Anssi Suokas

Privileged Accounts Protection with Multi-factor Authentication

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

5 March 2023

PREFACE

This thesis was a fascinating peek into the world of different authentication methods and implementation possibilities of Multi-factor Authentication. This work deepened my knowledge about various authentication factors and related challenges.

Writing the final thesis progressed in varying ways, some days it progressed smoothly and others slowly. The ideas related to the topic matured as the work progressed, but the writing part took time.

I would like to thank my supervisors for their guidance and help in my final thesis.

The most excellent thanks belong to my wife and my children’s, who supported and encouraged me during this journey.

Vantaa, 5.3.2023
Anssi Suokas

Abstract

Author:	Anssi Suokas
Title:	Privileged Accounts Protection with Multi-factor Authentication
Number of Pages:	64 pages + 1 appendix
Date:	5 March 2023
Degree:	Master of Engineering
Degree Programme:	Information Technology
Professional Major:	Networking and Services
Supervisors:	Antti Orava, Manager Sami Sainio, Principal Lecturer

Identity protection for securing digital environments is of paramount importance to all companies using digital infrastructure. This thesis was a study of building the recommendations for improving the protection of organization's most critical user accounts in the on-premises infrastructure with additional layers of authentication. Improving (legacy) companies digital credentials protection is one step in providing secure digital infrastructure. In this process, it is necessary to balance the level of security and usability carefully with the value of the privileged account(s).

This work is a combination of literature survey and applied action research, aiming to provide recommendations for the organization in their approach to implement multi-factor authentication (MFA). This work resulted in specific guidelines for (i) privileged account protection, and (ii) MFA selection.

The expectation of this study was also to increase the knowledge of the subject in organization. This research gives the organization the capabilities to implement improvements to its environment in accordance with the lines and recommendations presented in the results of the work.

Keywords: MFA, Multi-factor Authentication, Identity Protection, Privileged Identity

Contents

List of Abbreviations

2FA	Two-factor Authentication
ATM	Automatic Teller Machine
Azure AD	Azure Active Directory
CBA	Certificate-based Authentication
CTAP	Client-to-Authenticator Protocols
FIDO	Fast ID Online
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
HOTP	Hash-based One-time Password
IDSA	Identity Security Alliance
IAM	Identity and Access Management
IP	Internet Protocol
IR	Infra-red
IT	Information Technology
MFA	Multi-factor Authentication
NCSC	National Cyber Security Centre
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OTP	One-time Password
OWASP	Open Web Application Security Project
PAW	Privileged Access Workstation
PCI DSS	Payment Card Industry Data Security Standard
PoLP	Principle of Least Privilege
RFID	Radio-frequency Identification
SHA-256	Secure Hash Algorithm 256 bits
SIM	Subscriber Identity Module
SMS	Short Message Service
TOTP	Time-based One-time Password
TPM	Trusted Platform Module
U2F	Universal Second Factor
UAF	Universal Authentication Framework
USB	Universal Serial Bus
VPN	Virtual Private Network

1 Introduction

Protecting privileged information and securing digital environments is of paramount importance to all companies using digital infrastructure. Today, this means that nearly all companies from small to multinational giants need to make rational decisions on what is important in identity management to provide access to their systems for privileged users while preventing unauthorized access. It is important to realize, that solutions suitable for one company is not necessarily the right approach for another. Thus, selecting the properly balanced approach to identity management and security is very important.

Cybersecurity has become a popular topic of interest due to multiple worldwide news threshold-breaking events [1]. Example the recent incidents: The psychotherapy centre Vastaamo data breach, where confidential patient records were stolen [2,3], Twitter massive data leak of user´s email addresses [4] and LastPass data breaches resulted in confidential customer information to be compromised [5,6]. According to Segal [7], the cyber-attacks could be expensive for the target companies in many ways and the number will increase in the future. The current digitalization transfers more and more businesses online, making it ever more interesting for crackers to do their business.

For several years, it has also been possible to see how work has changed in nature, for example, remote working and virtual teams due to various innovative technical solutions [8]. Recent COVID pandemic has further accelerated the change from traditional office work to remote work and hybrid environments [9]. These pose new challenges in how identities and systems should be protected and with what kind of methods.

Electronic identity is an entry ticket to several different information systems and services. In western digitalized economies electronic identity is crucial for both work and private life. There can be many different identities for users, which are used for different needs and tasks.

Identity management is important on all levels, since even private access to banking, social media and other platforms is lucrative enough for malicious users to fraud private privileged users for their access to these systems. Identities with elevated permissions are potentially even more interesting. Thus, it is important to protect users log-in privileges with appropriate means and methods.

The Open Web Application Security Project (OWASP) is an international non-profit organization dedicated to improving software security. It maintains a list of the Top 10 Web Application Security Risks. Associated with this list, users´ identity confirmation, authentication, and session management are essential in protecting against authentication-related attacks. The recommended solution, when possible, is to implement multi-factor authentication (MFA) to prevent different attacks against identities. [10]

According to Identity Defined Security Alliance (IDSA), a group of identity and security vendors, solution providers, and practitioners recently conducted a report “2022 Trends in Securing Digital Identities” [11], key findings include that identity-related attacks are rising, and impactful, but preventable. For example, in the report, 84% of respondents said that an organization has experienced an identity-related-breach in the past year and what kind of breach the top three were: phishing attacks (59%), inadequately managed privileges (36%) and stolen credentials (33%) as can be seen in Figure 1 below.

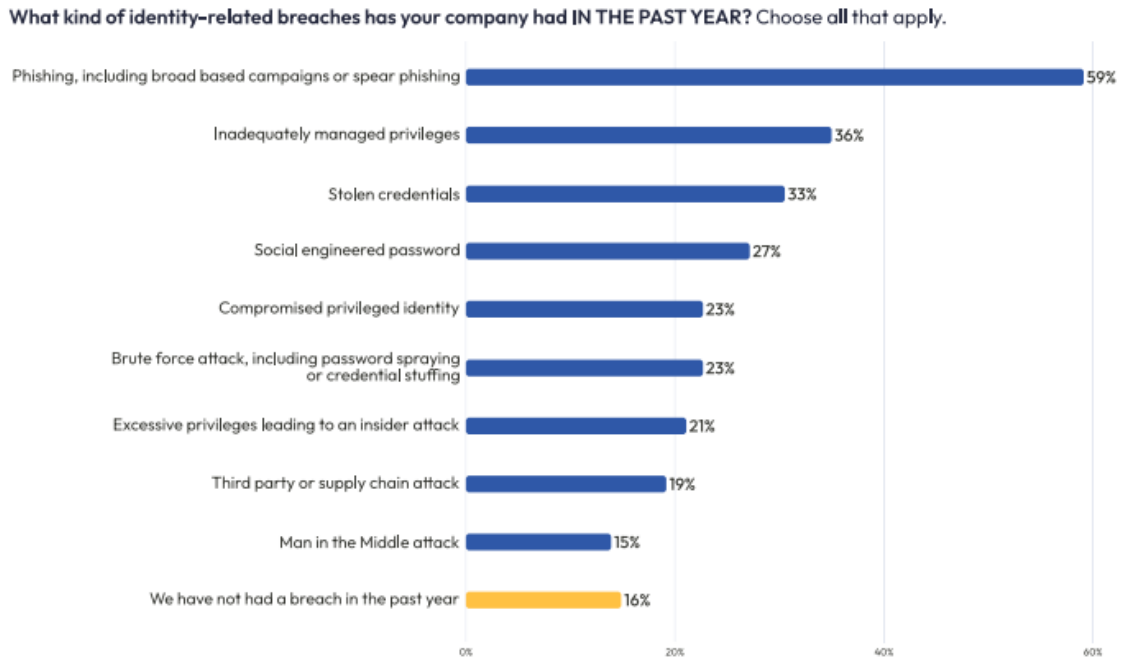

Figure 1. Most often reported identity-related breaches from the 2022 Trends in Securing Digital Identities report by IDSA. [11]

According to information presented in [11], of those who experienced an identity-related breach, 78% said that direct business impact was associated with it and the top four impacts were:

- Costs to recover from a breach
- Significant distraction from core business
- Negative impact on the reputation
- Loss of revenue

Implementing capabilities like MFA is necessary, particularly for privileged user access. Privileged credentials provide the broadest and most sensitive access, meaning that compromise or misuse of these causes the most significant impact. [12]

This thesis gives an overview of the general challenges related to privileged identity protection and the possibilities for the security of MFA. This thesis aims to map out the organization's current state and operating model regarding elevated user rights in the on-premises infrastructure by interviewing key persons

and observing current solutions, practices, and policies. The state of will for change and feedback of most suitable solution for the organization are gathered during interview sessions. The theoretical background chapter briefly summarizes different options available based on relevant literature. A policy proposal is drafted based on these findings. This proposal aims to cover the most suitable way to protect privileged accounts in the given environment.

1.1 Case Company´s Business Challenge and Objective

The case company is a cultural and educational organization. It was established about ten years ago and consists of multiple units in Finland. It provides the highest level of education in Finland for different areas and is an international forerunner in research and education.

The case company is developing its ability to protect identities with privileged access in the on-premises and cloud environments. The organization has implemented a solution for cloud service to protect identities with privileged permissions. The organization knows that information security of centrally managed identities can be enhanced by requiring MFA. The case company needs a clear policy for protecting privileged identities and knowledge of what kind of solution works best for this specific environment. The policy should cover possible additional verification methods necessary to secure privileged accounts' access to the corporate on-premises resources, such as services, servers, or admin laptops.

This work aims to create a policy proposal on how and in what situations centrally managed identities with privileged permissions should be protected and what kind of MFA solution best meets the organization's requirements.

1.2 Research Questions and Approach

This thesis project aims to find out the current state of the case company centrally managed privileged identity protection by interviewing key persons and by research work. Furthermore, this subject's requirements and development plans

are under interest. The task of the research is to identify the best practices with the help of theoretical information and thereby bring the most suitable approach and solution proposal to the case company. Applied action research approach is used in this study [13]. The work does not include confidential company information.

Research questions are:

1. How centrally managed privileged accounts are protected in the case company´s on-premises environment?

2. What could be the most suitable solution for protecting privileged accounts by following the best practices and organization requirements?

1.3 Thesis Structure

This thesis has been divided into six chapters. First chapter, introduction, briefly describes the need for MFA in general. The case company, the business challenge, and the study’s objectives are described in this chapter. Second chapter, method, and material describe the study's research type, data collection methods, and content analysis phase.

Third chapter called, theoretical background, introduces the possibilities of MFA and different authentication factors. Security challenges will also be covered in this chapter. Next chapter, current state analysis explains how the organization currently protects privileged identities and what are the development wishes and needs.

Developing guidelines to implement MFA in case company chapter covers the proposal of policies and procedures for implementing MFA. The last chapter concentrates on the results and conclusions. In this chapter summary of the research work and results are explained.

2 Method and Material

This thesis uses the basics of qualitative research in data collection and analysis. When analyzing the data and presenting the results, it will be described what kind of perception the researcher had about the researched topic and what meanings were formed from the data analysis. In qualitative research, the researcher decides on the research layout based on his understanding. [14]

This thesis uses applied research to acquire new knowledge of some specific problem or objective and focuses on practically solving the issue [15]. The qualitative research method is used as a research strategy. The qualitative research method can be used to understand specific operations and explain some phenomenon or event [16]. In this study, the organization's employee feedback and visions of the on-premises centrally managed privileged identities state are gathered from the organization using this method.

When doing qualitative research, the researcher must know what he is researching and at least what kind of qualitative research he is not doing. Conducting qualitative research always involves ethical problems. In this study, some ethical questions arise, e.g., How to do research and not reveal possible environmental weak spots, whether some problems need to be fixed before explaining those to the larger audience, to name a few. Researcher must consider what can be written without revealing the organization's faults/vulnerabilities. [14]

2.1 Data Collection

Interview methods were used for the data collection. As a data collection method, the advantage of the interview is its flexibility. During the interviews, it is possible to repeat the question, correct misunderstandings, and talk with the interviewee. The order of the questions can also be changed during the interview. The most important thing is to get as much information as possible about the matter under investigation. The discussion's advantage is that people with experience or knowledge of the subject under study can be selected as interviewees. [14,17]

The reason for choosing the interview as the data collection method was that all the essential participants could be involved in the study to obtain comprehensive information. If a questionnaire method were selected, it could be possible that not everyone would answer the anonymous survey. The interview method was also chosen to provide the researcher with more experience and expand skills in this regard.

The interviews were carried out using a semi-structured theme interview. Semi-structured interviews proceeded with predefined topics with more detailed questions, and the benefit of this is an option to ask more detailed questions based on the interviewee's answers. All the interviewees were asked additional questions under the same thematic topic, and the aim was to get replies to the research topic by the research task. [14,16]

In this study organization's feedback on the current state of the Privileged Identities that are centrally managed was gathered by interviewing the organization's full-time employees. Interviews focused on two more important main topics and built an analysis of the current state of the environment and possible development needs. The first topic consisted of questions related to the technical aspect, documentation, and use practices. The second topic focused on forming an ideal solution for the current environment considering the observations of interviewed persons.

Main topics and more detailed questions were built for the interviews in May 2022. The survey included a total count of 12 broader questions, which 7 focused on the current state of the environment, documentation, and practices. Five questions focused on possible ideal solutions for the environment that should be developed.

