Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Diploma Thesis

Graphical representation of identity management data

Vojtěch Zelený

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Bc. Vojtěch Zelený

Informatics

Thesis title

Graphical representation of identity management data

Objectives of thesis

The main objective of the thesis is to visualise data from identity management system in a selected company.

Partial goals of thesis are such as:
- characteristics of current options for object visualization and localization within an organization,
- development of a basic application capable of working with organization's building floor plans and information from identity management system, and
- evaluation and comparison of designed solution.

Methodology

Methodology of the thesis is based on study and analysis of information resources. The findings will be used for designing and implementing web application. The design process and implementation will be described and evaluated. Based on the theoretical findings and results of the practical part, final conclusion and recommendation will be formulated.

The proposed extent of the thesis

60 -80 pages

Keywords

Active Directory, Identity management, graphical presentation, Facility management, web development, windows server, information system, thin client.

Recommended information sources

Active directory fast start: a quick start guide for active directory [online]. Seattle, Washington: [RP Media], 2014 [cit. 2016-06-12]. ISBN 978-1-62716-216-6. Dostupné z: http://sfx.techlib.cz

BERTINO, Elisa a Kenji TAKAHASHI. Identity management: concepts, technologies, and systems [online]. London, UK: ARTECH, c2011 [cit. 2016-06-13]. ISBN 9781608070404. Dostupné z: http://site.ebrary.com/lib/techlib

FORD, Jerry Lee. Microsoft Windows powershell programming for the absolute beginner [online]. Third edition. Boston, Massachusetts: Cengage Learning PTR, 2015 [cit. 2016-06-13]. ISBN 978-1-305-26035-1. Dostupné z: http://sfx.techlib.cz

GUSTAFSON, J. M. HTML5 web application development by example: beginner's guide [online]. Birmingham: Packt Pub., 2013 [cit. 2016-06-12]. ISBN 9781849695947. Dostupné z: http://sfx.techlib.cz

RATNAYAKE, Rakhitha Nimesh. WordPress web application development [online]. Birmingham: Packt Publishing, 2013 [cit. 2016-06-13]. ISBN 978-1-78328-076-6. Dostupné z: http://sfx.techlib.cz

STANEK, William R. Microsoft Windows Server 2012: kapesní rádce administrátora. Brno: Computer Press, 2015. ISBN 978-80-251-3817-5.

Expected date of thesis defence

2016/17 SS – FEM

The Diploma Thesis Supervisor

Ing. Miloš Ulman, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 21. 10. 2016	Electronic approval: 24. 10. 2016
Ing. Jiří Vaněk, Ph.D.	**Ing. Martin Pelikán, Ph.D.**
Head of department	Dean

Prague on 30. 03. 2017

Declaration

I declare that I have worked on my diploma thesis titled "Graphical representation of identity management data" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the diploma thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on 31.3.2017 ____________________________

Acknowledgement

I would lid to thank Ing. Miloš Ulman, Ph.D. for his professional and very helpful supervising and for his attitude. Then I would like to thank Petr Čech for his supervising and his ideas during the work on thesis. And I have to thank to all ICZ employees, who aided me and took a bit of their time to help me with the project.

Grafická reprezentace dat z Identity management systému

Souhrn

Tato diplomová práce s názvem "Grafická reprezentace dat z Identity management systému" se zabývá procesem vývoje a implementace webové aplikace pro lokalizování zaměstnaců a tiskáren. Práce je rozdělena do dvou hlavních sekcí, teoretickou a praktickou. Teoretická část představuje zásadní termíny a metody související s identity managementem. Zaměřuje se zejména na identity management.metody a technologie, které jsou implementovány v praktické části, a na popsání řešení třetích stran na trhu. Praktická část aplikuje získané a analyzované informace z teoretické části. Jejím cílem je vývoj web systému pro společnost ICZ dle daných požadavků. Vývoj začal výběrem a oslovením klíčových osob projektu. Byla vytvořena nalýza procesů, system nadesignován a popsán jeho dopad na podnikové procesy. Závěr popisuje jakým způsobem byly dosaženy cíle projektu a k jakým problémům během vývoje došlo. Budoucí vývoj a jeho cena jsou navrženy.

Klíčová slova: Active Directory, Identity management, grafická prezentace, Správa objektu, vývoj webu, windows server, informační systém, tenký klient.

Graphical representation of identity management data

Summary

The thesis “Graphical representation of identity management data” deals with the implementation process and design of a web based application for employee seating and printer locating. The thesis is divided into two main sections, theoretical and practical. The theoretical part introduces essential terms and methods related to identity management. It focuses mainly on identity management methods and technology, which is implemented in practical part and on describing of third party solutions on market. The practical part applies the gathered and analysed information from the theoretical part. Its goal is developing of a web based system in ICZ company for given requirements. The development began by selecting and engaging key project stakeholders. Then process analysis was created, system designed, and its influence on business processes described. The conclusion describes how the project goals were achieved and what issues were encountered during the development. Then future development and its cost is proposed.

Keywords: Active Directory, Identity management, graphical presentation, Facility management, web development, windows server, information system, thin client.

Table of content

List of figures

List of tables

1 Introduction

Nowadays, a global information infrastructure - the Web - connects remote parties worldwide through the use of large scale networks, relying on application-level protocols and services, such as recent Web service technology. Enterprises are increasingly taking advantage of computing resources available on the web through the use of cloud computing and virtualization technologies.

Company ICZ a.s. was founded in 1997 by merging top leading IT companies in Czech and Slovak Republic. Today within central Europe, ICZ a.s and associated companies in ICZ group belong amongst the most important providers of programming accessories, design and implementation of infrastructure and solutions of security of information systems.

This thesis is aimed on issues related to development of an information system aiding ICZ employees with orientation in company's offices in terms of finding location of employees or printers.

Having system presenting default position for such objects, could significantly improve efficiency of the company's end user support and other departments like human resources or facility management department.

2 Objectives and Methodology

2.1 Objectives

The main objective of the thesis is to visualise data from the identity management system in a selected company.

Partial goals of thesis are to characterize current options for object visualization and localization within an organization, to develop a basic application capable of working with organization's building floor plans and information from the identity management system, and to evaluate and compare proposed solution. The company ICZ was selected to demonstrate the proposed solution.

2.2 Methodology

Methodology of the thesis is based on study and analysis of information resources. The practical part aims to create information system for defined users. The system will use object information from SAP or Active Directory and project it into a building floor map. The design and implementation process will be described. Based on the theoretical findings and results of the practical part, final conclusion and recommendations will be formulated.

3 Literature Review

3.1 Identity management

Before going in the details, Identity Management will be explained generally.

There are several different definitions of identity in the context of digital identity management. (Pfitzmann, 2009, Bishop, 2002) For example, some authors (Pfitzmann, 2009) define identity as: "An identity of an individual person may comprise many partial identities of which each represents the person in a specific context or role. A partial identity is a subset of attribute values of a complete identity, where a complete identity is the union of all attribute values of all identities of this person." That definition only covers persons as subjects of identities. However others (Bishop, 2002) define an identity that covers a wider range of subjects—not just people. Subjects of identities can be software agents (e.g., Web services and user client software) and hardware devices (e.g., PCs, mobile phones, and network equipment). Furthermore, as computing environments are becoming ubiquitous, identities are assigned to artificial objects (e.g., daily goods, machine parts, and buildings) and natural objects (e.g., livestock and crops) monitored and managed by sensors. (Bertino, Elisa Takahashi, Kenji, 2011, p. 21)

3.1.1 Standardization ITU-T Y.2720

ITU-T Y.2720 Recommendation (NGN Identity Management Framework) defines identity as “information about an entity that is sufficient to identify that entity in a particular context." According to Y.2720, an identity consists of three different types of data: identifier, credentials, and attributes.

• Identifiers: A series of digits, characters, and symbols or any other form of data used to identify a subject. Identifiers can be scoped by time and/ or space. For example, a URI is globally unique over time. Pseudonyms can be temporal and effective only for a specific service. Some examples are user account names, passport numbers, mobile phone numbers, employee numbers, pseudonyms, and URI.

• Credentials: A set of data providing evidence for claims about parts of or entire identities. A credential can be generated based on one or more credentials. Some examples are passwords, digital certificates, fingerprints, Kerberos tickets (Neuman, 1994), and SAML assertions.

• Attributes: A set of data that describes the characteristics of a subject. The data includes the fundamental information for identifying a subject (e.g., full name, domicile, and date of birth), his/her preferences, and the information generated as a result of his/her activities. Some examples are given/family names, domiciles, ages, genders, roles, titles, affiliations, activity records, and reputations. (Bertino, Elisa Takahashi, Kenji, 2011, p. 21-22)

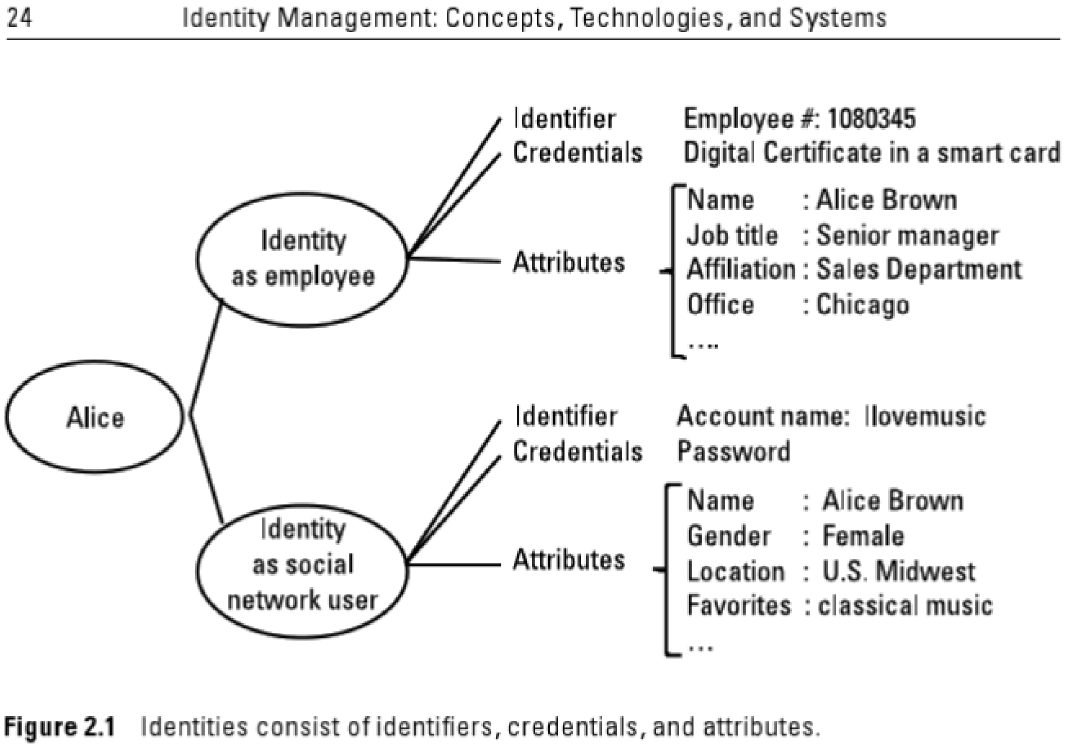
3.1.2 **Categorizations**

Identities can be categorized from different perspectives such as sociology, psychology, philosophy and as well as computer science. From a structural perspective, an identity is seen as a representation or a set of attributes characterizing the person (Nabeth, 2009). From aprocess perspective, an identity is conceptualized for the purpose of identification as "a set of processes relating to disclosure of information about the person and usage of this information" (Nabeth, 2009).

Another categorization is possible based on who owns and controls identities. The control over personal information is essential in protecting one's privacy. Semis proposed the concept of 'Medentity, Ourdentim and Theirdentity" (Searls).

- a Medentity is tied to a subject in a one-to-one manner. It is also called true identity (Nabeth, 2009). True identities came into existence when the subjects as natural persons were born.
- •Ourdentity is an identity that exists by mutual agreements between a subject and a third party, For example, a user account at an online bookstore is an ourdentity. The subject can create, modify, and delete the user account but the bookstore may also have SOIne control over the identity based on terms and conditions that the subject and the bookstore agreed upon. The bookstore may, for example, record the usage of a subject and recommend him or her books based on the usage record. Ourdentity is similar to the notion of assigned identity, that is, an identity assigned by a third party (Nabeth, 2009), However, ourdentities are not necessarily assigned by others but created by their subjects. Theirdentity is an identity that a third parry guesses and internally creates without explicit consent from the subject. For example, a Web search service creates a theirdentity as an internal user model for customized advertisements to the subject and/or sells the usage logs associated with the theirdentity to market analysis specialists. Theirdentities can be generated based on cookies and/or source IP addresses.

The subjects are not aware of the existence, details, or accuracy of their theirdentities and do not have any control over them. Theirdentity is also called abstracted identity (Nabeth, 2009). (Bertino, Elisa Takahashi, Kenji, 2011, p. 22-23)



24 Identity Management: Concepts, Technologies, and Systems

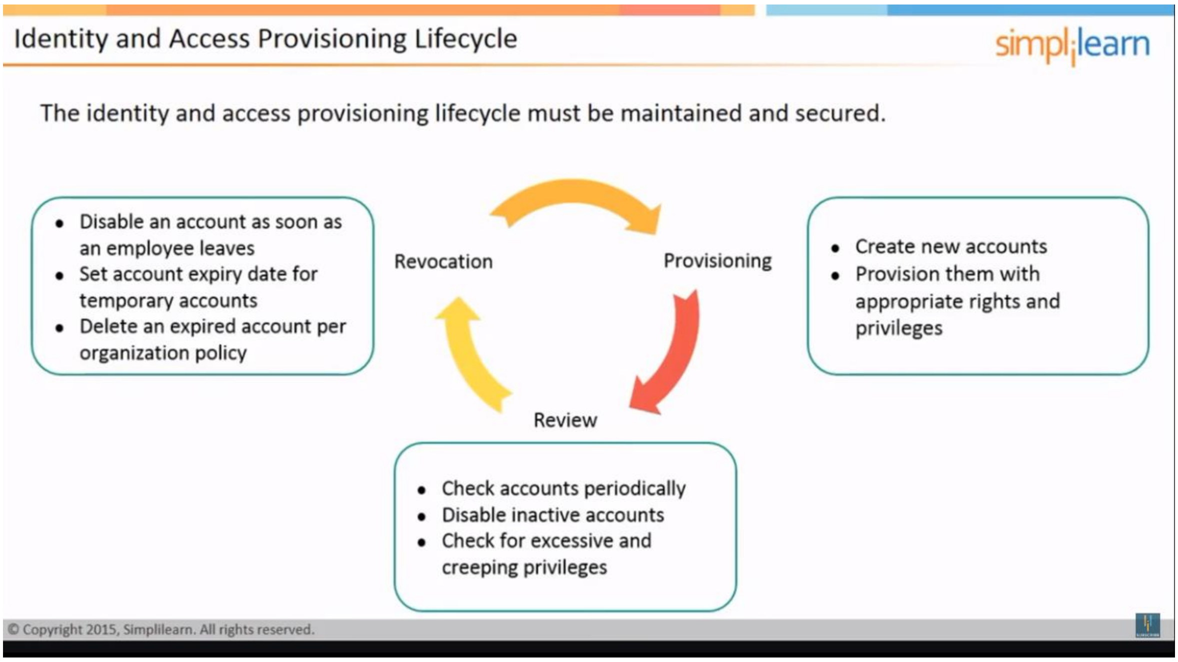
Figure 2.1 Identities consist of identifiers, credentials, and attributes.

Figure 1- Identities consist of identifiers, credentials, and attributes

Source: (Bertino, Elisa Takahashi, Kenji, 2011, p. 24)

3.1.3 Identity life cycle

The following picture provided by SimpliLearn describes life cycle of an identity.



Identity and Access Provisioning Lifecycle

The identity and access provisioning lifecycle must be maintained and secured.

- Disable an account as soon as an employee leaves
- Set account expiry date for temporary accounts
- Delete an expired account per organization policy

- Create new accounts
- Provision them with appropriate rights and privileges

- Check accounts periodically
- Disable inactive accounts
- Check for excessive and creeping privileges

Figure 2 - Life cycle of identity Source: (SimpliLearn youtube channel, 2015)

3.1.4 Identity and Credential

According to (Bertino, Elisa Takahashi, Kenji, 2011, p. 46-48) Identity and credentials are described as follows. “A credential is typically a collection of identity attributes and assertions about a specific subject issued by an identity provider, referred to as credential issuer. The issuer is crucial for a relying party in deciding whether or not to accept a credential provided by a subject, as the issuer attests for the integrity and possibly the validity of the credential content. Note that in this context integrity refers to assuring that the credential has not been tampered with; as such techniques like digital signatures and PKI infrastructures can be used for integrity assurance. Validity is a more difficult requirement in that it requires what is asserted in the credential to be truthful; that is, that it has undergone an assurance process. As different assurance processes may be adopted by different identity providers, depending also on the content and purpose of credentials, a credential may contain information, referred to as the assurance level, conveying indications about the specific assurance process adopted when issuing the credential. Subjects may also self-issue credentials that may be useful in many cases. For example, a user may use such a credential to indicate his hobbies in a Web site. Therefore, according to (Brands, 2002), we can classify credentials into the following types:

- Validated credential: digitally signed after the credential has been validated;
- Authenticated credential: digitally signed but has not been validated;
- Raw credential: digitally signed by the subject itself and is not validated. Another interesting classification of credentials is by NIST (MacGregor, 2006). This classification has been devised for physical credentials, such as passports and driving licenses. However, it is interesting in our context because it clearly identifies purposes and requirements for different classes of credentials. As technology and its application evolve, creating the electronic counterparts of these credentials will require determining how these purposes and requirements can be addressed in the cyberworld.

3.1.4.1 Primary Identity Credentials

Primary identity credentials are the (MacGregor, 2006): by-products of significant life events, including birth, marriage, graduation, military entry-on-duty and discharge, and death. Such events are recognized as social occasions requiring ceremony, and are typically witnessed by family, friends, and acquaintances of the subject. In most cases, an original primary identity credential is issued once per event. A primary identity credential describes the nature, place, and date of the event, and documents event-specific details such as birth weight. This description highlights several interesting aspects, one of which is that the event is witnessed by other subjects, whereas the other is the notion of the original primary identity credential. Also, the description indicates that often a credential may record context information, such as the place where the event took place that resulted in the creation of the identity attributes. These aspects point out, for example, that the digital counterpart of such a credential should have strong bounds to the electronic credentials of the witnesses and also that we need mechanisms to implement the notion of original primary identity credential.

3.1.4.2 Secondary Identity Credentials

Secondary identity credentials are (MacGregor, 2006): …issued in response to a request for authorization to perform an action (e.g., driver license to operate a vehicle), or demonstrate proof of affiliation (e.g., passport to prove claimed nationality). During a secondary identity credential application process, identity verification relies, to a great degree, on primary and other secondary identity credentials. Personal knowledge of the registrar or trusted third parties may also be relied upon during the application process. . . Because the application lacks the social context of a primary identity credential, the registrar should take great care to verify the authenticity and accuracy of source documents. Secondary identity credentials are often relied upon by law enforcement. Because the consequences of misidentification can be extreme, secondary identity credentials generally include an ID photo and possibly additional biometrics such as fingerprint or signature. Secondary identity credentials are usually government issued, multipurpose, and widely adopted. This definition points out that secondary credentials are often issued for a special purpose and that their validity depends on the validity of source documents and credentials. As such it is important that provenance information be maintained to record the derivation process.

3.1.4.3 Tertiary Identity Credentials

Tertiary identity credentials are (MacGregor, 2006): …issued by an authority or organization for a limited purpose, and include employee badges, membership cards, and loyalty program cards. The identity verification and proofing requirements vary enormously, from almost no requirements (loyalty program cards) to requirements comparable to secondary identity credentials (many employee badges). Tertiary identity cards are rarely multipurpose, and often include no biometric information. Their most common characteristic is an organization-specific unique number. These credentials have a specific lifetime to indicate transient association (e.g., visa for a country, travel club membership). This definition points out that, in addition to identity providers typically corresponding to governmental offices, there are many other identity providers issuing their own credentials with different purposes and that the assurance requirements for these credentials depend on the losses that the relying parties are willing totolerate because of identity theft. In the following sections we focus on digital credentials only. However, it is important to notice that today the distinction between digital credentials and physical credentials is disappearing as physical credentials often contain information that can be automatically read by computing devices or may directly be embedded in electronic devices. As such, physical credentials will tend to become small portable computing devices able to communicate with the environment and other devices.”

(Osmanoglu, 2014, p. 77) describes identity and credential components as follows. The identity and credential component of the framework addresses concerns related to identifying and authenticating entities such as people, hardware devices, and software applications.

This includes the following: The establishment of identities, management of credentials (authenticators such as passwords, security tokens, and certificates), particularly enforcement of relevant policies, resolution of potential conflicts, and creation of global identifiers (IDs); The processes associated with the request, generation, update, revocation, and retiring of identifiers and credentials; The maintenance of identity profile information including the authoritative sources or identity related data attributes and the life-cycle processes used to manage identifier attributes, and; The processes associated with credential quality and credential binding. Global IDs are specific attributes that uniquely reference an entity within an organization (such as an employee ID). A global ID is different from an account ID, which is an attribute used to represent a user on a system or an application. A user may possess many different account IDs in an organization but should have one and only one global identifier. A profile is formed by mapping an identifier with associated identifier attributes (such as location, job title, supervisor, and department). Profiles contain identifier attributes with various formatting, ownership, and quality rules and make them available to IAM processes for IAM initiatives. We group maturity indicators for the identity and credential component into the following nine functional focus areas:

1. **Generate**

"Generate refers to the processes and tools used to create identity/identifiers and create or initialize a credential (e.g., passwords, security tokens, certificates). A higher rating indicates that identity and credentials are generated or initialized with efficiency and with the appropriate level of strength/complexity based on risk profile, policy, and standards. A lower rating indicates processes that may produce weak credentials or be prone to error.

2. **Register**

Register refers to the processes and tools used to request a credential for an entity. A higher rating indicates that registration processes have been optimized enabling users to quickly ascertain and request the specific credential that is necessary to allow them to perform a job responsibility. A lower rating indicates inefficient processes that may result in loss of productivity or attempts to circumvent controls.

3. **Distribute/bind**

Distribute refers to the processes and tools used to communicate or transfer the credential to the appropriate user in a secure manner. A higher rating indicates that risk of exposure of credentials to inappropriate parties is reduced as a result of tested controls. Also important is the timely distribution of the credentials for new users or following compromise of an existing credential. A lower rating indicates a weak process that introduces the risk of compromise or theft of credentials or delayed productivity from a workforce not properly equipped to perform their job function.

4. **Proof**

Proof refers to the processes and tools used to validate someone’s identity using authoritative data sources and identity profile data. Proofing does not just rely on credentials. A higher rating indicates that risk of exposure of credentials to inappropriate parties is reduced. A lower rating indicates a weak process that introduces the risk of compromise or theft of credentials or delayed productivity from a workforce not properly equipped to perform their job function.

5. **Store/update**

Store/update refers to the processes, standards, tools, and repositories associated with the storage of a credential and update of identity profile data. A higher rating indicates a secure framework of technology and processes is used to protect the confidentiality and integrity of the credentials and identity profile data, reducing the likelihood of data loss to attackers. A lower rating indicates an increased risk of credentials being compromised during storage.

6. **Reset**

Reset refers to the processes and tools used to reset a forgotten credential. A higher rating indicates an organization that values enabling their users with tools to allow them to quickly become productive and recover from a forgotten or lost credential. A lower rating indicates inefficient usage of help desk personnel and a reduction in service quality to the business.

