Tallinn University of Technology
School of Information Technologies

Giorgi Sheklashvili 172680IVSM

Multi-Factor Authentication (MFA) on a Blockchain-based Decentralised Trust Network With Customizable Challenges

Master's thesis

Supervisor: Alexander H. Norta
PhD, Associate Professor
Co-Supervisor: Benjamin Leiding PhD

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Giorgi Sheklashvili 172680IVSM

Mitmetasemeline autentimine plokiahelapõhises detsentraliseeritud muudetavate väljakutsetega usaldusvõrgustikus

Magistritöö

Juhendaja: Alexander H. Norta
PhD, Dotsent
Kaasjuhendaja: Benjamin Leiding PhD

Tallinn 2020

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Giorgi Sheklashvili

12.06.2020

Contents

List of Figures

List of Tables

Acronyms

PGP Pretty Good Privacy - An Encryption Program

WoT Web of Trust

CA Certifcate Authority

MFA Multi-factor Authentication

IS Information Systems

Abstract

Central authorities are the prominent choice when two parties want to establish trust between each other. For example, web servers are using central authorities to establish a secure socket layer (SSL) connection with the browser. A significant flaw of central authorities is that, if the primary node is compromised, all of the nodes are rendered untrustworthy, because of the hierarchical structure. Another alternative to central authorities is the Pretty Good Privacy (PGP) web of trust (WOT), where each user acts as an authority. Still, a lack of incentives for correctly identifying another user as trustworthy and missing punishments for malicious actions are the main reasons why the WOT is not considered reliable. Additionally, sybil nodes represent a threat to the WOT since there is no defence mechanism for identifying a group of users who maliciously identify each other as trustworthy.

Multi-factor authentication (MFA) is the concept that emerged in the 1980s. However, most of the customers did not consent physically carrying another factor for authentication and thus, the market did not adopt it. After introducing smartphones that provide the possibility to send evidence of possession, inherence, knowledge, or context to another user, MFA is accessible for billions of people. MFA is used as a safer way to establish trust relations in a network. Security-critical organizations similar to banks, authenticate customers using their knowledge, inherence, and possesions. Furthermore, contextual information such as the time, location, and device model can be considered as an additional factor of authentication. The more factors are used during authentication, the safer the process becomes. Thus, if the attacker compromises one factor, it is not valuable for the authentication without other factors because until all of the factors are not validated, the user cannot be authenticated.

In this thesis, another alternative to public key infrastructures called Authcoin, is further developed using customizable challenges and MFA. Blockchain technology is utilized for storing authentication-related data, and hence, transparency, trustworthiness, and immutability of data are achieved. This thesis implements an additional layer of security for the Authcoin protocol by providing an MFA artifact and describing how to replace central authority and PGP/WOT systems by the implemented solution. The produced software artifact is documented and described for technical-oriented and managerial-oriented readers.

Kokkuvõte

Levinuim viis kahe osapoole vahel usalduse loomiseks on kolmanda, autoriteetse osapoole vahendus. Näiteks kasutavad veebiserverid keskset juhtorganit, et luua brauseriga suhtlemiseks turvaline soklite kiht (SSL). Keskse juhtorgani kasutamise oluline probleem on see, et kui autoriteetne sõlm on ohus, muutuvad kõik sõlmed hierarhilise struktuuri tõttu ebausaldusväärseks. Alternatiiv keskse juhtorgani kasutamisele on Pretty Good Privacy (PGP) usaldusväärne võrk (WOT), kus iga kasutaja tegutseb autoriteetse osapoolena. Siiski ei peeta WOT-i usaldusväärseks, sest puuduvad stiimulid teise kasutaja usaldusväärsuse korrektseks tuvastamiseks ja karistused pahatahtlike tegude eest. Lisaks puudub WOT-i puhul kaitsemehhanism, mis tuvastaks kasutajate gruppe, kes üksteist pahatahtlikult usaldusväärseks märgivad (Sybil nodes).