The participants for the study were selected based on their job roles and expertise. In qualitative research, it is essential that informants where data is collected know the topics and have some experience with it. Therefore, the selected persons for the interviews should fit the purpose. [16]

2.1.1 GDPR in Interviews

With the entry into force of the General Data Protection Regulation in 2018, which sets requirements to protection of natural persons regarding to the processing of personal data. Various documents are required, which describe, e.g., what and how personal data is processed and by whom? Personal data is information on which a natural person can be identified directly or indirectly. [18,19]

Before the interviews, the necessary reports and documents were prepared from a data protection point of view, such as a participant information sheet, including a privacy notice and participant consent form. The interview material was recorded for later review and analysis in this work. Since a person can be identified from the audio or video material, appropriate documents were prepared and delivered for the participants in advance. The user consent forms were prepared and delivered before the interviews and signed in advance by the person interviewed.

In this work, all the material collected in the interviews has been handled confidentially and according to the legislation. Individual participants have been nameless in this study. All the collected interview material was destroyed at the end of the work.

2.1.2 Interviews

The organization's IT services consist of two teams, the first performing production service development and maintenance tasks and the second providing user support. The case company´s IT department consisted around 20 employees when executing the interviews, and under half of them were employees working on the infrastructure and the solutions.

The interview invitation was delivered to 7 persons who were selected based on their role to achieve a comprehensive perspective of the environment’s current state. Interviewees had different roles and positions in terms of the job description. Identity and Access Management (IAM) group members were all

invited because they have essential information about the state of the organization based on their roles and expertise. In addition, three persons were selected from the management roles and one developer to give feedback. The purpose was to get a perspective from as many angles as possible and extensively, thereby comprehensively mapping the organization's current state with development needs.

The interviews were entirely voluntary, and invitations were sent to the selected seven employees, and these were scheduled for the beginning of June. For conducting the interviews, two different options were offered. The interviewee could choose whether the discussion was held as a virtual meeting or on the organization's premises in a conference room. One hour was allocated for every interview, which was enough in most cases. The interviews were recorded using audio or audio and video for later use.

The interviews aimed to build an overall picture of the current state of the environment to obtain essential information about how protection has been done in terms of policies and practices. This also made it possible to observe the different opinions and thoughts of the interviewees and what kind of technical solutions to secure privileged identities already existed in the environment. All invited attended the interview sessions. The sessions were divided as three people were interviewed at the organization’s premises, and 4 attended a virtual meeting.

At the beginning of August, the interview material review started by performing a content analysis based on the obtained material. Once the interview material had been put into a format that contained reduced expressions, these could be color-coded and classified, based on which a snapshot of the organization's current state of privileged identity protection could be formed. These formed two main categories, current practices, and ideal solutions, which will be discussed in more detail next.

2.2 Content Analysis

Content analysis can be used as an analysis method to analyze the material of all qualitative studies [14]. As the basic principle of content analysis, Tuomi J. and Sarajärvi A. [14] have broken down a rough guideline for doing content analysis. According to them, it is essential first to decide what is of interest in the collected material, go through it and mark the things from the material that are of interest, and leave all other material out of the study. The marked topics could be collected and separated from the other material. Then the material should be classified, themed, or typed, and a summary should be written based on this.

Thematization was chosen as the method of analysis in this thesis, because it was a logical way to help researcher thinking and understanding for gathering a coherent whole from the material, which would answer the research questions.
In the theming, the emphasis is on what has been said about each theme in the interview. An idea in the analysis phase was to collect views describing specific themes from the material. Since the material was collected through thematic interviews, structuring and splitting the material was simple because the themes of the discussions already formed the idea of structuring. [14,17]

The content analysis of my thesis was based on theory. The analysis was guided by the research topic and the interview themes that emerged from the theory. The theory-based analysis framework can be loose. The issues that belong to the researched topic are selected for the analysis frame. [14]

The material-based content analysis creates visibility and clarity of research data so that reliable conclusions can be made about the research phenomenon. Logical reasoning and interpretation are used in data analysis, and data will be broken into parts, reduced, classified, and assembled back into a coherent whole for analysis. [16] It is appropriate to write down the recorded interview material in a purely written form. This is called transcription. [17] The analysis phase started by reducing expressions and removing irrelevant things [14]. The content analysis started by transcribing all the interviews into written form one at a time into their files.

After that, irrelevant text was cut out from the transcribed material. After this step, the content of the questions was extracted from the interview material using bullet points and got the material into a more manageable form.

Then started the phase in the analysis where reduced things and color-coded the answers related to the same theme. With the help of color codes, similarities in the material were searched and marked with the similarities with the same color. At the end of the first phase of analysis, there was an idea of how this research topic manifested itself in the case company. In addition, understanding of the organization’s wishes and development needs increased.

After this step, the color-coded similarities that emerged from the interview’s material were combined. Then similarities that emerged from the different interviews were grouped, which helped in forming the themes from the material. In the theming, things were picked from the material describing the privileged accounts' driving factors. The content analysis was guided by the research questions, and based on that, the main categories for the analysis were created. The upper classes in content analysis were the current practices and ideal solutions. Table 1 shows an example of how classification is done. Table 2 is an example of reduced expressions from the subclass.

Table 1. Example of thesis content analysis phase.

Upper class	Original expression	Reduced expression	Subclass
Current practices	*"Access to the resource needs to be opened separately at the network level or arranged using a terminal server or similar method. The user account itself is a standard account with password protection."*	Access is restricted by network level, a standard user account with password protection.	Access Management
Ideal solutions	*"Practice unification would be clear that it is known that we always act this way."*	*In every case working using the same practices*	Common practices

Table 2 is an example of how subcategories were formulated from the material using thematization.

Table 2. Example of subclass thematization.

Common practices
In every case working using the same practices
Standard policies are done together
Some good practices from cloud service to on-prem
Policy with categorization
Creating missing practices
Standardization of external users' protection
Unifying practices
Variable practices how access is granted to the server

This chapter explained the information details about the research topic formed through analyzing the material based on privileged account protection in on-premises infrastructure. Chapter 4 describes the information obtained through analysis in a condensed and general form. In research, the information obtained from the analysis must be explained and interpreted [17]. An interpretation will be made in chapter 5, where the results of the content analysis are reflected and developing guidelines for implementing MFA and conclusions made based on theoretical knowledge. Last chapter 6 summarizes the research outcome. The next, chapter 3, focuses on going through authentication methods and theory.

3 Theoretical Background

A traditional electronic identity enables logging into a service or system and using the content in the service. Usually, separate digital accounts are used for tasks related to development and maintenance compared to standard accounts when accessing the services. It depends on the environment, requirements, and technical solution abilities to secure those.

A privileged account is any account that provides access and privileges beyond those of non-privileged accounts [20]. These separate accounts have one thing in common. They have more permissions than a standard user account to different resources or objects. This type of identity can be called identities with elevated permissions or privileged user accounts. An example of a privileged account is an IT system administrator or service configurator, which might have a standard user account for daily tasks, but a separate user account for performing operations related to the system or service with special permissions [1]. Privileged accounts should be used only when absolutely necessary and appropriate [21]. Because of their access and elevated capabilities, privileged accounts pose significantly larger risks than standard users [20].

3.1 Privilege Levels

The privilege granted to an account is a special permission or advantage above the regular company user. Rights could be defined according to the organization’s needs to granular fundamental levels. Figure 2 shows an example of five basic levels of privileges used by organizations according to reference [21].

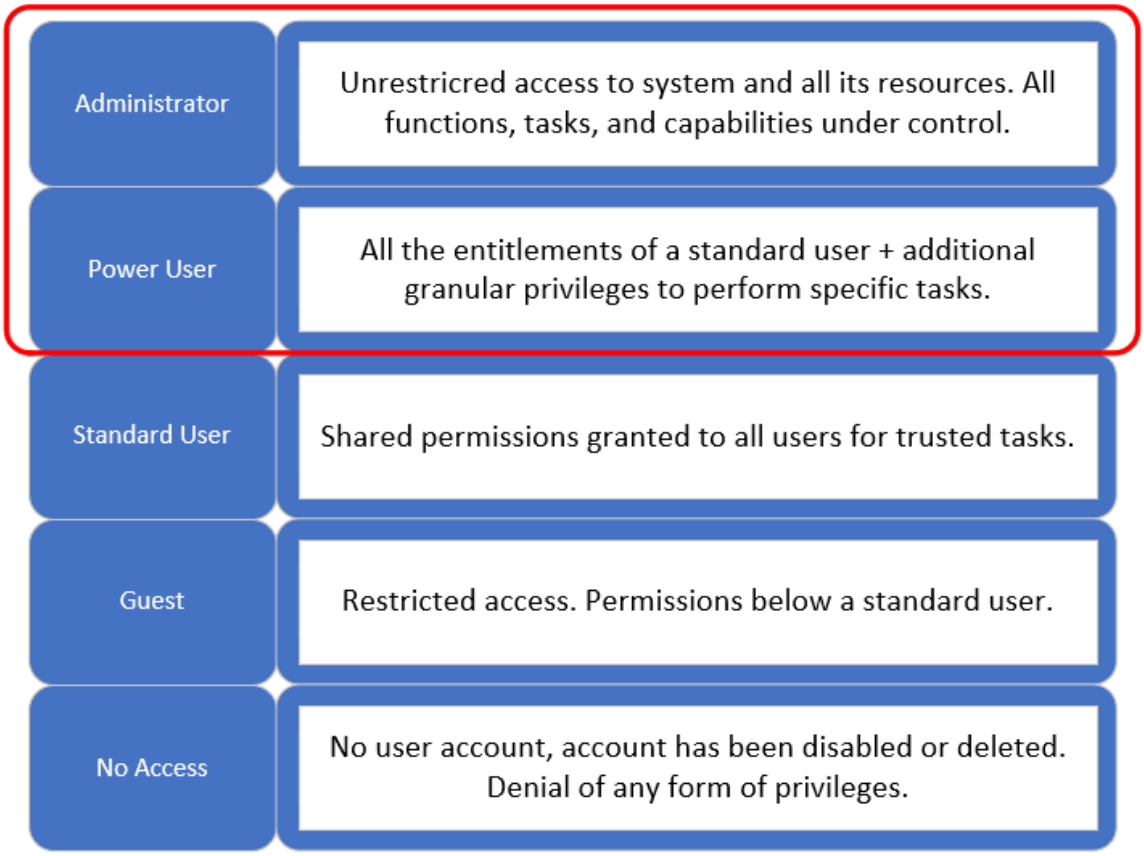

Figure 2. Example of five fundamental levels of privileges. [21]

In Figure 2, Administrators and Power Users are marked inside a red area which in this context means fundamental levels with privileged permissions. Particular attention should be pointed to these user accounts. When comparing these levels in general, Power Users are typically associated with roles in help desk, development, application, and database administration or similar positions. The Administrator level of privileges is the highest and consists of an administrator or root-level permissions to the system, service, or environment. In reference [21], Haber M. discloses, "*Obtaining administrator or root access represents privileged access that is considered the crown jewels to a threat actor.*" [21] This thesis's main scope was to study organization practices and policies related to privileged identities of fundamental level administrators and power users.

3.2 Principle of Least Privilege

The Principle of Least Privilege (PoLP) works as fundamental idea, which can be used when defining access control policies. By following this principle, users

should not be given access to any resources no more than they absolutely need to complete the necessary tasks. This principle is typically focused on ensuring restricting user privileges, but could apply to other subjects also, such as applications and processes. Privilege in this context includes permissions to the data and rights to access to systems and perform tasks. [22,23]

A good example of this approach and why principle of least privilege is important on protecting environment, described by Chapple et all. in reference [23]:

> *“Historically, administrators often gave these service accounts full administrative privileges without considering the principle of least privilege. If attackers compromise the application, they can potentially assume the service account's privileges, granting the attacker full administrative privileges.”*

3.3 Identification and Authentication

The process when a subject claims identity is called identification. To start the authentication, authorization, and accountability processes, a subject must provide an identity to a system. This can be typically done by entering a username, using a smart card, positioning your finger to the fingerprint reader, or showing your face or hand in front of the camera. In authentication, the core principle is that all subjects must have unique identities. [23] User identification and authentication are vital for ensuring the assurance of the user´s rights before granting access to the computers or organization resources [1].

Confirming the identity of the user accessing the services goes through an authentication process. The authorization process tells what users are allowed or denied to do or access. Logging is a process that records the information of who has accessed the system, when, and what has been done. [1]
The subject´s identity is verified in the authentication process by comparing factors against a database of valid identities, for example, user accounts. The authentication information used for this is private and must be protected. Together identification and authentication occurred as a single two-step process,

where the first step is providing identity. The second step is providing authentication information. A Subject cannot gain access to a system without both measures. [23]

In [1], Boonkrong presents an easy-to-understand example of authentication using an Automatic Teller Machine (ATM) cash point.