7. **Expire/Renew**

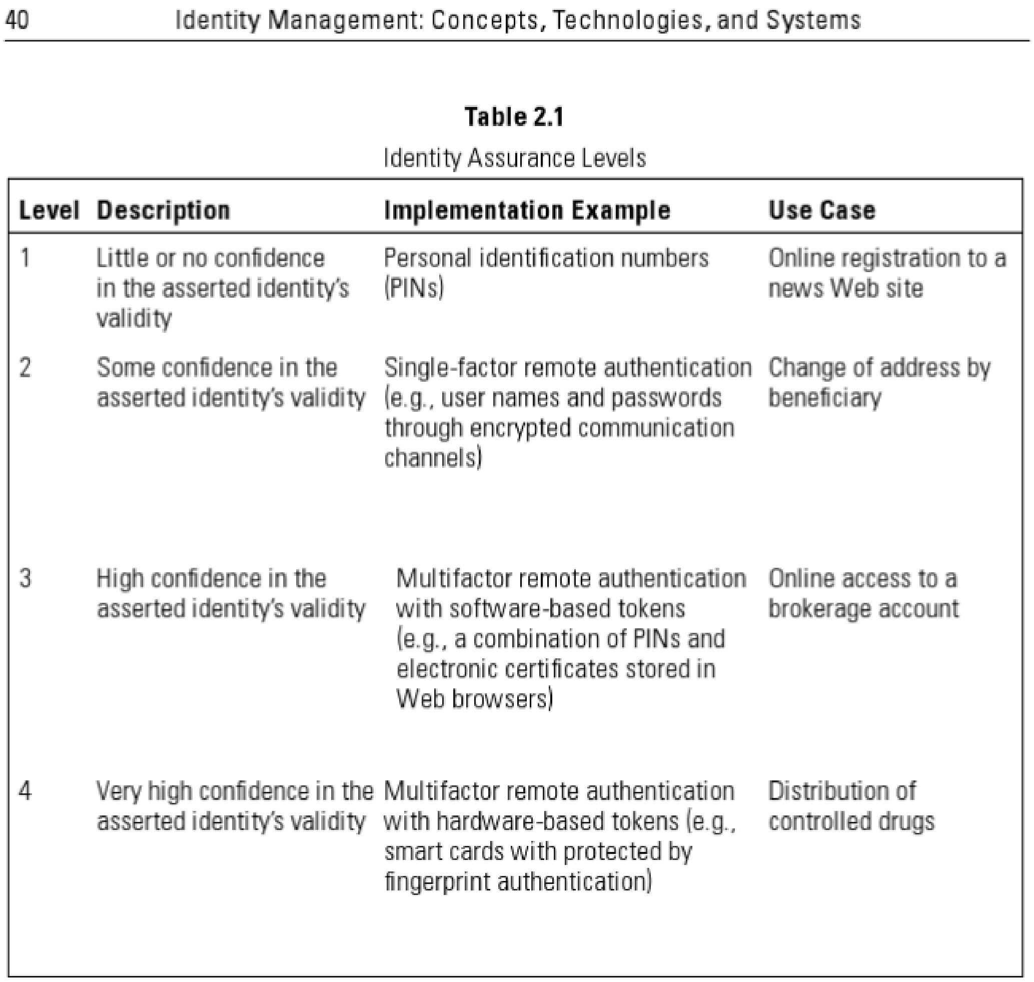
Expire refers to the processes, standards, and tools associated with the automatic suspension of a credential after a specified duration. Renew refers to the processes, standards, and tools associated with the extension of a previously established credential expiry date. A higher rating indicates a strong integration between the policy and the mechanisms present in platforms and applications to enforce expiration policies and to support automated extensions to expiry dates when approved. This integration helps reduce the risk of inappropriate access and persistence of active authenticators after their intended usage. This integration also helps reduce the risk of loss of productivity that results from a credential being expired before a real world need for use has concluded. A lower rating indicates increased risk that credentials are active beyond their intended life cycle. A lower rating can also indicate that there is risk that a credential will be expired before the business needs to maintain it as current has concluded.

8. **Recover**

Recover refers to the processes and tools used to recover from a lost or stolen credential. A higher rating indicates a strong framework present to allow the organization to quickly recover one or more credentials, enabling users to return to normal operation. A lower rating indicates that recovery operations can be costly from a time and resource requirement.

9. **Revoke/dispose**

Revoke refers to the processes and tools used to suspend or disable a credential, typically due to suspected compromise. A higher rating indicates strict understanding and control of credentials across the enterprise enabling quick and decisive action to be taken to disable a compromised credential and provide mechanisms to inform relying applications and parties that the credential should no longer be trusted. This includes the integration with provisioning processes and a level of automation necessary to ensure a closed-loop process that is successful when executed. A lower rating indicates increased risk that a compromised credential will continue to be active and trusted, leading to unauthorized access to protected resources. Dispose refers to the processes and tools used to destroy a credential after it has expired or been revoked. A higher rating indicates that the final step in the life cycle of a credential is properly managed and executed, reducing the risk of credential being enabled and used for malicious purposes. A lower rating indicates weak controls and potential for process breakdown allowing for expired or revoked credentials to exist in a state that still pose a risk of inappropriate access.” (Osmanoglu 2014, p. 78-79)



40 Identity Management: Concepts, Technologies, and Systems

Table 2.1

Identity Assurance Levels

Level	Description	Implementation Example	Use Case
1	Little or no confidence in the asserted identity's validity	Personal identification numbers (PINs)	Online registration to a news Web site
2	Some confidence in the asserted identity's validity	Single-factor remote authentication (e.g., user names and passwords through encrypted communication channels)	Change of address by beneficiary
3	High confidence in the asserted identity's validity	Multifactor remote authentication with software-based tokens (e.g., a combination of PINs and electronic certificates stored in Web browsers)	Online access to a brokerage account
4	Very high confidence in the asserted identity's validity	Multifactor remote authentication with hardware-based tokens (e.g., smart cards with protected by fingerprint authentication)	Distribution of controlled drugs

Figure 3 - Identity Assurence Levels Source: (Bertino, Elisa Takahashi, Kenji, 2011, p. 40)

3.1.2 Public-Key Certificates and Public-Key Infrastructures

The most well known type of digital credential is the public-key certificate, which binds identity attributes of a subject with a cryptographic public-key of the subject (Figure 4). Public keys represent an interesting form of identity attributes in that, unlike most other identity attributes, they do not have a correspondence to some physical equivalent in the real world. Their motivation is the need to encrypt messages so that only the intended receiver can decrypt them without the need of having to share secrets between the sender and the receiver. However, since typically each subject has a different public key, a public key may be seen as a form of identifier. (Bertino, Elisa Takahashi, Kenji, 2011, p. 48-49)

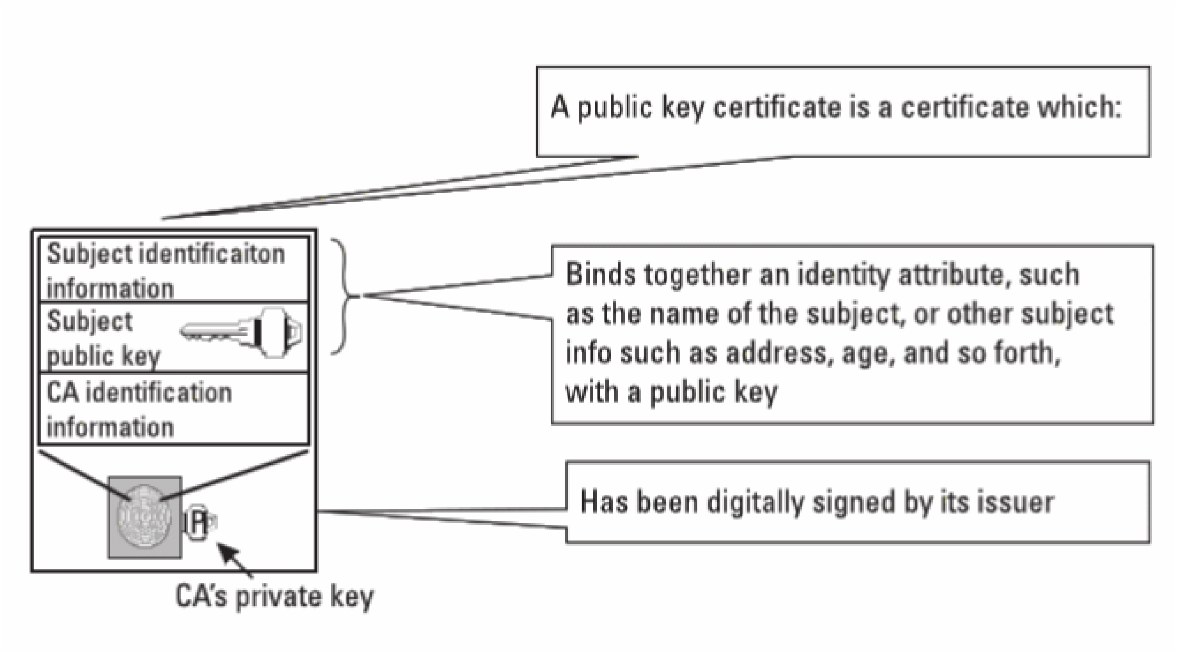

A public key certificate is a certificate which:
Subject identificaiton information
Subject public key
CA identification information
Binds together an identity attribute, such as the name of the subject, or other subject info such as address, age, and so forth, with a public key
Has been digitally signed by its issuer
CA's private key

Figure 4 – Public key certificate Source: (Bertino, ElisabTakahashi, Kenji, 2011, p. 49)

Public-key certificates are issued by entities known as certification authorities (CA). The actual organization of such certificates is based on the wellknown X.509 standard certificate structure (IETF), which includes the following components:

- Version number (1, 2, or 3);
- Serial number (unique within the CA) identifying the certificate;
- Identifier of the digital signature algorithm;
- Issuer X.500 name (CA); • Period of validity (from– to dates);
- Subject X.500 name (distinguished name, DN), which, in turn, consists of the following elements:
- CN (common name);
- O(organization or company);
- OU (organization unit);
- L (city/locality);
- ST (state/province);
- C (country);
- Subject public-key info (algorithm, parameters, key);
- Issuer unique identifier (only in version 2 or higher);
- Subject unique identifier (only in version 2 or higher);
- Extension fields (only in version 3);

• Signature (of hash of all fields in certificate). An important requirement when using such certificates is the ability to verify the digital signature of the issuer in order to determine the integrity of the certificates. Such requirement is addressed by the Public-Key Infrastructure (PKI), a (distributed) infrastructure providing the functions and the services needed to support the lifetime of public-key certificates and their use (Figure 5). The management of public-key certificates involves several processes and functions (Adams, 2005); we discuss some of these below.

3.1.2.1 Subject Registration Subject registration is the process in which the identity of an individual user or process is established and verified. The "strength" of the applied procedural control depends on the operational procedures of the CA, which is stated by Fundamental Technologies and Processes 51 the Certification Practice Statement (CPS). Also the CA also has a certificate policy (CP) stating the applications for which the CA declares a specific public-/private-key fit for (e.g., digital signature, encryption of data, verification of Web site identity, and so forth).

3.1.2.2 Key Pair Generation Key pair generation is a function that performs the actual creation of the private-/public-key creation. A key pair can be generated at different locations: at the subject system (e.g., user's PC); at the CA; or at a trusted third-party key-generation facility. The selection of the location depends on several factors, including: performance (e.g., generating a key pair in a mobile phone); assurance (if there is a requirement to generate the key pair according to specific cryptographic guidelines— e.g., FIPS 140-1); and intended key usage (e.g., confidentiality versus nonrepudiation).

3.1.2.3 Certificate Distribution Certificate distribution is the process in which the certificate (and the public key, if generated at the CA) is delivered directly to the (subject) owner of the key, or to a remote repository (certificate repository), or both. Requesting and receiving a certificate back from a CA requires the use of secure protocols, such RFC2510, the Internet X.509 Public Key Infrastructure Certificate Management Protocols (CMP).

3.1.2.4 Key/Certificate Use The key/certificate use process involves first retrieving the key upon request of a relying party and then verifying the integrity of the certificate, which in turn requires the public key of the CA that issued the certificate. The process by which a party retrieves such public key is based on the notion of certification path and may involve several CAs that have some trust relationship among each other; typically such a trust relationship simply means that they know each other's public keys. The proper use of a certificate also requires verifying that the certificate has not expired or has not been revoked. (Bertino, Elisa Takahashi, Kenji, 2011, p. 49-51)

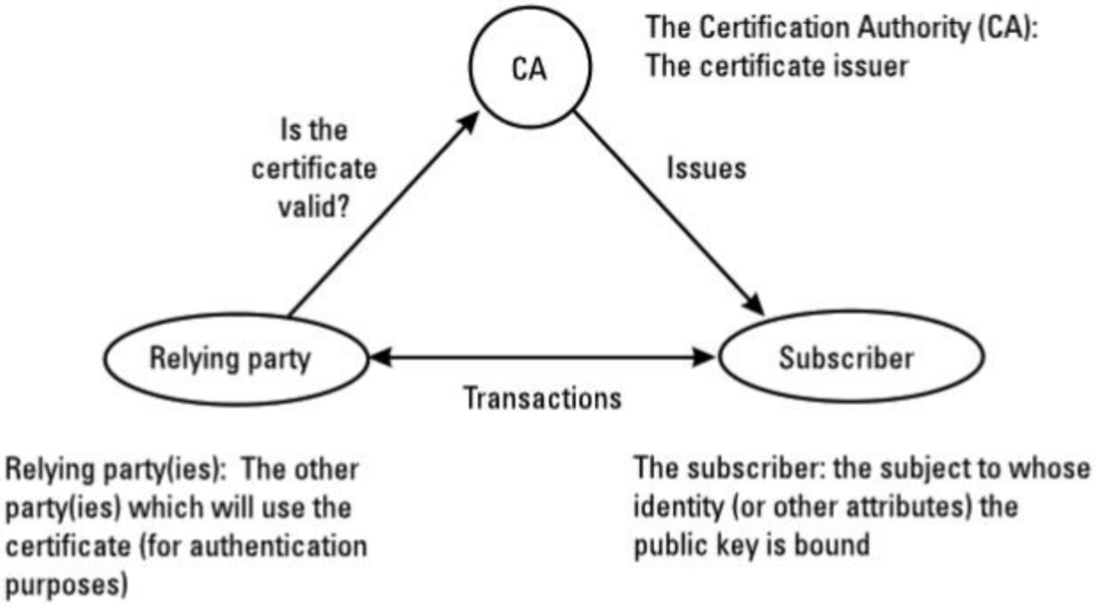

CA
The Certification Authority (CA): The certificate issuer
Is the certificate valid?
Issues
Relying party
Subscriber
Transactions
Relying party(ies): The other party(ies) which will use the certificate (for authentication purposes)
The subscriber: the subject to whose identity (or other attributes) the public key is bound

Figure 5 - The main parties of PKI. Source: (Bertino, Elisa Takahashi, Kenji, 2011, p. 40)

3.1.5 Single Sign-On

"Authentication systems can be implemented to provide SSO services, which aggregate identities and permit access to multiple systems through a target system authentication method. Users want to provide one password, one time, and work for the entire day. The security debate continues about allowing users to maintain these credentials for an entire day; however, within any organization, some reasonable time limit can be determined within which users will feel they have the access they need, and security professionals will feel they have protected the environment adequately.

If all applications, databases, and operating systems used a single set of user-IDs to uniquely identify all of the users, SSO would be a lot simpler to implement than it is today. An SSO system that supports multiple entities requires either a centralized shared directory or secure synchronization across directories. Most SSO systems have built-in connectors to popular commercial applications and enterprise systems. They also have APIs that would allow an organization to create its own connectors to other applications or organization's custom applications.

As shown in Figure 6 in its most simple form, SSO starts with the initial logon to the personal computer. The system requests the user ’s user-ID and password and creates a credential that is stored either in memory or on disk. This may be referred to as a credential, a cookie, a token, and other various names. Essentially, the personal computer will store information that can be shared with other systems and applications. This information typically contains information about the user, the identification used by the system, user-ID, some expiration information, and other data elements that can be used for validation by end systems. Many SSO deployments use elements of Lightweight Directory Access Protocol (LDAP) services to house much of the information and help navigate the exchange of data between clients and servers.” (Osmanoglu 2014, p. 374-375)

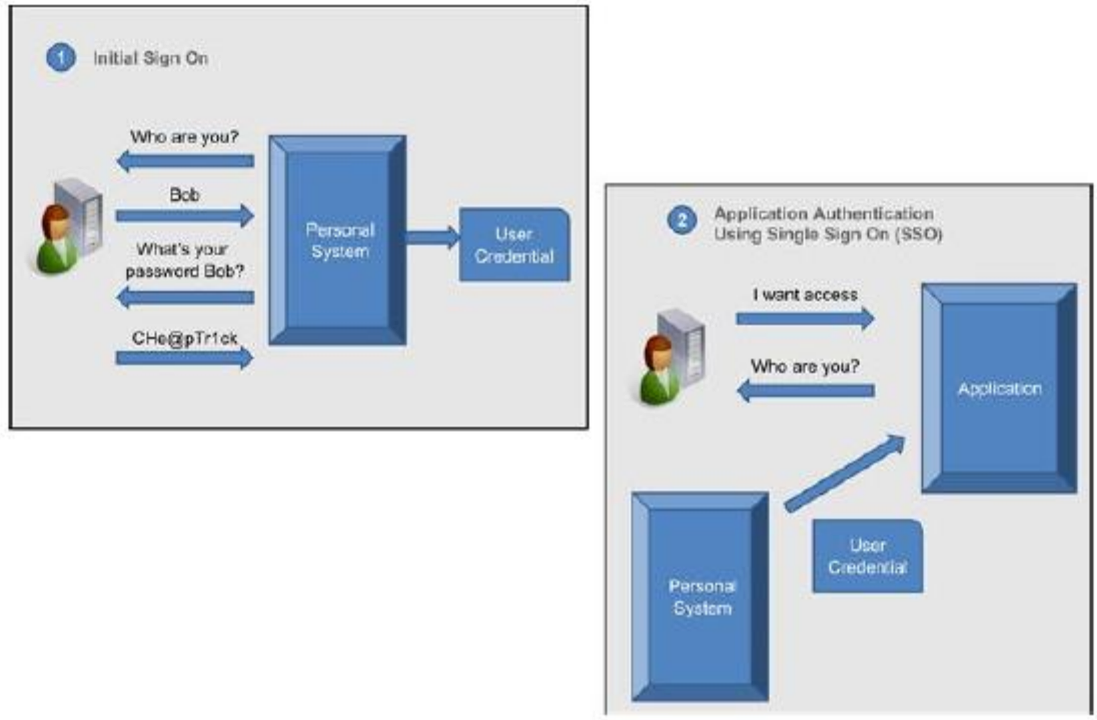


Figure 6 - Single sign on. **Source: (Osmanoglu, 2014, p. 375)**

“Once the user has completed the initial logon transaction, they no longer need to provide a user-ID/password pair in order to access SSO enabled systems. They connect to the application, and instead of the application requesting a user-ID and password, the user ’s computer and the application system communicate to determine if their user credential exists, is valid, and has not timed-out. If these conditions are met, the user is permitted access to the application as though they had entered a user-ID and password.

Web SSO works in a similar fashion to traditional SSO. The goal is to sign-in once and to gain authenticated access to multiple, independent Web-based services. The biggest differentiator is that the credential is not produced when the user first logs on to their personal computer. Instead it is generated and stored the first time that the user interacts with a web-based application that is integrated with the Web SSO infrastructure.

An SSO system can also help enforce centralized policy management across both Web and non-Web-based SSO." (Osmanoglu, 2014, p. 375-376)

3.1.6 **Privacy**

"Although a digital identity system offers many benefits, there are circumstances at which a subject would prefer to keep its identity hidden. In the extreme cases, whistle-blowers, political dissidents, and activists may be afraid of improper punishment or reprisals for their views and work (Bertino, 2011). At a more mundane level, many people search for health information online while assuming their searches will not be revealed in embarrassing ways. Similarly, a user of a discussion forum may wish to express an unpopular opinion, but may not feel comfortable with other users knowing how they feel (Bertino, 2011). All of these are examples of the desire for anonymity. In common understanding, anonymity implies that certain actions and behavior cannot be traced back to the person responsible. While this intuition serves as a starting point, it does not capture the essence of anonymity as defined within the field of digital identity management. Instead, we define anonymity in terms of the linkability of items of interest (Pfitzmann, 2008). Items of interest are any distinct features that might reveal information about users. Examples of items of interest include nyms[1], e-mail messages, and search engine queries. Furthermore, the user's identity and real name may themselves be considered items of interest. Two or more items of interest are linkable if an eavesdropper or attacker can determine that they are related. If two messages have been cryptographically signed, and the same public key is used to verify the signature, the messages can be linked to the same signing key. However, if a user performs a search query about a health condition, an observer should not be able to connect the query with the user's real-world identity. In the latter case, the query and the user's identity are unlinkable. Several approaches have been proposed to address the privacy problem in the context of identity management. These approaches can be classified into approaches to achieve unlinkability of nyms, known

[1] A nym gives a user and identity under which to operate when interacting with a computer systém or network; examples of nyms include login names and pseudonyms.

as pseudonym systems, and approaches to achieve privacy and/or unlinkability of credentials. Also, the various approaches can be classified into (Layouni, 2007):

- Multiple-show approaches, if multiple showings of the same nym or credential cannot be linked to each other;
- Single-show approaches, if multiple showings of the same nym or credential can be linked to each other.