Mitmefaktoriline autentimine (MFA) on mõiste, mis tekkis 1980ndatel. Enamik kliente ei nõustunud aga autentimiseks füüsilist lisaseadet kandma ja seega ei võtnud turg seda omaks. Pärast nutitelefonide levikut, mis võimaldavad teisele kasutajale edastada infot, konteksti, tõendeid omamisest ja olemusest, on MFA kättesaadav miljarditele inimestele. MFA-d kasutatakse turvalisema viisina usalduslike suhete loomiseks võrgus. Pankade-sarnased turvakriitilised organisatsioonid autendivad kliente nende teadmisi, olemust ja omandit kasutades. Lisaks võib kontekstipõhist teavet, nagu aeg, asukoht ja seadme mudel, pidada täiendavaks autentimisfaktoriks. Mida rohkem tegureid autentimisel kasutatakse, seda turvalisemaks protsess muutub. Seega pole ründajapoolne ühe teguri ohtu seadmine ilma muude teguriteta autentimiseks väärtuslik, sest enne kui kõiki tegureid pole kinnitatud, ei saa kasutajat autentida.

Selles lõputöös arendatakse avaliku võtme infrastruktuuridele välja veel üks alternatiiv nimega Authcoin, mis kasutab kohandatavaid väljakutseid ja MFA-d. Autentimisega seotud andmete hoidmiseks kasutatakse Blockchain tehnoloogiat, mis tagab andmete läbipaistvuse, usaldusväärsuse ja muutmatuse. See lõputöö lisab Authcoini protokollile täiendava turvalisuse kihi pakkudes MFA artefakti ja kirjeldades, kuidas kesksel autoriteedil ja PGT/WOT-l põhinevaid süsteeme antud lahendusega asendada. Implementeeritud tarkvara on dokumenteeritud ning nii tehnilistele kui ka juhtivatele osapooltele sobivalt kirjeldatud.

1 Introduction

Trust and security have become complicated in today's fast-evolving technology era. Trust models and metrics of authentication in public key infrastructure (PKI) systems focus on data integrity and confidentiality [27]. These aspects are crucial for a user to trust the technology that performs a request. Data integrity and -confidentiality are aspects of the security model, hence the terms trust model and security model are used interchangeably. Still, other factors such as reliability, availability and privacy are as important as security for users [27].

Blockchain is a distributed, open ledger that records transactions between two parties in a verifiable and permanent way [28]. Every transaction in the public ledger is verified by the consensus of a majority of the participants [13]. Every block in the blockchain contains the hash of the previous block, hence data integrity is addressed by the nature of blockchain. The decentralized peer-to-peer digital currency called Bitcoin is the first use case of blockchain technology [13][48]. In this thesis, the problem of authentication in the blockchain network is examined.

Advancement of blockchain technology creates new threats such as money laundering and financing terrorists. The legislation is rather slow when trying to catch up with innovations similar to blockchain [52]. Additionally, threats that are not new to internet infrastructure are a danger for blockchain users as well. Since cybercrime is a globally operating profit-driven, major industry, and hence, a threat to the business- and financial world [58], people distrust the security of software. For example, because of fear of credential theft, users are writing a private key on paper [32].

Challenge-response based authentication is widely used by companies that need to verify identity in insecure environments [42]. Challenge-response based authentication is characterized by one entity sending a challenge to another entity to prove her/his identity. For example, service providers such as a bank, can send four digits to a user and ask them to enter a received passcode in their mobile application for successful authentication. In this thesis, authentication is made secure in Authcoin protocol, using challenge-based multi-factor authentication (MFA).

1.1 Existing Body of knowledge

There are two approaches practised to establish trust in networks. The first is a central authority, and the second is a web of trust (WOT) that uses an encryption program called pretty good privacy (PGP). Central authorities are used by domains, email accounts, and public keys to establish trust in a network. The web-of-trust solutions are frequently impractical to use because malicious users can easily create a smaller network of trust between each other and convince new users about their trustworthiness. As shown by Leiding and Dähn, approximately 40 per cent of the PGP/WoT email addresses are unreachable, meaning that signatures related to these emails cannot be trusted. Additionally, joining

is inconvenient for new users, since they have to meet with someone in person to have the public key signed and verify his or her identity. Also, the user is limited to choose another user as their **designated revoker**, who exclusively revokes the key if the private key is lost [21].

The certificate authority (CA) is an institution inside the network that is trusted by all of the parties, records the public key and distinguished name of the user's identity and is responsible for delivering digital certificates to network users. A CA's major flaw is that, if the root node is compromised, the whole network becomes untrustworthy. "The CA serves two purposes: it facilitates the verification that a user holds a certain public key, and it facilitates the lookup of public keys corresponding to users" [21]. Verification is carried out by using digital certificates issued to the user. Thus, the certificate states the following: The specific user holds a specified public key, signed by the CA while any user can request another user's public key.