> *”When the card is inserted into the machine, it is used as a claim of the user’s identity. The next step is for the user to prove that they are really the owner of the card. This is done by the cash point asking something that can only be provided by the actual owner of the card. It could be a four- to six-digit PIN code or a fingerprint. These are examples of factors of authentication.”*

3.4 Multi-factor Authentication

User accounts and organizational resources can be further protected by adding extra layers to the authentication process, i.e., requiring more than one evidence of user identity when accessing the services. The evidence is known as the authentication factor and is used to verify that the identity is what it claims to be. Several factors can be required for authentication before granting access. [1]

Multi-factor authentication uses more than one factor, while single-factor authentication relies on only one authentication factor. MFA is any authentication where multiple methods are used from different categories of factors to prove identity. [23]

- **Two-factor authentication (2FA)**: Requires two methods to verify identity to approve authentication. This is also known as two-step verification.
- **Multi-factor authentication (MFA)**: Requires two or more methods to verify identity to approve authentication. [1,23]

Three most common authentication factors are something you know, something you have, and something you are. When implemented correctly, these types are

progressively stronger. Something you know being the weakest and something you are the strongest. One authentication factor can be any of these methods, but any authentication system with only one has security problems. [1,22,23]

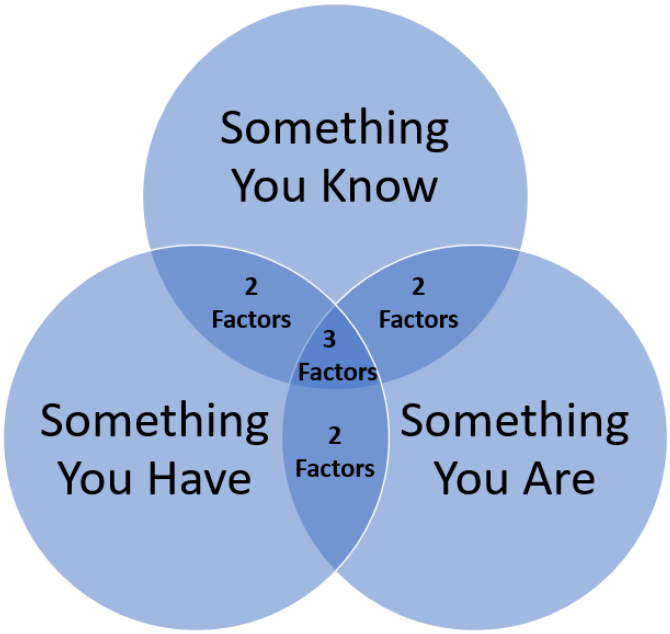

Figure 3. Example of most common authentication factors interaction.

3.4.1 Something You Know

The something-you-know authentication factor category includes memorized secrets such as passwords, personal identification numbers (PINs), and passphrases. Even answers to secret questions belong to this factor form. [1,22,23]

Password

These knowledge-based factors are things that only the user should know [24]. The password is the most common authentication technique, consisting of a user's string of characters. As a security mechanism, passwords are weak for many reasons. The password, which is easy to remember, will be easy to guess or crack. Password that is hard to remember causes users to write them down or forget them. Users tend to share passwords, and there might be problems with encryption protocols for securing transmissions. How password databases are

protected and located affects password security. Passwords are also vulnerable, for example, to brute-force attacks if weak passwords are used. [23]
The ideal password should follow the criteria in reference [1]:

- Possible to remember
- Computer system can verify
- No one else can guess
- Is long enough

Related to memorized secrets, there are recommendations provided by the National Institute of Standards and Technology (NIST) in SP 800-63B “Digital Identity Guidelines: Authentication and Lifecycle Management” document [25]. Following the recommendation, it is possible to improve password security, but the knowledge-based factor is still the weakest form of factor.

These password recommendations are updated regularly and are changing. The following list summarizes the latest changes recommended by NIST according to reference [23]:

- Password must be hashed
- Passwords should not expire
- Users should not be required to use special characters
- Users should be able to copy and paste passwords
- Users should be able to use all characters
- Password length should be between 8-64 characters
- Password system should screen passwords

Passwords storing or transmitting in cleartext could cause security problems, and hashing is needed. Hashing passwords means transforming the password string into a random looking string of letters and numbers before storing it in the database. This hash value will be compared to the hash value of the user password typed in when authenticating to the service, and in case of a match, the password is correct. Hashed passwords are a vulnerable example of the

rainbow table attack. The rainbow table is a database of precalculated password hashes that can be used to compare hashes, for instance, found from the database. Salting the password hashes makes these more secure against this type of attack. Salting means adding a random string of letters and numbers to the beginning or the end of a password before hashing. Extending password tolerance against this attack can be produced by using dynamically generated salt values (different salts concatenated to different passwords) and placing them in appropriate positions. [1]

Different algorithms can be used for hashing the passwords, which all transform strings into sequences related to the used algorithm. For example, SHA-256 transforms any string into a 256-bit sequence, representing 64 characters of hexadecimal. Currently original passwords cannot be recovered mathematically from these hashes because these are one-way transformations, but this could change in the future. [26]

Table 3. Example password hashes (SHA-256) values without salting.

Password	**Hash (SHA-256)**
password	5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
12345678	ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f
Salamipizza-On-Every-Friday4Me!	d49f12bde0395fc94aafe89511d0b6fcf26209e4ff4204fe6e3de733a1a0011c

Iterating means repeating that specific algorithm that uses computing power multiple times, causing password-cracking attacks to linearly slow down by iteration times. For example, Microsoft Azure Active Directory, a cloud-based identity and access management service, uses 1000 iterations of SHA-256 over salted passwords to generate per-user password hash when synchronizing passwords to the cloud service. [26,27]

NIST SP 800-63B recommends not requiring the expiration of passwords regularly because users tend to use easy-to-remember passwords and change only a single character, which does not add security while still complying with the requirements of password change. The same methods can be used when guessing passwords by hackers. This differs from the Payment Card Industry Data Security Standard (PCI DSS) version 3.2.1, where passwords should expire at least every 90 days. Organizations should at least follow the standard minimum requirement when a specific standard needs to comply. [23]

The requirement of special characters in the user's passwords challenges the user´s memory and could lead to writing these down. Copy and paste capability with password manager software allows users to create and store complex passwords. One password is required to remember for accessing the stored passwords, and these could be used from there. If there are restrictions for copying and pasting, users must retype passwords many times, which might lead to using easier passwords. [23]

Allowing the use of all characters in passwords, such as spaces, users can create longer passwords while still being easier to remember. In preventing attacks by rejecting special characters, the system can be avoided by adequately hashing the password for masking these characters. When allowing longer lengths for passwords enables users to create meaningful passphrases. [23] The minimum password length of 8 characters generated by the user is found from NIST SP 800-63B recommendation and should be possible to use up to 64 characters [25].

Some differences exist between recommendations for the minimum lengths; for example, PCI-DSS (version 3.2.1) is defined as seven at least [23]. European Union Agency for Cybersecurity (ENISA) recommends that users use a long and random password. Password length of 14 or more characters makes it virtually un-cracable with currently available computing power, because every added character increases the cracking time by orders of magnitude [28]. However, the computing power available for password cracking increases exponentially following Moore's Law. This means, that if current password-hashes are stored by malicious users it is possible to crack the password later. Before accepting a

new password, systems should check that it is not in a list of commonly used passwords. [23]

Grid-Based Passwords

An alternative form of knowledge-based authentication is a grid-based password. Graphical password use pictures within a given grid. The reason for this is the fact that humans can remember pictures better than text. This method works by having users select a precise set of images instead of a traditional password.

One example of a graphical password is an android pattern lock, where the password is given by drawing a pattern and connecting dots. [1]

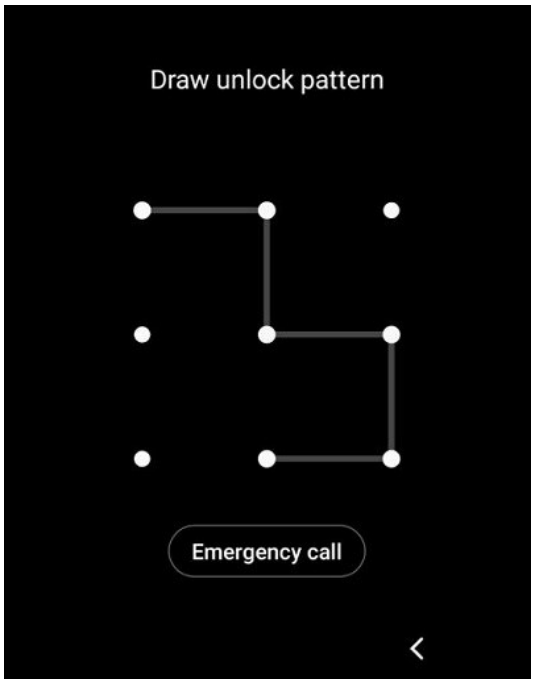

Figure 4. Android drawing pattern example.

Personal Identification Number (PIN)

PINs are the most commonly used to unlock mobile phones or tablets and in card transitions. [24] Typically, PINs are four, six, or eight numbers long. [23]

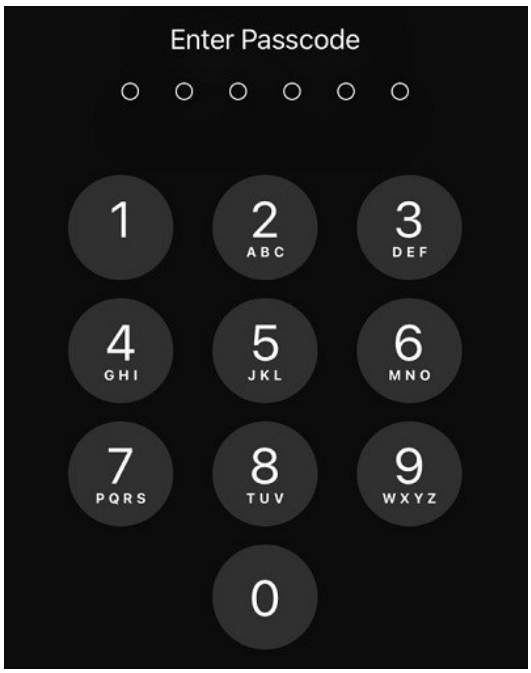

Figure 5. Apple mobile phone PIN-code example.

Security Questions

Security questions are a knowledge-based method and a common social technique used by organizations, for example, when setting up a new account. Private and personal information can be asked and used to verify the user against their account. Because information related to these questions could be available, for example, in social media, stolen in a data breach, or might be information other people know, there are risks when used. Preventing an exploit based on the security questions and answers [21]:

- Never re-use security questions and answers
- Consider providing false information when responding
- Consider using the password complexity philosophy in answers

Security questions are also vulnerable to social engineering because they are facts about yourself. [21] These questions could be more secure if responses are false information. Password complexity philosophy can be used in the answers.

Table 4. Examples of security questions and false information are given in the answers.

Security question	Answer with false information
What is your favorite food?	Porsche911-is-expensive-Car$
What is your mother´s middle name?	Course-Is-Starting-At-8-On-Mondays.
Where have you born?	Salamipizza-On-Every-Friday4Me!

3.4.2 Something You Have

Possessing a physical item that can be used for authentication inheres to something you have a factor of authentication. This includes authentication tokens and smartcards. [1] The “magic links”, hyperlinks with an embedded one-time code emailed to the address associated with the account, inheres to this authentication factor because clicking on the link proves possession of the email account [22]. The possession type of factor is commonly combined with other factors for providing multi-factor authentication, but it is rarely used by itself. [23]

Popular authentication methods via this factor are tokens that may be connected, disconnected or contactless. Universal Serial Bus (USB) key and a smart card are common forms of connected tokens; when disconnected tokens are usually in the form of a key fob or soft token used in the authenticator app on the mobile phone. [24]

Short Message Service (SMS) is also a disconnected token in authentication, which works by receiving the code to a mobile phone as a text message and code used to authenticate the user´s identity. This very popular authentication factor has many problems. When SMS OTP is sent to the user´s mobile phone, there is no way for the OTP transmitter, e.g., the website, to know OTP has arrived at the intended destination. [1] SMS OTP is also vulnerable to SIM jacking, which is account hijacking and takeover attack. A threat actor can capture the SIM number and recode another device using the same number to obtain access to phone data. This is a significant privileged vector of attack. [21]

Contactless authentication does not require device used for authentication to touch a reader but be close enough. Radio-frequency Identification (RFID) and Near Field Communication (NFC) are two standard technologies involved in contactless authentication. [24]

Certificates

Digital certificates provide assurance that the people they are communicating with truly are whom they claim to be for communicating parties. [23] Cryptography is used to protect communication and information and is typically done by using techniques to scramble plain text into ciphertext and reverse it. Encryption is the process of scrambling and decryption is the reverse process. Two types of encryptions exist, that are symmetric encryption and asymmetric encryption. The same key for encryption and decryption is used in symmetric encryption. Asymmetric encryption uses two mathematically related keys, which are used to perform encryption and decryption. One key is public, used for encryption, and the other is private, used for decrypting. [29]

Digital certificate construction is governed by an international standard X.509 and contains the following data: version, serial number, signature algorithm, issuer name, validity period, subject´s name, and public key. [23]

Certificate-based authentication (CBA) uses a digital certificate derived from cryptography to identify a user or a device. It is more secure than the username + password combination and can be used for strong user authentication or phishing-resistant MFA. Certificate-based client authentication leverages what the user has (a private key), which is impossible to gain using phishing, guessing, or social engineering. [30]

Authentication Tokens

A password-generating device used in authentication is a token device or hardware token. [23] A hardware authentication token is a device that has been used traditionally as the second factor of authentication. Two authentication tokens are used today, a synchronous token and an asynchronous token. [1] These devices use dynamic one-time passwords (OTP), which makes them more secure than static passwords [23].