In what follows we first discuss pseudonym systems, and the approaches to anonymous credentials." (Bertino, Elisa Takahashi, Kenji, 2011, p. 65-66)

3.2 **Facility management**

Facility Management is comprehensive interdisciplinary discipline that focuses on configuration, performance and management support services, whose added value can be seen in increased efficiency of main activities. As each other field of management, FM also includes management of operational, tactical and strategic activities, different roles and process workflows. In terms of long-term analysis of the costs of conventional companies, the labor costs followed by costs associated with ownership, development, rehabilitation and maintenance and management of fixed assets and services connected to such assets comes as the highest. The FM activities are described in detail in the first three parts of standard ČSN EN 15221. (Hampl, 2016)

FM mission is to provide all support services for personnel performing key activities, so that greater effectivity is achieved. It is this efficiency increase in main activities, that adds value to the chain of economic activities of the company. Focusing on human being brings a stochastic element to the FM information systems. But how the worker will enjoy his lunch today in a canteen is actually a probabilistic phenomenon. The fact, that the FM and its IS focuses mainly on artificial environments and asset management, leasing and maintenance of equipment, must not distract from the midpoint, which is human being. There are numerous automation tools, whose ease of use and meaningful management is part of the CAFM systems, and which are important for a personnel comfort. (Hampl, 2016)

3.2.1 **CAFM/IWMS**

Facility management automation (computer-aided facility management or CAFM and integrated workplace management system or IWMS) primarily is viewed as a facility management departmental tool that supports facility management (FM) operations. Proper selection and implementation of technology tools are critical in determining the current and future value of the FM department to the organization. Optimization of the organizational value of the FM department occurs when the tools facilitate processes that deliver facility departmental objectives in support of an organization's mission. (Teicholz, 2012, p. 3)

3.2.2 Value of facility management automation to the organization

The value of FM to the organization normally can be evaluated by a variety of metrics such as employee attraction and retention, improved productivity, risk mitigation, sustainable initiatives, and strategic business planning support. All of these can be supported and enhanced by processes facilitated by FM automation tools. These tools provide value to the organization in three ways: interoperability, reorganization, and culture. (Teicholz, 2012, p. 6)

3.2.3 Location Management based on GIS

Utilization of GIS tools is a trend, which can be observed in real IWSM systems. The procedure from a general overview to a detail provide is aided by map backgrounds and 3D map visualizations. Energy consumption and achieved LEED scores for individual areas and buildings illustrated with colourful symbols provide management reports. The choice of location for planned investment is with a GIS tools representative procedure, which reduces the entropy of the decision and can save badly or carelessly incurred costs, that never produce return. (Hampl, 2016)

3.2.4 Conclusion

IWSM matured and now can provide its users with several advantages and rapid responses, whose processing would need considerable amount of work without existence of such systems. There are simple IWSM systems, which eg. solve only renting issues. Implementation of such dedicated system is although shorter and easier, and at the moment only solves just one of the functionality that the user requires, compared with the implementation of a comprehensive module of an IWSM system. Complexity will show advantage in time of need for additional modules or integration. (Hampl, 2016)

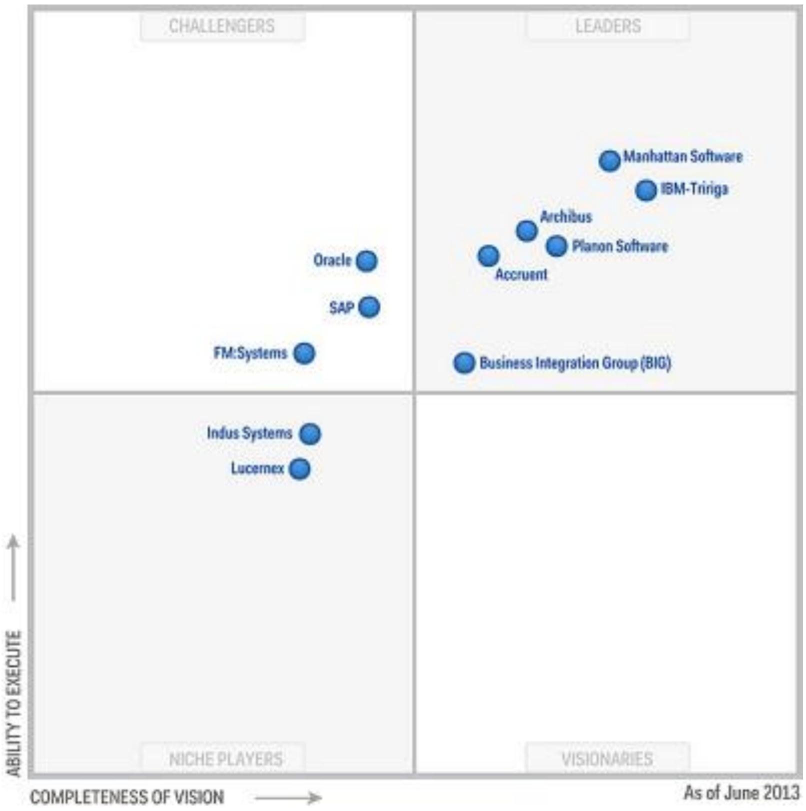


Figure 7 - IWSM systems Source: (Gartner 2013)

The risk of choice is reduced by selecting one of the foreign and for local standards localized systems. Their list is given by the so called Magic Quadrant of IWSM systems by Gartner company. Nonlocalized systems have difficult position on Czech market and advanced systems of Czech origin will not make it into a Gartner comparisons. Their scope and level are often incomparable and they merit to have similar article. (Hampl, 2016)

3.3 Windows server

MS Windows Server 2012

Operating system Windows Server 2012 is a flexible and scalable server platform that provides the flexibility needed for creating, deploying and managing Web sites and applications within the company, in the cloud or in a hybrid environment using a consistent set of tools and interfaces. It provides easy-to-manage platform optimized for the cloud with high availability. Thus ensuring flexible data storage, continuous availability, and effective management. Windows Server 2012 provides better support for open interfaces, open source applications and programming languages. PHP and web standards are supported. The .NET Framework 4.5 also brings new features and improvements, such as better work on site and in the network or supporting asynchronous file operations.

Microsoft offers Windows Server 2012 in four editions, which are based on the organization's size and needs of virtualization and cloud computing. Datacenter Edition is suitable for highly virtualized environments, private and hybrid clouds. Standard version is intended for slightly or completely non-virtualized environment. For small organizations with up to 25 users and 50 devices is favored Windows Server 2012 Essentials server and economical choice for general use is called Foundation. (Microsoft Windows Server 2012, 2013)

Hardware requirements specified by Microsoft for Windows Server 2012 are as follows:

- At least 1.4 GHz 64-bit processor
- At least 512 MB of RAM memory
- At least 32 gigabytes of disk space for the system partition.

These are the minimum requirements. For normal operation, the computer parameters need to be higher. These parameters should be sufficient for a successful installation.

(Microsoft Windows Server 2012, 2013)

3.3.1 Server Roles, Role Services, and Features for Windows Server 2012

A server role is a related set of software components that allows a server to perform a specific function for users and other computers on a network. A computer can be dedicated to a single role, such as Active Directory Domain Services (AD DS), or provide multiple roles.

Role services A role service is a software component that provides the functionality for a server role. Each role can have one or more related role services. Some server roles, such as Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP), have a single function, and installing the role installs this function. Other roles, such as Network Policy and Access Services and Active Directory Certificate Services (AD CS), have multiple role services that you can install. With these server roles, you can choose which role services to install.

Features A feature is a software component that provides additional functionality. Features, such as BitLocker Drive Encryption and Windows Server Backup, are installed and removed separately from roles and role services. A computer can have zero or more features installed depending on its configuration. Roles, role services, and features are configured by using Server Manager, a Microsoft Management Console (MMC). Some roles, role services, and features are dependent on other roles, role services, and features. As user install roles, role services, and features, Server Manager prompts him to install other roles, role services, or features that are required. Similarly, if user tries to remove a required component of an installed role, role service, or feature, Server Manager warns that he cannot remove the component unless he also remove dependent roles, role services, or features.

Because adding or removing roles, role services, and features can change hardware requirements, user should carefully plan any configuration changes and determine how they affect a server's overall performance. Although combining of complementary roles is typical, doing so increases the workload on the server, so there is a need to optimize the server hardware accordingly. Table 1 provides an overview of the primary roles and the related role services you can deploy on a server running Windows Server 2012. (Stanek, William R., 2012, p. 32)

Table 1 - Primary Roles and Related Role Services for Windows Server 2012
Source:(Stanek, William R., 2012, p. 33-35)

ROLE	DESCRIPTION
Active Directory Certificate Services (AD CS)	Provides functions necessary for issuing and revoking digital certificates for users, client computers, and servers. Includes these role services: Certification Authority, Certification Authority Web Enrollment, Online Responder, Network Device Enrollment Service, Certificate Enrollment Web Service, and Certificate Enrollment Policy Web Service.
Active Directory Domain Services (AD DS)	Provides functions necessary for storing information about users, groups, computers, and other objects on the network, and makes this information available to users and computers. Active Directory domain controllers give network users and computers access to permitted resources on the network.
Active Directory Federation Services (AD FS)	Complements the authentication and access management features of AD DS by extending them to the World Wide Web. Includes these role services and subservices: Federation Service, Federation Service Proxy, AD FS Web Agents, Claims-Aware Agent, and Windows Token-Based Agent.
Active Directory Lightweight Directory Services (AD LDS)	Provides a data store for directory-enabled applications that do not require AD DS and do not need to be deployed on domain controllers. Does not include additional role services.
Active Directory Rights Management Services (AD RMS)	Provides controlled access to protected email messages, documents, intranet pages, and other types of files. Includes these role services: Active Directory Rights Management Server and Identity Federation Support.

Application Server

Allows a server to host distributed applications built using ASP.NET, Enterprise Services, and Microsoft .NET Framework 4.5. Includes more than a dozen role services.

DHCP Server

DHCP provides centralized control over IP addressing. DHCP servers can assign dynamic IP addresses and essential TCP/IP settings to other computers on a network. Does not include additional role services.

DNS Server

DNS is a name-resolution system that resolves computer names to IP addresses. DNS servers are essential for name resolution in Active Directory domains. Does not include additional role services.

Fax Server

Provides centralized control over sending and receiving faxes in the enterprise. A fax server can act as a gateway for faxing and allows you to manage fax resources, such as jobs and reports, and fax devices on the server or on the network. Does not include additional role services.

File And Storage Services

Provides essential services for managing files and storage, and the way they are made available and replicated on the network. A number of server roles require some type of file service. Includes these role services and subservices: BranchCache for Network Files, Data Deduplication, Distributed File System, DFS Namespaces, DFS Replication, File Server, File Server Resource Manager, Services for Network File System (NFS), File Server VSS Agent Service, iSCSI Target Server, iSCSI Target Storage Provider, and Storage Services.

Hyper-V

Provides services for creating and managing virtual machines that emulate physical computers. Virtual machines have separate operating system environments from the host server.

Network Policy and Access Services (NPAS)

Provides essential services for managing network access policies. Includes these role services: Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP).

Print And Document Services

Provides essential services for managing network printers, network scanners, and related drivers. Includes these role services: Print Server, LPD Service, Internet Printing, and Distributed Scan Server.

Remote Access

Provides services for managing routing and remote access to networks. Use this role if you need to configure Virtual Private Networks (VPN), Network

	Address Translation (NAT), and other routing services. Includes these role services: DirectAccess and VPN (RAS) and Routing.
Remote Desktop Services	Provides services that allow users to run Windows-based applications that are installed on a remote server. When users run an application on a terminal server, the execution and processing occur on the server and only the data from the application is transmitted over the network.
Volume Activation Services	Provides services for automating the management of volume license keys and volume key activation.

3.4 **Active Directory**

Active Directory is an extensible directory service that enables centralized management of network resources. It allows you to easily add, remove, or relocate accounts for users, groups, and computers as well as other types of resources. Nearly every administrative task you perform affects Active Directory in some way. Active Directory is based on standard Internet protocols and has a design that helps you clearly identify the physical and logical components of your network's structure.

Active Directory provides the necessary infrastructure for designing a directory that meets theneeds of your organization. A directory is a stored collection of information about various types of resources. In a distributed computing environment such as a Windows network, users must be able to locate and use distributed resources, and administrators must be able to manage how distributed resources are used. This is why a directory service is necessary.

A directory service stores all the information needed to use and manage distributed resources in a centralized location. The service makes it possible for resources to work together. It is responsible for authorizing access, managing identities, and controlling the relationships between the resources. Because a directory service provides these fundamental functions, it must be tightly integrated with the security and management features of the network operating system.

A directory service provides the means to define and maintain the network infrastructure, perform system administration, and control the user experience. Although users and administrators might not know the exact resources they need, they should know some basic characteristics of the resources they want to use. If so, they can use the directory service to obtain a list of resources that match the known characteristics. As illustrated in Figure 1, they can use the directory service to query the directory and locate resources that have specific characteristics. For example, users can search the directory to find a color printer in a particular location or to find a color printer that supports duplex functionality. Figure 1 Working with directory services. (Training Solutions, 2014, p. 7-8)

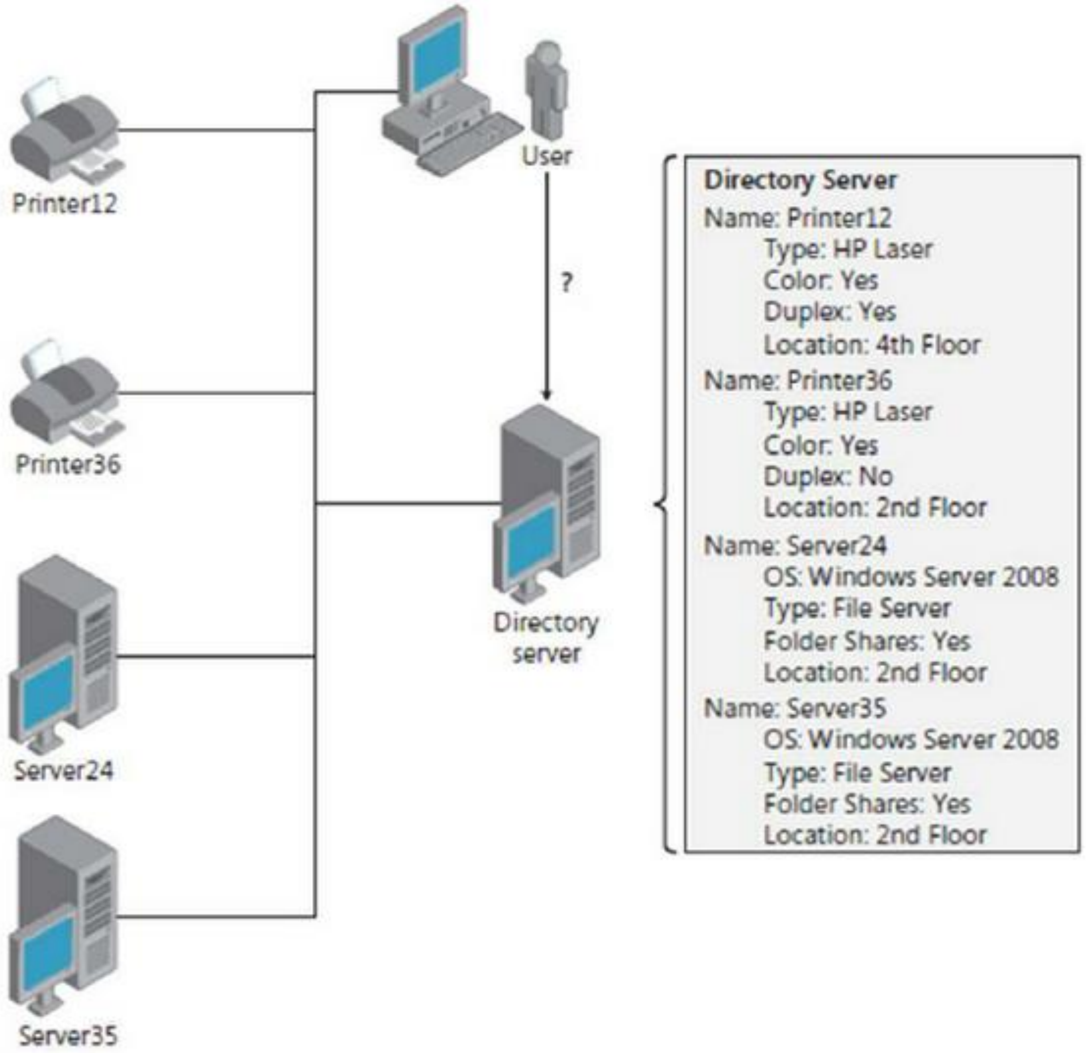


Figure 8 - working with directory services **Source:[Training Solutions, 2014, p. 7-8]**

3.4.1 **DNS Domains**

Active Directory uses Domain Name System (DNS). DNS is a standard Internet service that organizes groups of computers into domains. DNS domains are organized into a hierarchical structure. The DNS domain hierarchy is defined on an Internet-wide basis, and the different levels within the hierarchy identify computers, organizational domains, and top-level domains. DNS is also used to map host names to numeric TCP/IP addresses. Through DNS, an Active

Directory domain hierarchy can also be defined on an Internet-wide basis, or the domain hierarchy can be separate from the Internet and private.

When you refer to computer resources in a DNS domain, you use a fully qualified domain name (FQDN), such as zeta.microsoft.com. Here, *zeta* represents the name of an individual computer, *microsoft* represents the organizational domain, and *com* is the top-level domain. Top-level domains (TLDs) are at the base of the DNS hierarchy. TLDs are organized geographically by using two-letter country codes, such as *CA* for Canada; by organization type, such as *com* for commercial organizations; and by function, such as *mil* for U.S. military installations. (Stanek, William R., 2012, p. 217-218)

3.4.2 **Domain controllers**

Domain controllers manage all aspects of a user's interaction with Active Directory domains. They validate user logon attempts, locate objects, and much more. Within Active Directory, directory information is logically partitioned. Each domain controller stores a copy of all pertinent partitions. The pertinent partitions for a particular domain controller are determined by where the domain controller is located and how the domain controller is used. Domain controllers manage changes for information they store and replicate changes to other domain controllers as appropriate. Because of how replication works, a conflict can occur if an attribute is modified on a domain controller, because a change to the same attribute on another domain controller is propagated. Active Directory resolves the conflict by comparing each attribute's property version number (a value initialized when an attribute is created and updated each time an attribute is changed) and replicating the changed attribute with the higher property version number. Normally domain controllers are readable and writable. However, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 and later also support read-only domain controllers. A read-only domain controller (RODC) is a domain controller that hosts a read-only replica of a domain's directory. By default, RODCs store no passwords or credentials besides those used for their own computer account and the Kerberos Target (krbtgt) account. This makes RODCs ideal for branch offices where a domain controller's physical security cannot be guaranteed. (Training Solutions, 2014, p. 17-18)

Figure 9 shows an RODC deployed to a branch office. Here the main office has multiple domain controllers with writable data. The branch office has an RODC with read-only data. The RODC is placed at the branch office because the physical security of the server cannot be guaranteed. Figure 9 A read-only domain controller deployed to a branch office.

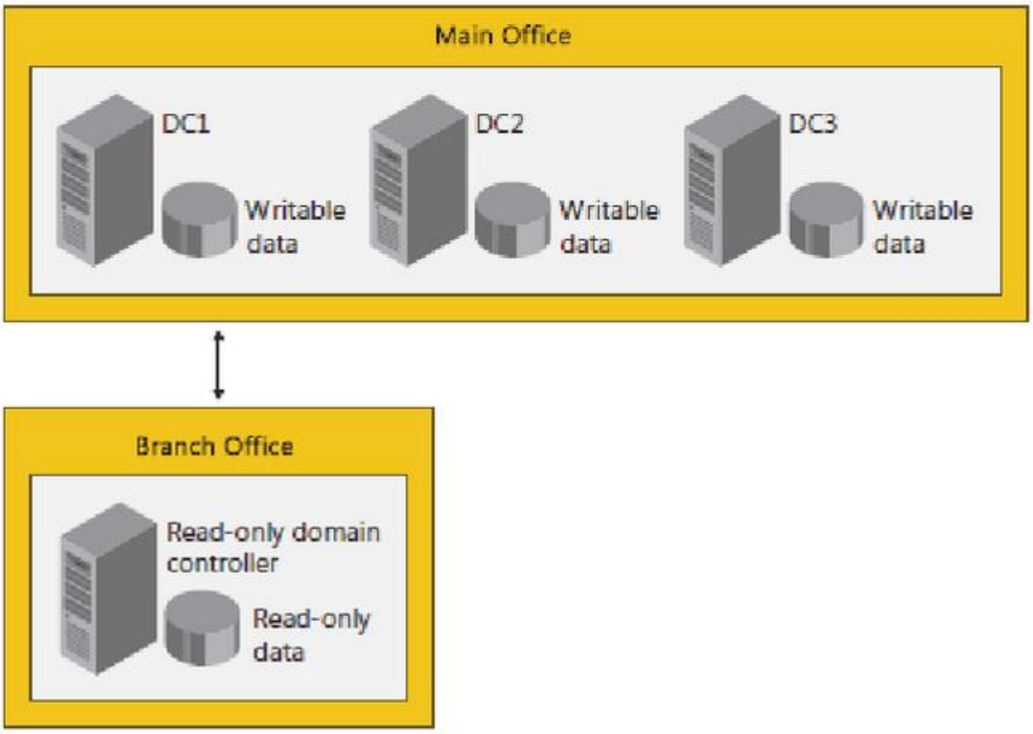


Figure 9 - A read-only domain controller deployed to a branch office
Source: [Training Solutions, 2014, p. 18]

3.4.3 **Active Directory Objects**

Resources that you want to represent in Active Directory are created and stored as objects. Objects have attributes that define the kinds of information you want to store about resources. For example, the User object in Active Directory has attributes that help describe users, including first name, middle initial, last name, and display name. The Computer object in Active Directory has attributes that help describe computers, such as the computer’s name, description, location, and security identifier. Objects in the directory are either leaf objects or container objects. Objects that can’t contain other objects are leaf objects, or simply leaves. Objects that hold other objects are referred to as container objects, or simply containers. The directory itself is a container that contains other containers and objects. In Figure 10, the Users object is a container that contains User objects, the Computers object is a container that contains

Computer objects, and the Printers object is a container that contains Printer objects. Each object created within the directory is of a particular class. The Active Directory schema defines the available object classes and provides rules that determine how you can create and use objects. Available object classes include User, Group, Computer, and Printer. (Training Solutions, 2014, p. 19-20)

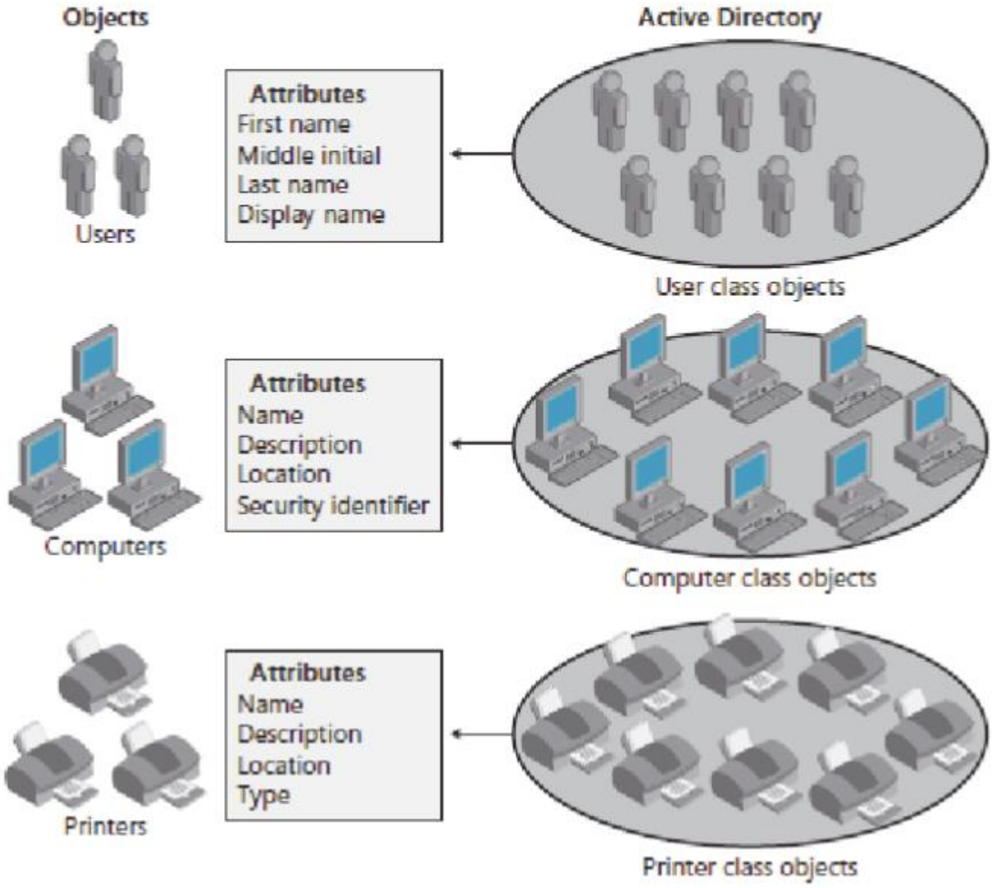


Figure 10 - Objects and attributes in Active Directory   Source: [Training Solutions, 2014, p. 20]

3.4.4 Active Directory Schema

“Essentially, the schema is a list of definitions that determines object classes and the types of information about the object classes that can be stored in the directory. The schema definitions themselves are stored as one of two types of objects: Schema class objects, or simply schema classes. Schema attribute objects, or simply schema attributes as shown in Figure 7, schema class objects and attribute objects are defined separately in the directory. You can refer to both sets of objects collectively as schema objects. Schema class objects describe the objects you can create. They function as templates for creating new objects. Within a particular schema class, the schema attributes store the information that describes related objects. For example, the User, Group, Computer, and Printer classes are composed of many schema attributes. The User class has attributes that describe users. The Group class has attributes that describe groups of users. The Computer class has attributes that describe computers. The Printer class has attributes that describe printers." (Training Solutions, 2014, p. 21)