1.1.1 Authcoin

The Authcoin protocol provides an alternative to widely used public-key infrastructures such as the PGP/WOT and CA. "Authcoin combines a challenge-response-based validation and authentication process for domains, certificates, email accounts, and public keys with the advantages of a blockchain-based storage system" [36]. The blockchain technology provides distributed and decentralized data storage that is transparent, fault-tolerant and cannot be altered. Using the Authcoin protocol, the entity can send challenges to other entities they have to fulfil.

Even though Leiding et al. explains the protocol using private- and public keys, the Authcoin protocol is not limited to private-public keys, and depending on chosen challenges, can be extended to validate email accounts, certificates and domains using other public-key cryptography-based scenarios. Authcoin also provides a feature of randomly sending automated validation and authentication requests during the mining process that verifies entities are reachable and responding.

1.1.2 Multi-Factor Authentication

Currently, single-factor authentication mechanisms mainly use the following factors:

- Something that the user knows (e.g., password, PIN);
- Something that the user has (e.g., card) and
- Something that the user is (e.g., biometrics)

Authentication methods that use more than one factor, are more difficult to compromise than single-factor methods [11]. MFA requires more than one method of authentication to verify the user's identity. MFA is becoming more popular

because of the General Data Protection Regulation (GDPR), which restricts verifying a user's identity with personal secret questions [3]. Using two-factor authentication is a powerful deterrent for cybercriminals because a hacker is doubly challenged and likely deterred by the higher level of security [54].

Nonetheless, MFA incurs some challenges regarding the comfort of usability. MFA is not standardized, and thus, different authentication factors may be used in different organizations. Furthermore, even if two different organizations use the same authentication factor, it is not always interoperable, since possession and knowledge factors can be unique for different organizations. As a result, users have to remember more than one unique passwords, or carry multiple physical items for either one-time password (OTP) generation, or to present different identifiable documents [56]. This problem is more significant in the case of possession factors because carrying several physical items can be problematic.

1.1.3 Authentication Using Blockchain Technology

Trust management is tied to authentication mechanisms as a means to identify the trustee and the trustor [44]. Since the creation of bitcoin, blockchain has many applications in industry as a cheaper and secure way to manage a distributed database for digital transactions [13].

The implementations of authentication and identity management in a blockchain system is still in the early stage. Moinet et al. describe how decentralized sensor-systems could use blockchain as an authentication platform. Since sensor systems network security relies on information contained in the blockchain, mining proposed by Moinet et al. does not add blocks only by providing a solution to header hash requirement, that is less or equal than target hash. In other words, there has to be requirement other than solving a mathematical problem, to mine new blocks. In the proposed design, only authenticated nodes can mine new blocks when the same node is not trying to add a payload in the block. To conform with these requirements and include payload in the block, miners must choose payloads which comes from an authenticated user, and check that author of payload and miner are not identical [44]. Moinet et al. also notes to maintain accurate predictions, good behaviour should be rewarded, and harmful behaviour must be punished.

1.1.4 Contributions - Detecting a Gap

The primary goal of this thesis is to secure the authentication process of an entity in the Authcoin protocol by proposing an artifact of MFA using text- and image-based authentication factors. Security of the Authcoin protocol is based on blockchain technology that keeps the challenge requests and responses on the ledger and keeps it transparent and unaltered, so the other entities can view information about authentication. Since MFA may use four kinds of evidence (knowledge, possession, inherence, and context of an authentication candidate) to authenticate the user, the initial binding is more reliable between an entity

and her/his claimed domain, email, or any other belonging [11].

1.2 Research Methodology and Research questions

The research method applied in this thesis is design science, that seeks to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts [25]. According to Peffers et al., the steps for creating a design artifact include the identification of a problem, the definition of objectives, design and development, demonstration, and evaluation. Design-science products are of four types: constructs, models, methods, and implementations [38].

1.2.1 Design Science Research - Theory

Design science aims to create utility and is a process and a product as well [25]. The resulted artifact provides intellectual and computational tools that broaden people's abilities to solve problems. Theories about the application of resulted artifact should also be provided. Artifacts have a structured form and can be software, rigorous mathematics, formal logic, or informal natural language descriptions [25].

