended version of SAML protocol known as Enhanced Client or Proxy (ECP). ECP implements SAML functionality for non-web based clients. Disadvantage of Shibboleth is non-trivial configuration and complicated deployment based on Java programing language.

4.3 Active Directory

Active Directory is Microsoft implementation of Lightweight Directory Access Protocol. Active Directory is a centralized and standardized system that automates network management of user data and distributed resources. Active Directory is primarily focused on distributed networking environments.

Masaryk University operates one instance of production Active Directory under fully qualified domain name *ucn.muni.cz*. It provides access and authentication to university identity via LDAP protocol. One of the disadvantages of Microsoft Active Directory is missing support for multiple user passwords.

4.4 Azure Active Directory

Azure Active Directory (Azure AD or AAD) is Microsoft multi-tenant cloud based directory and identity management service. Azure AD provides an affordable, easy to use solution to give employees and business partners single sign-on (SSO) access to thousands of cloud softwares as a service applications.

Azure AD also includes a full suite of identity management capabilities including multi-factor authentication, device registration, self-service password management, self-service group management, privileged account management, role based access control, application usage monitoring, rich auditing and security monitoring and alerting. These capabilities can help secure cloud based applications, streamline IT processes, cut costs and help ensure that corporate compliance goals are met.

Additionally, Azure AD can be integrated into an existing on-premise Active Directory. Every Office 365 or Azure tenant is actually an Azure AD tenant.

Disadvantage of Azure AD is a missing full support of features available in on-premise Active Directory. It also needs to store password information which in our case violates Masaryk University password policy described in section 5.1.3.

4.5 Office 365

Office 365 refers to subscription plans that include access to Office applications plus other productivity services that are enabled over the Internet as a software and a service. Office 365 includes plans for use at home, business or education. For consumers, the service allows the use of Microsoft Office applications on Windows and MacOS

platform. Office 365 is broadening communication and collaboration capabilities.

Masaryk University has education subscription [35] which includes following applications:

- Exchange online
- Sharepoint online
- OneDrive
- Skype for Business
- Teams
- Planner
- Delve
- Sway
- Yammer

4.6 Active Directory Federation Services

Active Directory Federation Services (AD FS) is a service that allows to secure sharing of identity information between trusted entities (known as a federation). When a user needs to access a Web application from one of its federation entity, the user's own organization as the second trusted entity is responsible for authenticating the user and providing identity information in the form of "claims" to the entity that hosts the Web application. Trust policy is used to map the incoming claims to claims that are understood by its Web application which uses the claims to make authorization decisions.

AD FS is Microsoft implementation of the WS-Federation Passive Requestor Profile protocol [25]. Passive indicates that the client requirements are just a cookie and JavaScript-enabled Web browser. AD FS implements the standard based WS-Federation protocol and SAML. AD FS may be used as identity provider for Microsoft cloud environment and is tied up with Active Directory.

Disadvantage of Active Directory services is orientation at Microsoft products as requirement of additional licenses to Windows server. From previous experiences of identity management team, it misses some features required for academic federated access such as unique identificator of IdP metadata based on attribute entityId. Some of missing features are implemented in latest version of AD FS with number 3.0 that is missing reliability.

4.7 Azure Active Directory Connect

Azure Active Directory Connect (AD connect) integrates on-premises Active directories with Azure Active Directory. This allows to provide a common identity for Office 365 users and software as a service applications integrated with Azure AD. AD Connect is made up of three primary components:

- The synchronization services
- The optional Active Directory Federation Services component
- The monitoring component named Azure AD Connect Health

Azure Active Directory Connect is required in case of integration of on-premise and Azure Active Directory. Disadvantage of Azure Active Directory Connect is missing option of clustered deployment.

4.8 Powershell

PowerShell including Windows PowerShell and PowerShell Core is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language built on the .NET Framework. PowerShell provides full access to COM[1] and WMI[2], enabling administrators to perform administrative tasks on both local and remote Windows systems as well as WS-Management [27] and CIM[3] enabling management of remote Linux systems and network devices.

1. Component Object Model
2. Windows Management Instrumentation
3. Common Information Model

Powershell is widely used in current deployment of Office 365 at Masaryk University. Disadvantage of Powershell is performance issue in case of larger amount of operations on remote resources as Office 365.

4.9 Network load balancing

The Network Load Balancing (NLB) feature in Windows Server enhances the availability and scalability of internet server applications such as those used on Web, FTP, firewall, proxy, virtual private network, and other mission-critical servers. A single computer running Windows Server provides a limited level of server reliability and scalable performance.

NLB allows hosts in the cluster to be addressed by the same set of cluster IP addresses. It also maintains a set of unique, dedicated IP addresses for each host. For load-balanced applications, when a host fails or goes offline, the load is automatically redistributed among the hosts that are still operating. When a host fails or goes offline unexpectedly, active connections to the failed or offline server are lost. The drainstop command allows to correctly bring down the host. The offline host can transparently rejoin the cluster and regain its share of the workload which allows the other computers in the cluster to handle less traffic.

Network load balancing technology is widely used at Masaryk University. Disadvantage is dependency on Microsoft Windows Server including paid license.

Technologies mentioned in this chapter are all used at Masaryk University except Active Directory Federation Services. This technology will not be used in following analysis and design because of mentioned disadvantages. Following chapter will describe analysis of environment and options helping retrieve results required for final design of integration Masaryk University identities to Office 365 cloud environment.

5 Analysis

Considering current environment, identities and available technologies regarding the new concepts of mentioned systems at Masaryk University, analysis needs to cover problems with ongoing transformation to new identity management, MU unified authentication and problems with Office 365 identity management. Therefore, this chapter meets following points:

- Synchronization of objects with Office365
- Unified authentication at Masaryk University
- Integration of solution to existing architecture
- Impact on existing environment

5.1 Unified authentication at Masaryk University

Masaryk University is using several authentication methods and protocols. The main reason why more protocols and methods are used is that systems which need to cooperate are heterogeneous and require implementation of various authentication protocols. For authentication and identity distribution across internal systems of Masaryk university is mainly used LDAP authentication and Active Directory authentication. In case of authentication in systems which require cooperation with external systems of other entities, federated identity and authentication is preferred. It allows to use external identity in internal systems and authenticate users in home environment. Federated authentication mainly uses SAML 2.0 protocol which was created for this purpose. Considering Microsoft Office 365, federated authentication or Azure Active Directory authentication solution implemented in Microsoft cloud can be used.

5.1.1 Active Directory authentication

Masaryk University offers two options of authentication via Active Directory. Lightweight Directory Access Protocol and Kerberos.

Lightweight Directory Access Protocol is defined as a protocol for storing data and accessing to the directory services. LDAP is used as standardized protocol for access to Masaryk University Active Directory. In LDAP, authentication is supplied in the "bind" operation. Last version of LDAP supports three types of authentication. It is anonymous, simple and SASL [28] authentication. A client that sends a LDAP request without doing a "bind" is treated as an anonymous client. Simple authentication consists of sending the LDAP server the fully qualified domain name of the client (user) and the client's clear-text password. This mechanism has security problems because the password can be read from the network. To avoid exposing the password in this way, you can use the simple authentication mechanism within an encrypted channel (such as SSL).

Finally, SASL is the Simple Authentication and Security Layer. It specifies a challenge-response protocol in which data is exchanged between the client and the server for the purposes of authentication and establishment of a security layer on which a subsequent communication is carried out. By using SASL, LDAP can support any type of authentication agreed upon by the LDAP client and server.

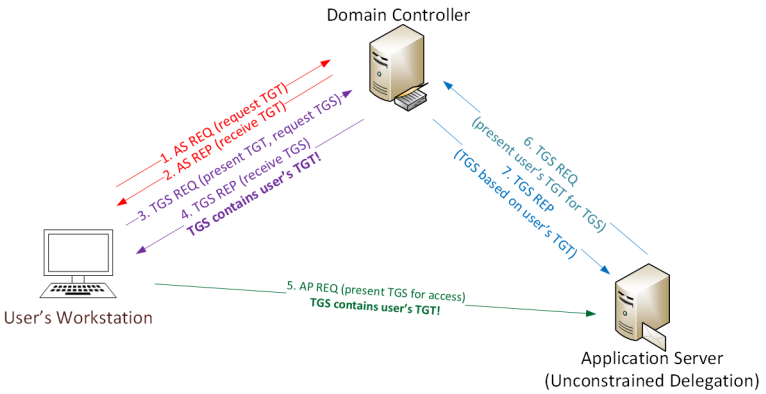

Figure 5.1: Kerberos client-server communication [2]

Kerberos [2] is a computer network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client–server model and it provides mutual authentication both the user and the server

verify each other's identity. Kerberos protocol messages are protected against eavesdropping and repetitive attacks. Figure 5.1 depicts Kerberos client-server communication.

5.1.2 Federated identity

Federated identity and authentication is using Security Assertion Markup Language 2.0 protocol that allows to redirect authentication request to home organization which has defined trust with requesting service. It also allows to obtain identity information from home system. Security Assertion Markup Language 2.0 (SAML 2.0) is a version of the SAML standard for exchanging authentication and authorization data between security domains. SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a principal between a SAML authority, named an Identity Provider and a SAML consumer, named a Service Provider. SAML 2.0 enables web-based authentication and authorization scenarios including cross-domain single sign-on (SSO) which helps reduce the administrative overhead of distributing multiple authentication tokens to the user. Following picture demonstrates authentication mechanism via SAML 2.0 protocol.