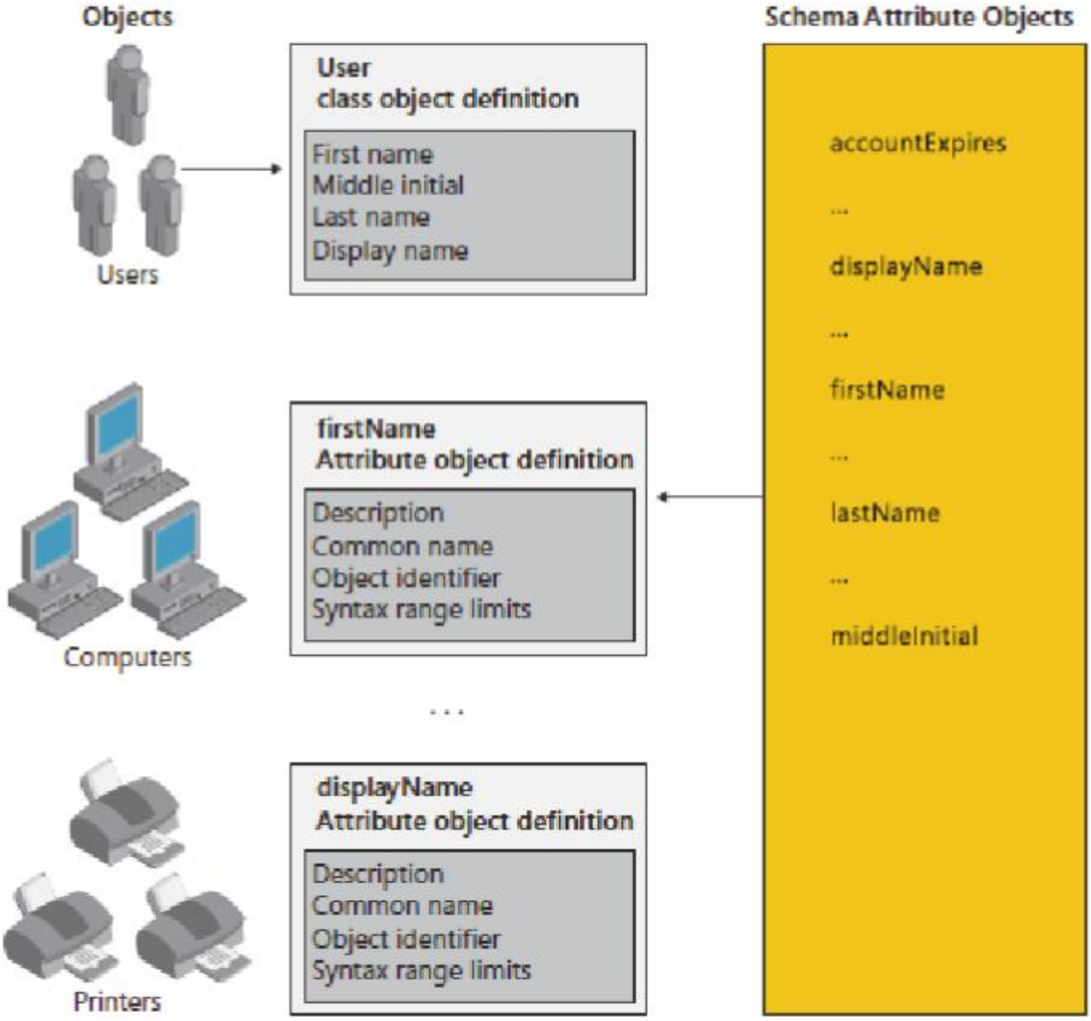


Figure 11 - Objects within a schema source: [Training Solutions, 2014, p. 22]

3.4.5 **Windows PowerShell**

Windows PowerShell 3.0 is an essential management and automation tool that brings the simplicity of the command line to next generation operating systems. Included in Windows 8 and Windows Server 2012, and portable to Windows 7 and Windows Server 2008 R2, Windows PowerShell 3.0 offers unprecedented power and flexibility to everyone from power users to enterprise network administrators and architects. (Wilson, 2013)

3.4.5.1 Cmdlets

The most basic component of Windows PowerShell is the built - in commands, called cmdlets (pronounced command - lets). Almost all the work done through Windows PowerShell is done through the use of cmdlets. Cmdlets are similar to built - in commands found in other shells; for example, the built - in command DIR found in cmd.exe . In Exchange Management Shell, cmdlets that perform a specific administrative function are often referred to as tasks. All cmdlets share the same basic structure. They have a name and take one or more parameters as input. Entering the name of a cmdlet, followed by any necessary parameter names and values, will result in the execution of the cmdlet. For example, the cmdlet Get-ExchangeServer returns a list of all Exchange servers in the organization in a formatted list. (Wilson, 2013)

3.5 Software solutions for facility and space management

There are more applications combining floor plans and objects, but they often offer more features then is required in the goals. Their characteristics and features will be described and they will be summarized in chapter 3.5.6.

3.5.1 IKA DATA Archibus Space management

ARCHIBUS is the world´s number one in software for real estate management, infrastructure and management, and solutions for facility management. The total annual turnover of based products and services based around ARCHIBUS exceed 1.7 billion USD. Through effective innovation and business transformation ARCHIBUS saves its users over 100 billion USD annually. By using ARCHIBUS organization can use a single, comprehensive and in depth integrated solutions based on which strategic decisions that optimize return of capital, reduce costs associated with this type of property and increase overall productivity and profitability can be performed. ARCHIBUS is worldwide promoter of ideas and the realization of sustainable development.

ARCHIBUS is the world´s number one TIFM (Total Infrastructure & Facilities Management) solutions. More than 4 000 000 ARCHIBUS users manage more than 5 000 000 real estates by it. Organizations using this software show 34% savings. With over 1 600 ARCHIBUS business partners there is regional support in more than 130 countries and ARCHIBUS is available in more than 20 world languages including Czech. (*IKADATA.cz: Archibus Inc.*)

3.5.1.1 Space management module

Modul for space administration is the most efficient CAFM software and is included in every product, which is considered as one of CAFM modules. Information systems specialized on FM support uses for visualization of real estate surfaces differently sophisticated graphical tools from the family of CAD, GIS and CAD / BIM originally used for vector graphics. All these tools are used for visualization of real property and its condition, employee or department location, placement of furniture or equipment, highlighting economic and technical conditions. Facility manager works with space management on all management levels – strategic, tactical and operational. KPI describing occupancy reporting, free space, energy consumption, costs characteristics, the amount of investment, etc. can be displayed. Typical working requirements also consist of display of comparison of individual real estates.

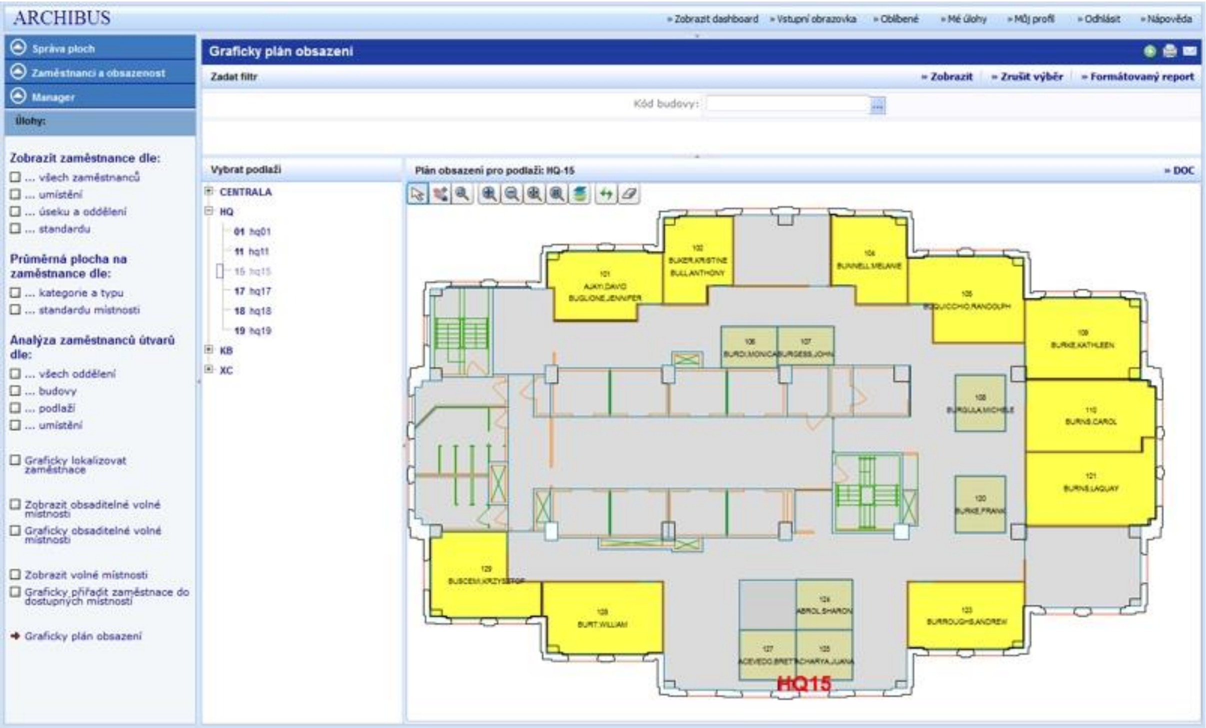
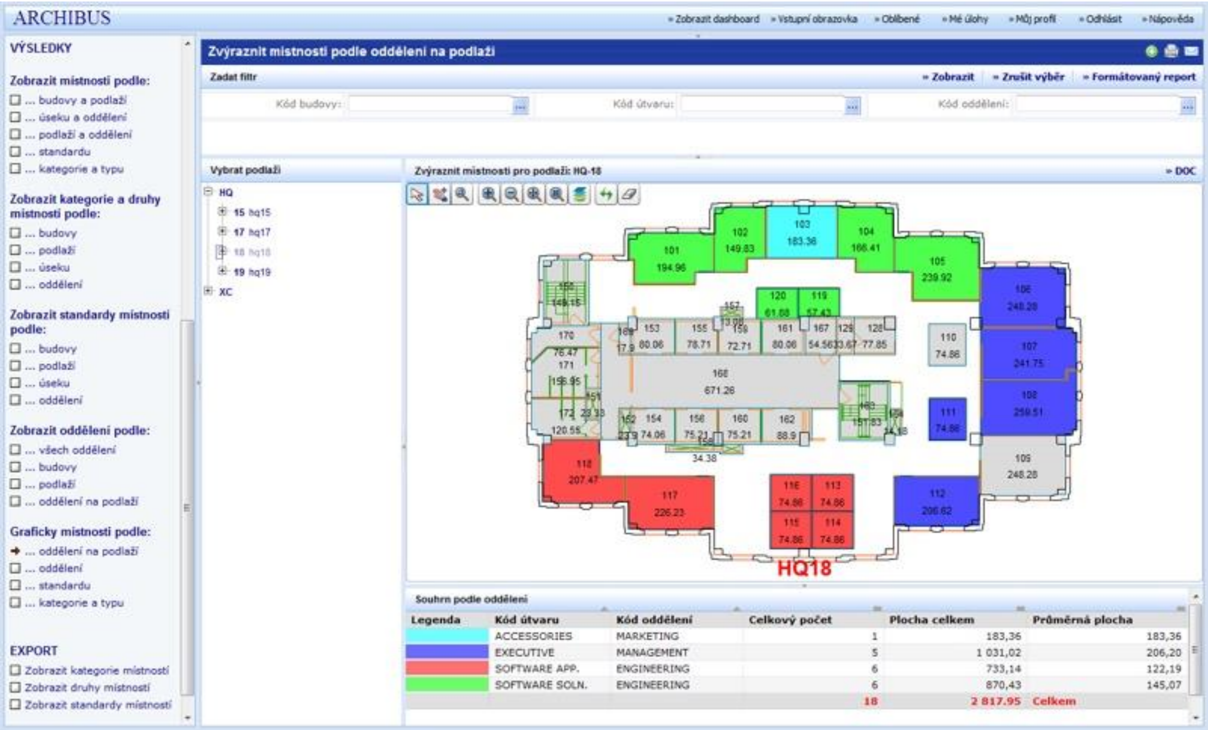


Figure 12 - Archibus - room occupation Source: (IKA DATA: Space management)

Access to data on physical assets should follow the ways of thinking and working practices of real estate managers. At first they require visualization of clear global data (here GIS user interfaces are best proven) with their refining and easy access to the desired detail (here CAD or CAD BIM are best proven). Also the way the CAFM software works with the native formats of CAD and GIS is important. If the data is embodied in these files, actively used and there is a workflow and setting of standards (eg. CAD standard) allowing these connections to be kept and used on long term basis, we can assume that it bridges the gap and covers the data loss, which are encountered during switching life cycle stage of a building from one to another.



Souhrn podle oddělení

Legenda	Kód útvaru	Kód oddělení	Celkový počet	Plocha celkem	Průměrná plocha
🟦	ACCESSORIES	MARKETING	1	183,36	183,36
🟦	EXECUTIVE	MANAGEMENT	5	1 031,02	206,20
🟥	SOFTWARE APP.	ENGINEERING	6	733,14	122,19
🟩	SOFTWARE SOLN.	ENGINEERING	6	870,43	145,07
			18	2 817.95	Celkem

Figure 13 - Archibus - departments divided by colours   Source: (IKA DATA: Space management)

Recently there is a lot of talk about the transition to modelling properties using technologies collectively known as BIM. There are also evaluated condition survey projects using 3D laser scanning of internal and external space of building, by obtaining a “point cloud” and its subsequent processing in BIM CAD software to obtain at least partial BIM model. While CAFM system Archibus is ready to take advantage of BIM modelling, in current BIM data structures the most important data are not included (eg. Leases, history of space usage, etc.) By adding this data to BIM data structures arises so called EIM (Enterprise Information modelling) and their acceptance and management is the basis for new system of space governance, which is based on the 3D model including data describing the technical and economical characteristics of structural elements. (*IKA DATA: Space management)*

These data can be used not only for classical KPI, their time series trends and other statistical variables based on surfaces, but also for analyses and simulations based on volumes, such as thermal technical and economical calculations. Calculation of return of building “insulation” envelope can be built on much more credible data so valid data for decision-making across the entire real estate portfolio can be obtained. (*IKA DATA: Space management)*

3.5.2 **Floor Plan Mapper- http://www.floorplanmapper.com**

Floor Plan Mapper is an application intended to take care of the basic issue of locating people, printers and meeting rooms inside an office building.

Floor Plan Mapper is a web based application hosted entirely on your own web servers. We do not offer a Software as a Service (SaaS) solution at this point.

Floor Plan Mapper fully integrates with the Windows Active Directory. Basically, Floor Plan Mapper ships with an administration tool allowing you to assign a unique ID to an XY location on your floor plan. You then take that unique ID and enter it into your AD (for whatever object you wish to display on the floor plan). You can use a custom AD field, or one of the pre-defined fields. Then, when you search for that object using Floor Plan Mapper the object will show up in the correct location. To move the object (printer, person, meeting rooms, etc) all you need to do is enter a new ID into the AD. Floor Plan Mapper does not write to the AD, only read. Floor Plan Mapper can display data from any AD field including the thumbnail photo field (employee photo).(*FloorPlanMapper: Frequently asked questions*)

Floor Plan Mapper integrates with Microsoft SharePoint Calendar/Room Booking.

The Floor Plan Mapper cost is based on the number and complexity of Floor Plans. The usual cost per floor plan is around $150 per floor plan. In the event numerous floor plans are involved (>10), discount pricing applies. There are no licensing fees associated with Floor Plan Mapper. SharePoint employee directories are an efficient portal for locating employee information. However, SharePoint only provides a single field to display information with regards to where an employee sits. Floor Plan Mapper can be embedded into SharePoint via web part. This integration provides the ability to actually display an employees location on an interactive floor plan, right from SharePoint. Enabling SharePoint with interactive floor plans to help locate meeting rooms and employee locations greatly adds usability and value to your SharePoint investment. (*FloorPlanMapper: Floor Plan Mapper with microsoft sharepoint*)

3.5.3 **POC System**

POC (Point Of Contact LTD) is a software and service company, developing data visualization systems, managing yielding real-estate, office space and professional resources. POC develops unique systems that present and manage multi-layers of information, on top of AutoCAD drawings, designated for HR and Operations use. POC solutions are offered in a SaaS model. (*POC System)*

The company offers 2 main products:

1. **Space Management System**, designed especially for corporates that hold and manage mass office space or yielding commercial property, such as Realty companies, Mall owners, Commercial Centers, Banks, Insurance companies, governmental and municipal organizations.
2. **Seating Allocation and Objects Management System,** designed for mid-to-large scale companies, facing challenges of continuous transition in employees' seating arrangements and the constant need to optimize their office space. (*POC System: Products*)

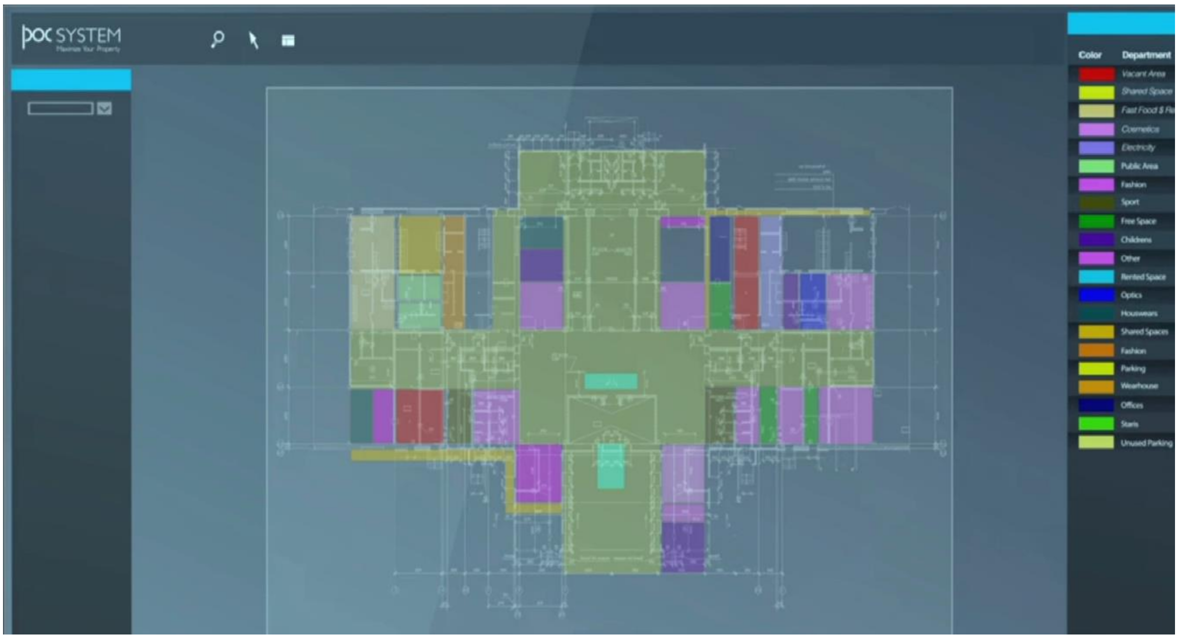
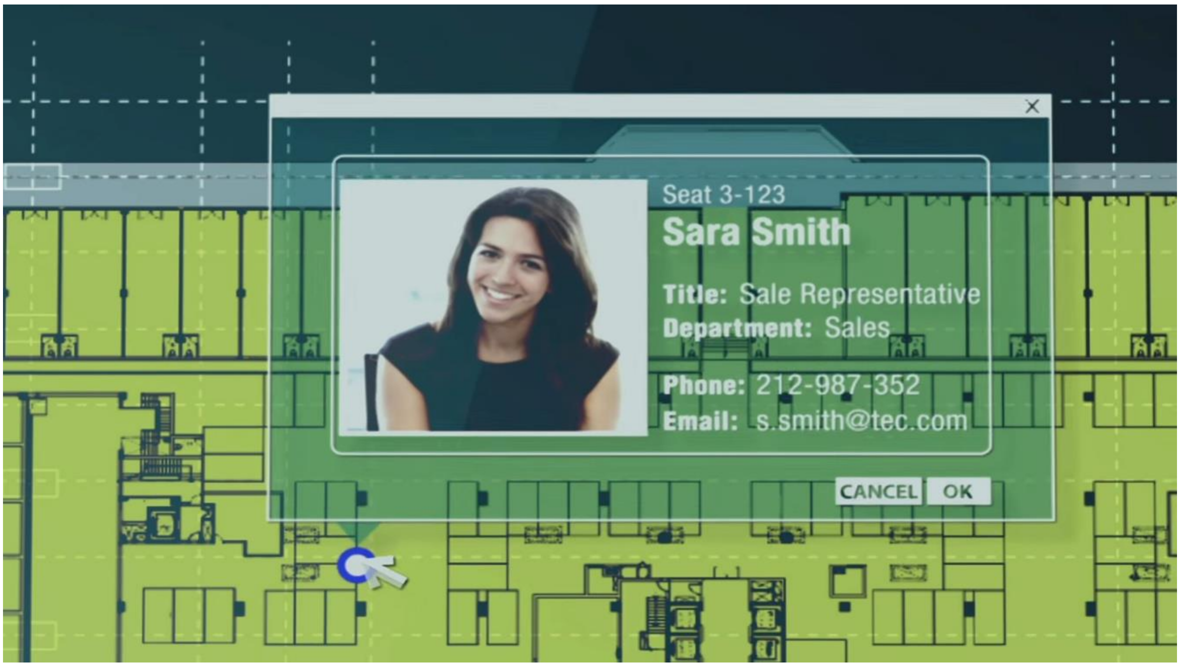


Figure 14 - POC Space Management System Overview **Source: (*POC System: Space Management System)***



Seat 3-123

Sara Smith

Title: Sale Representative
Department: Sales

Phone: 212-987-352
Email: s.smith@tec.com

Figure 15 - POC Seating Allocation system **Source: (*POC System: Seating Allocation Solutions)***

3.5.4 **OfficeSpace Software - SaaS & Hosting**

OfficeSpace Software is the perfect solution for small to mid-sized organizations looking to address the challenges associated with allocating workspace. OfficeSpace Software is a comprehensive, intuitive space and move management system that utilizes cutting-edge technology that helps companies effectively manage everything from day-to-day employee relocations to large-scale organizational moves.