1.2.2 Design Science Research - Practice

March and Smith identify two processes needed to produce design-science research in information systems: build and evaluate. Artifacts are built to address unsolved problems, and evaluation is performed to the produced utility in solving those problems. Figure 1 shows the conceptual framework that combines behavioural-science and design-science paradigms. This framework is used to understand, execute, and evaluate information-system research. According to Hevner et al. [25], behavioural science contributes to research by development and approval of theories that explain, or predict the fact concerning the identified business needs. The study notes that design science contributes to research by building and evaluating the artifacts to meet business needs. To conclude, Hevner et al. [25] claims that the goal of behavioural-science research is to find the truth, and the goal for design-science research is to build utility. Furthermore, the study also states that truth and utility are inseparable.

Artifacts produced after design-science research, most of the time, are not fully finished information system that are products. Denning [17] and Tsichritzis [63] claim that artifact represents an innovation that define the ideas, technical capabilities, practices and products with the help of which the design, analysis, implementation and usage of information systems can be accomplished.

Figure 1 is the design-science research framework instantiation within the context of this thesis, as outlined by Hevner et al. [25]. The left column represents the environment whose needs artifact addresses. The environments comprise people, organizations, technology, organization processes and strategy. The knowledge base column on the right provides the foundations and methodologies used in the artifact. The produced artifact contributes to the knowledge base and by applying to the environment, addresses the initial need.

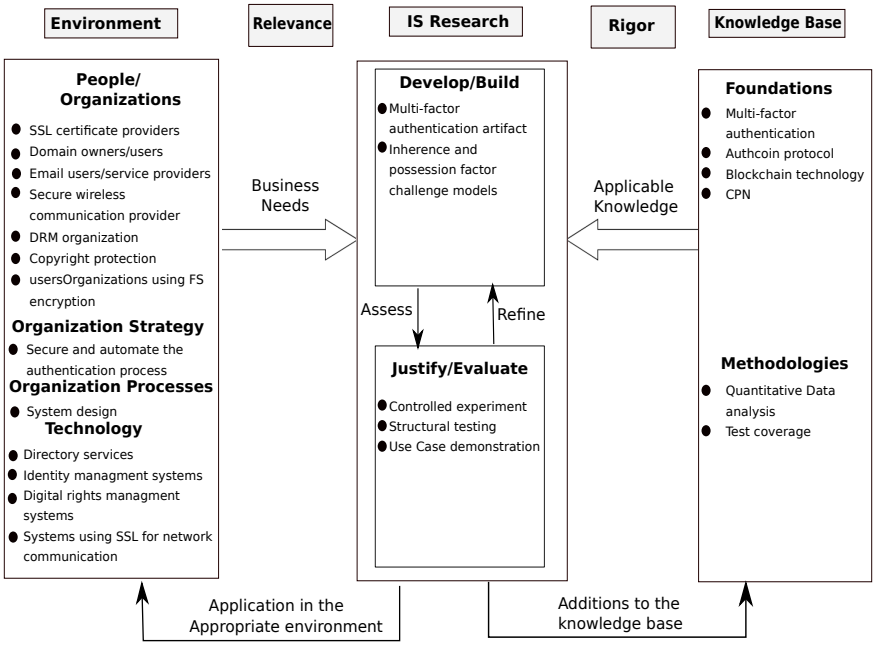


Figure 1: Information systems research framework (Source: [25])

Additionally, to the research framework, Hevner et al. [25] presented guidelines for design-science research process Table 1. The following sections explain the application of the guidelines within this thesis and in the context of presented design-science research framework instantiation.

Guidline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contribution	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations,and/or design methodologies
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Table 1: Design-science Research - Guidelines (Source: [25])

1.2.2.1 Design as an Artifact

As explained in Section 1.1.4 main goal of this thesis is to close the gap in the knowledge base by proposing a MFA artifact on top of Authcoin protocol. This thesis proposes the safest option for authentication in Authcoin protocol and presents the advantages and disadvantages of different challenges used during MFA. The Artifact demonstrates the use case of MFA in Authcoin protocol and gives directions to technical and managerial readers about the usage of MFA in Authcoin protocol.

1.2.2.2 Problem relevance

The primary relevance of this thesis is to help propose Authcoin as an alternative to PGP/WOT by securing the authentication process with MFA. Additional security layer of MFA makes authentication safer than using single-factor authentication [11]. Validation and authentication are the critical steps in Authcoin protocol on which the whole protocol is based. MFA makes validation and authentication more trustworthy, hence it is easier to prove that Authcoin protocol can be used as an alternative to PGP/WOT and central authorities.