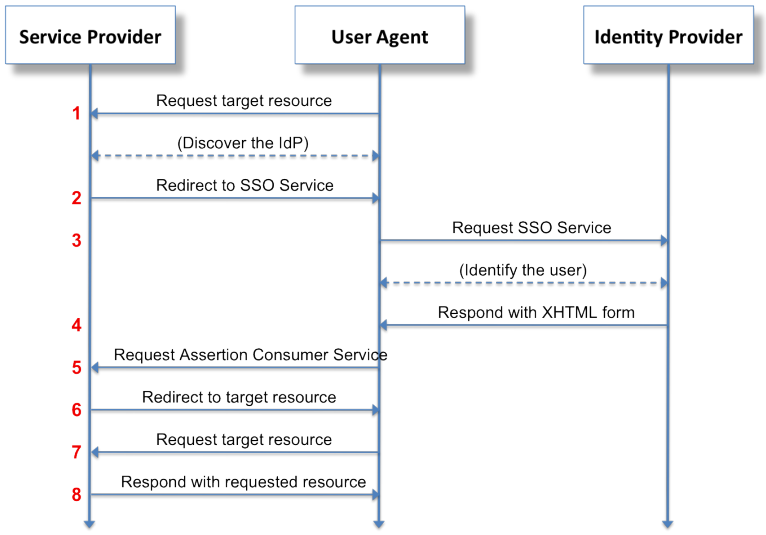

Figure 5.2: SAML 2.0 authentication process [15]

5.1.3 Masaryk University password policy

Masaryk University enforces security policy which requires two different passwords for every user of main information systems. IS MU defines these passwords as primary password and secondary password.

Primary password

Primary password is mainly used for systems where sensitive data is stored. For these purposes, primary password is used only in IS MU, mainly used by academics and students and on the other hand INET MU is mainly used by employees. Strong password policy is enforced for this type of password and by recommendations of system administrators this password should not be used in other systems, saved by browsers or other third party systems intended to password storing.

Secondary password

Secondary password is used for purposes of third party systems which can be university Active Directory, e-mail systems and other proprietary systems using university authentication. In case of secondary password, system administrators count with possibility of storing this password for better usage and with possibility of password leaks. Therefore, secondary passwords should not be used to access sensitive data.

5.1.4 Office 365 identity and authentication

Microsoft Office 365 is a software as a service product offered by Microsoft Azure cloud. In standard way it comes with two major types of identity and authentication solutions.

- Cloud identity and authentication [33]
- Hybrid identity and authentication

Cloud identity and authentication solution are standard ways of using cloud services and environment. All data and authentication pro-

cess is provided with cloud utilities. Hybrid identity and authentication solution allow combination of on-premise and cloud resources. Identity data are synchronized to cloud and authentication is made in on-premise solution. It prohibits sharing of sensitive data such as passwords with cloud environment.

Cloud authentication mechanisms

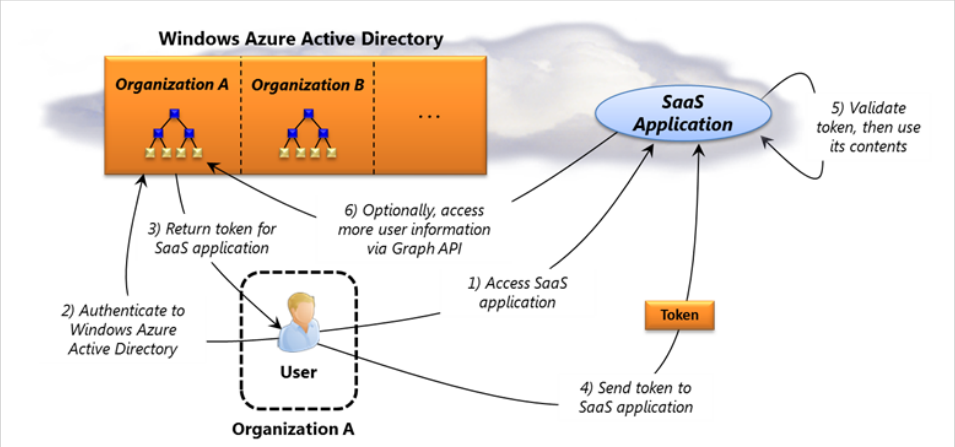

Figure 5.3: Office 365 cloud authentication mechanism [1]

Microsoft Azure cloud offers three different technologies for identities. Each of this technology has its own scope of usage and different type of authentication.

- Windows Server with Active Directory in the cloud using virtual machines created with Azure Virtual machines can be used. This approach makes sense when you're using Azure to extend your on-premises datacenter into the cloud.

- Azure Active Directory with a single sign-on to software as a Service application can be used. Microsoft Office 365 uses this technology. Applications running on Azure or other cloud platforms can also use it.

- Applications running in the cloud or on-premises can use Azure Active Directory Access Control to let users log in using identities from Facebook, Google, Microsoft and other identity providers.

In our case we are going to use software as a service application primary using Azure Active Directory. Azure Active Directory allows us to store required information about identities. In this case Microsoft offers cloud single sign-on solution for authentication based on Azure Active Directory. This authentication can be extended with multi-factor authentication enhancing better security of authentication. Figure 5.3 depicts mechanism of cloud authentication with Azure Active Directory.

Hybrid authentication mechanism

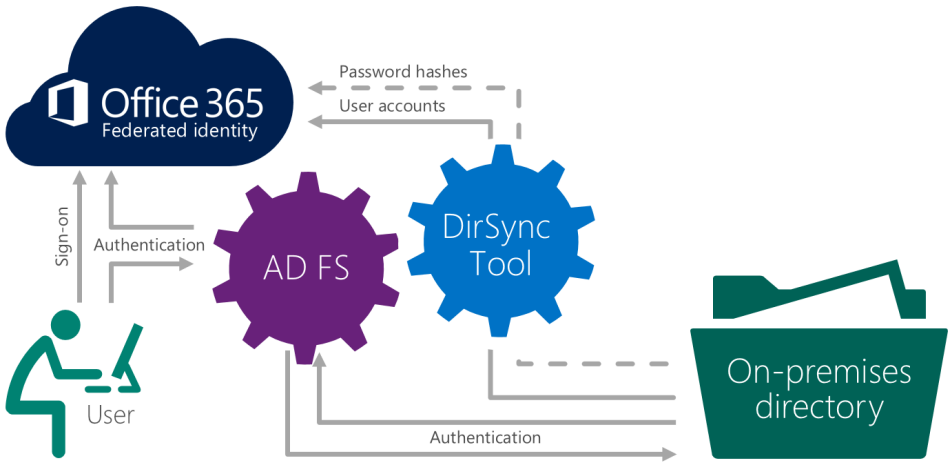

Figure 5.4: Office 365 hybrid authentication mechanism [30]

Microsoft hybrid deployment offers possibility of using on-premise solution in combination with Azure cloud environment. Hybrid deployment can be used for migration from on-premise solution to cloud environment or to long term solution based on combination of local and online resources. The biggest advantage of hybrid deployment is possibility of using on-premise authentication mechanisms allowing to store sensitive data as passwords in local environment. In case

of local authentication mechanisms, Azure Active directory is responsible for standard authentication in cloud and can be extended with on-premise Active Directory synchronization and systems for authentication. In our case authentication is provided by combination of SimpleSAMLphp and Shibboleth identity providers. This combination of systems requires installation of AAD connect with responsibility for synchronization of critical object attributes as NameID and IDPE-mail. Azure Active Directory connect then allows to use on-premise AD as local source of identities for identity providers. Figure 5.4 depicts hybrid authentication mechanism.

5.2 Synchronization of objects with Office365

Synchronization of objects with Office 365 requires the analysis of objects that are available in Office 365 cloud environment and objects available in on-premise environment. These objects need to be specified and relationship between cloud and on-premise objects must be described as well.

5.2.1 Office 365 objects

Software as a service which is used by Masaryk University in Office 365 environment requires following objects to be analyzed and mapped to on-premise environment.

- User – Simple Identity. Attributes describe name, location, contact and job title.
- Contact – Object which represents external e-mail address or user in system.
- Mailbox – It contains information about e-mail account of user. It is created after license is assigned to user object.
- Distribution list – List of e-mails. It can be replaced with security mail enabled group.
- Security group – Users can be members of group for better access management.

- Security mail enabled group – It is security group extended with e-mail. All security groups can be replaced by security mail enabled groups.

- Shared mailbox – Object that allows to share one e-mail account between several users.

- Office 365 group – Special type of group that groups resources such as sharepoint web, e-mails and others. Resources are limited, therefore, access to this type of object must be managed by administrator.

5.2.2 On-premise Active Directory objects

Masaryk University does not have its own on-premise Exchange[1] server. Therefore, on-premise Active Directory stores only following objects:

- User – Simple Identity. Attributes describe name, location, contact and job title.

- Contact – Object which represents external e-mail address or user in system.

- Distribution list – List of e-mails. It can be replaced by security mail enabled group.

- Security group – Users can be members of group for better access management.

Mentioned list of cloud and on-premise objects is not the same. This situation requires implementation of object attribute mapping to achieved successful synchronization and same objects in cloud and on-premise solution. This mapping can be managed by Active Directory connect or logic in Perun.