- Synchronous Dynamic Password Tokens

  Time-based and synchronized with an authentication server or with an authenticator. New numeric code is generated periodically, such as every 30 or 60 seconds. The time is used to generate a number used during the user login phase in the authentication. Accurate time is required for token and authentication server or authenticator. Synchronous tokens use the time-based one-time password (TOTP) algorithm. [1,23] Figure 6 is an example of a traditional key fob, a synchronous hardware token. Another example of this type is the OTP process, where time is a moving factor, as illustrated in Figure 7.

Figure 6. Example of an RSA key fob, is a synchronous hardware token. [31]

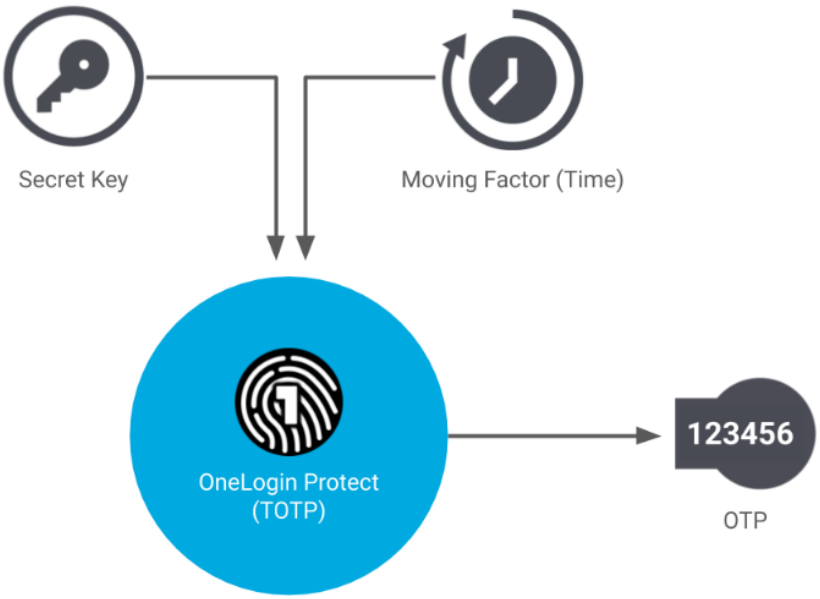

Figure 7. OneLogin example of synchronous OTP process. [32]

A mobile phone´s authenticator application is an excellent example of a software-based security token used for authentication. Software tokens can be stored on desktops, laptops, mobile phones, and other electric devices. Software tokens can use the TOTP algorithm. A slightly modified presentation of logging into a Microsoft service with Microsoft Authenticator without a password is shown in Figure 8.

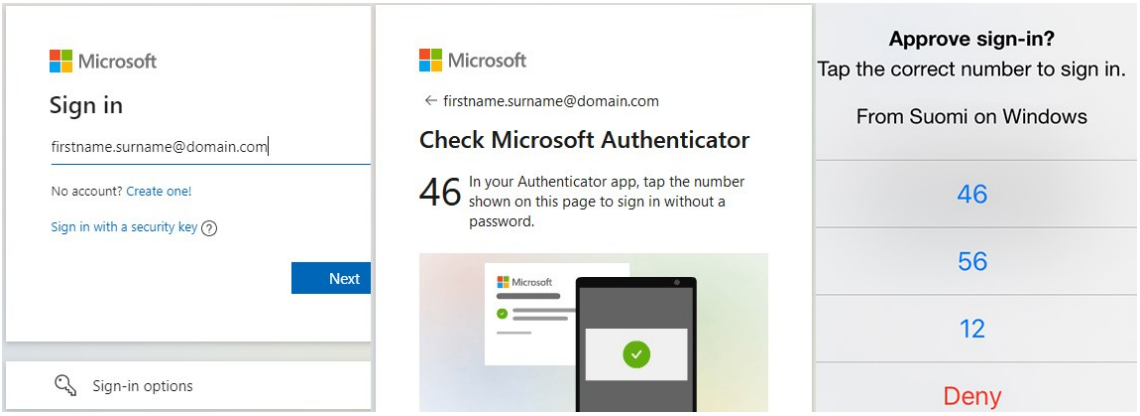

Figure 8. Microsoft authenticator passwordless sign-in.

- Asynchronous Dynamic Password Tokens

Hardware token generates numerical codes based on an algorithm and an incremental counter. Time is not used in asynchronous tokens, and authentication servers and tokens are not required to be time-synchronized. Dynamic one-time passcode stays the same until used for authentication. For example, the user authenticates to the system, the authentication server sends a random sequence of digits to the user which will be entered into the token. An authentication token will generate a passcode from the entered values as a response. Then the user enters the one-time password into the system to gain access. Asynchronous token uses a hash-based one-time password (HOTP) algorithm. [1] Figure 9 shows how the moving factor of counter affects OTP generation.

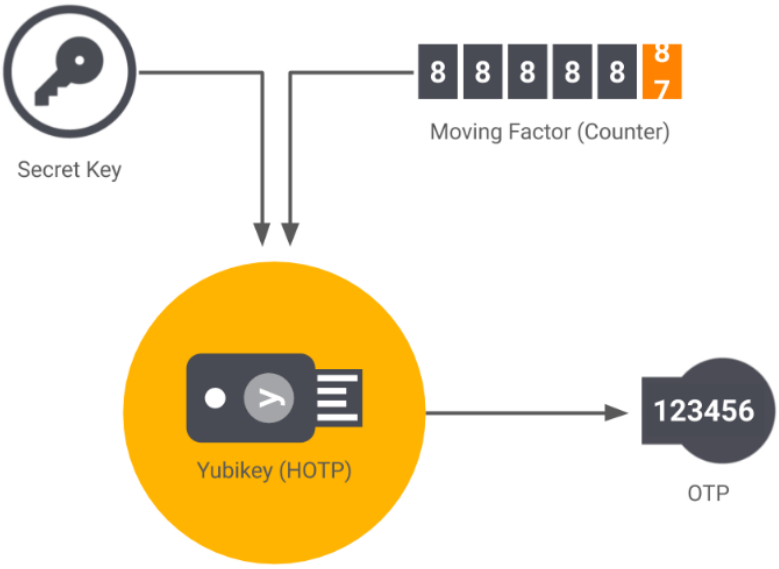

Figure 9. OneLogin example of OTP with YubiKey asynchronous token. [32]

The One-time Password works only once, and a new one is generated every time a hardware token is used. In Figure 10, encrypted OTP is built of unique passcode and counterparts.

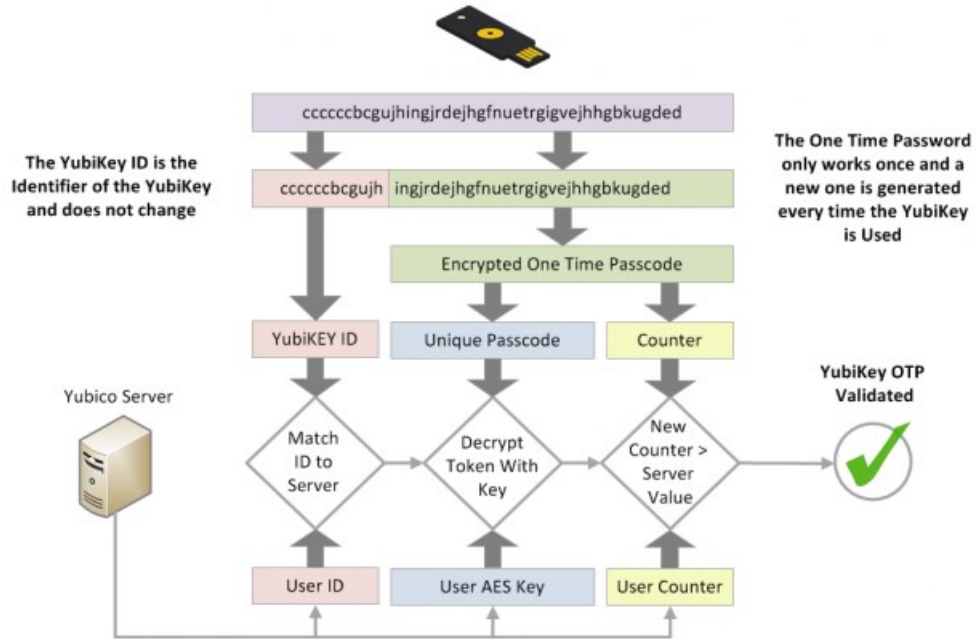

Figure 10. YubiKey OTP generation with the counter. [33]

When using hardware tokens such as YubiKey to access the services, it is possible to require other factors before granting access. For example, in Figure 11, the YubiKey model 5 NFC token is set to require a knowledge factor by the user entering a PIN and touching an external button in the security key to verify the user's presence.

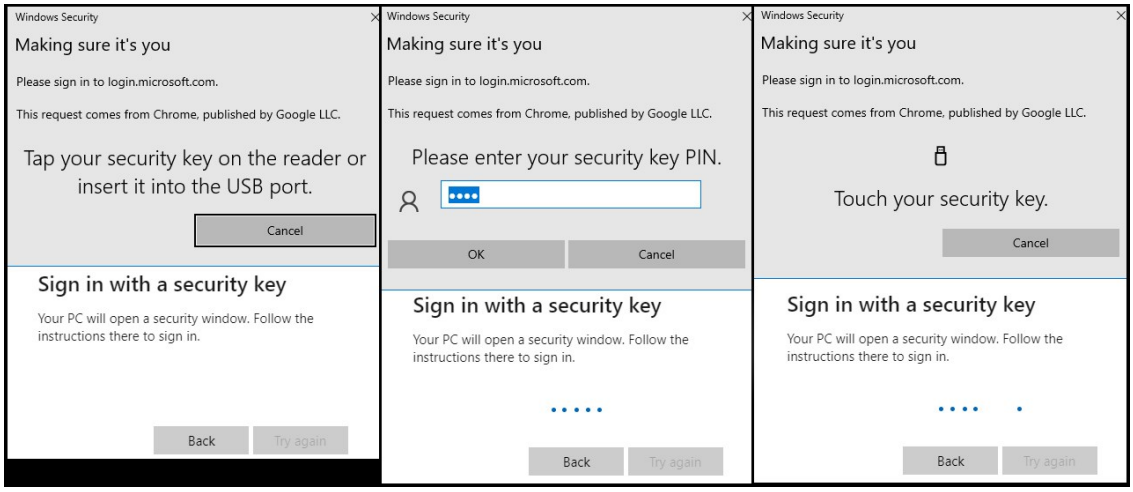

Figure 11. YubiKey security key sign-in with PIN.

The Fast ID Online (FIDO) Alliance is an open industry association working to change the nature of authentication with open standards that are more secure than passwords and simpler to use and manage. Three sets of specifications are published by the Alliance, which are: FIDO Universal Authentication Framework (FIDO UAF), FIDO Universal Second Factor (FIDO U2F), and the Client to Authenticator Protocols (CTAP). This last (CTAP) is complementary to the W3C´s Web Authentication (WebAuthn) specification, and together these are known as FIDO2. FIDO2 supports passwordless, second-factor, and multi-factor authentication user experience with embedded authenticators such as PIN in Figure 11 used with a hardware token. [34]

The hardware security keys, such as YubiKey, can also be used for smartcard login purposes. Still, a security key is required with the application as the credentials reside on the hardware token. This security enhancement makes it possible to use these for allowing access to smartcard-protected resources, such as certificate-based virtual private networks (VPN) or email. Depending on the organization’s security requirements, these can be used similarly to smartcards in the authentication. For example, YubiKey 5 Cryptographic module is validated with the Federal Information Processing Standard Publication 140-2 (FIPS 140-2) validation process, which is issued by NIST to coordinate the requirements and standards for cryptography modules, including both hardware and software components. Certificates of validation and levels of security can be used for the requirements and to use security keys for logging into laptops, desktops, and mobile devices. YubiKey 5 Cryptographic module meets FIPS 140-2 requirements with level 2 overall and level 3 on physical security with certificate. [35]

Strong authentication can be provided by using hardware tokens. Attention must be paid to cases where the device is lost, breaks, or runs out of battery. When this happens, users cannot gain access to the systems. [23]

Smart Cards

A smart card is a regular card with a circuit integrated into it, which will be read when the circuit interacts with the device reading it. A bank card is an example of a smart card that requires a PIN code as an additional measure when performing authentication. [24] Smartcards can be used for authentication with desktops, laptops, and other electric devices, but additional smart card hardware or smart card reader is needed — Figure 12 Finnish ID card with smart card chip which can hold citizens' certificate for electronic transactions.