1.2.2.3 Design evaluation

Hevner et al. provided design-science research evaluation methods, those are presented in Table 2. Testing and experimental evaluation methods are used for this thesis: controlled experiment, structural testing and use case demonstration. Scenario for authentication is presented to display use case of artifact.

Evaluation Method	Description
Observational	Case Study: Study artifacts in depth in business environment
	Field Study: Monitor use of artifact in multiple projects
Analytical	Static Analysis: Examine structure of artifact for static qualities (e.g., complexity)
	Architecture Analysis: Study t of artifact into IS architecture
	Optimization: Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact
	Dynamic Analysis: Study artifact in use for dynamic qualities (e.g., performance)
Experimental	Controlled Experiment: Study artifact in controlled environment for qualities (e.g., usability)
	Simulation: Execute artifact with articial data
Testing	Functional (Black Box) Testing: Execute artifact interfaces to discover failures and identify defects
	Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artifact implementation
Descriptive	Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility
	Scenarios: Construct detailed scenarios around the artifact

Table 2: Design Science Evaluation methods (Source: [25])

Based on Baskerville [6], evaluation methods must demonstrate utility, quality and efficiency of design artifacts rigorously. Hevner et al. [25] suggests that descriptive methods should be used when artifact is so innovative that other evaluation methods are not applicable. Since our artifact is a proof-of-concept, we can apply evaluation methods which are closer to a real-life scenario. Observational methods cannot be used since it needs to have artifact used in the business environment. Analytical methods also need to have the artifact used at least in one project to analyze its performance. Hence, experimental and testing methods can be applied to our artifact since they can be used in an isolated environment with an unfinished proof-of-concept.

1.2.2.4 Research contribution

This thesis secures the Authcoin protocol by producing implementation of application-system as a proof-of-concept and methods to provide future developers with practices and examples of MFA on Authcoin protocol. Moreover, with the help of this thesis, managerial-oriented readers can analyze advantages and disadvantages of using Authcoin MFA in their context.

1.2.2.5 Research rigor

According to Hevner et al. rigour is generated from the effective use of knowledge base, such as theories and research methodologies and it "must be assessed with respect to the applicability and generalizability of the artifact" [25]. In our context, rigour of Authcoin protocol is already achieved by Leiding using CPN models and CPN modelling language [31].

1.2.2.6 Design as a Search Process

Based on Authcoin paper [36], the implementation of the protocol is started and this paper contributes by adding an additional layer of security using multi-factor challenge-based authentication.
Design-science research is an iterative process to find the optimal solution. However, because of complexity of information systems research problems, the problems are decomposed into subproblems. The main goal of this thesis is to propose Authcoin MFA as a safer alternative to PGP/WOT and central authorities. This goal is decomposed into three smaller problems: proposing MFA as a safer authentication method, choosing optimal challenges and sharing results of application-system implementation.

1.2.2.7 Communication of Research

The conducted research is documented so future developers and researchers can reconstruct the solution, hence achieve repeatability of the research. For management-oriented audiences, the importance, effectiveness, and usefulness of the solution, is emphasized.

1.2.3 Research questions

The main research question for this thesis is as follows:
How to Apply MFA with Customizable Challenges to Authcoin Protocol?
This question is divided into three sub-questions:

- **RQ-1: How to Secure the Identity Authentication Process with MFA for the Authcoin Protocol?**
- **RQ-2: How to Manage Identity Authentication for the Authcoin Protocol?**

- **RQ-3: How to Implement MFA for the Authcoin Protocol?**

Answering RQ-1 is started by presenting MFA as an additional, safer alternative to single-factor authentication. Subsequently, the levels of MFA are presented, and factors of authentication are compared for Authcoin context to find the best option. Finally, risk assessment is performed, and the workflow of authentication in Authcoin context is presented.
Answering RQ-2 is started with presenting risk-based authentication and its influence on challenges. Also, we present how context is stored and later compared to current context information. Subsequently, we analyzed attack vectors on biometric authentication, since biometrics are an important part of MFA. Finally, examples were given about how MFA would happen between machine and person.
Answering RQ-3 is started with introducing the usability of different biometrics that can be a part of MFA. Subsequently, the facial recognition is chosen for implementation. After implementing, lessons are shared and an example of authentication is presented.