1. Microsoft implementation of mail server

5.3 Integration to existing architecture

As was mentioned in motivation and current environment description, integration of identities and authentication to Microsoft Office 365 requires implementation that will be part of a larger identity management system. Therefore, it must consider analysis of source of identities. This section analyzes the process of identity management in main information systems and its aggregation and provisioning to connected services via system of identity and access management called Perun. Perun is system that offers connectors to different data sources, collects connected data and by specified rules provisioning changes to target services.

5.3.1 INET MU and human resources

INET MU is source of identities which covers human resources and all identities that have connection to staff at Masaryk University. It manages organization infrastructure and all identity changes connected to it. In reality, it means, that process of new employee is managed via human resources department and all information is available via INET MU. All employees are divided into groups that represent organization units at Masaryk University. In context of source of identities, it needs to work with groups based on organization units which require to implement a connector to INET MU and synchronize required information to Office365.

On the other hand, INET MU offers graphical user interface as single management point for members of university. Due to, graphical user interface for Office 365 resources needs to be implemented as a part of INET MU.

5.3.2 IS MU

IS MU is source of information connected to academic part of university. It holds information about teachers, students, subjects and their relationships. Relationship information are collected as special groups. These groups define functions of membership. Mentioned groups can be created in IS MU by users with appropriate authorization, therefore,

there is strong assumption that IS MU groups will be needed in Office 365 as well.

5.3.3 External systems

External systems for the purpose of this thesis are defined as systems where information about identities are not documented yet. Considering global architecture of identity management, there must exist a way to connect any new source of identities via existing identity management system. Option like this is covered by Perun identity management system offering connectors to standard protocols. If non-standard protocol is only available in external system, new system specific connector must be created.

5.4 Impact on existing environment

Considering that Office 365 is responsible for e-mail communication at university, it is one of the very critical applications. Working with application in production requires analysis of all possible impacts on common users during every change which is provided in Office 365 environment. Implementation as a part of a larger architecture also requires to make changes on production Active Directory. Situation can be solved with new Office 365 tenant and Active Directory for testing purposes. Test environments allow us to test all possible changes without an impact on user or production environment.

5.4.1 Statistics

Office 365 contains approximately 42 000 accounts and 200 Office 365 groups in current configuration. It includes all active members of university. On-premise Active Directory contains approximately 270 000 objects. This number includes user accounts and groups.

5.4.2 Estimated number of objects

Based on information from departments responsible for e-mail communication and collaboration, there is masive deployment of Office

365 at Masaryk University and it is estimated that numbers of objects and usage of Office 365 applications will rise. Analysis of user and group life cycle shows that 10 000 user objects and hundreds of groups will be added every year.

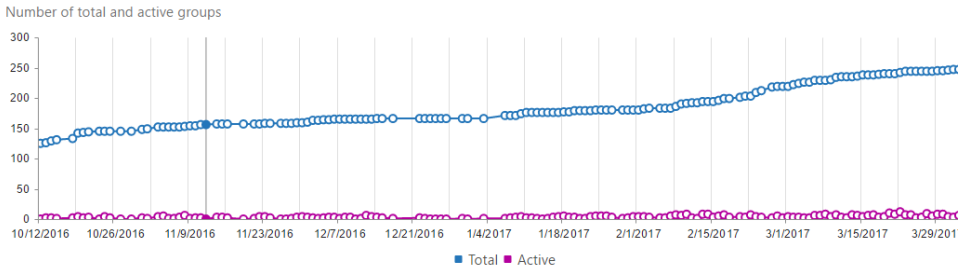

Figure 5.5: Number of Office 365 groups for six months

Figures 5.5 and 5.6 depicts upward trend of Office 365 usage. Statistics are based on data during last six months. Possible reason of active objects stagnation is short lifetime of object from view of user.

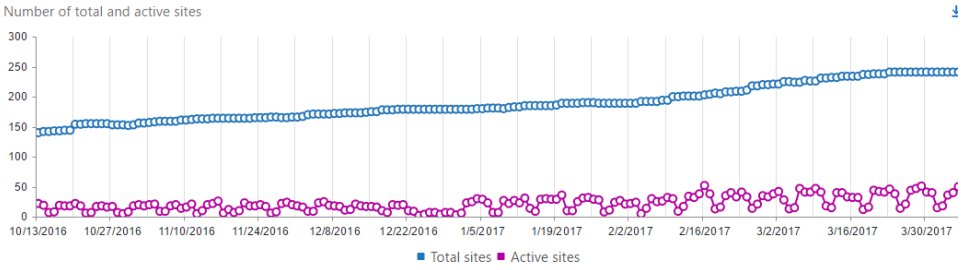

Figure 5.6: Number of Sharepoint sites for six months

To sum up, mentioned analysis describes options of MU unified authentication, possible sources of identities at MU, estimated numbers of objects and integration options regarding the existing components. Following chapter will introduce design based on this facts.

6 Design of integration

Proposed design of integration is based on previous analysis regarding the best practice of Microsoft. Considering current user requirements to collaboration platform, current environment analysis and available technologies, design of integration is created regarding to university concepts and architecture of identity management. This design consists of two main parts:

- Design of Microsoft Office 365 identities synchronization
- Design of Hybrid authentication mechanism

Microsoft Office 365 identities synchronization is responsible for managing identities in cloud environment based on rules specified in on-premise systems and regarding to analyzed university concepts.

Hybrid authentication mechanism is used to prevent synchronization of user password to cloud environment and is connected to single sign-on authentication across the systems used at university.

These two parts are closely connected. Authentication requires correct identities and its synchronization especially in hybrid environment. Identities are also required for achieving the best possible of all software as service products offered by Microsoft and used by university users.

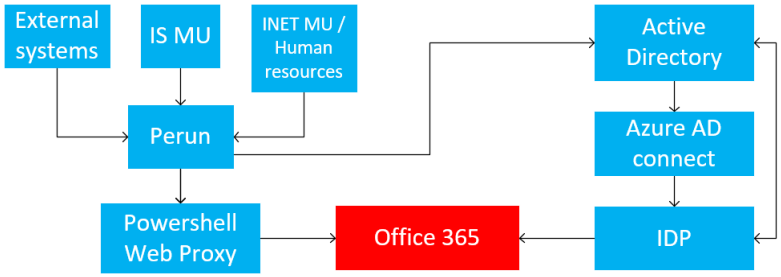

Figure 6.1: Design of identity integration and unified authentication

Figure 6.1 depicts proposed design in general including source of identities, identity management system and synchronization connectors required by Office 365. Second part of figure depicts identity provider and selected hybrid authentication.

6.1 Data flow of synchronization

Design of Microsoft Office 365 identities synchronization requires specific data flow between selected systems where data for Office 365 are created and managed. Therefore, data flow diagram is created that describes how data are managed in object life cycle. It covers sources of objects, management, evaluation and propagation to target system. Second part of section covers design of hybrid authentication and its components.

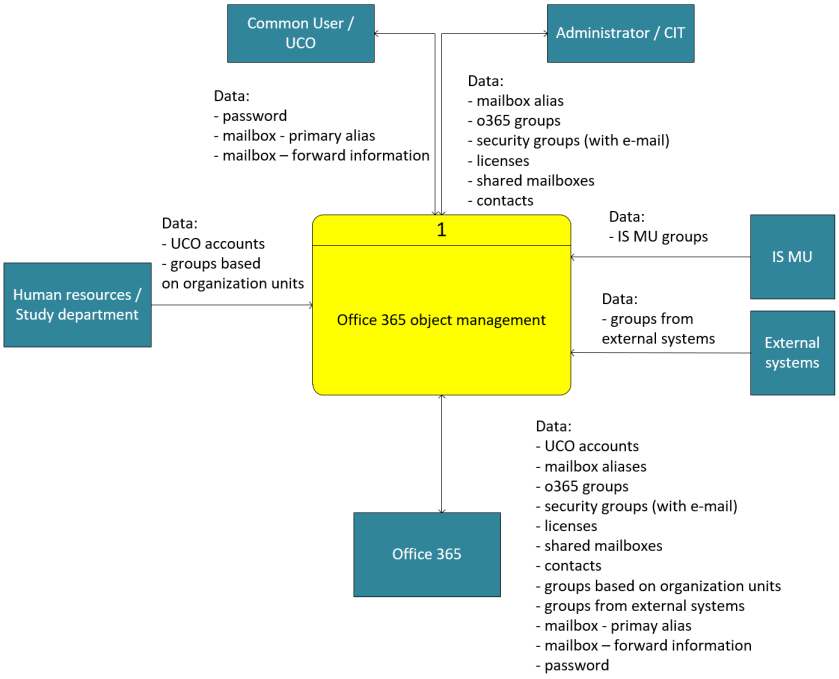

Figure 6.2: Data flow diagram – context diagram

6.1.1 Identities

Data flow diagram of system which will manage identities for Microsoft Office 365 is divided into several levels. Figure 6.2 depicts data flow diagram also known as context diagram of system responsible for handling required identities and attributes to Microsoft Azure cloud. This system cooperates with five main internal entities and one

external entity which is Microsoft Office 365. Entities have effect on processed identities. Proposed design follows all existing components and integrates them into expected system.