Figure 12. Picture of Finnish ID card with smartcard chip from European Council Public Register of Authentic identity and travel Documents Online (PRADO). [36]

Smart cards provide tamper-resistant storage for protecting private keys and other personal information. Isolation of security-critical computations, such as authentication from other parts of the computer, is performed on the smart card. Smart cards offer portability between computers at home and work. [37]

Virtual smart cards have similar functionality than physical smart cards, but those are always inserted. Virtual smart cards can be used, for example, to logon authentication. When a Trusted Platform Module (TPM) chip is found in a device such as a laptop, it can be configured and used to provision a sign-in certificate. Similar to with physical smart card, the user need only provide the PIN for the virtual smart card to sign in to the domain example. [38]

3.4.3 Something You Are

Today devices and computer systems are designed to provide password-free authentication using biometrics. Physiological or behavioural characteristics unique to individuals can be used in biometrics. Many organizations are adopting methods to enable employees to enter buildings, access the services in the cloud, and log in to mobile phones and computers using biometric authentication. [39]

The body measurements are used in the process of biometric authentication. This authentication requires biometric information, such as fingerprint, palm print, face, iris, or retina. A good example is a person entering a bank and being identified and authenticated by a bank official based on the biometric parameters of face by comparing an ID card picture to a natural person. [1]

When a system needs to identify an individual, it first takes biometrics in which to compare and then searches a biometric pattern database to attempt to identify the person correctly. This identification method is a one-to-many comparison. When biometrics are used in authentication, it is a one-to-one comparison by matching the captured biometrics with a registered biometric template in the system database, as shown in Figure 13. [39]

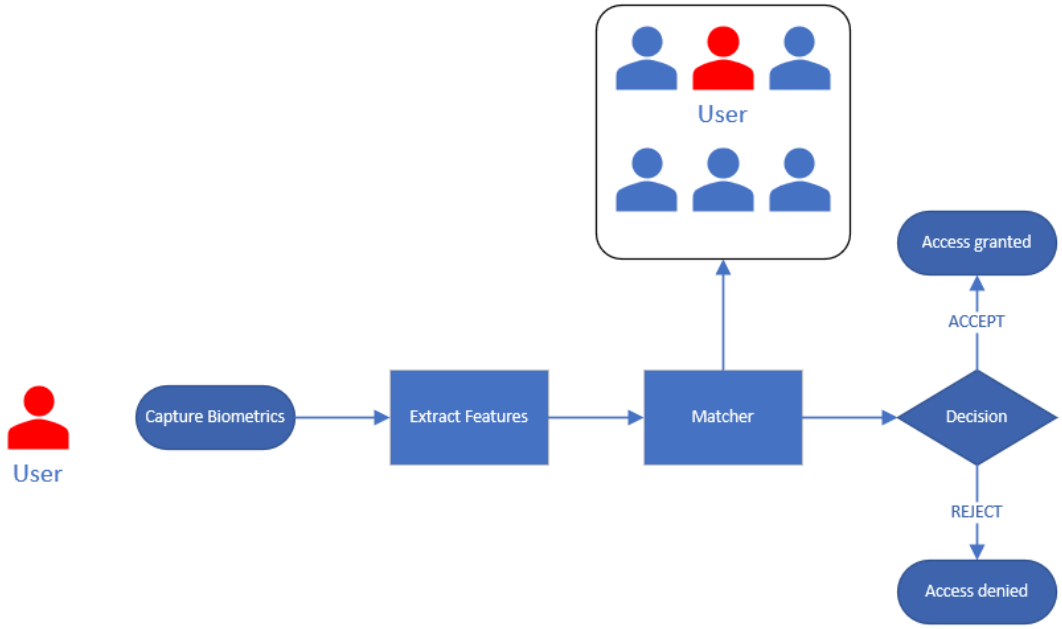

Figure 13. Biometrics used in authentication is a one-to-one comparison. [39]

The biometric authentication process works in two main parts: registration and authentication. Biometric data can be captured using sensing devices, such as fingerprint scanners for fingerprints or cameras for facial recognition, and utilized later in authentication for recognition. [1]

Physiological attributes in biometrical authentication include the following common methods according to the reference [39]:

- **Fingerprint recognition**

  Recognition of fingerprints is optimal biometrics. This is because the fingerprints are unique and have detailed characteristics. This is one of the very first biometrics used.

- **Iris recognition**

  The iris, or the coloured part of the eye, is used for iris recognition, which presents a unique, non-invasive biometric. The participant does not have to touch a device because the camera captures the image.

- **Facial recognition**

  A person´s face is scanned by the camera and measured face including eye spacing, the width of the nose, the forehead, and the chin.

- **Hand geometry**

  For reading hand geometry, the device measures each finger and the hand when placed on the device. This is one of the oldest automated biometrics.

Related to biometrics, there are research challenges of the measurement of the quality of biometric samples. Fingerprint recognition systems can suffer degrading performance because of poor-quality fingerprint images, leading to incorrect detection. The usability of the sensor affects the quality of the sample.

Environmental factors like humidity and temperature might affect the quality of a biometrics on fingerprints, for example. Facial recognition has challenges, and quality measures are an essential feature of modern face biometric systems. This is because there are a lot of possible variations in face images. Face recognition performance is affected, for example, pose, illumination, expression, and noise. [40]

The trend shows that using a biometric authentication technology is replacing traditional methods. There are many advantages to using biometrics, including the fact that they cannot be forgotten, such as passwords, they may be lost only in rare cases, and they are always with you. [39]

Security concerns in biometric authentication

Biometric authentication can be used for achieving passwordless authentication for the users as a more secure and convenient option for credentials as well as one factor in MFA. One widely adopted passwordless authentication system is Microsoft´s Windows Hello. It enables login using PIN, fingerprint, or facial recognition. Windows Hello facial recognition authentication requires a specific type of camera with two separate sensors that work together as one USB device. A standard camera which is supporting RGB and infra-red (IR) sensor. [41,42]

According to Cyber Ark, in the hopes of strengthening biometric security overall, the research team had exploring potential weaknesses of these biometric solutions. CyberArk Labs research team did research in 2021, where the team were able to use vulnerability against the face recognition mechanism of Windows Hello. The team showed how Windows Hello could be bypassed using an external crafted USB device. A successfully exploiting vulnerability required that an attacker had physical access to the device and the user was already enrolled in Windows Hello face authentication. They were then manipulating the authentication process by capturing the IR frame of the target or recreating a photo of the target´s face and subsequently plugging in a custom-made USB device to inject the spoofed images into the authentication host. Microsoft

addressed this vulnerability in 2021, implementing restrictions that only trusted cameras were allowed to use. [41,43]

According to reference [22], the most significant disadvantage of inherence factors is that biometric characteristic can be cheated or duplicated. Related the United States Office of Personnel Management (OPM) data breach announced in 2015, where hackers took 5.6 million federal employees' fingerprints, demonstrates that these are also prone to thefts [44]. There is little recourse once a biometric identification characteristic is compromised. It´s not easily issued new irises or fingerprints to replace the compromised ones. [22]

3.5 MFA Protection Types

Multiple types of MFA combination possibilities are available based on different factors used and the protection strength. According to reference [45], Microsoft has a concept of MFA strengths in Azure Active Directory (Azure AD) divided into the following way:

- ***MFA strength***, which means requiring more than one factor of authentication, including knowledge-based factors.
- ***Passwordless MFA strength*** is a combination of methods satisfying MFA, but knowledge-based factors are not used, such as passwords.
- ***Phishing-resistant MFA strength*** requires an interaction between the authentication method and the sign-in surface.

Authentication method combination	MFA strength	Passwordless MFA strength	Phishing-resistant MFA strength
FIDO2 security key	✅	✅	✅
Windows Hello for Business	✅	✅	✅
Certificate-based authentication (Multi-Factor)	✅	✅	✅
Microsoft Authenticator (Phone Sign-in)	✅	✅	
Temporary Access Pass (One-time use AND Multi-use)	✅		
Password + something you have[1]	✅		
Federated single-factor + something you have[1]	✅		
Federated Multi-Factor	✅		
Certificate-based authentication (single-factor)			
SMS sign-in			
Password			
Federated single-factor			

Figure 14. Multi-factor authentication strengths in Microsoft Azure AD. [45]

Depending on the need for MFA authentication, these combinations can achieve the needed protection level. For example, because knowledge-based authentication is vulnerable to many authentication attacks, passwordless MFA or phishing-resistant MFA could be appropriate solutions for higher protections needs.

3.6 Conditional Factor

Other conditions can be used with something-you-know, something-you-have, and something-you-are authentication factors for verifying authentication requirements.

Privileged Access Workstations

Privileged Access Workstations (PAW) are computers that have specific configurations for performing remote administration tasks. The reason to use this kind of computer are security concerns, which rely on the fact that servers are only as secure as the computer used for managing them. Security incidents may occur when privileged users´ computers are infected with malware and used for administering servers. This PAW computer is used only for administering, not for example, reading email, or browsing the internet. [46]

National Cyber Security Centre (NCSC) has guidance on securing system administration with five principles that could be applied to Information Technology (IT) systems. The one principle deals with management devices according to the reference [47]:

> *"**Gain trust in your management devices***
> *You need to be able to trust the devices you use to access your system administration interfaces. If not appropriately secured, an attacker could use them to gain access to your systems, leveraging legitimate administration functionality."*

Referring to this guidance, management devices used by administrators or similar privileged user accounts must be trusted. Administration interfaces are accessible only from trusted sources for securing those because, in case of compromise, the attacker could inherit the same level of access. A dedicated Privileged Access Workstation solution is widespread to use when administering higher-tier services. Typically, these workstations have restrictions and controls that reduce the device's attack surface. [47]

Somewhere You Are

This location-based authentication factor could be used to support other factors. The physical location of the supplicant could be used when requesting to have access directly to the computer, appliance, or device instead of using the network for accessing the service. Internet Protocol (IP) address could be used to detect the location of the supplicant. This can be useful if geolocation is required by the service or access is restricted by the IP level. [1]

Geofencing could also be used to define the location of the device. [39] According to reference [22], location factors are not commonly secure enough to be used for authentication on their own.

4 Current State Analysis

In the research work on the organization’s current state, the aim was to find out the existing policies and procedures related to the on-premises infrastructure centrally managed privileged accounts, and current protection methods, as well as the state of will for change. This work also mapped out what technical procedures there were and the technical possibilities currently for protecting privileged accounts.

Ideas and thoughts were asked during the interviews about what kind of development ideas have been observed and identified in this regard. With the help of the interviews, it was easier to find out what kind of technical implementation would best serve to protect the privileged accounts and secure the data in this environment.

The work started by familiarizing with the topic in terms of literature and other related material, observing activities in the environment, and going through existing documents. Decision was made that detailed information regarding the current state of the environment could best be collected by conducting a semi-structured thematic interview for selected personnel using a qualitative method. The qualitative method works well here because it allows understanding of the solutions and the ways of working, and at the same time, ask for opinions on how these could be improved or what should be considered. During the interviews and later, when familiarized with the recorded material, it emerged that the environment contains multiple different systems and services. Different persons are responsible for their own areas of the environment; there were many aspects of how things are done in many ways.

4.1 Current Practices

The research data reveals that the practices of identity protection are varied and somewhat fragmented. Different parties in the environment handle these privileged accounts with a variety of requirements. There was no clear, uniform

practice regarding these. The guidance of how different roles interact with fundamental levels of privileged accounts needed improvements.

Based on the material obtained, the holders of the various roles had a good picture and understanding of how the protection of these accounts is done regarding their systems, as well as a well-established operating method. However, the functions of the organization IT services are working in their own way related to privileged identity protection and could benefit if having unified guidelines for the requirements. Several interviewees pointed out that there is quite a lot of silent information, and at the system level protections are handled in various ways regarding these privileged accounts.

It was strongly pointed out that a change is needed. Clear, uniform practices and guidelines were needed. The material revealed the need for documentation of these practices and possibly some "checklist"-style instructions when protecting privileged accounts. Two interviewees pointed out that there is much tacit information regarding practices, what is transferred to colleagues, how to operate and what is required of the systems. Tacit to the tacit form of knowledge sharing that creates knowledge for the individual rather than the organization [48].

The organization's tacit knowledge can be seen as community-shaped operating procedures and jointly built expertise. Unspoken knowledge is considered an asset of the expert community, in which case it is located both physically in a particular place and psychologically in the communal activities of specific individuals working efficiently together. [49]

4.2 Technical Implementation

The environment strongly relies on a single factor for authentication in the on-premises infrastructure, often a combination of a username and a password. There were different kinds of restrictions in place related to password length or life cycle. All the interviewees mentioned that restricting access to the services as additional protection is network-based. There were also other ways for securing authentication, such as certificate-based authentication, biometric

identification, and restricting access with a local firewall. However, these were alternative ways of doing authentication, but not mandatory in an on-premises environment.

All the interviewees felt that the password and username combination alone does not provide enough protection for these privileged accounts, and more factors are needed. This topic was considered very current and essential to promote. Various technical restrictions have been implemented regarding the centrally managed privileged accounts. Administrator accounts and similar accounts with more permissions are generally differentiated from standard accounts, and there are different requirements in place. The environment consists of subject areas tied to different functions. Some of these have followed best practices regarding elevated access rights and built various protection mechanisms. However, there is variability as a whole.

4.3 Ideal Solutions

The interviews also discussed what kind of solution would be ideal for improving the current model. Improvements and development were wanted regarding these privileged account’s protection. Many of the interviewees pointed out that the mobile phone authenticator app, which is already commonly used in many places, has been perceived as a good and easy way to use in authentication.

Several interviewees pointed out that the solution should be easy to use. It should not hinder or paralyze work. However, the solution should be sufficiently secure and based on some classification, enabling different requirements regarding these identifiers. Regarding the number of different factors, two factors are sufficient for the organization's environment and provide good additional security in most cases.

From the material, it could be observed that Identities that have much influence on the environment, such as domain administrator credentials, felt that there could be more than two factors. This was not perceived as harmful because these credentials are used less often.

The solution should therefore enable the classification of accounts and different requirements based on the identity effectiveness or fundamental privilege level. Based on the material, some also brought up that, in addition to the authenticator, there could be backup methods for logging in if the phone where the authenticator is located is lost. Hardware security keys such as YubiKey were brought up, which could serve as a good backup and possibly an additional factor, e.g., for domain admins or similar high permission level accounts.