1.3 Thesis Structure

The rest of the thesis is structured in the following way: Chapter 2 provides an overview of Authcoin protocol and emphasizes authentication-related parts which are relevant in our context, and introduces MFA as a concept. Chapter 3 proposes MFA as a safer alternative to single-factor authentication. The supporting arguments are built for MFA, that convince the reader about the safety of MFA. Chapter 4 explains how challenges should be chosen for reliable verification. Chapter 5 demonstrates the use case of MFA and shares lessons learned during implementation. In Chapter 6 evaluation is performed on proposed concepts from Chapter 3 and 4, also use case on developed artifact is evaluated. Chapter 7 concludes the thesis and provides future work possibilities.

2 Presuppositions

This chapter introduces and explains concepts that are used and further developed in this thesis. The Section 2.1 follows the explanation started in section 1.1.1, by providing a detailed, high-level explanation of the Authcoin protocol. The original Authcoin paper [36] is used as the main source of this chapter.

Section 2.2 explains how key and signature data on the blockchain are expired and revoked. The following Section 2.3 provides information about how Authcoin related data is stored on the blockchain. Furthermore, Section 2.4 and 2.5 explain how challenges and validation and authentications requests work. Finally, Section 2.6 explains and presents examples of the concepts of MFA.

2.1 Overview

The Authcoin protocol uses PKI for initial binding between generated key pair and its owners, such as email account, domain or certificates [36]. Key pair consists of public and private keys, that are mathematically linked to each other in such a way that only private key can decrypt the message if encryptor is the public key, and vice versa. Moreover, it is impossible to deduce one key from another.

On step one, a key-pair is generated, then the public key is associated with an entity that is owning it. Next, on step two, public key and information about established binding are posted to the blockchain.

Step three verifies the validity of the key by checking if the length is sufficient and if the key revoked [36]. Then the validation and authentication process starts between two entities.

Validation and authentication procedure of entities takes place on the fourth step, after which follows the final, fifth step of posting information about validation and authentication to the blockchain. There are separate processes for validation and authentication. Validation's goal is to verify that the entity has access to a particular account, private key, public key, and key-pair corresponds to the tested account. All of these requirements does not verify the identity. They check whether the owner has access to the account or domain. To verify the identity authentication is needed. Authentication depends on the challenge that is chosen and also on what kind of information channels are available. Challenges are explained in subsection 2.4

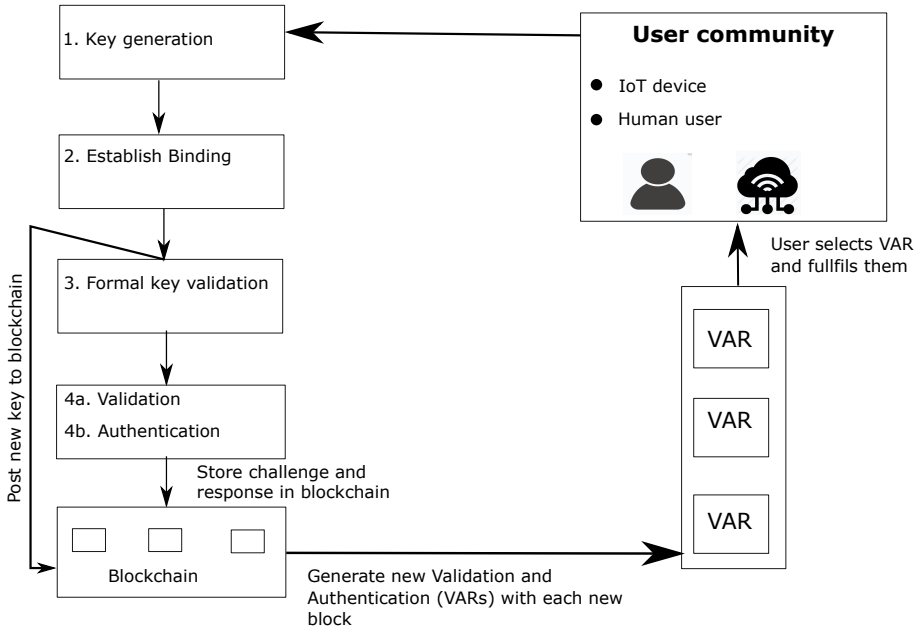


Figure 2: Workflow of Authcoin protocol (Source: [36])

2.2 Revocation And Expiration

As Leiding et al. explains, in the context of Authcion, a key revocation occurs by posting a revocation certificate on the blockchain. Similar to key revocation, certificate of signature revocation is also posted on the blockchain, and it additionally renders signing key as untrusted [36].
The author states that there is an expiration date for both keys and signatures, and the expiration period for keys and signatures are 12 months but can be customized by the users. Signatures become expired automatically if the singing key gets expired [36].