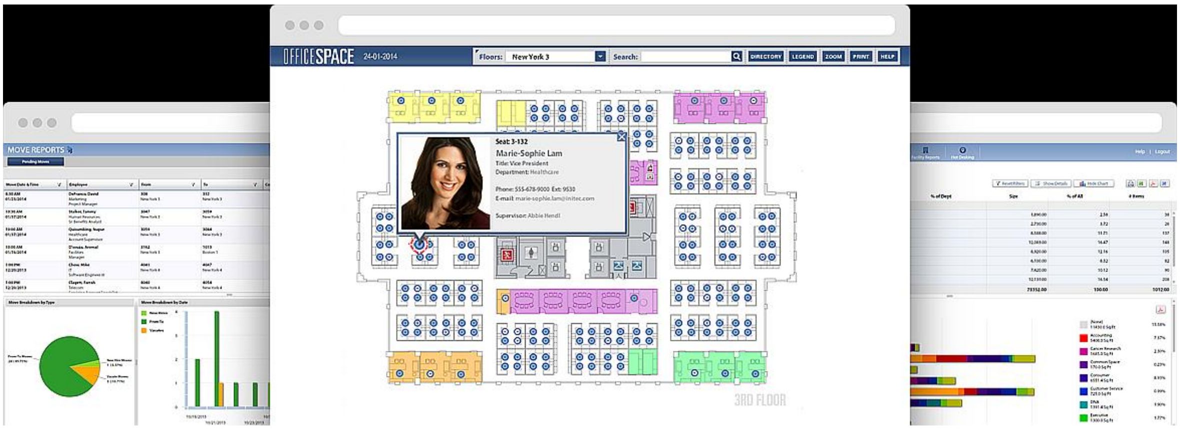
OfficeSpace Software is a powerful visual tool that not only manages employee moves but also tracks rooms, cubicles and other spaces and all their related assets like phones, computers, copiers, etc. Its friendly, web-based interface offers a centralized repository for critical workspace data that seamlessly integrates with existing complementary solutions.

Visual Directory is an especially useful component that allows users to locate coworkers and their contact information as well as resources like equipment and spaces company-wide. Individual and group moves can be planned in seconds with the solution's streamlined workflow, which also offers automated move notification emails to all involved departments.

OfficeSpace Software provides robust on-demand or auto-generated reports that show scheduled, completed and archived moves that give administrators the visibility they need to make informed move and allocation decisions. (Feintzeig,2013)

Pricing for the solution is based on the number of seats, with professional services for setup, installation and training. The software can be used across a variety of industry segments, including banks, government entities, healthcare organizations, real estate and telecommunications firms. The OfficeSpace Software is recomended to any organization looking for a flexible, scalable space and move management solution.

SaaS & Hosting -Ultimate flexibility: cloud hosted or internally hosted in customer´s data center. (OfficeSpace Software. *Softwareadvice.com*)



Seat: 3-132
Marie-Sophie Lam
Title: Vice President
Department: Healthcare

Phone: 555-678-9000 Ext: 9530
E-mail: marie-sophie.lam@initec.com

Supervisor: Abbie Hendl

Figure 16 – preview of OfficeSpace Source: (OfficeSpace Software. *Softwareadvice.com)*

3.5.5 GISA - Facility Management

GISA – Facility management (hereinafter "GISA") allows to register arbitrary types of objects with spatial and descriptive information, and their management. Data from GISA can be vied in two ways. By using spreadsheet or map interface. Both are functionally linked together. Spreadsheet interface is written in the programming language PHP. Nette-framwork is used for coding and the data is handled by MySQL. However GISA understands all databases running on the database servers (Oracle, PostgreSQL). GISA also allow connection to an already existing type of such database. Spreadsheet interface is used to control the system and to display individual pages. Each page (a contract offer, event, documents, etc.) can easily be edited, have order and settings of columns changed, then the data can be filtered or exported eg. to xls. Map interface is written in JavaScript language and uses OpenLayers, GeoEXT and ExtJS libraries. A window with graphical information is the basis of the map interface. Foundations are the imported building plans or geodetical surveys. Additionally the map window can be connected to any WMS server so a valid cadastral map or orthophoto can be displayed. Map window allows distance measurement, quantifies contained data and also entering any new buildings in conjunction with spreadsheet interface, where at first it is necessary to define the type of object and its properties. Analytical tools are part of the map interface (emphasis rooms with Wi-Fi coverage, etc.), which can be defined by customers specific requirements.

The spreadsheet interface on the left links to information about registered buildings with all support functions are organized in a tree structure menu.

Objects in GISA are defined into four levels: area, building, floor, element (lounge, doors, windows, etc.) For each level of object or for each object itself infinite number of properties can be defined. For rooms GISA can carry information about the area, height, the number of data and electrical outlets, Wi-Fi coverage, the type of floor coverage, etc. A user with appropriate privileges can define these properties. Selected objects like electrical outlets can be place into the map interface. List of descriptive information for relevant objects is displayed after clicking on selected floor. There is a link for graphical display in the map interface for each object. (GISA -fm

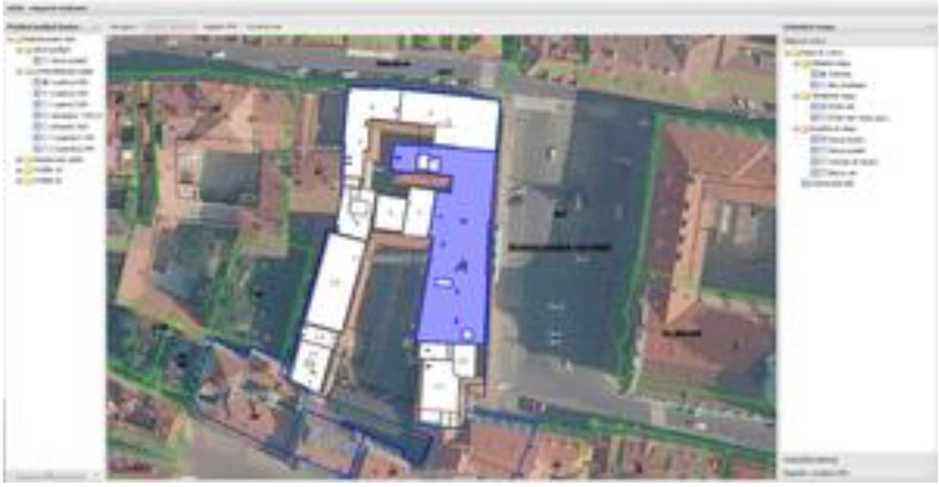
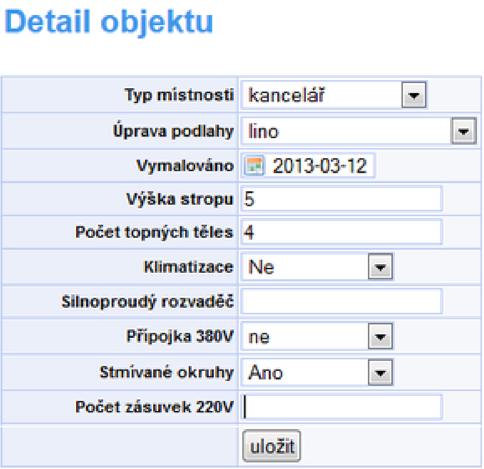


Figure 17 – GISA FM main window overview Source: (GISA -fm)



Detail objektu

Typ místnosti	kancelář
Úprava podlahy	lino
Vymalováno	2013-03-12
Výška stropu	5
Počet topných těles	4
Klimatizace	Ne
Silnoproudý rozvaděč	
Přípojka 380V	ne
Stmívané okruhy	Ano
Počet zásuvek 220V	
	uložit

Figure 18 – Object detail Source: (GISA -fm)

Through the map interface there is also a possibility to display or edit an object information by selecting it. Every record has possibility of setting its description attributes through GISA.

Besides functionalities mentioned above GISA system also offers evidence of photographs of individual objects or building floor plans files. Based on individual specific requirements it is possible to extend the system for a new functionality. Final cost for GISA system is set after individual consultation with a customer. The cost is derived from size and number of registered buildings and from complexity of database populating method.

The final price will be a sum of following items:

Own application

Graphical data import

Application hosting (rental server maintenance and upgrades)

The following table shows the approximate prices for our services.

Table 2 - GISA - fm - price list Source: (Cenik FM)

Number of buildings	1-4	5-10	More than 10
Number of users	**neomezený**	**neomezený**	**neomezený**
Cost of GISA – fm application system [CZK]	24 900	29 900	34 900
Graphical data import from digital vector format [CZK] *)	10 000	15 000	20 000
Graphical data import from analog format [CZK] *)	20 000	25 000	30 000
Total cost	**24 900 - 34 900**	**34 900 - 49 900**	**49 900 - 74 900**
*) cost for graphical data import can vary depending on complexity of demanded import (floor size and number of imported layers)			

Monthly maintenance and GISA system upgrade [CZK/mnth] This item mainly contains: server rent, helpdesk, system maintenance, continuous development of system core and superstructure for facility management	**500 a více**

Mentioned prices are without VAT.

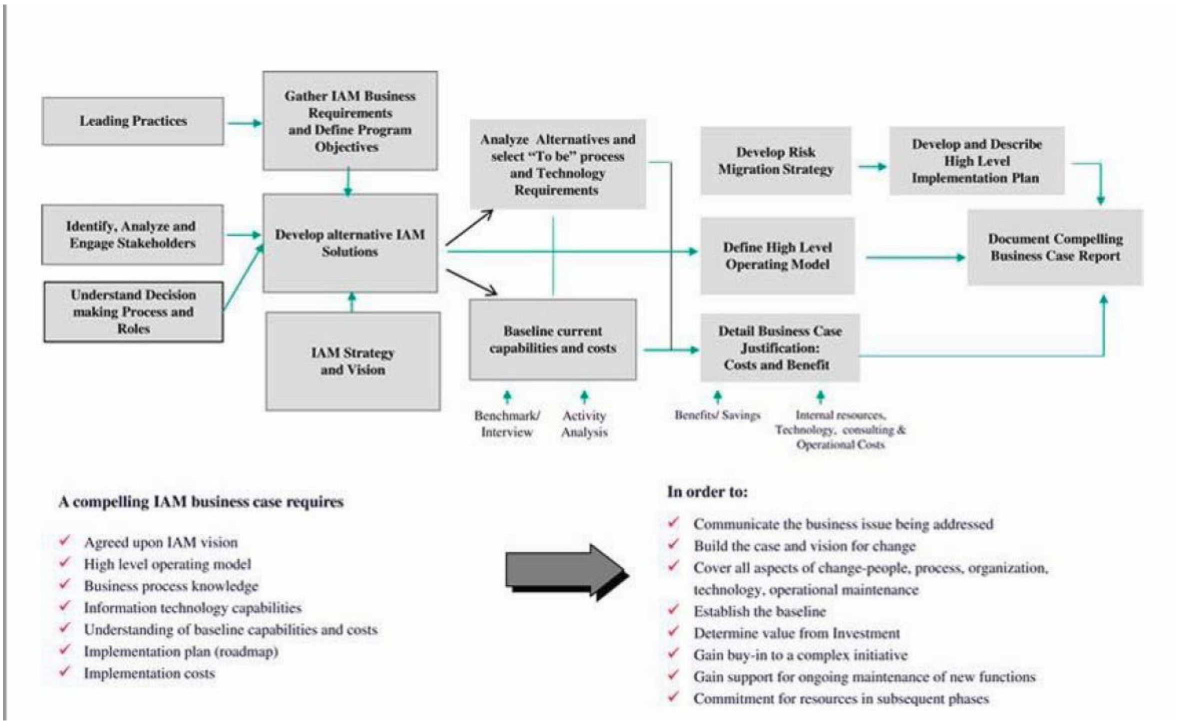
The cost also includes potential construction or simplified object measurement, which the company also offers.

3.5.6 Conclusion

The IKA DATA and GISA solutions are most relevant for this project mainly because they are top Czech FM system suppliers. ARCHIBUS solution of IKA DATA is proved by the Gartner research from chapter 3.2.4 to be amongst the top Market leaders, its features exceed any competitors on Czech market. These two companies will be approached with cost calculation for their solution of the project so the comparison with own application can be made.

3.6 A Strategic Approach to Developing an IAM Business Case

An effective IAM business case can be developed by understanding certain business and IT stakeholders’ business objectives and values and then structuring your IAM program to respond to them. The ultimate objective of the business case is to demonstrate to executive decision-makers that the IAM program is a worthy investment. The approach you ultimately decide to use for developing your IAM business case will depend on your specific organizational roles, your experience with engaging key stakeholders, your business culture, and finally your IAM vision, program goals, and objectives. There is a common framework that has proven to be successful in developing compelling IAM business cases. Typically, we have seen IAM program owners follow an approach similar to the steps outlined in Figure 19. (Osmanoglu, 2014, p. 27-28)


Leading Practices
Gather IAM Business Requirements and Define Program Objectives
Identify, Analyze and Engage Stakeholders
Understand Decision making Process and Roles
Develop alternative IAM Solutions
IAM Strategy and Vision
Analyze Alternatives and select "To be" process and Technology Requirements
Baseline current capabilities and costs
Benchmark/ Interview
Activity Analysis
Develop Risk Migration Strategy
Develop and Describe High Level Implementation Plan
Define High Level Operating Model
Document Compelling Business Case Report
Detail Business Case Justification: Costs and Benefit
Benefits/ Savings
Internal resources, Technology, consulting & Operational Costs

A compelling IAM business case requires

- ✓ Agreed upon IAM vision
- ✓ High level operating model
- ✓ Business process knowledge
- ✓ Information technology capabilities
- ✓ Understanding of baseline capabilities and costs
- ✓ Implementation plan (roadmap)
- ✓ Implementation costs

In order to:

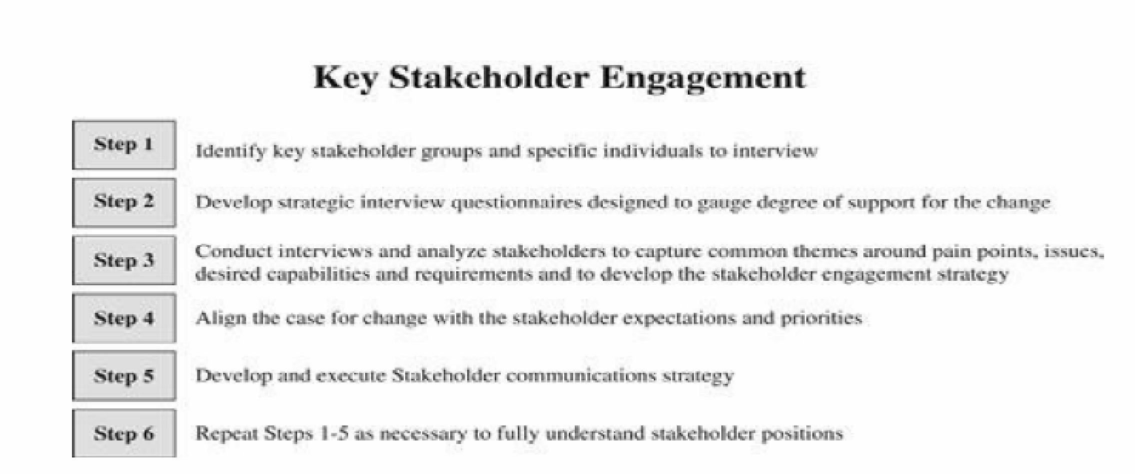
- ✓ Communicate the business issue being addressed
- ✓ Build the case and vision for change
- ✓ Cover all aspects of change-people, process, organization, technology, operational maintenance
- ✓ Establish the baseline
- ✓ Determine value from Investment
- ✓ Gain buy-in to a complex initiative
- ✓ Gain support for ongoing maintenance of new functions
- ✓ Commitment for resources in subsequent phases

Figure 19 IAM business case developement approach Source: (Osmanoglu, 2014, p. 28)

The IAM business case process flow in Figure 1.1 shows a high level set of process steps that, if followed, will raise your chances for developing a winning IAM business case. What follows is a walkthrough of each of those steps, a discussion of the key activities of each step, and some examples of the important elements which should be derived from each step.

3.6.1 **Identify, Analyze, and Engage Key Stakeholders**

One of the first and most critical steps is to identify and engage your key decision-making stakeholders in the process. The principle behind this is that these individuals are typically influencing all spending decisions and therefore are the best representatives of the strategic values of the company. By engaging them early in the process, you will be better able to understand what issues are important to your key stakeholders. You can align with their priorities and be in a position to structure your messaging with how they absorb information. How much detail is enough for them, how much it too much? What role do they play in the decision-making process? What is the organizational appetite for change? Before you even start the business case development, you should spend time understanding the decision-making and funding processes your organization uses for business cases, who is involved, and what roles they play. This information will help you target your audience in the right form, with the right level of detail and focus on the right issues to win a positive outcome. Implementing an IAM program impacts virtually every part of the business and IT organization. Sometimes it impacts customers and business partners external to your organization. Understanding the priorities and motivations of each of these internal and external stakeholders will help you to craft the business case value proposition. Early analysis of key stakeholders needs will assist in developing the appropriate communications strategy to obtain buy-in. In Figure 20, the high-level process for engaging key stakeholders is describe. (Osmanoglu, 2014, p. 28-29)



Key Stakeholder Engagement

Step 1	Identify key stakeholder groups and specific individuals to interview
Step 2	Develop strategic interview questionnaires designed to gauge degree of support for the change
Step 3	Conduct interviews and analyze stakeholders to capture common themes around pain points, issues, desired capabilities and requirements and to develop the stakeholder engagement strategy
Step 4	Align the case for change with the stakeholder expectations and priorities
Step 5	Develop and execute Stakeholder communications strategy
Step 6	Repeat Steps 1-5 as necessary to fully understand stakeholder positions

Figure 20 - IAM stakeholder engagement Source: (Osmanoglu, 2014, p. 29)

The objective of this step of the process is to establish a dialog with each primary stakeholder and decision-maker to allow you to proactively manage the outcome. The chart in Figure 21 provides a useful tool for characterizing your stakeholders and modelling the level of communications necessary to most effectively engage them.

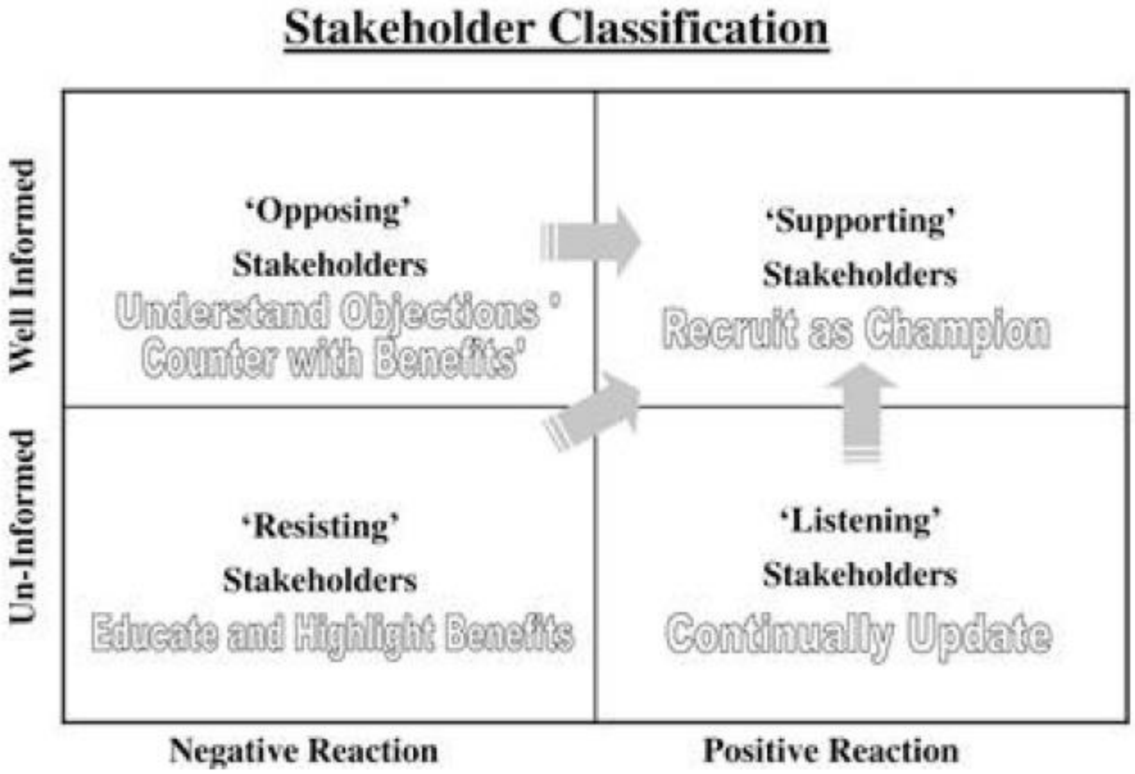


Figure 21 - IAM stakeholder classification Source: (Osmanoglu, 2014, p. 29)

3.6.2 Develop Risk Mitigation Strategy

Every project comes with risks. Not acknowledging them or planning for them will only make the program vulnerable to those risks and potentially put the program at risk of failure. How thoroughly you acknowledge your business case risks and how you plan to mitigate the impact of any realized risks will make your business case stronger. There is a number of risk categories you should consider when thinking about your business case risks. Categories of risk include the following: People/rare skill risks: The risk that you won't have the proper skill sets to design, implement, or maintain the technology. Cultural and process risks: The risk that changing long-standing processes and practices in your organization will be met with resistance and circumvented. You will likely need the support at the highest levels of leadership in your organization to be successful with your IAM program. Technology risks: You will be introducing new technology to the organization; will it integrate well with other solutions? Will it operate as you expect? Project or program risks: Implementing an IAM solution is a long and complex process. Strong program management discipline is required to detect and respond to issues in a timely manner to keep the project on course. As you identify each risk, consider its likelihood and impact. If a risk is realized, what is the impact to the business or your program? Finally, what will you do to either avoid or mitigate the impact of the risk? Summarizing each identified risk, it’s associated likelihood, impact, and the mitigation plan into a matrix, as shown in Figure 1.5 is an effective way to communicate this significant amount of risk information. (Osmanoglu, 2014, p. 33)

#	Risk Cathegory	Risk Description	Likelihood	Impact	Impact Description	Counter Meassures
1	Sustainable Benefits	Unable to realize the savings of FTE´s, as only part roles can be transfered	M	H	Level of benefits is lower than expected: Project not approved: negative key stakeholder perception	Seek ways of changing the profile of future jobs: look to share resources across BU´s and functional teams
2	Sustainable Benefits	Clear visibility on where benefits will come from	L	H	Project cancellation: lost project investments: negative effect on key stakeholder perception	Form steering committee with representation and responsibility for aligning project to corp strategy: review strategy at key project milestones
3	Sustainable Benefits	Insufficient data to benchmark and baseline the operation	M	H	Loss of confidence in the business case if errors, incorrect or incomplete data is used to drive benefits	Include as many BU´s in the data collection exercise. Assign ownership, supplement with workshops to understand how the process actually works: use HR data to validate
4	Project Governance	Case for change not sufficiently built or bought into	M	H	Loss of confidence in the initiative and not supported by business: Project not approved	Build a clear rationale for the project supported by a robust business case: communicate widely with road shows: maintain regular contact with the sponsors and business

5	Project Governance	Project objectives and scope are not clarified or changed	M	M	Medium impact as can be managed: difficult to plan and mobilize team: impacts to project delivery costs and timing	Clear scope definition and agreement as outcome of business case phase: establish scope management process as part of overall programme management
6	Project Governance	Project lacks clarity and direction	M	M	Medium impact as can be managed: difficult to plan and mobilize team: impacts to project delivery costs and timing	Establish clear project charter: emphasis on strong programme management and regular communication
7	Project Governance	Project does not have adequate / correct sponsorship	L	H	Delays: failure to gain key support: failure to achieve full benefits	Engage required sponsorship to achieve maximum benefits: gain sponsor commitment
8	Mobilization Risks	Unable to commit full-time skilled or appropriate resource to the project team	H	H	More difficult to gain access to company knowledge or project team resourced with wrong skill sets	Sufficient, knowledgeable team resource must be provided: possible to sub contract other project skills: resource must be committed full-time on team

Table 3 - Sample - business case risks Source: (Osmanoglu, 2014, p. 34)]

Depending on the severity of risks identified and the impact they might have on your decision making process, it can be decided whether to include the risk matrix as a part of the body of the business case or just make reference to it as one appendix.