Increasing the understanding of the subject and in which situations it would be possible to use additional identification methods sensibly would serve well, as well as understanding these limitations. Passwordless login (“pwless”) also came up in a few interviews, either as a mere alternative for specific needs or as factors such as passwordless MFA. This authentication verification method would be the best solution when targeted at high protection needed privileged identities. Regarding workstations, it was felt that some additional security would also be desired for administrators' laptops.

5 Developing Guidelines to Implement MFA in Case Company

Implementing MFA for all organization users, including standard non-privileged accounts, is recommended. This helps protect the organization's identities and assets by increasing security. In the case of privileged accounts and special types of privileged accounts which have unrestricted access to the environment or a major business impact, it is highly recommended to protect them using strong authentication with additional authentication factors. Potential impact on the environment, if compromised, could cause a catastrophic condition. [20]

Different levels of security can be used for the organization to start to implement a security strategy, and it should be kept simple to achieve. Figure 15 is an example of Microsoft's Privileged Access strategy, which has three levels of security, which are: Enterprise Security, Specialized Security and Privileged Access. This strategy model and these levels are designed to provide simple and straightforward technical guidance for organizations. Each role in the environment should be pointed to one of these security levels. Clear written documentation must be in a place where the criteria for each level are defined. [50]

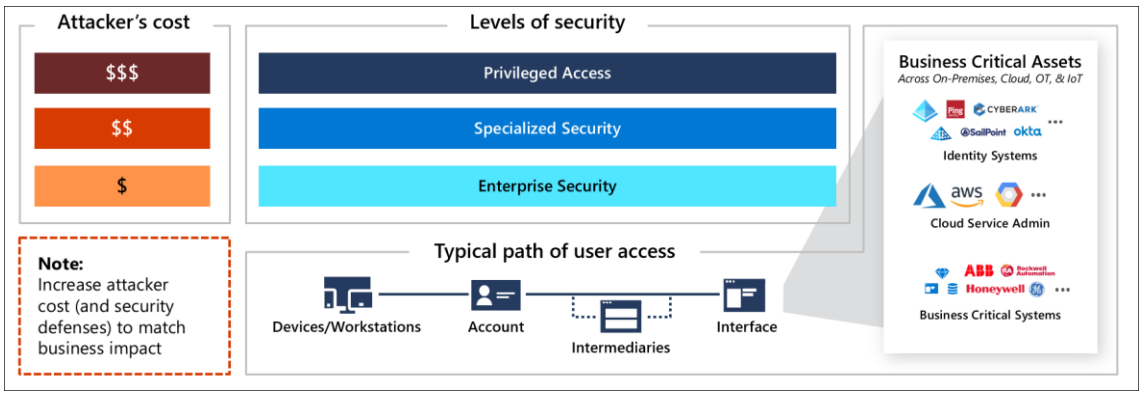

Figure 15. Microsoft example of a Privileged Access Security strategy with three levels of security. [50]

In this example, Enterprise Security is the basic level of security required and suitable for all organization users. Specialized Security provides more security controls for the roles with an elevated business impact. Roles that could belong to the Specialized Security requirements are, for example, organization

developers, executives, or other business-sensitive role holders. Privileged Security is the highest level of security and typically includes, for example identity management roles with administrative permissions, enterprise admins, domain admins, and other accounts with much influence on the environment. [50]

This thesis aims to build guidelines for protecting privileged user accounts with MFA. As shown in Figure 15, a similar approach can be applied to these fundamental privilege levels suitable for the organization, as in Figure 16 for Power Users and Administrators.

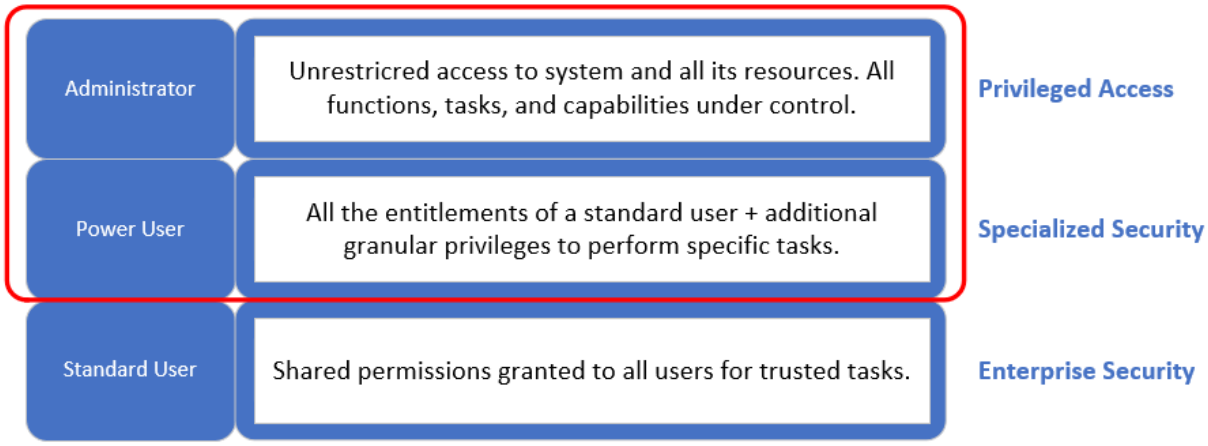

Figure 16. Privileged Accounts and security levels. [21,50]

Special types of privileged accounts, such as superusers, for example, domain administrators with unrestricted access to the environment workstations and servers, belong to the Privileged Access security level. The accounts at this type of level should be closely monitored, and prevention methods should be used. Prevention methods mean adding different controls to restrict usage of the accounts to the designated workstations, devices, and intermediaries for protection. [20,50]

This differs from the Specialized Security level, the fundamental level of Power Users, which should also be protected with MFA, but no prevention methods are mandatory. These users could be working using same laptops on daily basis tasks and when using systems with Power Users permissions. A terminal server

or intermediate path to the assets can be used, but a dedicated restricted laptop, i.e., PAW is not mandatory. [50]

At the beginning of the work, the interviews also mapped out an alternative where additional security would be implemented for the administrators' portable workstations with MFA. This is a good way to improve information security, but acquiring separate workstations for maintenance activities is recommended, where privileged access levels are used. In addition, there should be exact restrictions on how these devices can be used and what resources are allowed to access. [50]

For example, surfing the internet or reading e-mail is not allowed with a dedicated PAW device. This can reduce attack vectors and enable a safer environment for maintenance activities. Separate dedicated laptops should be used for high-level handling tasks and if the credentials have a very broad and potentially critical business impact. In this way, credentials with elevated user rights can be better secured against lateral movement attacks, e.g., standard user account machine is compromised, and password hashes are obtained by an attacker. This will not cause losing privileged user account password hash, and permit possible access to more sensitive accounts or resources, such as servers because hash does not exist in this machine. [46,51]

5.1 Policy

It is essential to define a clear written policy for the organization on how privileged user accounts are to be protected. For example, the conditions when a specific user account will be assigned to a category of privileged accounts, and to which type. Before categorizing privileged user accounts the least privilege principle must be used with multiple security layers.

According to reference [50], Microsoft defined category levels of security consists the following types of accounts that could be used for categorizing the organization privileged accounts based on the features:

*"**Specialized security** provides increased security controls for roles with an elevated business impact (if compromised by an attacker or malicious insider)."*

*"**Privileged security** is the highest level of security designed for roles that could easily cause a major incident and potential material damage to the organization in the hands of an attacker or malicious insider. This level typically includes technical roles with administrative permissions on most or all enterprise systems (and sometimes includes a select few business critical roles)*
Privileged accounts are focused on security first, with productivity defined as the ability to easily and securely perform sensitive job tasks securely. These roles will not have the ability to do both sensitive work and general productivity tasks (browse the web, install and use any app) using the same account or the same device/workstation. They will have highly restricted accounts and workstations with increased monitoring of their actions for anomalous activity that could represent attacker activity."

Two different types of categories are at least to be recommended for the case company for privileged access accounts. Those categories should be based on the impact of business, privileged account type, and features. [21,50] The categories have different requirements for MFA and can be utilized with the solution proposal.

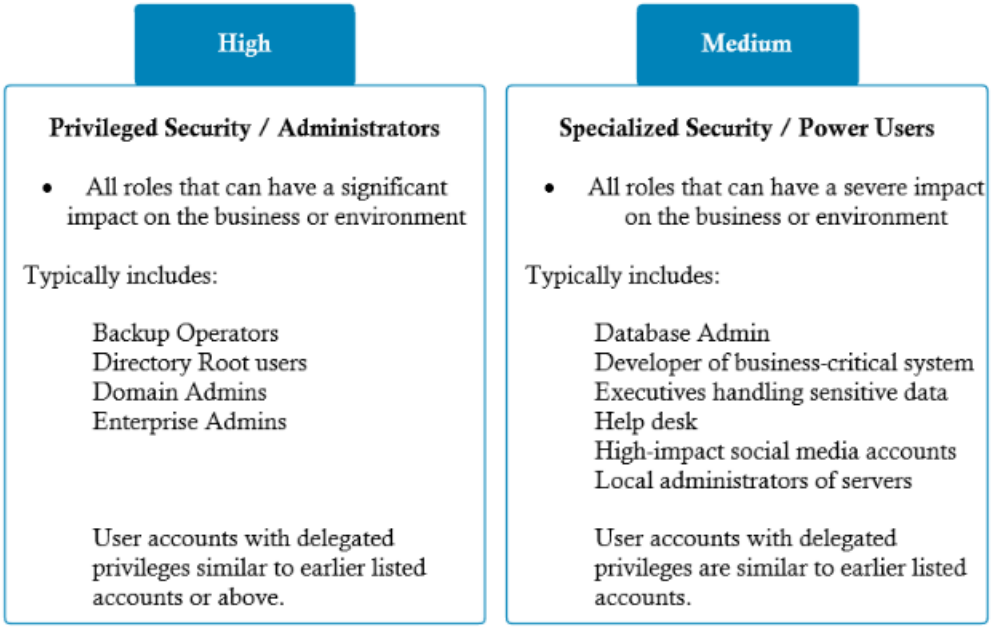

Figure 17. Categorizing privileged user accounts to different levels of security. [20,21,50]

Summary of the policy steps before utilization with the solution:

- Finding and identifying the organization's privileged identities, and documentation of results
- Organization having the least privilege principle in use and different levels of security
- Classifying privileged identities into categories

These categories are to be used later with the MFA solution.

5.2 Solution Proposal

Based on the feedback from the organization and the best practices emerging from the literature, at least two categories are needed to meet the organization´s requirements. Protecting privileged user accounts in the case company by adding more authentication layers for protection according to the categories will increase attacker cost to match business impact [50]. However, usability can be maintained at a high level when the MFA solution implements a sufficient security

level by category. To avoid resistance to the new process and MFA fatigue, the system must be considered usable from the user´s perspective [1].

Currently, it is not ideal for this organization to start implementing a new solution that can provide permissions elevation for user accounts in an on-premises environment with approval workflows when more permissions are needed. However, using separate user accounts for the tasks which require privileged access to the case company resources is a good solution at the moment, which decreases the attack surface and risk of security [50].

The category “High” is for privileged accounts that have a big impact on business but are used less often. The authentication requirements include at least three authentication factors for providing more security against threats. The second category needed is “Medium”, which is suitable for the rest of the organization internal user accounts, which have elevated permissions to the environment. Two factors are required for this type of account. In addition, separate categories for service accounts and external users with privileged access are recommended. This approach makes more granular authentication factor requirements possible based on the category type. Figure 18 shows the different options suggested for the case company to protect privileged accounts with MFA.

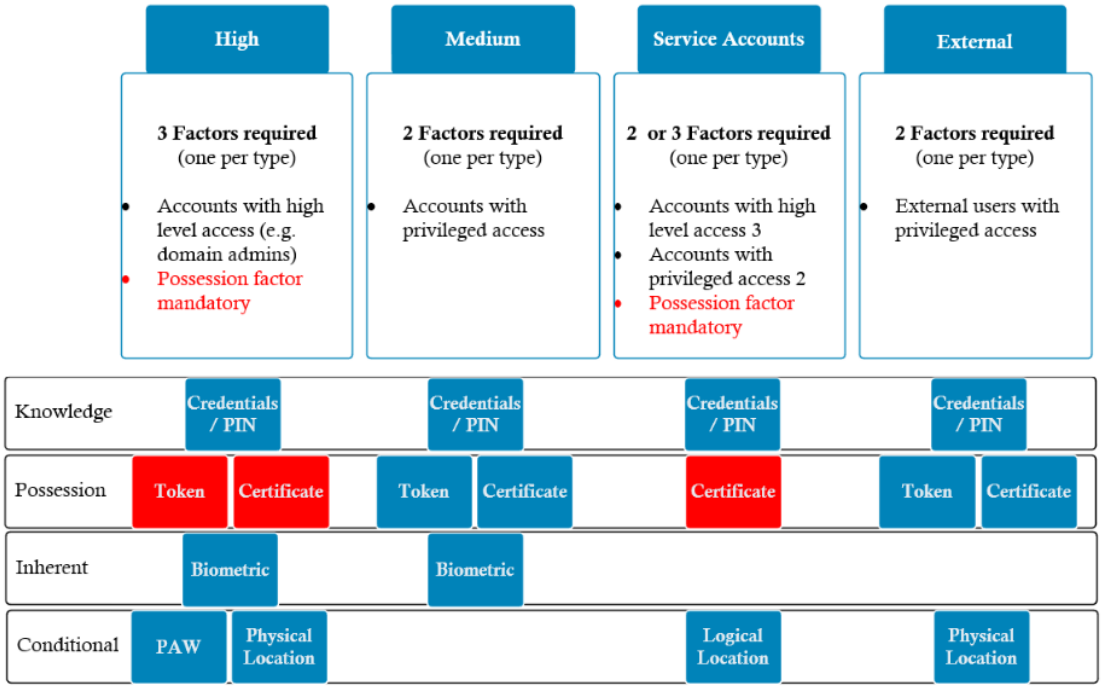

Figure 18. Privileged account categories and requirements of factor types.