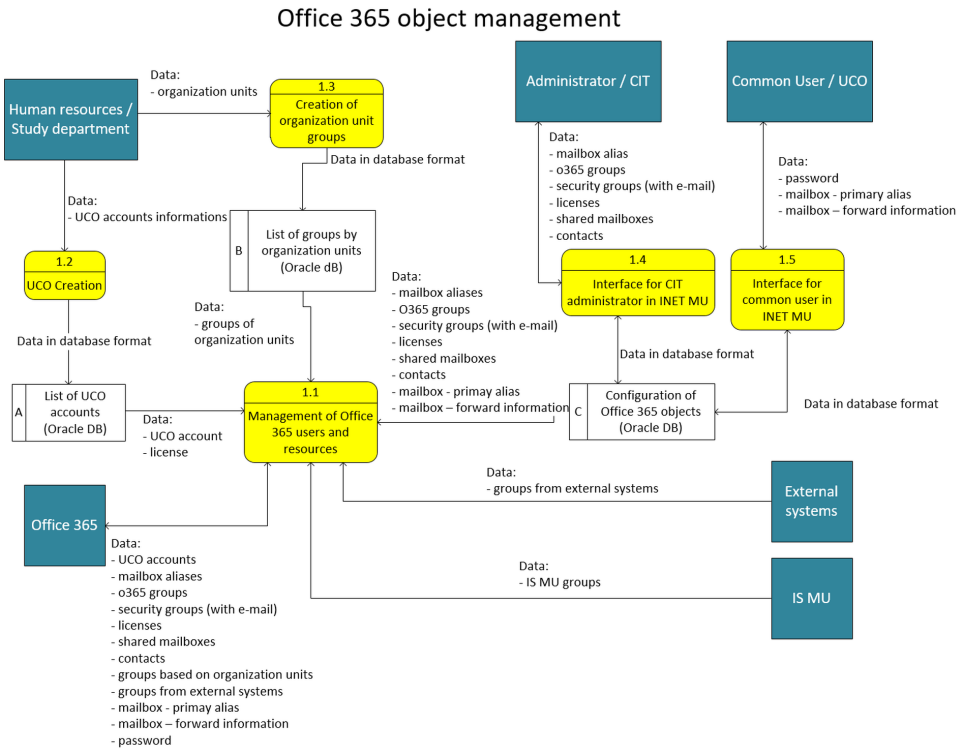

Figure 6.3: Data flow diagram – 1st level

Figure 6.3 depicts first level of data flow diagram which describes inputs from several systems and user interfaces to system for managing Microsoft Office 365 identity. In this figure we can see which databases are needed to be queering for data and what type of data is managed by this databases. It also describes how user and administrator can interfere synchronized data via graphical user interfaces that are available via INET MU. All selected systems have their administrators, therefore their cooperation is required to reach final integration.

Figure 6.4 describes data of managed Microsoft Office 365 identity in detail. Management of data consists of several systems responsible for managing identities at Masaryk University. Microsoft Office 365

offers several interfaces for communication and data synchronization. Not all interfaces are able to manage all types of tasks required to fulfill requirements of working identity. Only Powershell interface is able to manage all types of tasks. Unfortunately, this interface is not suitable for management of large amount of groups and group membership. This situation requires implementing several data flows that implements different interfaces. Some tasks need to be synchronized with each other such as user and mailbox creation. Because of this problems, correct data flows was specified and Powershell Web Proxy was used for Powershell interface that is developed and set as part of design.

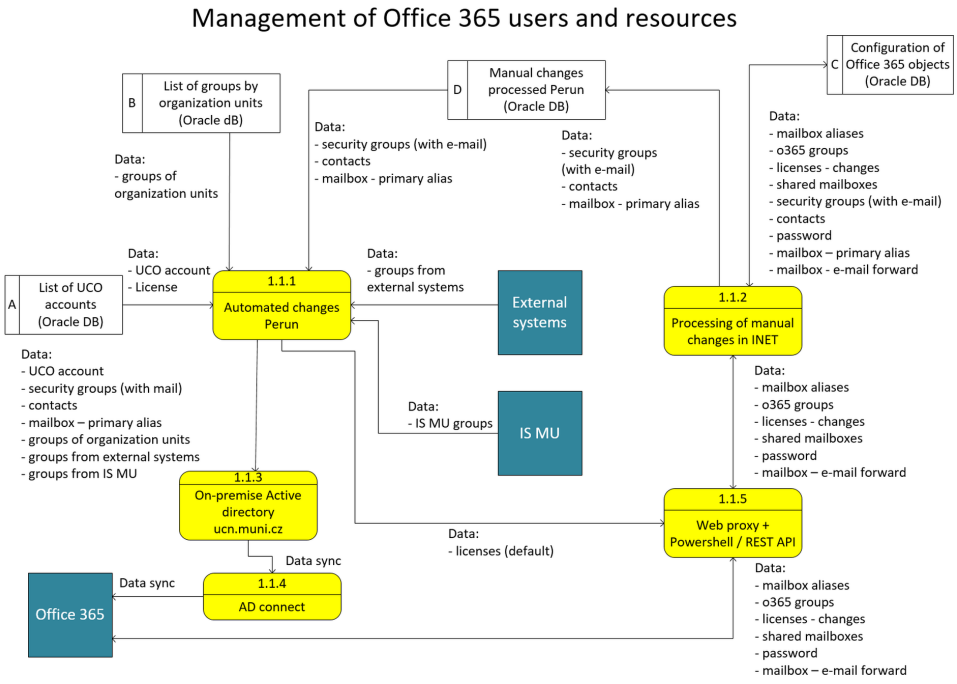

Figure 6.4: Data flow diagram – 2nd level

Figure 6.5 and 6.6 depict second level of data flow diagram and its data flows specific for user graphical interfaces implemented in INET MU. Graphical user interface is divided into two main parts. One part is available for system administrators and the second part is oriented to common users and their personal changes.

Solution of managing Microsoft Office 365 identities is complex system consisting of existing information systems, databases and im-

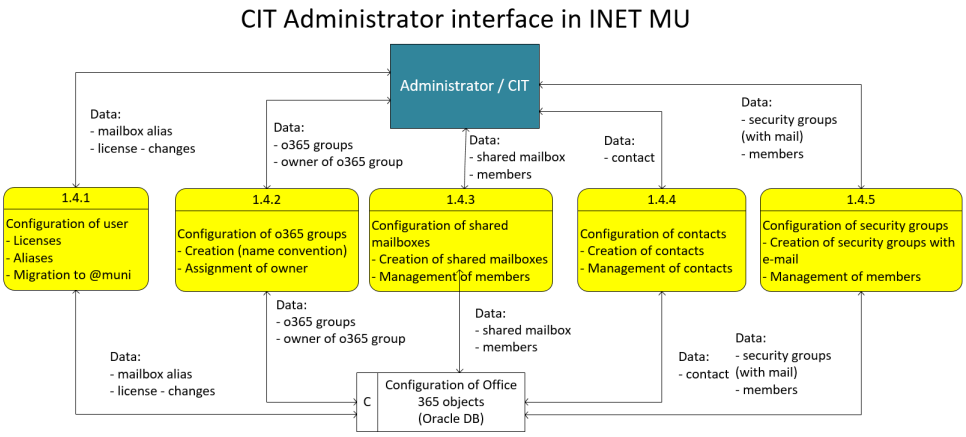

Figure 6.5: Data flow diagram – second level administrator GUI

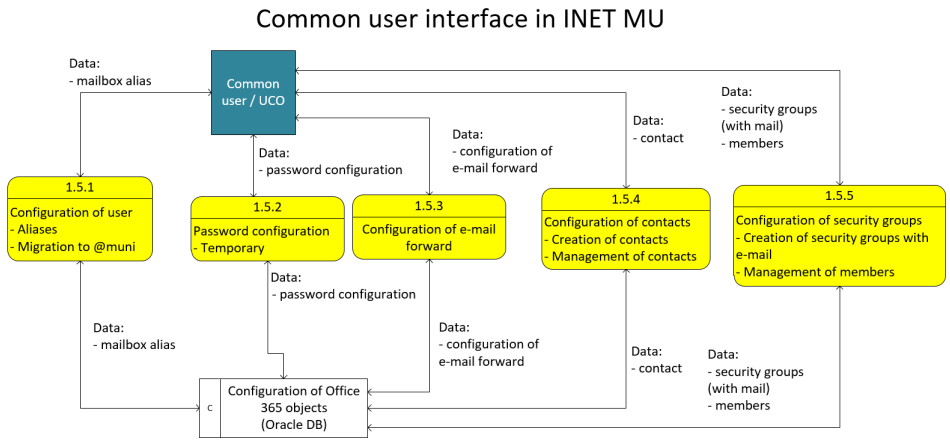

Figure 6.6: Data flow diagram – second level common user GUI

plements Microsoft office 365 interfaces. Goal of this solution is in specification of correct data flow, synchronization rules and use of available interfaces in the best possible way.

6.1.2 Authentication

Microsoft Hybrid deployment is using Active Directory Federation services as authentication provider by best practice. Microsoft Cloud environment introduces study cases where this type of service is used,

explained and supported solution. Authentication in Masaryk University cloud is designed to be able to use European federated identities. It allows to extend its usage with multi-factor authentication. These are the reasons SimpleSAMLphp was selected as identity provider for passive type of requests using SAML 2.0 protocol. Active requests using ECP extension of SAML 2.0 must be handled in separate instance of identity provider. For this purpose, Shibboleth identity provider is also installed and configured as part of MU unified identity provider. Identity providers are installed and managed by identity management team from ICS MU.

To be able to use Hybrid cloud authentication, Azure Active Directory requires synchronization of identities via Azure Active Directory Connect with on-premise Active Directory. Figure 6.7 describes schema of requests and responses that are made in hybrid deployment. User tries to access resources in cloud environment. Cloud environment checks existence of user identity and authenticates identity over predefined identity provider which is SimpleSAMLphp or Shibboleth based on type of request. Identity is synchronized between on-premise and cloud environment and must share same ImmutableID attribute. User is then authenticated and based on ImmutableID sent by identity provider back to service provider. Service provider decides whether user is allowed to access requested resources.