3.6.3 **Detail Business Case Justification: Costs and Benefits**

This is the heart of the business case. Here you will link the values intended by IAM program to strategic business needs and show how the requested investment will manage risk, improve efficiency, and deliver other meaningful business value to the organization. You will need to understand and communicate your justification so it touches on each decision-maker 's priorities. Your statements should include enough detail to convince your decision-makers that the proposed IAM program is a good investment but not overwhelm them with detail. A technique that has proved successful is to summarize justifications and financial information in the body of the business case and create references to more detailed supporting information in an appendix. Key questions to answer in this step may include the following:

- How will the IAM project enhance business capabilities?
- How will it enable the business?
- What risks are we mitigating?
- What will our regulatory posture be at the end of the project?
- How will IAM service improve at the end of your project? What will we be able to do upon completion of this project that we weren't able to do before?

These are a few of the potential justifications for an IAM business case. The steps you have completed up to this point should provide a clear understanding of what is important to the business stakeholders and decision-makers. A careful selection of right justification is what separates a business case that resonates with all of your stakeholders from a business case that doesn't. (Osmanoglu, 2014, p. 34)

4 Practical Part

The practical part focuses mainly on analyzing current state of employee and printer locating solution including process analysis. Then, a web based application will be proposed based on the analysis. The project is developed according to the waterfall system development life cycle, which consists of 5 phases listed below. (Web Design, 2014)

1. Initiation phase
2. Definition phase
3. Design phase
4. Development phase
5. Implementation and maintenance phase

The waterfall model was selected because the project phases does not overlap the project is small with very specific requirements and during the development phase, there is no need for customer interaction. Methodology from chapter 3.6 was utilized on developing the business case. Initiation phase

Purpose of this project is to enhance process workflow around locating certain identities mainly printers and employees. Currently, any ordinary employee from ICZ company does not have an opportunity to locate his colleagues or printers without having connections to facility management team and their building floor plans. The only solution for locating identities is to call colleagues who might know the location.

The goal of the project is to create a system combining ICZ office floor plans with database of employees and printers.

This system will be at disposal for any employee with access to the internal network and with an Active Directory account. However, main users will be the End-user Support Group members who need to locate the identities most of the time. Editing the application will be allowed only to specific users for ensuring data integrity.

The main content of the system will be a database of employees and printers working with a web interface showing building floor plans depending on selected floors or whom or what is the user searching for.

4.1 Definition phase

The task is to create a web based application working with floor plans for locating printers and employees default working location. Upon consultations with an IT manager and a programmer consultant, it was decided to use HTML5, CSS and Javascript for the application and MySQL for the database in the back-end. The application will receive data about employees and printers from SAP or Active Directory and will become a part of the company intranet.

4.1.1 Identify, Analyze and Engage Key Stakeholders

For this project, the IT department manager is the contract owner, main users will be the Facility Management Department consisting of a facility manager and his assistant who will be eligible to edit main floor plans – tables, chairs, reconstructions of rooms. Moreover, the assistant will create calculations of floor space per department as an input for Accounting Department. Thedisplay and look up features will be mainly used by the end user support, but will be accessible to all other users.

The task from the contract owner is to create a web based system for locating printers on each floor and also to locate the working position of an employee.

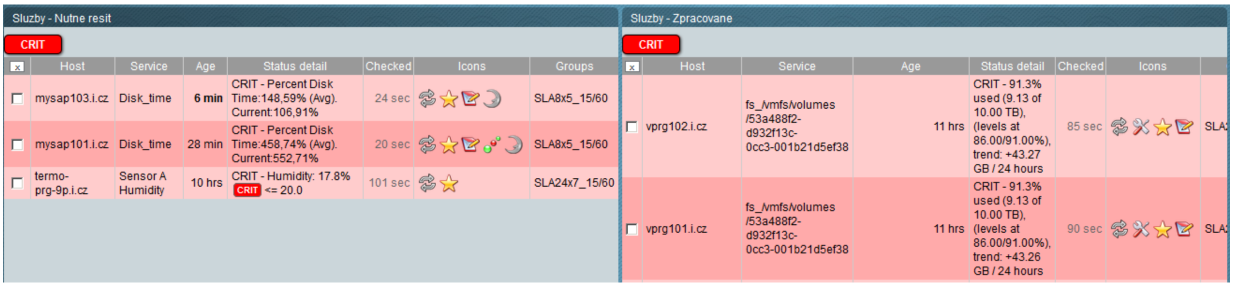
Upon consultations with the facility manager, for a successful project, there will be need for creating user-friendly environment for editing working space. Meaning there will be possibility for editing inner work space including walls. Critical information from a facility manager is that some employees move quite often which makes very hard to keep track of that movement. The idea is that section assistants will be in charge of editing employee work locations of his or her section. Facility Management Department is now the only department having direct access to the building floor maps. They use AutoCAD and MS-Visio for editing current building plans also with current default seating of employees. The problem is that the work becomes quickly outdated due to frequent changes and this process is also unsupported. Meaning that there is no official business process behind.

MS-WIN group is responsible for administering of Microsoft products like operating systems, Active Directory (AD), printer servers, accounts for ServiceDesk application, which are projected from AD. By consulting one of the administrators there was possibility of using active directory as an information source for the web application database. Specifically by accessing attributes of users and printers.

End-user Support group interests are represented by the head IT manager who is a direct supervisor of this group.

4.1.2 Business process analysis

Currently, the printers are monitored in special web interface along with other internal network components. The interface offers monitoring of acknowledged and unattended services, which are in critical state, and enables searching for all monitored devices, which are in green status.



Sluzby - Nutne resit

CRIT

☒	Host	Service	Age	Status detail	Checked	Icons	Groups
□	mysap103.i.cz	Disk_time	**6 min**	CRIT - Percent Disk Time:148,59% (Avg). Current:106,91%	24 sec	⟳ ★ ✎ ☾	SLA8x5_15/60
□	mysap101.i.cz	Disk_time	28 min	CRIT - Percent Disk Time:458,74% (Avg). Current:552,71%	20 sec	⟳ ★ ✎ ● ☾	SLA8x5_15/60
□	termo-prg-9p.i.cz	Sensor A Humidity	10 hrs	CRIT - Humidity: 17.8% CRIT <= 20.0	101 sec	⟳ ★	SLA24x7_15/60

Sluzby - Zpracovane

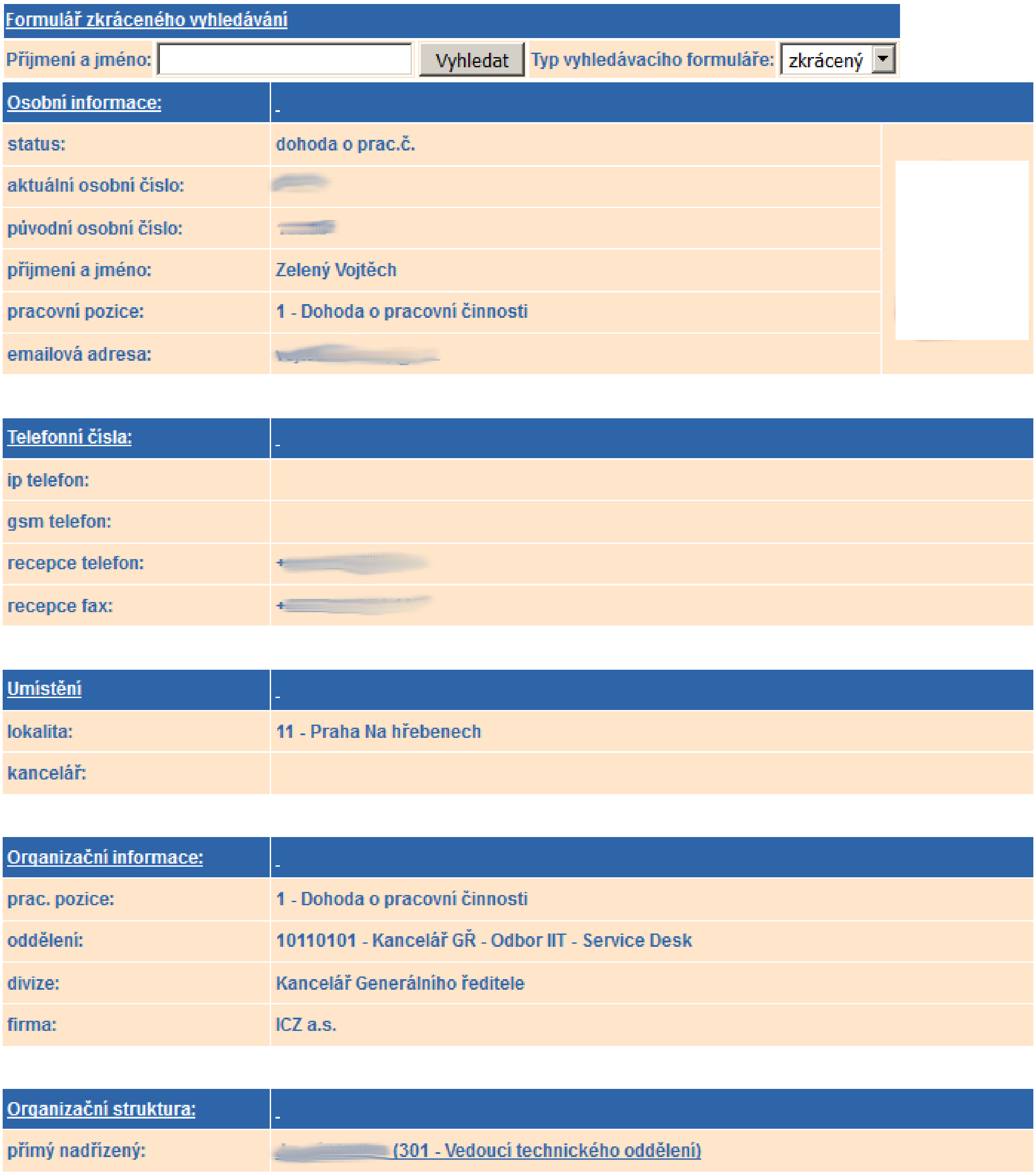
CRIT

☒	Host	Service	Age	Status detail	Checked	Icons	
□	vprg102.i.cz	fs_/vmfs/volumes /53a488f2-d932f13c-0cc3-001b21d5ef38	11 hrs	CRIT - 91.3% used (9.13 of 10.00 TB), (levels at 86.00/91.00%), trend: +43.27 GB / 24 hours	85 sec	⟳ ✂ ★ ✎	SLA
□	vprg101.i.cz	fs_/vmfs/volumes /53a488f2-d932f13c-0cc3-001b21d5ef38	11 hrs	CRIT - 91.3% used (9.13 of 10.00 TB), (levels at 86.00/91.00%), trend: +43.26 GB / 24 hours	90 sec	⟳ ✂ ★ ✎	SLA

Figure 22 - Current network device monitoring web application Source: (accesed from own ICZ account)

Figure 22 shows what information is currently monitored. It is the host name, service name, age of the critical status, brief information about the status, when the last check of the service was executed, icons showing brief info about notifications or acknowledgement and the last column describes the type of the Service Level Agreement. The problem is that this solution does not provide any option for physical locating of the devices.

Information about employees can be viewed in via the company´s intranet web site.



Formulář zkráceného vyhledávání

Příjmení a jméno: [ ] Vyhledat Typ vyhledávacího formuláře: zkrácený ▾

Osobní informace:	_
status:	dohoda o prac.č.
aktuální osobní číslo:	[redacted]
původní osobní číslo:	[redacted]
příjmení a jméno:	Zelený Vojtěch
pracovní pozice:	1 - Dohoda o pracovní činnosti
emailová adresa:	[redacted]

Telefonní čísla:	_
ip telefon:	
gsm telefon:	
recepce telefon:	+[redacted]
recepce fax:	+[redacted]

Umístění	_
lokalita:	11 - Praha Na hřebenech
kancelář:	

Organizační informace:	_
prac. pozice:	1 - Dohoda o pracovní činnosti
oddělení:	10110101 - Kancelář GŘ - Odbor IIT - Service Desk
divize:	Kancelář Generálního ředitele
firma:	ICZ a.s.

Organizační struktura:	_
přímý nadřízený:	[redacted] (301 - Vedoucí technického oddělení)

Figure 23 - intranet user information Source: (accesed from own ICZ account)

The information such as personal information, telephone numbers, location, organizational information or organizational structure can be found on the intranet. This data is exported from Active Directory. Current solution also does not offer option for searching specific location of an employee. The only options are to either go directly to SAP, which can be accessed only by SAP Department, or to go directly to the Active Directory database, which can be accessed only by MS-WIN group, Helpdesk Department and by IT managers.

Service Desk is an application for management of customer requests and incidents. It serves as a contact place between users and service providers. The Service Desk is used for handling processes connected with incident management and request resolving with the aim to restore regular flow of service as soon as possible. Requests are handled in form of tickets. Every ticket created by an end-user[2] should be taken over by a researcher who is solving the ticket. Every researcher should be member of a working group.

Intranet serves as a company´s internal website for publishing documents, news, tutorials and for searching for basic employee information.

Currently, the printer information is stored in SAP, from which it is exported to Active Directory. All printers can be managed through their own web page and all printers and their services are monitored in one webpage which is monitored by company´s helpdesk.

4.1.2.1 Printer processes

When a new printer arrives to the company it needs to be set up and connected on selected location by End-user Support group. They create two tickets in the Service Desk application. One for Unix group which adds printer´s MAC address to dhcp, and second one for MS-WIN group which is responsible for adding printer on the print server, installing drivers on it, setting up configuration for snmp for monitoring and smtp for scanning into mailbox.

The process of removing printer consists of uninstalling it from print server by MS-WIN group and then physically removing it from its location by the End-user Support group.

4.1.2.2 Employee processes

For a new employee in the Czech branch, the process is as following:

1. HR department creates a ticket for opening access like Active Directory account, mail account, telephone for the new employee.
2. The ticket is automatically directed to MS-WIN which creates an Active Directory account and email, and then redirects the ticket to Operators group.
3. Operators redirect the ticket to the Facility Management group. This group creates telephone line and selects which IP telephone will need to be set up. Then it redirects the ticket to operators.
4. Operators move the ticket to IPT-Alcatel group which installs the line into IP telephony. Then they redirect the ticket to operators.

[2] In this case it can be employee or a customer

5. Operators moves the ticket to End-user Support group, which picks up IP telephone on logistics, installs it on end user´s location and closes the ticket.

The process is different for Slovakian employees in the Slovakian branch. The ticket from HR group is transferred to MS-WIN group then redirected to operators who only check if all accesses were created and then closes the ticket.

For external users the process is also different in a few ways:

1. Supervisor, HR department of security manager creates a ticket for opening access for extern.
2. If the ticket is not automatically redirected to ICZ-External users group, the operators will do that and set the state of the ticket to "for approval". If the ticket was created by security manager, it is automatically considered as approved. The ticket is moved to operators group.
3. After the ticket is approved, operators move it to MS-WIN group, which creates all approved accesses. The ticket is moved to operators group.
4. When the ticket is returned to operators group, operators do the following:
    a. If an email and certificate is approved, operators contact the extern, explains how the extern can generate his/her own certificate and if necessary operator can generate the certificate personally and send it to the extern via a secure combination of email and password over SMS.
    b. If a VPN access is approved, operators move the ticket to End-user support group and ask for antivirus check of the extern laptop, VPN client installation and the certificate installation. After the installation, the End-user support closes the ticket.

For quitting employees the process is also defined:

For Czech employees:

1. HR department creates a ticket for cancelling accesses.
2. If the ticket is not automatically redirected, operators group will move it to MS-WIN group.
3. Helpdesk operators revoke all user´s certificates and check if anybody of the cancelled users had access to the server room, if yes operator informs helpdesk supervisor to edit server room access list.
4. Operators move the ticket to UNIX group.

5. After the ticket returns, operators move it to APP-PostSignum group for revocation of PostSignum certificates.
6. After the ticket returns, operators redirect it to End-user Support group for physical disconnection of an IP telephone. The ticket is moved back to operators.
7. Operators move the ticket to IPT-Alcatel group for revoking the line on telephone exchange. The ticket is moved back to operators.
8. The ticket is moved to Facility Management group for deleting phone numbers of lines in IPT user list. The ticket is moved back to operators.
9. Operators close the ticket.

For Slovakian employees the process is less complicated:

1. HR department creates a ticket for cancelling accesses.
2. If the ticket is not automatically redirected, operators group will move it to MS-WIN group.
3. Helpdesk operators revoke all user´s certificates.
4. Operators move ticket to APP-PostSignum group for revocation of PostSignum certificates. The ticket is moved back to operators.
5. The ticket is moved to UNIX group.

For external users the process is as following:

1. HR department creates a ticket for cancelling accesses.
2. Operators move the ticket to Extern group for cancelling of user in SAP by security managers.
3. After the ticket returns operators move it to MS-WIN group. The ticket is moved to operators group.
4. Helpdesk operators revoke all user´s certificates.
5. Operators move ticket to APP-PostSignum group for revocation of PostSignum certificates. The ticket is moved back to operators.
6. Operators redirect the ticket to UNIX group.

4.1.3 Business Case Justification: Costs and Benefits

For successful business case justification all relevant questions from chapter 3.6.3 were answered.

The business will be enhanced from three different views. From HR perspective this application will significantly increase new employee company process adaptation. From service providing perspective the process of finding identity will increase from 1-3 minutes (approximation of one or two phone calls) to maximum of one minute. Next the process of entering a location of a new identity into the system will have increased time from days to minutes (Currently FM team saves the location sometimes and updates it on ad-hoc basis.) The effectivity of employees will be ensured even in more difficult conditions. Meaning substituting employees for sick colleague on different office location in different city will not have such problems with familiarizing in a new environment. Last view on the business enhancement is form information management perspective. The process especially for printers will be codified. Meaning there will be a possibility of defining KPI for displaying how effective is the service management.

The business will be enabled by using web interface instead of the need to call or talk to other employees. The process of implementation and maintenance phase will be described in chapter 4.4.

Because facility management team currently does not work in ServiceDesk system, their actual work is currently hard to report. Especially in terms of company floor maps and employee seating.

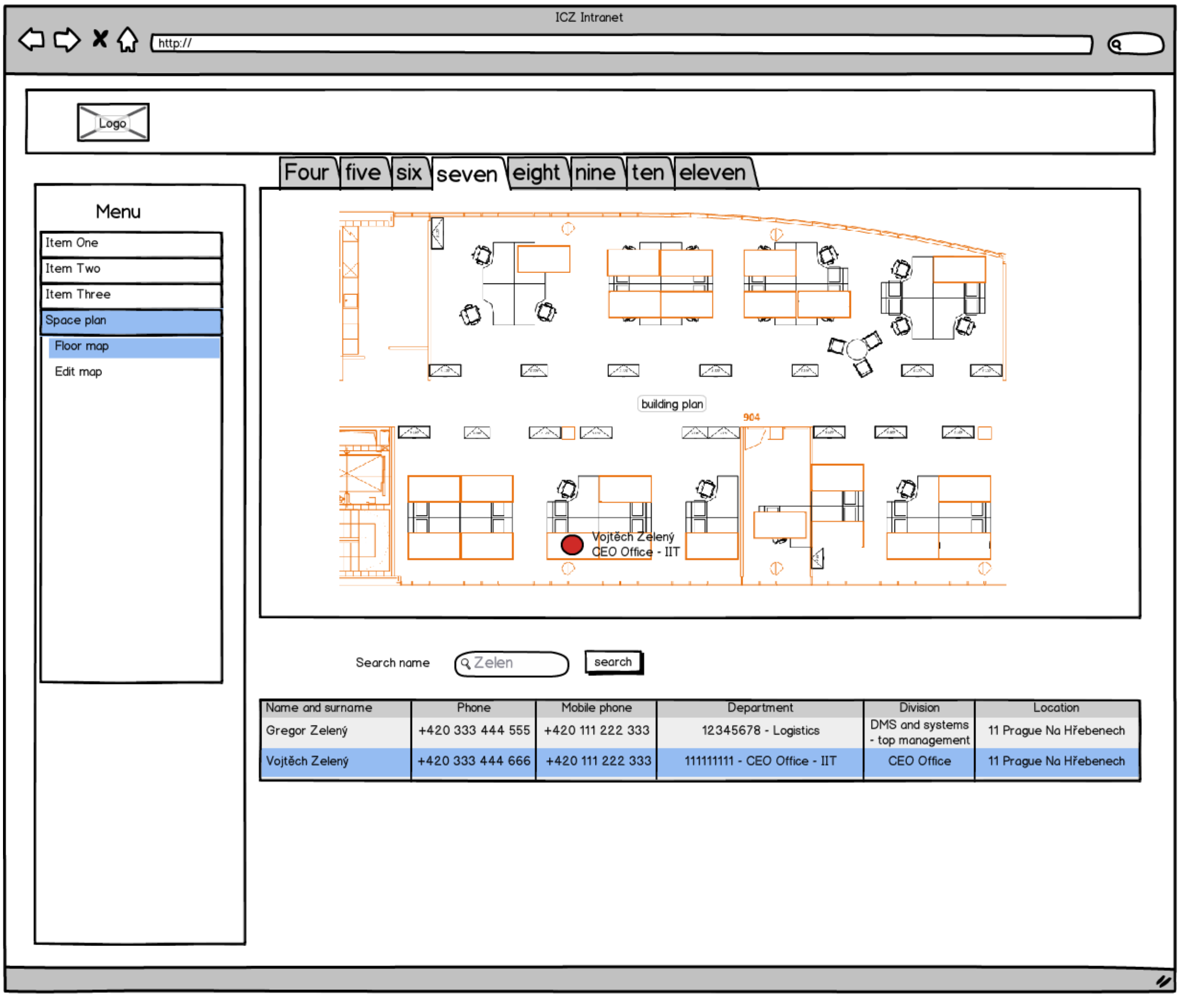
At the end of the project the service will improve delivery times and increase comfort by standardizing the whole process.

4.2 Design phase

Solution for the project will be done by putting the web application on the company´s intranet web page. One part of the application will be solution for searching and second part will be focused on editing the data.

4.2.1 Mockup design phase

Following mockups were created in trial version of Balsamiq mockups wireframing application.