This type of categorization provides security for the critical accounts while keeping usability high for the rest of the privileged user accounts with secure access to the resources. Different categories with allowed combinations of authentication factors are explained in more detail with examples in the following part of this chapter.

High

This category level requires the highest level of protection in organization, and three factors are needed. Based on the organization feedback, this is acceptable because these accounts are used less often, and this is not paralyzing the daily work. Privileged accounts in this category have major impact on the business if fallen into the wrong hands. They must be protected with multiple layers to make them more resistant to cracking attacks or other attack vectors. The higher security level should cause attacks to be more expensive to produce as shown in Figure 15 related to different levels of security [50]. Identities with high-level access to the on-premises environment belong to this category, such as accounts belonging to the Administrator fundamental level.

Multi-factor authentication combination strengths are shown in Figure 14, and based on reference [45], Phishing-resistant MFA could be achieved by using a FIDO2 security key (hardware token), Windows Hello for Business (biometrics), or using Certificate-based authentication (MFA). Passwordless MFA strength can be achieved using above-mentioned methods, but also using Microsoft Authenticator (Phone Sign-in) [45]. Therefore, these robust authentication methods are favored in this category.

The decision of the mandatory possession factor is based on the fact that it provides the possibility of using Phishing-resistant MFA and Passwordless MFA in authentication, as explained earlier. This also guides away using passwords, which are, according to reference, Chapple et al. [23], the weakest form of authentication. When implemented correctly, biometric factor is a stronger authentication factor than the possession factor, according to reference [23]. Biometric authentication is not always available for use in this case company environment based on the organization's feedback and is left as an optional factor form of authentication. Two more factors are required in this category with the mandatory possession factor. For covering all necessary cases, flexibility is still left to the solution because all systems do not work in the same way and solution should be fitted to the organization needs while maintaining security. The physical location or a dedicated hardened admin workstation (such as PAW) could be an alternative factor type in this category with a combination of possession factor and knowledge or inherent factor.

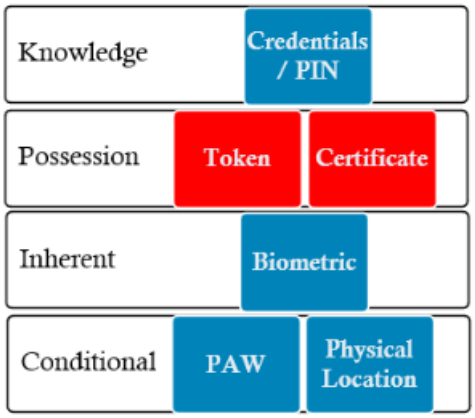

Figure 19. "High" category MFA factor types and combination possibilities. Three factors are required, and the possession type factor is mandatory.

Example case: Passwordless and phishing-resistant MFA

The case company domain admin accounts are classified as privileged user accounts requiring category level “High” for protection. A privileged user account is allowed to gain access to the resource if all the following example three requirements are valid, as shown in Figure 20:

- FIDO2 security key (possession)
- Biometrics (fingerprint) used to access a hardware token (inherent)
- Privileged Access Workstation in use (conditional)

Figure 20. Passwordless and phishing-resistant MFA with a conditional factor of PAW.

This authentication is suitable for protecting “High” category privileged user accounts. There is not a knowledge-based factor used, which is vulnerable to different attacks. When possible, this kind of authentication factor combination offers good protection for this category. This combination of factors is considered passwordless and phishing-resistant MFA [45].

Example case: MFA strength

The case company domain admin accounts are classified as privileged user accounts requiring category level “High” for protection. A privileged user account is allowed to gain access to the resource if all the following example three requirements are valid, as shown in Figure 21:

- Credentials are correct (knowledge)
- Authenticator application approved (possession)
- Physical location (conditional)

Figure 21. MFA strength with physical location requirement.

This type of authentication factors protects “High” category privileged user accounts; physical location is required as the third factor. The knowledge-based factor is used with a combination of mobile phone authenticator application.

Medium

The medium category level requires a total count of two for the authentication, and possible options are based on knowledge, possession, or inherent. For this category level, two factors will protect against different threats but keep usability high. Identities with privileged permissions on the fundamental level of “Power Users” belongs to this category, and “Specialized Security” is needed for protection. These accounts include i.e. help desk, developers, and main application users. No mandatory factor is defined for these, allowing flexibility and usability. In the organization feedback, it was essential to keep usability while maintaining security. The following example cases demonstrate some guidelines based on this study´s recommendations for the case company.

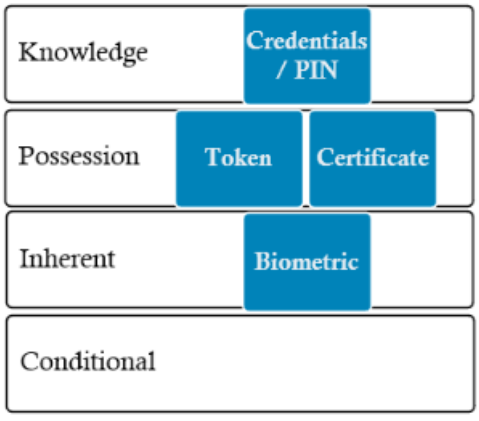

Figure 22. MFA factor types for the “Medium” category. Two factors are required, but no mandatory type is specified.

Example case: Passwordless and phishing-resistant MFA

The case company mission-critical service developer account is classified as a privileged user account. The required protection category for this type of account is “Medium.” A privileged user account is allowed to gain access to the resource if all the following example two requirements are valid, as shown in Figure 23:

- FIDO2 security key (possession)
- Biometrics (fingerprint) used to access a hardware token (inherent)

Figure 23. Passwordless and phishing-resistant MFA.

This combination will provide secure and easy-to-use authentication for this category of users.

Example case: MFA strength

The case company helpdesk user accounts are classified as privileged user accounts, requiring the category “Medium” for protection. These users must authenticate against the systems multiple times a day, so the methods used must be easy-to-use, secure, and fit in many cases. A privileged user account is allowed to gain access to the resource if all the following example two requirements are valid, as shown in Figure 24:

- Credentials are correct (knowledge)
- Authenticator application approved (possession)

Figure 24. MFA uses knowledge-based and possession-based factors for easy-to-access.

Implementing MFA instead of using only credentials will protect these privileged identities better against threats.

Service Accounts

This category requires two or three factors which must include the possession factor of the certificate. This is because these accounts are used for automation and must be operational while maintaining security. Another factor can be either credentials or logical location that is explicitly granted for this account and restricted from other users. In the case of a service account operating using high-level permissions, all three factors must be required.

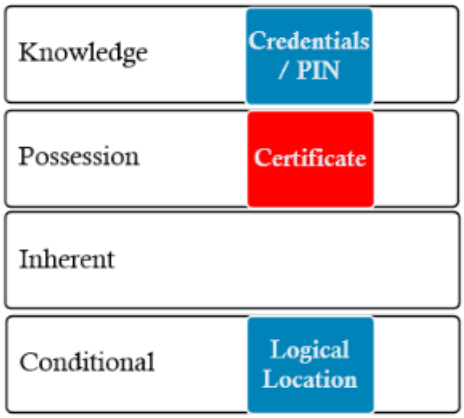

Figure 25. MFA factor types for the “Service Accounts” category. Two or three factors are required depending on the privilege access level. The possession type factor is mandatory.

Example case: MFA strength with two factors

The case company service accounts with privileged permissions are classified as privileged user accounts in this example and belong to the category “Service Accounts”. This example service account access level is similar to the “Medium”

category, and two factors are required. A service account is allowed to gain access to the resource if at least all the following example requirements are valid, as shown in Figure 26:

- Certificate (possession)

  AND
- Credentials are correct (knowledge)

  OR
- Logical Location

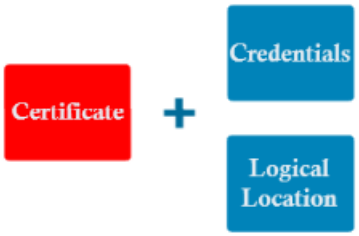

Figure 26. The minimum factor requirements for the service accounts.

Example case: MFA strength with three factors

The case company service accounts with privileged permissions are classified as privileged user accounts in this example and belong to the category “Service Accounts”. This example service account has privileged access similar to the “High” category. A service account is allowed to gain access to the resource if at least all the following example requirements are valid, as shown in Figure 27:

- Credentials are correct (knowledge)
- Certificate is valid (possession)
- Logical location explicitly defined (Conditional)

Figure 27. Three factors are required for a service account with high-level permissions.

With this service account category, it is impossible to use factors requiring user interaction, such as approving sign-in from mobile devices, because these accounts are usually used for executing automation tasks. The certificate, a factor of possession, offers good protection when combined with other factors, allowing stronger and phishing-resistant authentication [30].

External

These users are persons or entities which do not belong to organization users but need, for some reason, access to the services. If privileged permissions are granted to these user accounts, those must also be adequately secured. Two factors should be requested for external company users with privileged accounts, like case company users in the “Medium” level. If privileges are higher than the “Medium” category, shall apply “High” category level requirements for these user accounts.

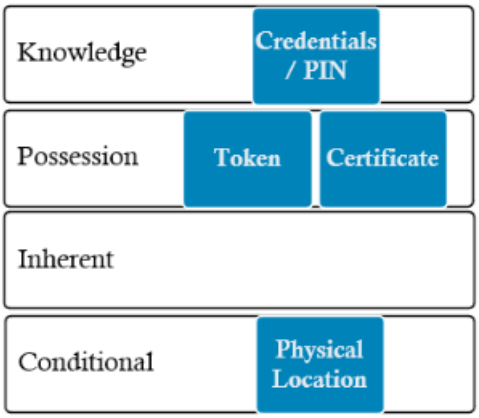

Figure 28. MFA factor types for the “External” category. Two factors are required.

In this example, users are required to provide a knowledge factor and possession factor but can replace one with a conditional physical location factor. This could occur if an external consultant needs to access devices or systems in the case company data center. Before an external user is allowed to access the data center, an escort is needed, and external user must be identified first. After that, using example, a certificate as a possession factor or knowledge-based credentials are allowed to use in authentication.

Another example is external user, such as consultant, which needs access to the services. According to reference [52], direct paths to systems should not be allowed. Allowing entry only through a dedicated terminal server, which is in a dedicated firewall-protected zone, would be a working solution. VPN connection to a terminal server or a dedicated restricted laptop can be used to make a connection to the terminal server. Before access is granted to the server, two factors are required, as shown in Figure 29.

Figure 29. External consultants are required to use Two-Factors when authenticating against a protected terminal server.

From external users, it could be difficult to require an inherent factor for authentication or provide a dedicated organization-owned PAW device for use. In a case similar to the “Medium” category, two factors in authentication will provide efficient protection for these privileged accounts and make them more protected against threats.

6 Summary and Conclusions

The objective of this study was to create a proposal of policy on how to protect the organization´s centrally managed privileged accounts and what kind of MFA solution best meets the organization's requirements following best practices.

To achieve the target, it was necessary to understand how the case company was currently protecting its assets. Key person interviews offered a way to present detailed questions about the topic and for understanding the current practices and technical solutions implemented in the case company and state of will, a qualitative approach was used. Data collection and analysis were approached by thematization of the material and classification of the results which outlined the requirements for the solution. Different MFA factors and current best practices related to these factors and a combination of those are approached by researching relevant literature. From the feedback and theory of recommendations, improvements to the current state of the organization are desired, and guidelines for a suitable solution for this specific organization could be made.

This study improved the case company's understanding of the need for protecting privileged accounts and what are the possibilities and options for implementing MFA solutions. During this work, the case company started testing hardware security tokens with biometric authentication to gain experience with passwordless MFA. Hardware security tokens with a long passphrase, stored in the password manager software, were also investigated for understanding their possibilities and functionalities. Understanding the importance of the principle of least privilege supports the organization when categorizing privileged entities following proposed guidelines. The guidelines for the MFA solution help the case company to start implementation of stronger protection for these critical accounts.

This study can also work as preliminary work for future improvements in the case company, such as Zero Trust security. Zero Trust security is a modern identity-centric approach to security enforcing the principles of least privileges for networks and applications for securing the environment from unauthorized

access [53]. In reference [53], Garbis J. and Chapman JW disclose, *“Identity is at the heart of Zero Trust”*. This highlights the importance of identity protection, which is partly covered in this thesis for privileged user accounts with MFA.

Regarding MFA, the best solution for implementation always depends on the use case. Whereas security token with biometric identification (e.g., fingerprint) offer very good protection against remote attacks, it is exposed to other types of threats. The challenges may arise because of an identical copy of the fingerprint or using the finger against the user´s will. In the case of facial recognition, there are possibilities for spoofing systems if vulnerabilities exist to get access. This places additional requirements on how example devices, such as security tokens, should be stored. Good protection could also be achieved by a combination of a possession factor, such as a security token and a long and complex passphrase stored in the password manager software.