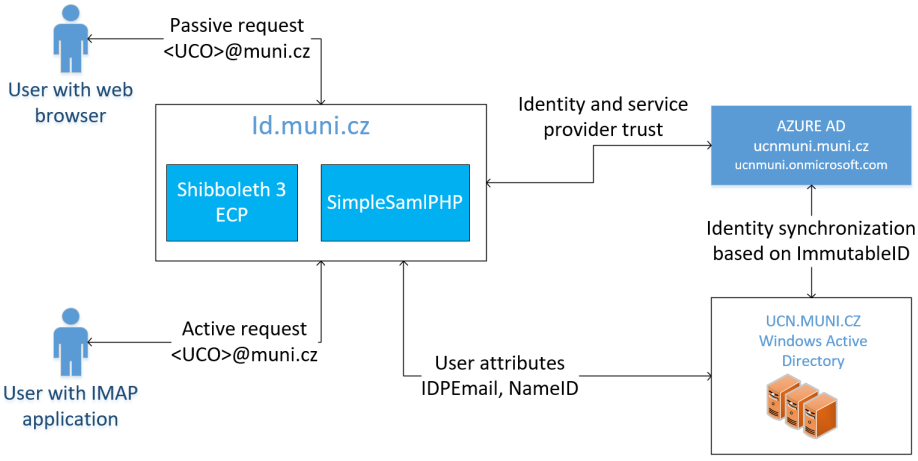

Figure 6.7: Authentication scheme

6.2 Test environment

Office 365 at Masaryk University is in production, therefore any changes require to implement test environment. In this environment changes can be safely tested and results may be analyzed before deployment in production. Test environment is build by specification based on result of analysis and design of identity synchronization process and MU unified authentication. Deep analysis of available protocols, their usage, configuration options of selected technologies and performance tuning is not possible without testing. Management of identities and authentication regarding the existing concepts and best practice require correct setup of available attributes and processes as well. All this is possible only in test environment especially if the production environment is in daily use. Different configuration was tested in this environment and results were analyzed. Positive aspects were transformed into the final design. Figure 6.8 describes architecture of test environment.

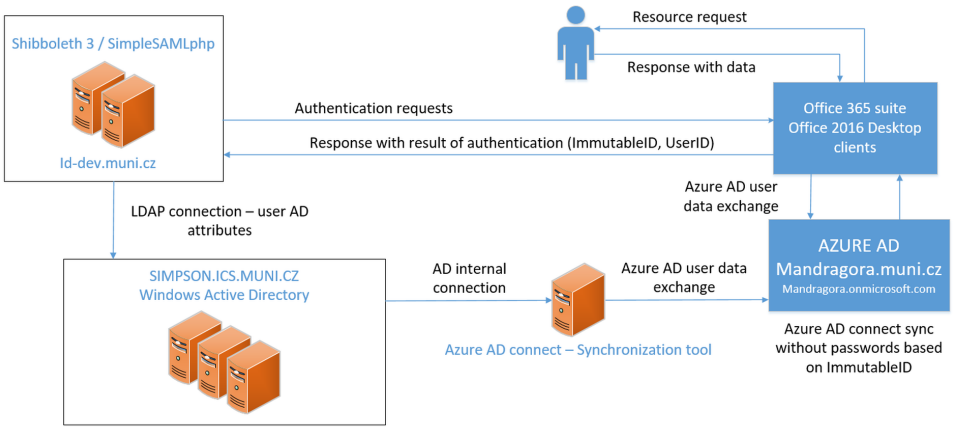

Figure 6.8: Test environment architecture

Environment consists of following parts:

- Microsoft Active Directory – simpson.ics.muni.cz
- Active Directory Connect server
- Office 365 tenant – mandragora.onmicrosoft.com

- SimpleSAMLphp and Shibboleth IDP – id-dev.muni.cz
- NLB with Powershell Web Proxy – nlb.simpson.ics.muni.cz

Implementation of described test environment is part of following chapter that is dedicated to the proof of concept implementation. SimpleSAMLphp which is selected identity provider will be implemented by team of ICS MU.

7 Implementation – proof of concept

Chapter implementation – proof of concept focuses on utilization of obtained outputs from analysis, design and available technologies. Implementation covers current environment, required changes regarding the created design and implementation of solution considering the best practice and usage of available technologies. It meets following points:

- Active Directory configuration
- Perun configuration – provided by team from ICS MU [1]
- Office 365 configuration
- Azure Active Directory connect configuration
- Powershell Web Proxy implementation

7.1 Active directory configuration

Masaryk University is using implementation of Microsoft Active Directory without all attributes required by Microsoft Office 365. This state is due to Masaryk University is not using on-premise installation of Microsoft Exchange as implementation of university mail server. In case of Active Directory which does not include required attributes, scheme of Active Directory needs to be extended. Section 7.1.1 describes purposes of required schema extensions.

7.1.1 Schema extensions

Installation of Microsoft Exchange server allows to extend schema of Microsoft Active Directory. This extension is required in case of installation of on-premise Microsoft Exchange server. In our case, it was decided not to install the whole Microsoft Exchange server, because this operation requires licensed product. Schema extension

1. Identity management team from Institute of Computer Science at Masaryk University

scripts which activate additional schema attributes required by Office 365 will be used in described scenario. Additional schema attributes allow to use Azure Active Directory synchronization for more attributes saved in cloud and then minimize requirements for manual changes via other Office 365 interfaces. Figure 7.1 describes commands used to schema extensions and its output.

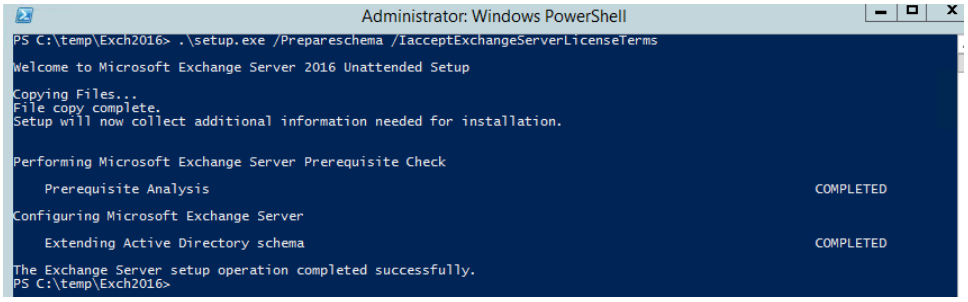

Figure 7.1: Schema extensions command and its output

An appendix A.2 depicts name of attributes which need to be filled in Active Directory and then synchronized by Azure Active Directory connect. List of attributes is based on specific requirements on cloud identity of Masaryk University.

Active Directory is working with three main object types. For all these objects another set of available attributes can be set. Active Directory defines these attributes as extension attributes.

- User – 20 attributes "msDS-cloudextensionattribute"
- Group – 15 attributes "extensionattribute"
- Contact – 15 attributes "extensionattribute"

A msDS-cloudextensionattribute1 is used for storing UserPrincipalName specified as e-mail address of user in form of <uco>@muni.cz. It is required attribute for hybrid authentication and Azure Active Directory connect. Based on this attribute cloud environment distinguishes user during authentication. Standard UserPrincipalName attribute can not be used because it is specified in different format

for on-premise Active Directory purposes. An attribute msDS-cloudextensionattribute2 is used for managing access to Office 365 services. Attribute specifies validity in form of LDAP based time stamp is used in Azure Active Directory Connect synchronization rules. If date in time stamp is less than current date, user is excluded from Azure Active Directory and Office 365 services.

7.2 Office 365 configuration

Design of integration described in previous chapters requires environment specific changes of Office 365 cloud configuration. This change includes new definition of authentication endpoints and trusts, object synchronization via Active Directory Connect, specification of authentication protocols and restrictions to object management via cloud graphical user interface. Following subsections describe required changes in detail.

7.2.1 Azure Active Directory

Configuration of Azure Active Directory for hybrid authentication and active Directory connect requires to provide changes in two steps. First step is to connect domain which will be used in cloud environment via Azure Active Directory Connect. This step will be discussed in following section where Active Directory Connect configuration is described. Second step consists of transformation of authentication for defined domain into federated. This step is made via commands in Powershell. Transformation requires specification of identity provider endpoints, certificates which ensure trust between service and identity provider and configuration of correct authentication protocol. Following code describes commands used in transformation.

```
1 $domain = "muni.cz"
2 $url = "https://id.muni.cz/idp/profile/SAML2/POST/SSO"
3 $ecpUrl = "https://id.muni.cz/idp/profile/SAML2/SOAP/ECP"
4 $uri = "https://id.muni.cz/idp/shibboleth"
5 $logouturl = "https://id.muni.cz/logout/"
6 $certificate = "MIIFYzCCBEugAw...2tLRtyN"
7 Set-MsolDomainAuthentication -DomainName $domain `
```

```
8             -Authentication Federated  `
9             -PassiveLogOnUri $url `
10            -SigningCertificate $certificate `
11            -IssuerUri $uri `
12            -ActiveLogOnUri $ecpUrl `
13            -LogOffUri $logouturl `
14            -PreferredAuthenticationProtocol SAMLP `
```

Office 365 at Masaryk University consists of three main applications with separated configuration requirements:

- Skype For bussines Online
- Exchange Online
- Sharepoint Online

Majority of settings is used from Azure Active Directory configuration but all applications require change in configuration of authentication to provide single sign-on capability. Following commands describe configuration of authentication per individual application.