Name and surname	Phone	Mobile phone	Department	Division	Location
Gregor Zelený	+420 333 444 555	+420 111 222 333	12345678 - Logistics	DMS and systems - top management	11 Prague Na Hřebenech
Vojtěch Zelený	+420 333 444 666	+420 111 222 333	111111111 - CEO Office - IIT	CEO Office	11 Prague Na Hřebenech

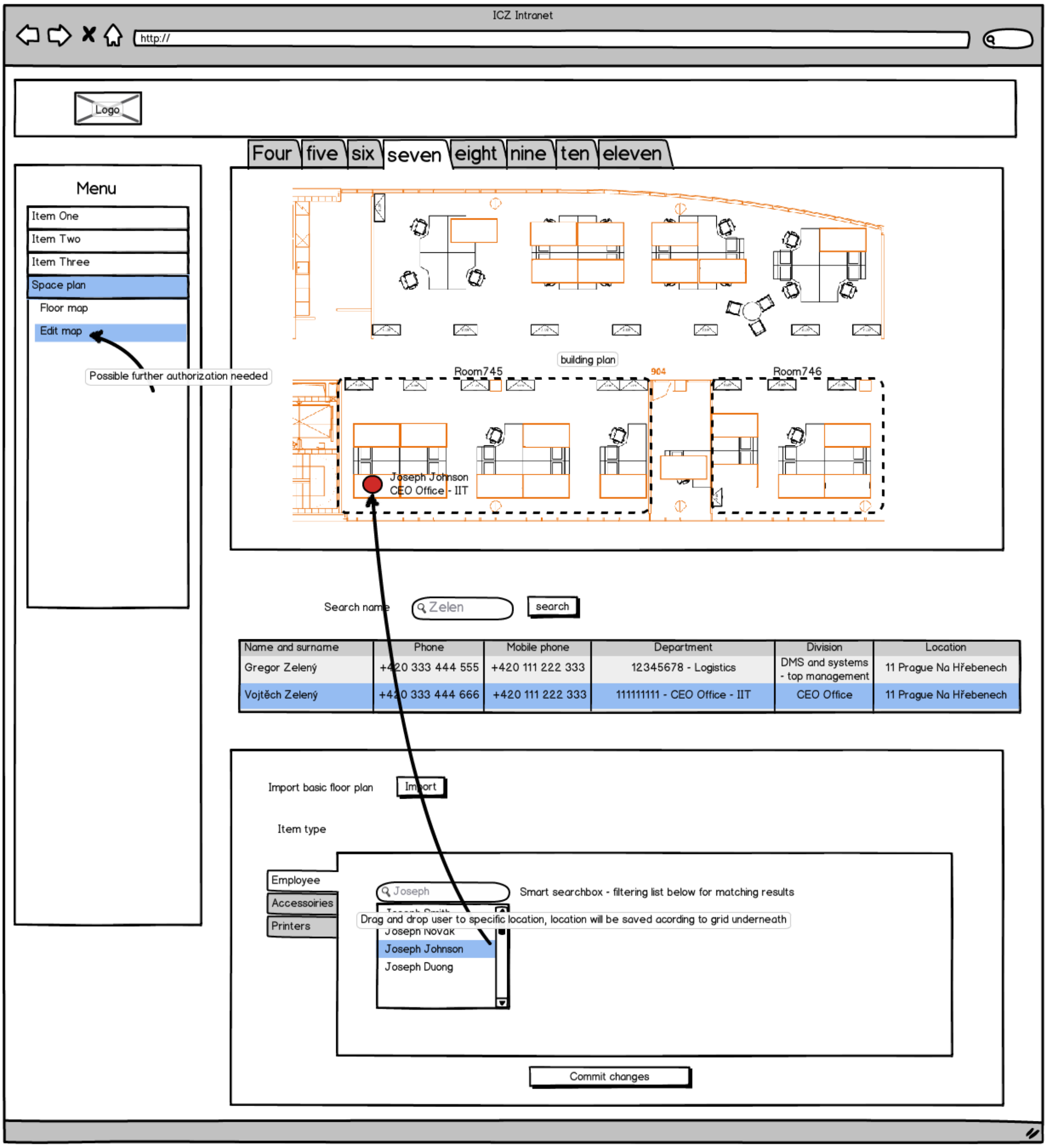
Figure 24 - main window of the application Source: (Own design)

Left menu and top bar with logo represent the ICZ intranet webpage, where the application will be located. Main part of the application will be the building floor map with possibility to switch between floors by selecting tabs on the top of the window. Next part will be a search box giving table fulfilling search box requirements. The search box will be able to search through printer and employee data. So, the process of finding an employee and printer is the same.

By consulting the Facility Manager, several requirements were arisen. The application should be very easy to handle so that department assistants could easily edit the data. Next part was to create the solution for possibility of editing working space the similar way like in MS Visio.

Communication problem

After the first consultation with the Facility Manager, the department stopped responding to messages and the Facility Manager assistant shared the information that the application is not wanted by the department. The next design phase had to be managed with as least involvement of Facility Management department as possible. Because the department already works with building floor plans and creates the building interior in MS Visio, the only thing needed from them will be importing of the current floor plan situation.



Possible further authorization needed

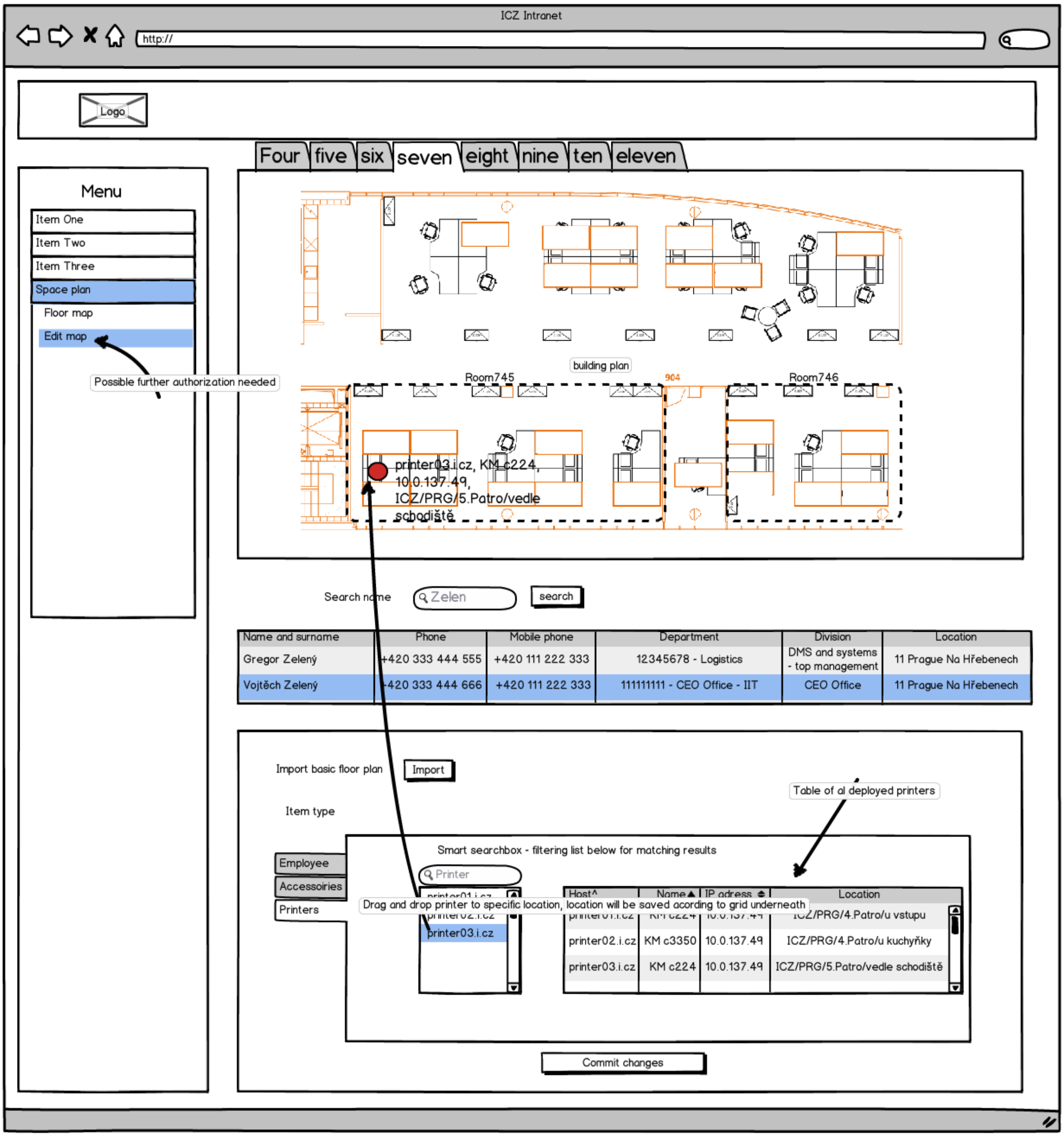
Name and surname	Phone	Mobile phone	Department	Division	Location
Gregor Zelený	+420 333 444 555	+420 111 222 333	12345678 - Logistics	DMS and systems - top management	11 Prague Na Hřebenech
Vojtěch Zelený	+420 333 444 666	+420 111 222 333	111111111 - CEO Office - IIT	CEO Office	11 Prague Na Hřebenech

Smart searchbox - filtering list below for matching results

Drag and drop user to specific location, location will be saved acording to grid underneath

Figure 25 - Adding of a selected employee to a location on the map Source: (Own design)

Figure 25 shows process of putting selected employee on a grid. The location will be stored by drag and dropping an employee on the map panel. Every located employee will not be on the list. Similar window will be used for the printers. Displayed rooms are part of the imported document from the Facility Management team. Deleting users location connection will be done by finding the user, selecting his location and pressing “delete” button.



Name and surname	Phone	Mobile phone	Department	Division	Location
Gregor Zelený	+420 333 444 555	+420 111 222 333	12345678 - Logistics	DMS and systems - top management	11 Prague Na Hřebenech
Vojtěch Zelený	+420 333 444 666	+420 111 222 333	11111111 - CEO Office - IIT	CEO Office	11 Prague Na Hřebenech

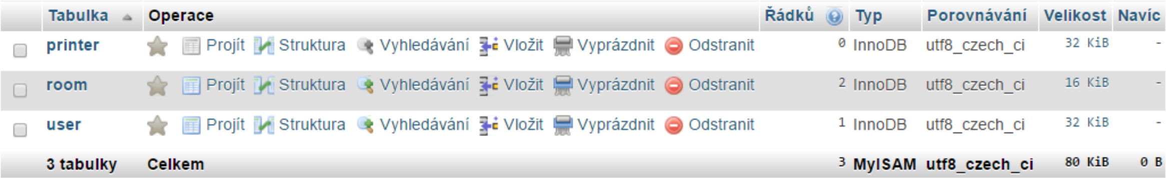
Host^	Name ▲	IP adress ≑	Location
printer01.i.cz	KM c224	10.0.137.49	ICZ/PRG/4.Patro/u vstupu
printer02.i.cz	KM c3350	10.0.137.49	ICZ/PRG/4.Patro/u kuchyňky
printer03.i.cz	KM c224	10.0.137.49	ICZ/PRG/5.Patro/vedle schodiště

Figure 26 - adding printers window with table of all deployed printer Source: (Own design)

On figure 26 there will be a list of not deployed printers. The list will have also drag and droppable items. Next part of the window will be a table showing all deployed printers with a brief information. In case of the figure 25, it was not advised to use table of all employees, because the number of rows would be around 500.

4.2.2 Database design phase

The database for the project was done in MySQL through phpMyAdmin free software tool.



	Tabulka	Operace	Řádků	Typ	Porovnávání	Velikost	Navíc
□	printer	Projít Struktura Vyhledávání Vložit Vyprázdnit Odstranit	0	InnoDB	utf8_czech_ci	32 KiB	-
□	room	Projít Struktura Vyhledávání Vložit Vyprázdnit Odstranit	2	InnoDB	utf8_czech_ci	16 KiB	-
□	user	Projít Struktura Vyhledávání Vložit Vyprázdnit Odstranit	1	InnoDB	utf8_czech_ci	32 KiB	-
	3 tabulky	Celkem	3	MyISAM	utf8_czech_ci	80 KiB	0 B

Figure 27 - simple databse with Printer, Room and User classes Source: (Own design)

Database class diagram was created by reverse engineering of tables using MySQL Workbench tool.

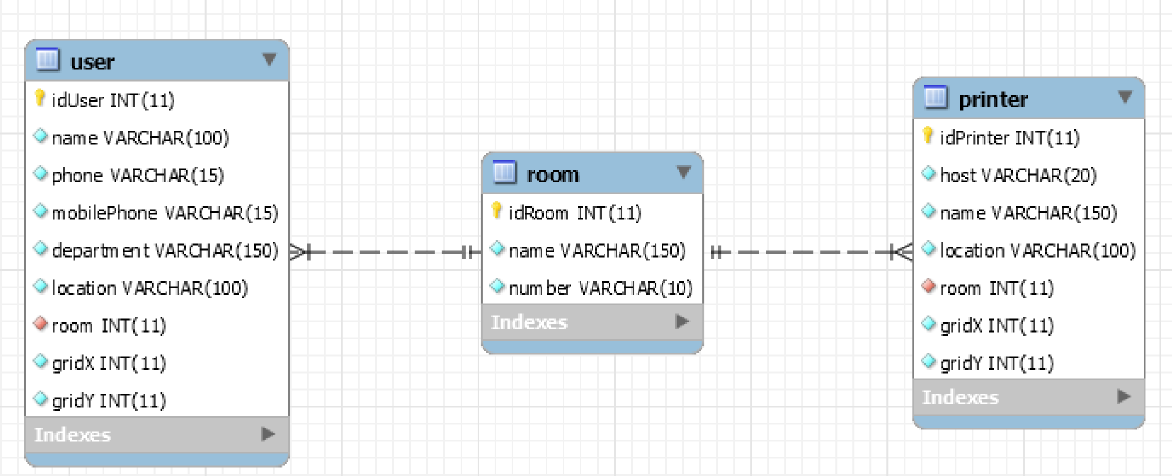


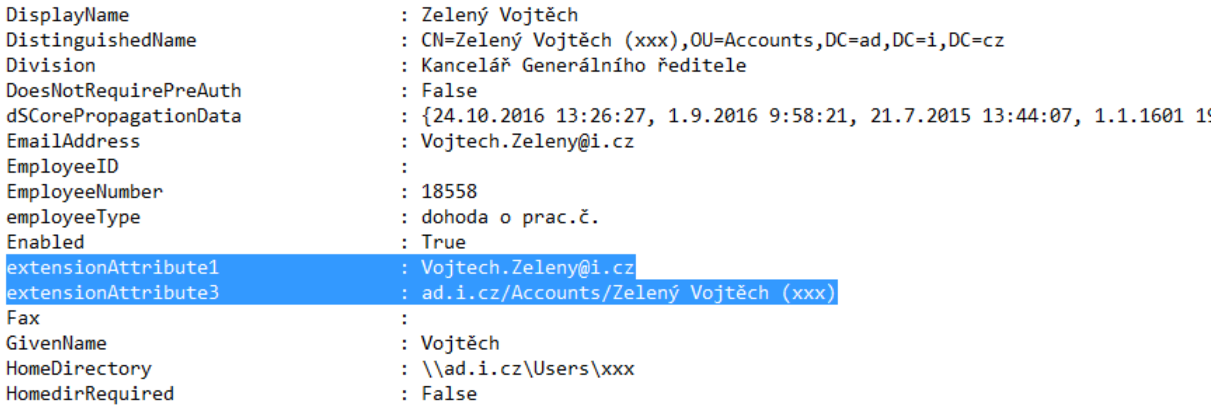
Figure 28 - Database class diagram Source: (Own design)

4.2.3 Location storing solution

The proposed solution was to export all the data for the application from AD and save it back in AD. For accomplishing that it was needed to find ideally some empty attributes. All user attributes were obtained by running script: “`Get-ADUser -Identity username -Properties *`”

in Windows PowerShell on server, where AD is installed.

By studying options with MS-Win administrator it was chosen to use extension attributes for storing data about room and grid coordinates shown in figure 28. In ICZ AD it is possible to use 15 extension attributes and company is now using only 3.

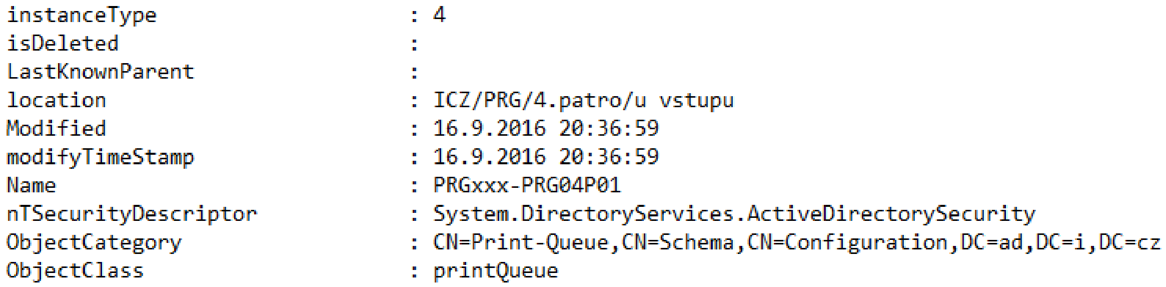


```
DisplayName                       : Zelený Vojtěch
DistinguishedName                 : CN=Zelený Vojtěch (xxx),OU=Accounts,DC=ad,DC=i,DC=cz
Division                          : Kancelář Generálního ředitele
DoesNotRequirePreAuth             : False
dSCorePropagationData             : {24.10.2016 13:26:27, 1.9.2016 9:58:21, 21.7.2015 13:44:07, 1.1.1601 1
EmailAddress                      : Vojtech.Zeleny@i.cz
EmployeeID                        :
EmployeeNumber                    : 18558
employeeType                      : dohoda o prac.č.
Enabled                           : True
extensionAttribute1               : Vojtech.Zeleny@i.cz
extensionAttribute3               : ad.i.cz/Accounts/Zelený Vojtěch (xxx)
Fax                               :
GivenName                         : Vojtěch
HomeDirectory                     : \\ad.i.cz\Users\xxx
HomedirRequired                   : False
```

Figure 29 - Screenshot of several user attributes   Source: (Own design)

The printer attributes were obtained by running:

“Get-ADObject 'CN=SPRG105-PRG04P01,CN=SPRG105,OU=Applications_servers,OU=PRAHA,OU=Servers,DC=ad,DC=i,DC=cz' -properties *|fl”



```
instanceType                     : 4
isDeleted                        :
LastKnownParent                  :
location                         : ICZ/PRG/4.patro/u vstupu
Modified                         : 16.9.2016 20:36:59
modifyTimeStamp                  : 16.9.2016 20:36:59
Name                             : PRGxxx-PRG04P01
nTSecurityDescriptor             : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                   : CN=Print-Queue,CN=Schema,CN=Configuration,DC=ad,DC=i,DC=cz
ObjectClass                      : printQueue
```

Figure 30 - Screenshot of several printer attributes   Source: (Own design)

Although MS-Win group will need to adjust some import data scripts it was chosen to store the data behind the data in location attribute. In the final application the data will be parsed into X Y coordinates and a room number will be added.

4.3 Development phase

The application will be developed in HTML 5, CSS and Javascript. The development will be paid the company as a part of the part-time job contract of the author.

Pre-alpha presentation part of the web application was created using Netbeans integrated development environment platform. Styling was done in CSS and Bootstrap. This version was released under an IT technologies client side project on http://kitlab.pef.czu.cz/1617zs/ete52e/03/floorMap.html.

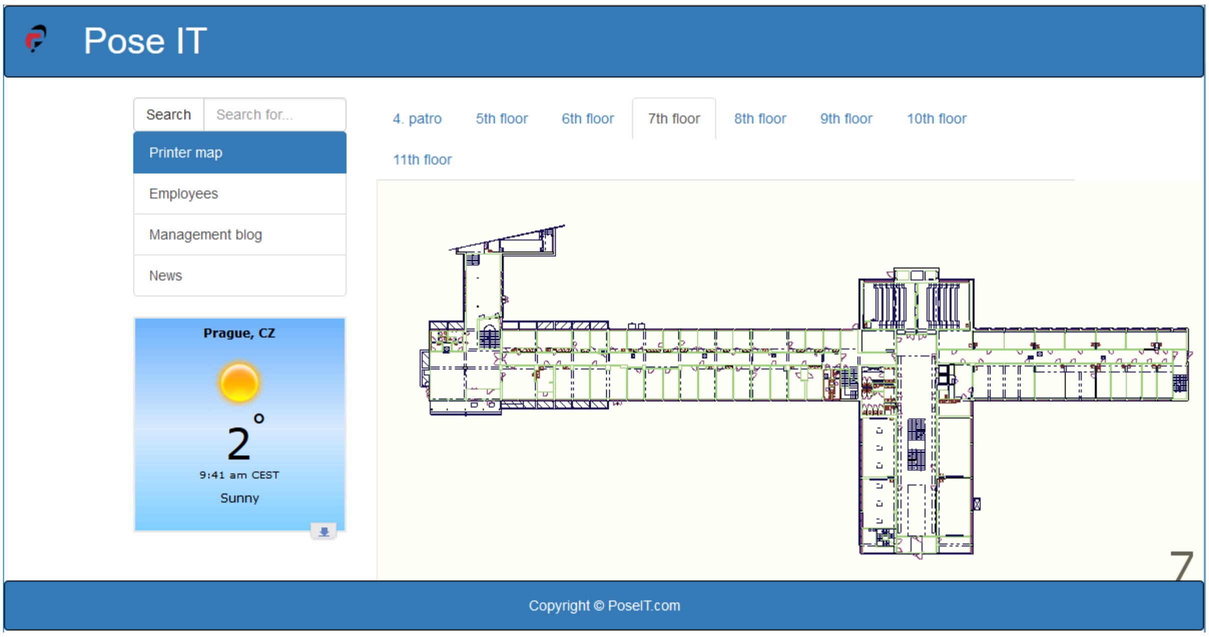


Figure 31 - Intranet simulation pre-alpha version Source: (Own design)

4.4 Implementation and maintenance phase

This section will describe implementation proposals based on the business process analysis.

4.4.1.1 Security

ICZ implements SSO on most of its platforms including intranet. That means no need for another identity verification. For editing purposes, it will be needed to enable access only to several users. That can easily be done by using already existing Active Directory user groups. Administration rights for the final products will be given to the author of the project, contract owner – IT manager and second IT manager.

4.4.1.2 Printer process changes

New Printer

End-user support group will be responsible for putting new printer location on the web application floor map.

Removed printer

Because End-user support group is responsible for physical working with printers, they will also be in charge of deleting removed printer location through the web application.

The ServiceDesk process remains the same.

4.4.1.3 Employee process changes

New employee

For the process to become official it is necessary to create ServiceDesk accounts for section assistants who have the most knowledge about employee seating. Each section assistant will need his/her own assignee group for handling his/her process workflow task. Their responsibility would be to set working position for each new employee.

Quitting employee

This part of the process would be easily handled by Helpdesk operators. When operator revokes user certificates he will also go to web application, finds the user and deletes his or her location.

5 Results and Discussion

The results and discussion is divided into three parts. Theoretical part provides and discuss results for the theoretical part, practical part describes results of practical part and costs estimation and discussion provides comparison of designed solution with other solutions on market and description of internal issues with the project.

5.1 Theoretical part

The theoretical section introduced technology and principles for working with identity management systems and provided methodology for creation of identity and facility management system.

Analysis of third party applications showed how such project is handled by professionals and gave a basic idea of how the application should look like.

5.2 Practical part

Practical part proposed solution for the given goals. Key stakeholders were selected and interviewed. This part was crucial for revealing all the technologies available. Business process analysis part introduced how the current technologies work and how goes the process workflow. Based on the analysis the system design was created. Design consist of wireframed application and simple model of database behind it. Than solution for data storing was interpreted. Development phase contains implementation of pre-alpha version. In last phase of the project one security issue was resolved and process changes were proposed.

5.3 Costs estimation and discussion

For estimating prices of third party applications two main Czech companies delivering similar solutions as this project were contacted. The problem was, that these companies are afraid of business competition and often do not offer any price list for their services. Next problem is that the companies does not listen to any student projects and it is not in their interest to provide any business information for free. A little information was offered, when the companies were contacted on behalf of ICZ company.

GISA company was asked to provide cost calculation based on provided application requirements. In brief telephone discussion the estimate was given to 100 000 CZK and further communication was confirmed. By that time the Facility Management team stopped responding on emails and call. The aim of next discussion was to obtain budget, that would be offered for such a project. Later, after communication in-person with the facility manager assistant, it was found that the facility management team does not want any new application and does not wish to be participated in the development process.

The second company contacted on behalf of ICZ was IKA DATA. Their website does not provide any information about prices. Further meeting was offered, but at that time it was found that there is no need for third party application.

For developing the final solution of the project, it was offered to create a contract. Considering slightly higher payment as helpdesk operators, necessary time for coding 80 - 130 hours based on previous experience with pre-alpha version development, the cost of the development would be 10,000 – 16,250 CZK.