Deploying strong enough identity protection for any organization is important. Thus, it is required to understand both the requirements and resources of the organization and based on these select the method(s) that provide at least the required amount of protection with smallest impact to the usability of the given system.

References

1. Boonkrong S. Authentication and Access Control: Practical Cryptography Methods and Tools [Internet]. 1st ed. APress Media, LLC; 2020; Available from: https://learning.oreilly.com/ https://doi.org/10.1007/978-1-4842-6570-3

2. Yle seurasi Vastaamon tietomurtoa: Näin kiristäjä ilmestyi Tor-verkon foorumille, poliisi pyytää harkintaa asiaan liittyvien yksityiskohtien julkaisemisessa [Internet]. Yle Uutiset. 2020 [cited 2023 Jan 13]. Available from: https://yle.fi/a/3-11612399

3. Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations | European Data Protection Board [Internet]. [cited 2023 Jan 13]. Available from: https://edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-psychotherapy-centre-vastaamo-data-protection_en

4. Satter R. Twitter hacked, 200 million user email addresses leaked, researcher says. Reuters [Internet]. 2023 Jan 6 [cited 2023 Jan 13]; Available from: https://www.reuters.com/technology/twitter-hacked-200-million-user-email-addresses-leaked-researcher-says-2023-01-05/

5. Newman LH. Yes, It's Time to Ditch LastPass. Wired [Internet]. [cited 2023 Jan 13]; Available from: https://www.wired.com/story/lastpass-breach-vaults-password-managers/

6. Powell O. LastPass facing lawsuit following data breach [Internet]. Cyber Security Hub. 2023 [cited 2023 Jan 13]. Available from: https://www.cshub.com/attacks/news/iotw-lastpass-facing-class-action-lawsuit-following-data-breach

7. Segal E. The 6 Most Common Cyberattacks That Could Impact Companies In 2023 [Internet]. Forbes. [cited 2023 Jan 13]. Available from: https://www.forbes.com/sites/edwardsegal/2023/01/02/the-6-most-common-cyberattacks-that-could-impact-companies-in-2023/

8. Chaumon M. Digital Transformations in the Challenge of Activity and Work: Understanding and Supporting Technological Changes [Internet]. Vol. 3. Wiley-ISTE; 304 p. Available from: https://learning.oreilly.com/library/view/digital-transformations-in/9781786305299/

9. Leskinen T. Tilastokeskus - Etätyö yleistyi eniten aloilla ja alueilla, joilla sitä ennen tehtiin vähiten | Tieto&trendit [Internet]. Tilastokeskus; [cited 2023 Jan 13]. Available from: https://www2.tilastokeskus.fi:443/tietotrendit/artikkelit/2021/etatyo-yleistyi-eniten-aloilla-ja-alueilla-joilla-sita-ennen-tehtiin-vahiten/

10. OWASP Top 10:2021 - A07 Identification and Authentication Failures [Internet]. [cited 2022 Nov 25]. Available from: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

11. 2022 Trends in Securing Digital Identities [Internet]. Identity Defined Security Alliance. [cited 2023 Jan 4]. Available from: https://www.idsalliance.org/white-paper/2022-trends-in-securing-digital-identities/

12. The State of Identity Security for 2022: Identity-Based… [Internet]. BeyondTrust. [cited 2023 Jan 4]. Available from: https://www.beyondtrust.com/blog/entry/the-state-of-identity-security-identity-based-threats-breaches-security-best-practices

13. Kananen J. Design Research (Applied Action Research) as Thesis Research : a practical guide for thesis research. Jyväskylä : JAMK University of Applied Sciences 2013; 232 p.

14. Tuomi J, Sarajärvi A. Laadullinen tutkimus ja sisällönanalyysi 2009. Tammi;

15. Statistics Finland - Statistics by topic - Government R&D funding in the state budget [Internet]. [cited 2022 Sep 10]. Available from: https://www.stat.fi/til/tkker/kas_en.html

16. Tuomi J, Sarajärvi A. Laadullinen tutkimus ja sisällönanalyysi [Internet]. Tammi; 2018 [cited 2022 Sep 6]. Available from: https://www.ellibslibrary.com/reader/9789520400118

17. Hirsjärvi S, Remes P, Sajavaara P. Tutki ja kirjoita. 15th ed. Tammi; 2009. 464 p.

18. Data protection in the EU [Internet]. [cited 2023 Jan 14]. Available from: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

19. What is personal data? | Data Protection Ombudsman’s Office [Internet]. Tietosuojavaltuutetun toimisto. [cited 2022 Sep 12]. Available from: https://tietosuoja.fi/en/what-is-personal-data

20. BeyondTrust - What is Privileged Access Management (PAM)? [Internet]. BeyondTrust. [cited 2022 Dec 4]. Available from: https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

21. Haber M. Privileged Attack Vectors: Building Effective Cyber-Defence Strategies to Protect Organizations [Internet]. 2nd ed. Apress; 2020. 403 p. Available from: https://doi.org/10.1007/978-1-4842-5914-6

22. Windley PJ. Learning Digital Identity [Internet]. O’Reilly Media, Inc.; 2023 [cited 2023 Jan 11]. 469 p. Available from:

https://learning.oreilly.com/library/view/learning-digital-identity/9781098117689/

23. Chapple M, Stewart JM, Gibson D. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide [Internet]. 9th ed. Sybex; 2021 [cited 2022 Oct 10]. 1248 p. Available from: https://learning.oreilly.com/library/view/isc-2-cissp-certified/9781119786238/c13.xhtml

24. Williamson J, Curran K. Best Practice in Multi-factor Authentication. Semiconductor Science and Information Devices. 2021 May 25;3.

25. NIST Special Publication 800-63B [Internet]. [cited 2022 Nov 27]. Available from: https://pages.nist.gov/800-63-3-Implementation-Resources/63B/

26. Weinert A. Your Pa$$word doesn't matter [Internet]. 2019 [cited 2022 Dec 3]. Available from: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/your-pa-word-doesn-t-matter/ba-p/731984

27. Neira B. What is Azure Active Directory? - Microsoft Entra [Internet]. [cited 2022 Dec 4]. Available from: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

28. ENISA: Authentication Methods [Internet]. ENISA. [cited 2022 Dec 7]. Available from: https://www.enisa.europa.eu/topics/incident-response/glossary/authentication-methods

29. Gremban K. Microsoft Learn - Understand Cryptography and X.509 certificates for Azure IoT Hub [Internet]. [cited 2022 Dec 13]. Available from: https://learn.microsoft.com/en-us/azure/iot-hub/tutorial-x509-introduction

30. What is Certificate-Based Authentication - Yubico [Internet]. [cited 2022 Dec 13]. Available from: https://www.yubico.com/resources/glossary/what-is-certificate-based-authentication/

31. SecurID [Internet]. RSA. [cited 2022 Dec 5]. Available from: https://www.rsa.com/products/securid/

32. OTP, TOTP, HOTP: What's the Difference? | OneLogin [Internet]. [cited 2022 Dec 5]. Available from: https://www.onelogin.com/learn/passwordless-authentication

33. OTPs Explained [Internet]. What is Yubico OTP? [cited 2022 Dec 5]. Available from: https://developers.yubico.com/OTP/OTPs_Explained.html

34. FIDO Alliance Specifications Overview [Internet]. FIDO Alliance. [cited 2022 Dec 7]. Available from: https://fidoalliance.org/specifications/

35. Computer Security Division ITL. Cryptographic Module Validation Program | CSRC | CSRC [Internet]. CSRC | NIST. 2016 [cited 2022 Dec 12]. Available from: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3914

36. European Council, PRADO, Document: FIN-BO-09001 [Internet]. [cited 2022 Dec 12]. Available from: https://www.consilium.europa.eu/en/

37. Matarazzo P. Smart Card Technical Reference (Windows) [Internet]. [cited 2022 Dec 7]. Available from: https://learn.microsoft.com/en-us/windows/security/identity-protection/smart-cards/smart-card-windows-smart-card-technical-reference

38. Matarazzo P. Virtual Smart Card Overview (Windows 10) [Internet]. [cited 2022 Dec 7]. Available from: https://learn.microsoft.com/en-us/windows/security/identity-protection/virtual-smart-cards/virtual-smart-card-overview

39. Bock L. Identity Management with Biometrics [Internet]. Packt Publishing; 2020 [cited 2022 Dec 12]. 368 p. Available from: https://learning.oreilly.com/library/view/identity-management-with/9781838988388/B15791_01_Final_AM_ePub.xhtml

40. Bharadwaj S, Vatsa M, Singh R. Biometric quality: a review of fingerprint, iris, and face. EURASIP Journal on Image and Video Processing [Internet]. 2014 Jul 2 [cited 2022 Dec 7];2014(1):34. Available from: https://doi.org/10.1186/1687-5281-2014-34

41. Bypassing Windows Hello Without Masks or Plastic Surgery [Internet]. [cited 2023 Jan 11]. Available from: https://www.cyberark.com/resources/threat-research-blog/bypassing-windows-hello-without-masks-or-plastic-surgery

42. Matarazzo P. Windows Hello for Business Overview (Windows) [Internet]. [cited 2023 Jan 11]. Available from: https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

43. KB5005478—Windows Hello CVE-2021-34466 - Microsoft Support [Internet]. [cited 2023 Jan 11]. Available from: https://support.microsoft.com/en-us/topic/kb5005478-windows-hello-cve-2021-34466-6ef266bb-c68a-4083-aed6-31d7d9ec390e

44. Sanger DE. Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says. The New York Times [Internet]. 2015 Sep 23 [cited 2023 Jan 11]; Available from: https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html

45. Hall J. Overview of Azure Active Directory authentication strength (preview) - Microsoft Entra [Internet]. [cited 2022 Dec 4]. Available from: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths

46. Orin T. Windows Server 2019 Inside [Internet]. 2020 [cited 2022 Dec 13]. 800 p. Available from: https://learning.oreilly.com/library/view/windows-server-2019/9780135492222/ch01.xhtml

47. National Cyber Security Centre. Secure system administration [Internet]. 2020 [cited 2022 Dec 12]. Available from: https://www.ncsc.gov.uk/collection/secure-system-administration

48. Vathanophas V, Chirawattanakij S. What are virtual walls to flow of knowledge in teamwork discussions? In: Trentin G, editor. Technology and Knowledge Flow. Chandos Publishing; 2011. p. 196.

49. Toom A. Hiljaista tietoa vai tietämistä? Näkökulmia hiljaisen tiedon käsitteen tarkasteluun. In: Toom A, Onnismaa J, Kajanto A, editors. Hiljainen tieto: Tietämistä, toimimista, taitavuutta: Aikuiskasvatuksen 47 vuosikirja. 47th ed. Helsinki: Kansanvalistusseura ja Aikuiskasvatuksen tutkimusseura; 2008. p. 359.

50. Flores J. Microsoft Learn - Securing privileged access security levels [Internet]. [cited 2023 Jan 2]. Available from: https://learn.microsoft.com/en-us/security/compass/privileged-access-security-levels

51. Engin T, Zagranichnov A. How to prevent lateral movement attacks using Microsoft 365 Defender [Internet]. Microsoft Security Blog. 2022 [cited 2023 Feb 7]. Available from: http://www.microsoft.com/en-us/security/blog/2022/10/26/how-to-prevent-lateral-movement-attacks-using-microsoft-365-defender/

52. Brändle M, Naedele M. Security for Process Control Systems: An Overview. IEEE Security & Privacy. 2008 Nov;6(6):24–9.

53. Garbis J, Jerry W. C. Zero Trust Security: An Enterprise Guide [Internet]. 1st ed. Apress; 2021 [cited 2023 Feb 6]. 306 p. Available from: https://learning.oreilly.com/library/view/zero-trust-security/9781484267028/html/495801_1_En_5_Chapter.xhtml

Appendix 1 Interview Questions

The following questions will be used for analyzing and gaining more information on the current state of on-premises centrally managed privileged accounts. A privileged account is, for example, an account with more permissions or access to the organization's resources than a standard user account.

- What kind of privileged accounts are there in the case company environment? Are there different types of these or different categories for these?
- How does access control generally protect privileged accounts in the current centrally managed on-premises environment?
- Are there written policies, documentation, or requirements related to these privileged identities? Where could this documentation be found for further analysis?
- Are there mechanism(s) to "elevate" standard user accounts permissions to get more access/permissions, or are there separate identities for tasks that require more privileges when accessing the resources?
- How does an organization protect access to the company-managed computers used by IT administrators?
- How does the organization currently protect and manage the company resources for external users with privileged access? (Consultant, etc.)
- What development needs are there for privileged Identity protection in an on-premises environment?

The following questions will be used to analyze and gain more information on the most suitable solution for protecting privileged accounts in the company's centrally managed on-premises environment.

- What kind of solution would be ideal for protecting these privileged accounts?

- What factors are preferred if more than one is required for protection factor options? For example:

    - Knowledge factor (credentials, PIN code)
    - Possession factor (hardware token, software token, certificate)
    - Inherent factor (biometric, such as fingerprint, face recognition, voice recognition)
    - Something else, such as location-based or behavior-based?

- How many factors/layers are enough for protecting and verifying identity right to access the system, and should there be options for those?

- Should the solution support multiple categorization policy levels for privileged identities, and how should those be defined?

- Are you familiar with some of the Multi-factor Authentication (MFA) solutions available, and are there some features to highlight?