Skype For bussines Online:

```
Set-CsOAuthConfiguration -ClientAdalAuthOverride 'Allowed'
```

Exchange Online:

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

Sharepoint Online:

Sharepoint online has enabled federated authentication features by default.

7.3 Azure Active Directory connect

Based on current environment and analysis, it was estimated that large amount of objects need to be synchronized to Office 365. Powershell

and Graph REST based API is not suitable, because it is not possible to synchronize this amount of objects within an acceptable time. Therefore Azure Active Directory Connect, application designed by Microsoft for hybrid deployment was chosen for basic object synchronization. This synchronization consists of users, groups and contacts synchronization. Azure Active Directory connect analyzes changes on on-premise Active Directory and Azure Active Directory. These changes are written in form of metaverse to local SQL database and then provisioned to cloud. This system allows us to synchronize changes within acceptable time. Figure 7.2 depicts principle of metaverse entries in Azure Active Directory Connect.

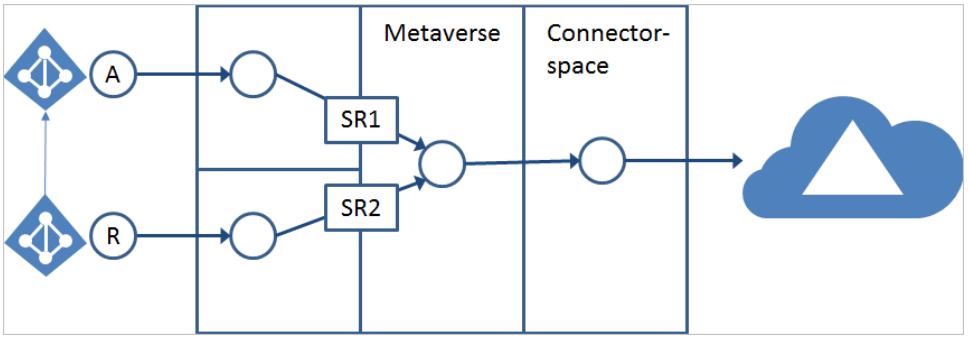

Figure 7.2: Principle of AAD Connect metaverse entries [29]

Synchronization of correct data is provided by rules which are specified by system administrator. These rules define evaluation process of objects. Rules are working with three basic operations create, remove, merge. To establish high availability of synchronization mechanism, Microsoft best practice [18] says that SQL server should be installed in cluster mode and AAD Connect should be installed in two separate instances where one instance is in active mode and second one is in passive also known as stagging mode[2].

7.3.1 Definition of connectors and rules

AAD Connect requires configuration of connectors and rules to be able to synchronize information across environments. Therefore, con-

2. Evaluation by rules is enabled but provisioning to cloud is disabled on passive node.

figuration of inbound and outbound connector is specified. Role of inbound connector is provided by on-premise Active Directory. In our test environment it is *simpson.ics.muni.cz* AD. Production environment will consist of connector to *ucn.muni.cz* AD. Role of outboud connector is provided by Azure Active Directory. Test environment consists of *mandragora*[3] tenant with AAD. Production will require connector to *ucnmuni*[4] tenant and its AAD.

Distribution of data between connectors is managed with rules. Implementation of AD Connect consists of standard rules defined by Microsoft [17] and one specific rule based on our environment specification. This rule is provisioning only enabled accounts based on time stamp specified in attribute msDS-cloudExtensionAttribute2. Appendix A.1 depicts configuration of rule via Powershell. Defined rules can be changed, added or removed as needed.

7.4 Powershell Web Proxy

Microsoft offers multiple ways of communication with its cloud environment. Applications are permitted to communicate with Microsoft cloud via REST APIs. Basic users can manage cloud via web GUI and system administrators can benefit from access via Powershell. Except Powershell, all available interfaces do not implement whole required functionality. Identity management requires to do more complex tasks, therefore Powershell Web proxy is implemented. This proxy is basic web service build with ODATA IIS[5] Extension. Web service enables to define own REST API calls and translate them to Powershell commands. It also enables role base access to resources. With Powershell Web Proxy we are able to define functionality implemented via Powershell Office 365 interface. It can be used for internal systems with management based on Powershell as well. Figure 7.3 describes implementation of Powershell Web Proxy.

3. Mandragora is test tenant of Masaryk University. Full address of tenant is mandragora.onmicrosoft.com
4. Ucnmuni is production tenant of Masaryk University. Full address of tenant is ucnmuni.onmicrosoft.com
5. Microsoft Internet Information Services is an implementation of web server in Microsoft environment

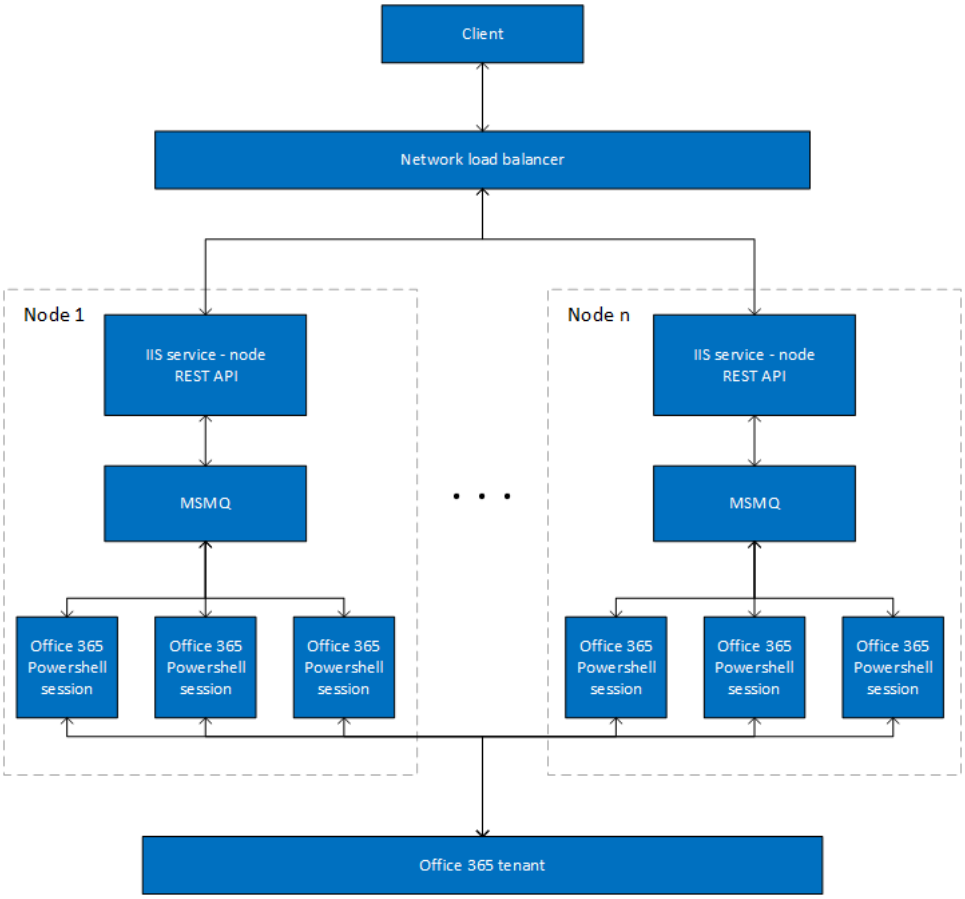

Figure 7.3: Architecture of Powershell Web Proxy

7.4.1 Network load balancing mode

Powershell Web proxy is running in Microsoft Internet Information server (IIS). IIS is implementation of web server by Microsoft. Microsoft IIS permits run of web applications in network load balancing mode also known as NLB cluster. This implementation is based on multiple nodes which communicate together and for user are visible as one endpoint. An implementation ensures scalability and in configuration of two nodes can be used as failover solution as well. Implemented Powershell Web Proxy is designed to be able to run in this mode.

7.4.2 Performance issues

Management of objects and settings in cloud over Powershell requires non trivial amount of computing time. In case of large amount of objects and settings which need to be managed, resulting process can take too long. This performance issue needs to be resolved in proxy implementation. Another issue is that Microsoft cloud environment applies policy implementing resource throttling. It ensures assignment of specific amount of resources per user and open Powershell sessions that can be used.

Performance tunning is based on elimination of described issues. Solution lies in implementation of a system that is running multiple Powershell session instances to Microsoft cloud under different administrator accounts. Open Powershell sessions are monitored, reused and in case of failure logged and reinitialized. This solution allows to speed up object synchronization with running multiple object synchronizations and solve problems with resource throttling. Our tests depict that described implementation is seventy five percent faster than standard way of powershell usage in current environment. In mentioned tests we have measured time required for synchronization of license information via standard Powershell remote session created during the request to Office 365 cloud and then via implemented Powershell Web Proxy that has preinitialized remote sessions.

Implementation of proof of concept is based on test environment and available technologies. Part of implementation is oriented to deployment of AD Connect. These technologies are deployed regarding to Microsoft best practice and environment of Masaryk University. Specification of cloud interfaces and on-premise environment requires to implement Powershell Web Proxy used in operations that are not available via AD Connect. Source code and deployment scripts of implemented Powershell Web Proxy are part of electronic appendix as well as AD Connect configuration.