6 Conclusion

Thesis was divided into two main sections - theoretical and practical part. In theoretical part technology and principles behind identity and facility management systems were investigated. Several third-party solutions were introduced focusing on Czech market. Then methodology for creation of IAM/FM systems was introduced. Practical part was focused on ICZ business case. Key stakeholders were approached and business processes related to identity management were analysed. Current systems used in the company and associated with the issues were briefly introduced. The application design was created based on the analysis. The design consists of application mockups simple database and solution for storing of location. Development phase was focused on creation of pre-alpha prototype version. Implementation and maintenance phase describes solving of security issues and proposes process changes related toimplementation of the application.

Goal of the project was to develop a system for locating printer and employees working with building floor plans. The goal was achieved by designing such system and analyzing its influence on current solution. During the project, several issues were encountered. The problem with Facility Management team was handled by omitting this team from the whole process. This decision was supported by key decision maker the head IT manager.

At the end, comparison and calculation of costs was performed. Cost of the further development was calculated to maximum of 16250 CZK, which is approximately six times cheaper then solution by external GISA company. The project is currently in early stage and further development will be part of a new contract approved by head IT manager. The proposed solution proved that it was beneficial to the company such as ICZ from HR perspective, IT service provision perspective and IT management perspective.

7 References

7.1 Literature references

Pfitzmann, A., and M. Hansen, “A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management,” 2009, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.

Bishop, M., Computer Security: Art and Science, Reading, MA: Addison-Wesley Professional, 2002.

NGN Identity Management Framework, ITU-T Recommendation, Y.2720.

Neuman, B. C., and T. Ts’o, “Kerberos: An Authentication Service for Computer Networks,” IEEE Communications, Vol. 32, No. 9, September 1994, pp. 33– 38.

Nabeth, T., “Identity of Identity,” in The Future of Identity in the Information Society, New York: Springer, 2009, pp. 19– 69.

Searls, D., “Mydentity & Ourdentity vs. Theirdentity,” http://doc-weblogs.com/2002/ 12/31#mydentityOurdentityVsTheirdentity.

Brands, S., and F. Legare, “Digital Identity Management Based on Digital Credentials,” Lecture Notes in Informatics, Vol. 19, 2002.

MacGregor, W., W. Dutcher, and J. Khan, “An Ontology of Identity Credentials. Part 1: Background and Formulation,” NIST Special Publication 800-103 Draft, 2006.

Adams, C., and S. Lloyd, Understanding PKI— Concepts, Standards and Deployment Considerations, 2nd ed., Reading, MA: Addison-Wesley, 2005

Bertino, E., et al., "Digital Identity Management," in Security in Computing and Networking Systems— The State of the Art , W. McQuay and W. W. Smari, (eds.), 2011.

Pfitzmann, A., and M. Hansen, "Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management— A Consolidated Proposal for Terminology," Version v0.31, February 15, 2008, http://dud.inf.tu-dresden.de/ Anon_Terminology.shtml.

Layouni, M., and H. Vangheluwe, "Anonymous K- Show Credentials," EuroPKI 2007, Springer, 2007, pp. 181– 192.

Osmanoglu, T. Ertem. *Identity and access management: business performance through connected intelligence*. Amsterdam, [Netherlands]: Syngress, an imprint of Elsevier, 2014. ISBN 978-012-4081-406.

STANEK, William R. *Windows Server 2012: pocket consultant*. Redmond, Wash.: Microsoft Press, c2012. ISBN 07-356-6633-4.

Microsoft. Windows Server 2012 [online], © 2013 [cit. 2017-01-31]. Available from www: <http://www.microsoft.com/cs-cz/server-cloud/windows-server/default.aspx>

WILSON, Ed. *Microsoft Windows Powershell step by step*. Redmond, WA: Microsoft Press, 2013. ISBN 978-0-7356-2395-8.

7.2 Online references

IETF, "Public-Key Infrastructure (X.509),"
http://www.ietf.org/dyn/wg/charter/pkixcharter.html

BERTINO, Elisa a Kenji TAKAHASHI. Identity management: concepts, technologies, and systems [online]. London, UK: ARTECH, c2011 [cit. 2016-06-13]. ISBN 9781608070404. Available from: http://site.ebrary.com/lib/techlib

TEICHOLZ, Eric. *Technology for facility managers: the impact of cutting-edge technology on facility management* [online]. Hoboken, NJ: John Wiley, 2012 [cit.

2017-01-30]. ISBN 978-1-118-44173-2. Available from: https://ebookcentral.proquest.com/lib/techlib-ebooks/reader.action?docID=918225

Training Solutions. *Active directory fast start: a quick start guide for active directory* [online]. Seattle, Washington: RP Media, 2014 [cit. 2016-06-12]. ISBN 978-1-62716-216-6. Available from: http://sfx.techlib.cz

CISSP Training Videos: Identity And Access Management. In: *Youtube* [online]. [cit. 2017-01-30]. Available from: https://youtu.be/8rYaUxgfhHM?t=594

HAMPL, Milan. *Integrated Work Space Management: aneb Softwarová podpora Facility Managementu* [online]. 2016 [cit. 2017-01-30]. Available from: https://www.systemonline.cz/clanky/softwarova-podpora-facility-managementu.htm

IKADATA.cz: Archibus Inc. [online]. [cit. 2017-01-30]. Available from: http://www.ikadata.com/o_spolecnosti_archibus_inc._r_004528

IKA DATA: Space management [online]. [cit. 2017-01-30]. Available from: http://www.ikadata.com/spr%C3%A1va+ploch+(space+management)_n_002582_r_4725

FloorPlanMapper: Frequently asked questions [online]. [cit. 2017-01-30]. Available from: http://www.floorplanmapper.com/frequently-asked-questions/

FloorPlanMapper: Floor Plan Mapper with microsoft sharepoint [online]. [cit. 2017-01-30]. Available from: http://www.floorplanmapper.com/integrate-floor-plan-mapper-with-microsoft-sharepoint/

POC System [online]. [cit. 2017-01-30]. Available from: http://www.poc-system.com/

POC System: Products [online]. [cit. 2017-01-30]. Available from: http://www.poc-system.com/products/

POC System: Space Management System [online]. [cit. 2017-01-30]. Available from: http://www.poc-system.com/space-management-system/

POC System: Seating Allocation Solutions [online]. [cit. 2017-01-30]. Available from: http://www.poc-system.com/seating-allocation-solutions/

FEINTZEIG, Rachel. *How Software Can Help Solve the Office-Layout Puzzle: Workspace-allocation software helps move employees and make the most of space* [online]. 2013 [cit. 2017-01-30]. Available from: https://www.wsj.com/articles/SB10001424127887324823804579014813846190706

OfficeSpace Software. *Softwareadvice.com* [online]. [cit. 2017-01-30]. Available from: http://www.softwareadvice.com/cafm/officespace-profile/
GISA -fm. *GISA* [online]. [cit. 2017-01-30]. Available from: http://gisa.cz/technicke-informace/gisa-fm/

Cenik FM. *GISA* [online]. [cit. 2017-01-30]. Available from: http://gisa.cz/cenik/cenik-fm/

6 Phases of the Web Site Design and Development Process. *Idesignstudios* [online]. Web Design, 2014 [cit. 2017-03-09]. Available from: http://www.idesignstudios.com/blog/web-design/phases-web-design-development-process/

8 Appendix

8.1 List of abbreviations

AD Active Directory

BIM Building Information Modelling

CAFM Computer-Aided Facility Management

DHCP Dynamic Host Configuration Protocol

FM Facility Management

GIS Geographical Information System

HR Human Resources

IAM Identity Access Management

IETF Internet Engineering Task Force

IS Information System

IWMS Integrated Workplace Management System

KPI Key performance indicators

SLA Service Level Agreement

SMPT Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

SSO Single sign-on

8.2 Results of Windows PowerShell commands

Note: Due to security reasons some data were anonymized.

User attributes

```
AccountExpirationDate              :
accountExpires                     : 9223372036854775807
AccountLockoutTime                 :
AccountNotDelegated                : False
AllowReversiblePasswordEncryption  : False
BadLogonCount                      : 0
badPasswordTime                    : 131207253602520081
badPwdCount                        : 0
```

```
CannotChangePassword            : False
CanonicalName                   : ad.i.cz/Accounts/Zelený Vojtěch (xxx)
Certificates                    : {System.Security.Cryptography.XXXCertificates.XXXCertificate}
City                            :
CN                              : Zelený Vojtěch (xxx)
codePage                        : 0
Company                         : ICZ a.s.
Country                         :
countryCode                     : 0
Created                         : 1.9.2014 10:02:56
createTimeStamp                 : 1.9.2014 10:02:56
Deleted                         :
Department                      : 10110101 - Kancelář GŘ - Odbor IIT - Service Desk
departmentNumber                : {10110101}
Description                     : 2014.09.01 USD 111248
DisplayName                     : Zelený Vojtěch
DistinguishedName               : CN=Zelený Vojtěch (xxx),OU=Accounts,DC=ad,DC=i,DC=cz
Division                        : Kancelář Generálního ředitele
DoesNotRequirePreAuth           : False
dSCorePropagationData           : {24.10.2016 13:26:27, 1.9.2016 9:58:21, 21.7.2015 13:44:07,
1.1.1601 19:16:33}
EmailAddress                    : Vojtech.Zeleny@i.cz
EmployeeID                      :
EmployeeNumber                  : 18558
employeeType                    : dohoda o prac.č.
Enabled                         : True
extensionAttribute1             : Vojtech.Zeleny@i.cz
extensionAttribute3             : ad.i.cz/Accounts/Zelený Vojtěch (xxx)
Fax                             :
GivenName                       : Vojtěch
HomeDirectory                   : \\ad.i.cz\Users\xxx
HomedirRequired                 : False
HomeDrive                       : H:
```

```
homeMDB                        : CN=PRG-C,CN=Databases,CN=Exchange Administrative Group
(FYDIBOHF23SPDLT),CN=Administrative                     Groups,CN=ICZ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=ad,DC=i,DC=cz
homeMTA                        : CN=Microsoft MTA,CN=SPRG113,CN=Servers,CN=Exchange
Administrative              Group              (FYDIBOHF23SPDLT),CN=Administrative
Groups,CN=ICZ,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=ad,DC=
                         i,DC=cz
HomePage                       :
HomePhone                      :
Initials                       :
instanceType                   : 4
isDeleted                      :
LastBadPasswordAttempt         : 12.10.2016 7:56:00
LastKnownParent                :
lastLogoff                     : 0
lastLogon                      : 131231557049155919
LastLogonDate                  : 5.11.2016 2:42:36
lastLogonTimestamp             : 131227837566620274
legacyExchangeDN                            :  /o=ICZ/ou=Exchange  Administrative  Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=user21b48099
LockedOut                      : False
logonCount                     : 1373
LogonWorkstations              :
mail                           : Vojtech.Zeleny@i.cz
mailNickname                   : zelenyv
Manager                        : CN=Jezný Vratko (xxx),OU=Accounts,DC=ad,DC=i,DC=cz
mDBUseDefaults                 : True
MemberOf                       : {xxx}
MNSLogonAccount                : False
MobilePhone                    :
Modified                       : 5.11.2016 2:42:51
modifyTimeStamp                : 5.11.2016 2:42:51
msDS-User-Account-Control-Computed : 0
```

```
msExchHomeServerName                : /o=ICZ/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=SPRG113
msExchMailboxGuid            : {133, 62, 233, 127...}
msExchMailboxSecurityDescriptor   : System.DirectoryServices.ActiveDirectorySecurity
msExchPoliciesIncluded         : {aefe5737-1047-4566-b826-5ec5a74d4c4d, {26491cfc-9e50-
4857-861b-0cb8df22b5d7}}
msExchRBACPolicyLink                          : CN=Default Role Assignment
Policy,CN=Policies,CN=RBAC,CN=ICZ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=ad,DC=i,DC=cz
msExchRecipientDisplayType       : 1073741824
msExchRecipientTypeDetails       : 1
msExchSafeSendersHash          : {231, 105, 34, 104}
msExchShadowMailNickname         : zelenyv
msExchShadowProxyAddresses                    : {smtp:Vojtech.Zeleny@ad.i.cz,
smtp:Vojtech.Zeleny@icz.cz, SMTP:Vojtech.Zeleny@i.cz}
msExchTextMessagingState         : {302120705, 16842751}
msExchUMDtmfMap                               : {emailAddress:8658324935369,
lastNameFirstName:9353698658324, firstNameLastName:8658324935369}
msExchUserAccountControl         : 0
msExchUserCulture              : en-US
msExchVersion                 : 44220983382016
msExchWhenMailboxCreated         : 1.9.2014 10:04:19
msSFU30GidNumber              : 18558
msSFU30UidNumber              : 18558
msTSExpireDate                : 11.12.2016 11:22:41
msTSLicenseVersion             : 393216
msTSManagingLS                 : 55041-011-1049176-84747
Name                        : Zelený Vojtěch (zelenyv)
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory               : CN=Person,CN=Schema,CN=Configuration,DC=ad,DC=i,DC=cz
ObjectClass                  : user
ObjectGUID                    : 19996339-3029-4e61-98e0-75644b96b42b
objectSid                   : S-1-5-21-2852610057-1294291396-2232196198-31000
```

```
Office                        : 11 - Praha Na hřebenech
OfficePhone                   :
Organization                  :
OtherName                     :
PasswordExpired               : False
PasswordLastSet               : 2.11.2016 8:58:17
PasswordNeverExpires          : False
PasswordNotRequired           : False
physicalDeliveryOfficeName    : 11 - Praha Na hřebenech
POBox                         :
PostalCode                    :
PrimaryGroup                  : CN=Domain Users,CN=Users,DC=ad,DC=i,DC=cz
primaryGroupID                : 513
ProfilePath                   : \\ad.i.cz\users\xxx\profile
ProtectedFromAccidentalDeletion    : False
protocolSettings              : {POP3§0§§§§§§§§§§§}
proxyAddresses                : {smtp:Vojtech.Zeleny@ad.i.cz, smtp:Vojtech.Zeleny@icz.cz,
SMTP:Vojtech.Zeleny@i.cz}
pwdLastSet                    : 131225470972948535
SamAccountName                : xxx
sAMAccountType                : 805306368
ScriptPath                    : usriczlogon.cmd
sDRightsEffective             : 15
ServicePrincipalNames         : {}
showInAddressBook             : {CN=New GAL,CN=All Address Lists,CN=Address Lists
Container,CN=ICZ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=ad,DC=i,DC=cz, CN=11 - Praha,CN=ICZ
Lokality,CN=All Address L
                                ists,CN=Address Lists Container,CN=ICZ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=ad,DC=i,DC=cz, CN=Default Global
Address List,CN=All Global Address Lists,CN=Address List
```

```
                    s                              Container,CN=ICZ,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=ad,DC=i,DC=cz,    CN=Global    Address
List,CN=All Global Address Lists,CN=Address Lists Container,CN=ICZ,CN=Micros
                    oft
Exchange,CN=Services,CN=Configuration,DC=ad,DC=i,DC=cz...}
SID                    : S-1-5-21-2852610057-1294291396-2232196198-31000
SIDHistory               : {}
SmartcardLogonRequired         : False
sn                    : Zelený
State                    :
StreetAddress               :
Surname                  : Zelený
Title                   : 1 - Dohoda o pracovní činnosti
TrustedForDelegation           : False
TrustedToAuthForDelegation       : False
uid                    : {xxx}
UseDESKeyOnly                : False
userAccountControl            : 512
userCertificate              : {xxx}
UserPrincipalName             : xxx@ad.i.cz
uSNChanged                 : 114808900
uSNCreated                 : 54887241
whenChanged                 : 5.11.2016 2:42:51
whenCreated                 : 1.9.2014 10:02:56
```

Printer attributes

```
CanonicalName               : ad.i.cz/Servers/PRAHA/Applications_servers/PRGxxx/PRGxxx-
PRG04P01
CN                    : PRGxxx-PRG04P01
Created                  : 16.9.2016 20:36:53
createTimeStamp              : 16.9.2016 20:36:53
Deleted                  :
Description                : KM C224e, A4, A3, barevná, duplex, multifunkce
```

```
DisplayName                 :
DistinguishedName           : CN=PRGxxx-
PRG04P01,CN=PRGxxx,OU=Applications_servers,OU=PRAHA,OU=Servers,DC=ad,DC=i
                    ,DC=cz
driverName                  : KONICA MINOLTA C554SeriesPCL
driverVersion               : 1025
dSCorePropagationData       : {1.1.1601 1:00:00}
flags                       : 0
instanceType                : 4
isDeleted                   :
LastKnownParent             :
location                    : ICZ/PRG/4.patro/u vstupu
Modified                    : 16.9.2016 20:36:59
modifyTimeStamp             : 16.9.2016 20:36:59
Name                        : PRGxxx-PRG04P01
nTSecurityDescriptor        : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory              : CN=Print-
Queue,CN=Schema,CN=Configuration,DC=ad,DC=i,DC=cz
ObjectClass                 : printQueue
ObjectGUID                  : xxx
portName                    : {10.0.136.41}
printBinNames               : {Bypass Tray, LCT, Tray4, Tray3...}
printCollate                : True
printColor                  : True
printDuplexSupported        : True
printEndTime                : 0
printerName                 : PRG04P01
printKeepPrintedJobs        : False
printMaxResolutionSupported : 1200
printMaxXExtent             : 8410
printMaxYExtent             : 12000
printMediaReady             : {Custom Size, SRA3, 8 1/2x11 Tab, A4 Tab...}
printMediaSupported         : {Custom Size, SRA3, 8 1/2x11 Tab, A4 Tab...}
```

```
printMinXExtent              : 900
printMinYExtent              : 1397
printOrientationsSupported     : {LANDSCAPE, PORTRAIT}
printPagesPerMinute            : 22
printRateUnit                : PagesPerMinute
printShareName               : {PRG04P01}
printSpooling                : PrintAfterSpooled
printStaplingSupported         : False
printStartTime               : 0
priority                   : 1
ProtectedFromAccidentalDeletion : False
sDRightsEffective            : 0
serverName                   : PRGxxx.ad.i.cz
shortServerName               : PRGxxx
uNCName                      : \\PRGxxx.ad.i.cz\PRG04P01
url                        : {http://PRGxxx.ad.i.cz/PRG04P01}
uSNChanged                    : 111783367
uSNCreated                   : 111783367
versionNumber                 : 4
whenChanged                   : 16.9.2016 20:36:59
whenCreated                  : 16.9.2016 20:36:53
```

8.3 Pre-alpha version – floor plan page source code

```
<!DOCTYPE html>
<!-- html,css with bootstrap and idealz with edited stzles,javacript-->
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <!-- The above 3 meta tags *must* come first in the head; any other head content must come *after* these tags -->
    <meta name="description" content="">
```

```
        <meta name="author" content="">
        <link rel="icon" href="../../favicon.ico">

        <title>Starter Template for Bootstrap</title>

        <!-- Bootstrap core CSS -->
        <link href="css/bootstrap.min.css" rel="stylesheet">
        <!-- Custom styles for this template -->
        <link href="style.css" rel="stylesheet">

    </head>

    <body>
        <nav class="navbar navbar-default">
            <div class="container-fluid">
                <div class="navbar-header">
                    <a class="navbar-brand" href="index.html">
                        <img                                        alt="Brand"
src="https://zeldic.github.io/ProjectWithCapitalP/PoseIT3.png">
                    </a>
                    <h1 class="navbar-text">Pose IT</h1>
                </div>
            </div>
        </nav>
        <div class="container">
            <div class="row">
                <div class="col-md-3">
                    <div class="input-group">
                        <span class="input-group-btn">
                            <a href="tableResult.html" class="btn btn-default" >Search</a>
                        </span>
                        <label for="searchbox" id="schovejto">search box</label>
```

```
          <input type="text" id= "searchbox" class="form-control" placeholder="Search for...">
        </div><!-- /input-group -->

        <div class="list-group">
          <a href="floorMap.html" class="list-group-item active">Printer map</a>
          <a href="searchEmployees.html" class="list-group-item">Employees</a>
          <a href="managementBlog.html" class="list-group-item">Management blog</a>
          <a href="news.html" class="list-group-item">News</a>
        </div>
        <a href="http://www.accuweather.com/en/cz/prague/125594/weather-forecast/125594" class="aw-widget-legal">
          <!--
          By accessing and/or using this code snippet, you agree to AccuWeather’s terms and conditions (in English) which can be found at http://www.accuweather.com/en/free-weather-widgets/terms and AccuWeather’s Privacy Statement (in English) which can be found at http://www.accuweather.com/en/privacy.
          -->
        </a><div id="awcc1481580976274" class="aw-widget-current" data-locationkey="125594" data-unit="c" data-language="en-us" data-useip="false" data-uid="awcc1481580976274"></div><script type="text/javascript" src="http://oap.accuweather.com/launch.js"></script>
      </div>

      <div class="col-md-9">
        <ul class="nav nav-tabs" id='tabs-floors'>
          <li role="presentation" class="active"><a href="https://zeldic.github.io/ProjectWithCapitalP/Floor4.png">4. patro</a></li>
          <li role="presentation"><a href="https://zeldic.github.io/ProjectWithCapitalP/Floor5.png">5th floor</a></li>
          <li role="presentation"><a href="https://zeldic.github.io/ProjectWithCapitalP/Floor6.png">6th floor</a></li>
```

```
            <li role="presentation"><a
href="https://zeldic.github.io/ProjectWithCapitalP/Floor7.png">7th floor</a></li>
            <li role="presentation"><a
href="https://zeldic.github.io/ProjectWithCapitalP/Floor8.png">8th floor</a></li>
            <li role="presentation"><a
href="https://zeldic.github.io/ProjectWithCapitalP/Floor9.png">9th floor</a></li>
            <li role="presentation"><a
href="https://zeldic.github.io/ProjectWithCapitalP/Floor10.png">10th floor</a></li>
            <li role="presentation"><a
href="https://zeldic.github.io/ProjectWithCapitalP/Floor11.png">11th floor</a></li>
          </ul>
          <div id="map">
            <img src="https://zeldic.github.io/ProjectWithCapitalP/Floor4.png" alt="4th
floor" style="width:872px;height:437px;">
          </div>
        </div>
      </div>
    </div>



    <!-- Bootstrap core JavaScript
    ================================================== -->
    <!-- Placed at the end of the document so the pages load faster -->
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
    <script src="/js/bootstrap.min.js"></script>
    <!--<button type="button"
        onclick="document.getElementById('demo').innerHTML = Date()">
      Click me to display Date and Time.</button>

    <p id="demo"></p>-->
    <!--<script>sub.on("click", function(e){alert("Submitcliked")})</script>-->
    <script>$('#tabs-floors>li>a').on('click', function (e) {
        e.preventDefault();
        $('#tabs-floors li').removeClass('active');

        $(this).parent().addClass('active');
        //script for picture changing:
        var imageUrl = $(this).attr('href');
        // console.log(imageUrl, this);
        $('#map img').attr('src', imageUrl);
    });
</script>
<script>
    $('.scroll-top').unbind('click').on('click', function () {
        $('html, body').animate({scrollTop: 0}, 200);
    });

    $('#search').on('submit', (e) => {
        e.preventDefault();
    });

    var persons = false;

    $('#search-field').on('keypress change', (e) => {
        var request = $('#search-field').val();
        $('#search-result').empty();
        if (request.length >= 1) {
            for (var i = 0; i < persons.length; i++) {
                var pers = persons[i];
                if (pers.name.indexOf(request) != -1) {
                    $('#search-result').append("<li>" + pers.name + "</li>");
                }
            }
        }
    });
```

```
            $(document).ready(() => {
                $.ajax({
                    type: 'POST',
                    dataType: 'json',
                    url: 'persons.json',
                    success: (d) => {
                        persons = d;
                    }
                });
            });
        </script>
        <footer>Copyright © PoseIT.com</footer>
    </body>

</html>
```