8 Migration plan

Considering created analysis, design of integration, an implementation of proof of concept in test environment and fact that Office 365 is in production, migration plan is established. Migration plan minimized an impact on existing users. It includes definition of process of transformation from old name convention of e-mail accounts in Office 365 environment to new convention and realization of unified university authentication via SAML 2.0 protocol. Figure 8.1 describes process of migration which meets following points:

- Change of UserPrincipalName attribute in existing accounts
- Client configuration and preparation for unified authentication
- Synchronization of required attributes between on-premise and cloud environment
- Realization of change in authentication
- Monitoring and resolving potential problems

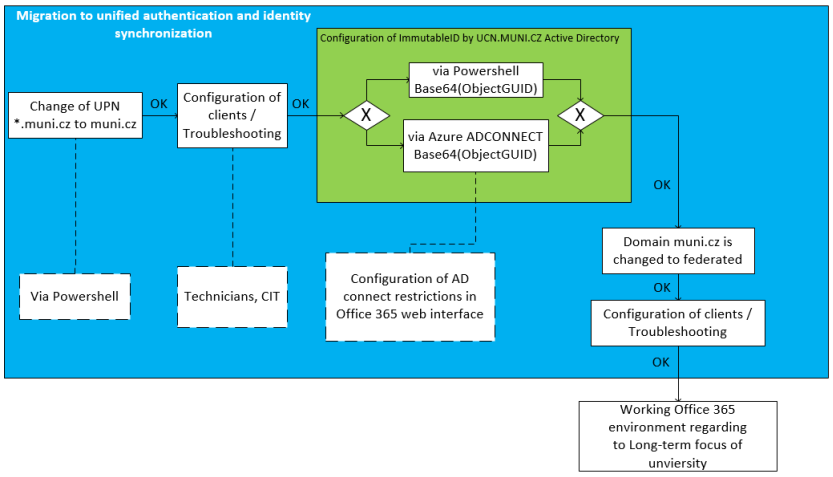

Figure 8.1: Process of migration plan

As part of migration plan, document describing test of migration plan was developed. Appendix B depicts this document and operations that need to be tested before final realization of migration plan. Migration plan was tested in cooperation of Support and Services Department of ICS MU.

9 Conclusion

The goal of this diploma thesis was to create a solution of integration of Masaryk University identities to Microsoft Office 365 cloud environment. When writing about integration we talk about the analysis of available systems and concepts at Masaryk University and also about how to define current environment and existing problems as well as how to create design and implement the solution with preparation of migration plan to production environment.

The topic of the thesis required to get familiar with current environment and available technologies. Result of familiarization and problem understanding can be seen in motivation, problem definition and analysis. These parts describes main problems such as production Office 365 tenant, complicated academic identity, multiple sources of information and need for unified identity and authentication.

Retrieved facts based on analysis and the best practice of Microsoft helped me create design of the solution based on the integration of existing systems, such as Perun and implementation of a Powershell Web Proxy. The Powershell Web Proxy simplifies management of required Powershell operations for Office 365 administrators and optimizes performance. Integration of Perun requires cooperation of ICS identity management team and implementation of the changes in a system itself to be able to fully cooperate with connected systems, such as Active Directory and Powershell Web Proxy.

Consolidation of identity sources to one place helped to create synchronization rules for AD Connect. This technology was chosen regarding the Microsoft best practice and amount of synchronized information. AD connect was a requirement for implementation of unified authentication of MU to Office 365. Unified authentication is also known as single sin-on which helps to integrate independent systems to one unit. Benefits for common user are in use of single login information for different systems.

Integration of Perun, Active Directory and AD Connect regarding to proposed design helps manage problems with speed of identity synchronization, licensing and straggled identities across MU. Performance limitations of cloud interfaces are minimized by implemented Powershell Web Proxy.

Integration of MU unified authentication to Office 365 is based on SAML protocol and trust with MU identity provider (IdP). Available Office 365 protocols such as IMAP or MAPI must be correctly configured to be able to cooperate with SimpleSAMLphp and Shibboleth technologies. These technologies are only supported by MU IdP.

Created solution of unified authentication and identity integration required deployment of test environment realized with test AD, AD Connect, Office 365 tenant and Powershell Web Proxy running on NLB cluster. This environment helped define changes, create proof of concept and migration plan for production environment. Implementation and deployment of Powershell Web Proxy, test Office 365 tenant and test Active Directory was my responsibility. Identity provider in test environment was deployed by ICS MU identity management team.

Migration plan was realized in the test environment with cooperation of ICS support team which will be responsible for migration to production environment in the future.

My diploma thesis required collaboration in team of professionals from several departments of ICS MU. We were meeting on weekly basis and discussing configuration options and problems regarding the topic of this thesis. One of my roles in this team was coordination of team members and I was also solution analyst responsible for proposed solution.

To sum up, first added value is created solution following MU concepts and simplify identity management and MU authentication in Office 365. Second added value is created background for GUI applications that will help common users and administrators of MU cloud environment.

Finally, it is important to mention that deployment of solution to production is dependent on several systems and MU concepts that were discussed in the time of thesis elaboration. Some of proposed configuration can be changed in order to reach the idea of concepts. Microsoft Office 365 is permanently developing cloud service. Created changes may affect final design and implementation as well. Proposed design is generalized as much as possible to be able to cover service changes in the future.

Bibliography

[1] CHAPPELL, David. *The fundamentals of Azure identity management* [online]. 2017. Available at: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals-identity.

[2] METCALF, Sean. *Active Directory Security Risk* [online]. 2015. https://adsecurity.org/?p=1667.

[3] PROCHÁZKA, Michal and Slávek LICEHAMMER. *Koncepce IAM na MU* [online]. 2016. Available at: https://projects.ics.muni.cz/attachments/download/1418/KoncepceIAMnaMU-2.pdf.

[4] SOLUTIONS REVIEW. *Identity and Access Management Solutions Directory* [online]. 2017. Available at: https://solutionsreview.com/identity-management/identity-management-solutions-directory/.

[5] DEVINE, Richard. *What is Microsoft Office 365* [online]. 2015. Available at: http://www.windowscentral.com/what-microsoft-office-365.

[6] LOVE, Curtis, *What is Azure Active Directory* [online]. 2017. Available at: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-whatis.

[7] MICROSOFT. *Active Directory* [online]. Available at: https://msdn.microsoft.com/en-us/library/bb742424.aspx.

[8] SIMPLESAMLPHP COMMUNITY. *SimpleSAMLphp* [online]. Available at: https://simplesamlphp.org/.

[9] SHIBBOLETH CONSORTIUM, *What's Shibboleth* [online]. Available at: https://shibboleth.net/about/.

[10] MATHERS, Bill. *What's new in Active Directory Federation Services for Windows Server 2016* [online]. 2017. Available at: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/overview/whats-new-active-directory-federation-services-windows-server-2016.

[11] MATHERS, Bill. *Integrate your on-premises directories with Azure Active Directory* [online]. 2017. Available at: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect.

[12] JOFRE, JuanPablo. *Powershell* [online]. 2016. Available at: https://msdn.microsoft.com/en-us/powershell/scripting/powershell-scripting.

[13] MCLLECE James. *Network Load Balancing* [online]. 2017. Available at: https://docs.microsoft.com/en-us/windows-server/networking/technologies/network-load-balancing.

[14] SEBESTIÁNOVÁ, Zora, Michal PROCHÁZKA, Slávek LICEHAMMER, Michal ŠŤAVA and Pavel ZLÁMAL. *Perun - user and resources management system*. 2013.

[15] OASIS SECURITY SERVICES TC. *Security Assertion Markup Language (SAML) V2.0 Technical Overview* [online]. 2008. Available at: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.

[16] HANDL Ralf, Martin ZURMUEHL and Mike PIZZO. *OData Version 4.0 Part 1: Protocol* [online]. 2013. Available at: http://docs.oasis-open.org/odata/odata/v4.0/cs01/part1-protocol/odata-v4.0-cs01-part1-protocol.html.

[17] KJELLMAN, Andreas. *Azure AD Connect sync: Understanding the default configuration* [online]. 2017. Available at: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-understanding-default-configuration.

[18] MICROSOFT. *Custom installation of Azure AD Connect* [online]. 2017. Available at: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-get-started-custom.

[19] MICROSOFT. *Enrollment for Education Solutions* [online]. 2017. Available at: https://download.microsoft.com/ download/F/6/6/F6611596-992F-498A-A8EE-B0B39A6A4D0A/Enrollment_for_Education_Solutions_Licensing_Guide.pdf.

[20] LICEHAMMER, Slávek. *Centralizovaná správa identit a přístupů na služby na MU* [online]. 2017. Available at: https://www.eduid.cz/_media/cs/centralizovana_sprava_identit_a_pristupu_na_sluzby_na_mu.pdf.

[21] NOVELL. *Lightweight Directory Access Protocol (LDAP): The Protocol* [online]. 2006. Available at: https://tools.ietf.org/html/rfc4511.

[22] KERVER, Bart and Jeroen de BEER. *A-Select Authentication System* [online]. 2002. Available at: http://www.aselect.org/home.html.

[23] PETRO, Andrew. *Central Authentication Service* [online]. 2015. Available at: https://wiki.jasig.org/display/CAS/Home.

[24] FITZPATRICK, Brad. *OpenID* [online]. 2006. Available at: http://openid.net/what-is-openid/.

[25] GOODNER, Marc, Maryann HONDO and Anthony NADALIN. *Understanding WS Federation* [online]. 2007. Available at: https://msdn.microsoft.com/en-us/library/bb498017.aspx.

[26] RICHER, Justin and Antonio SANSO. *OAuth 2 in Action*. 2017. ISBN 9781617293276.

[27] MICROSOFT. *WS-Management Protocol* [online]. 2017. Available at: https://msdn.microsoft.com/en-us/library/aa384470.aspx.

[28] MYERS. *Simple Authentication and Security Layer (SASL)* [online]. 1997. Available at: https://tools.ietf.org/html/rfc2222.

[29] MICROSOFT. *Understanding the default configuration* [online]. 2015. Available at: https://msdn.microsoft.com/en-us/library/azure/dn800963.aspx.

[30] ANDREW, Paul. *Choosing a sign-in model for Office 365* [online]. 2014. Available at: https://msdn.microsoft.com/en-us/library/azure/dn800963.aspx.

[31] PAYETTE, Bruce and Richard SIDDAWAY. *Windows PowerShell in Action, Third Edition*. 2015. ISBN 9781633430297.

[32] TULLOCH, Mitch. *Introducing Windows Azure for IT Professionals*. 2013. ISBN 9780735682894.

[33] THOMAS, Orin. *Exam Ref 70-346 Managing Office 365 Identities and Requirements 1st Edition*. 2013. ISBN 9781509300662.

[34] DESMOND, Brian and Joe RUCHARDS. *Active Directory, 5th Edition*. 2013. ISBN 9781449320027.

[35] MICROSOFT. *Office 365 Education plan* [online]. 2014. Available at: https://msdn.microsoft.com/en-us/library/azure/dn800963.aspx.

A An appendix

A.1 Azure Active Directory Connect rule

```
New-ADSyncRule  `
-Name 'OSS - in~from AD - Office365 User expiration 30 days' `
-Identifier 'bc102c97-4390-4d8b-aaa4-0014cc20cb24' `
-Description '' `
-Direction 'Inbound' `
-Precedence 99 `
-PrecedenceAfter '00000000-0000-0000-0000-000000000000' `
-PrecedenceBefore '00000000-0000-0000-0000-000000000000' `
-SourceObjectType 'user' `
-TargetObjectType 'person' `
-Connector '5963ac37-0af5-4b46-8c67-1a88152f331b' `
-LinkType 'Join' `
-SoftDeleteExpiryInterval 0 `
-ImmutableTag '' `
-OutVariable syncRule

Add-ADSyncAttributeFlowMapping  `
-SynchronizationRule $syncRule[0] `
-Source @('msDS-cloudExtensionAttribute2') `
-Destination 'accountEnabled' `
-FlowType 'Expression' `
-ValueMergeType 'Update' `
-Expression  `
 'IIF(CNum([msDS-cloudExtensionAttribute2])>NumFromDate(Now()),True,False)' `
-OutVariable syncRule

New-Object  `
-TypeName `
 'Microsoft.IdentityManagement.PowerShell.ObjectModel.ScopeCondition' `
-ArgumentList 'adminDescription','User_','NOTSTARTSWITH' `
-OutVariable condition0


```

```
34 Add-ADSyncScopeConditionGroup  `
35 -SynchronizationRule $syncRule[0] `
36 -ScopeConditions @($condition0[0]) `
37 -OutVariable syncRule
38
39 Add-ADSyncRule -SynchronizationRule $syncRule[0]
```

A.2 Attribute specification

O365 object name	O365 attribute name	Used technology	AD object and attribute name
Contact	ExternalEmailAddress	AD Connect	Contact, mail / targetAddress
Contact	Name	AD Connect	Contact, name
Contact	DisplayName	AD Connect	Contact, displayName
Contact	FirstName	AD Connect	Contact, givenName
Contact	LastName	AD Connect	Contact, surname
Contact	Organization	AD Connect	Contact, company
Contact	Initials	AD Connect	Contact, initials
Mailbox	EmailAddresses	AD Connect	User, proxyAddresses
Mailbox	DeliverToMailboxAndForward	Powershell	
Mailbox	ForwardingSmtpAddress	Powershell	
Mailbox	Languages	Powershell	
Mailbox	TimeZone	Powershell	
Mailbox	DateFormat	Powershell	
Mailbox	TimeFormat	Powershell	
Mailbox	Alias	AD Connect	User, Alias
Mailbox	AutoReplyState	Powershell	
Mailbox	ExternalAudience	Powershell	
Mailbox	InternalMessage	Powershell	
Mailbox	ExternalMessage	Powershell	
O365 Group	AccessType	Powershell	
O365 Group	AutoSubscribeNewMembers	Powershell	
O365 Group	HiddenGroupMembershipEnabled	Powershell	
O365 Group	Language	Powershell	
O365 Group	ManagedBy	Powershell	
O365 Group	Members	Powershell	
O365 Group	Notes	Powershell	
O365 Group	EmailAddresses	Powershell	
O365 Group	PrimarySmtpAddress	Powershell	
O365 Group	DisplayName	Powershell	
O365 Group	RequireSenderAuthenticationEnabled	Powershell	
O365 Group	Alias	Powershell	
O365 Group	GrantSendOnBehalfTo	Powershell	
O365 Group	HiddenFromAddressListsEnabled	Powershell	
O365 Group	RecipientType	Powershell	
O365 Group	RecipientTypeDetails	Powershell	
O365 Group	Identity	Powershell	
O365 Group	AccessRights	Powershell	
Security Group	Name	AD Connect	Group, CommonName
Security Group	Alias	AD Connect	Group, Alias
Security Group	DisplayName	AD Connect	Group, DisplayName
Security Group	Members	AD Connect	Group, Member
Security Group	Send as	Powershell	
Security Group	Send on behalf	AD Connect	Group, publicDelegates
Security Group	RequireSenderAuthenticationEnabled	AD Connect	Group, msExchRequireAuthToSendTo

Table A.1: List of attributes, part 1

O365 object name	O365 attribute name	Used technology	AD object and attribute name
Security Group	EmailAddresses	AD Connect	Group, ProxyAddresses
SharedMailbox	Shared	Powershell	
SharedMailbox	MessageCopyForSentAsEnabled	Powershell	
SharedMailbox	MessageCopyForSendOnBehalfEnabled	Powershell	
SharedMailbox	AlwaysShowFrom	Powershell	
SharedMailbox	AccessRights	Powershell	
SharedMailbox	AutoMapping	Powershell	
SharedMailbox	AccessRights	Powershell	
SharedMailbox	Languages	Powershell	
SharedMailbox	TimeZone	Powershell	
SharedMailbox	DateFormat	Powershell	
SharedMailbox	TimeFormat	Powershell	
SharedMailbox	Alias	Powershell	
SharedMailbox	DeliverToMailboxAndForward	Powershell	
SharedMailbox	ForwardingSmtpAddress	Powershell	
SharedMailbox	EmailAddresses	Powershell	
SharedMailbox	AutoReplyState	Powershell	
SharedMailbox	ExternalAudience	Powershell	
SharedMailbox	InternalMessage	Powershell	
SharedMailbox	ExternalMessage	Powershell	
SharedMailbox	City	Powershell	
SharedMailbox	Company	Powershell	
SharedMailbox	CountryOrRegion	Powershell	
SharedMailbox	Department	Powershell	
SharedMailbox	DisplayName	Powershell	
SharedMailbox	Fax	Powershell	
SharedMailbox	FirstName	Powershell	
SharedMailbox	LastName	Powershell	
SharedMailbox	Notes	Powershell	
SharedMailbox	Office	Powershell	
SharedMailbox	Phone	Powershell	
SharedMailbox	PostalCode	Powershell	
SharedMailbox	StateOrProvince	Powershell	
SharedMailbox	StreetAddress	Powershell	
SharedMailbox	Title	Powershell	
SharedMailbox	MobilePhone	Powershell	
User	BlockCredential	AD Connect	User, accountEnabled
User	City	AD Connect	User, City
User	Country	AD Connect	User, countryCode
User	Department	AD Connect	User, department
User	DisplayName	AD Connect	User, displayName
User	Fax	AD Connect	User, facsimiletelephonenumber
User	FirstName	AD Connect	User, givenName
User	ImmutableId	Powershell	
User	LastName	AD Connect	User, sn
User	Licenses	Powershell	

Table A.2: List of attributes, part 2

O365 object name	O365 attribute name	Used technology	AD object and attribute name
User	MobilePhone	AD Connect	User, mobile
User	Office	AD Connect	User, office
User	PasswordNeverExpires	AD Connect	User, PasswordNeverExpires
User	Password	Powershell	
User	Company	AD Connect	User, company
User	Manager	AD Connect	User, manager
User	PhoneNumber	AD Connect	User, telephoneNumber
User	PostalCode	AD Connect	User, postalCode
User	PreferredLanguage	AD Connect	User, preferredLanguage
User	State	AD Connect	User, state
User	StreetAddress	AD Connect	User, streetAddress
User	StrongPasswordRequired	Powershell	
User	Title	AD Connect	User, title
User	Notes	Powershell	
User	UsageLocation	AD Connect	User, usageLocation
User	UserPrincipalName	AD Connect	User, UserPrincipalName
Mailbox	PrimarySmtpAddress	AD Connect	User, mail

Table A.3: List of attributes, part 3

B Electronic appendices

- Powershell Web Proxy source code and scripts
- Example of the migration testing documentation