2.3 Storage

Authcoin uses blockchain as a storage system, where transactions inside the blocks are actual data that needs to be stored, such as challenges, keys, signatures, responses and such relevant data [36]. Blockchain consists of blocks, that are chained together in chronological order that cannot be tampered after

data has been added there. Each block contains a header, where metadata is present and body, where transactions are kept. When a new block is added on the blockchain, the network should reach consensus in order to add the block successfully. There are several mechanisms to reach consensus, but the widely used ones are proof-of-work, used by Bitcoin [48] and proof-of-stake used by Ethereum [8]. Each block has a hash that depends on previous block hashes, so manipulating a block is impossible, since it would never be accepted by other miners as a valid.
Ethereum is the name of the platform that provides blockchain-based storage and also Turing-complete programming languages, that can be used to program smart contracts [8]. In Ethereum blockchain, a smart contract is an executable code that is placed on the blockchain, so once the code is added there, it cannot be changed. The contracts are made to orchestrate and enforce negotiation conditions between two parties and have the code, account balance, and storage. The code is executed when a message is received, and it may use storage for reading or writing. Contracts can send and receive money on the account balance and also has a gas that is needed to execute code, and that prevents usage of loops infinitely. Before posting to the blockchain, contracts are compiled to bytecode.

2.4 Challenges and Privacy

The Authcoin protocol does not have challenges prescribed, and it can be customized based on need. The reliability of the protocol profoundly depends on the chosen challenges. Leiding et al. describes three types of challenges: "Global validation and authentication (V&A) without additional information" [36] , "global V&A with additional information" [36] and "local V&A with additional information" [36]. The word **global** in this context means that two entities cannot interact directly with each other and do not know how they look, and **additional information** means that they have some channel where they can communicate, email addresses, for example.

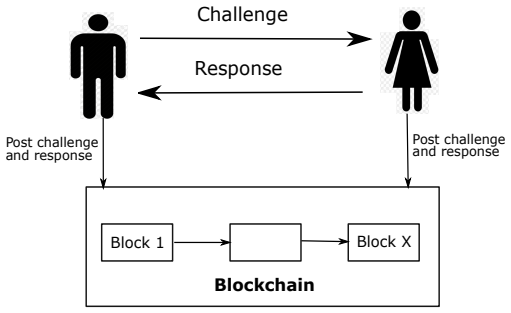


Figure 3: General validation/authentication process as deployed by Authcoin (Source: [36])

In Figure 3 Alice sends a challenge to Bob encrypted with Bob's public key. Bob opens the challenge with his private key, then fulfils the challenge, signs the response with his private key, and sends it back to Alice. Alice opens the challenge with Bob's public key and deduces the following from it: Bob has access to an email account, also has access to the private and public key, and key-pair belong to an email account. The validation request and response are stored on the blockchain.
Note that this example does not verify that the entity behind the email is Bob. For that, we have to assume that Bob and Alice had seen each other at some point in time. So Alice asks Bob to take pictures of himself with the current issue of the newspaper and send it back to her. In this way, authentication would take place. If Bob wanted to do the same, he would also ask for a picture from her, resulting in bidirectional verification.
One of the biggest advantages of Authcoin is that it performs bidirectional validation and authentication [36]. They can also be partially automated, that makes identifying malicious entities easier.

2.5 Var & Malicious Entities

As demonstrated in Figure 2, validation, and authentication requests (VARs) are generated randomly during the mining process. According to Leiding et al., VAR quantity depends on two characteristics of the blockchain: Time between new blocks and a number of existing entities in the blockchain. The faster the blocks are added, the fewer VARs are generated, and the more entities exist, the more VARs are generated [36]. This raises the chance to expose malicious entities accidentally. Identifying malicious entities leads to questioning all the other entities that validated it, hence identifying them as unreliable [36].

2.6 Authentication

Authentication is the process when a person's identity is verified. Authentication is conducted frequently in the digital age. Even though the most used authentication method used to be username/password combination [7], there are many other types, for example, such as four-digit passcodes (without a username) and biometrics, such as the face or eye retina scanning for unlocking the phone.

2.6.1 Multi-Factor Authentication

There are several ways of how single-factor authentication can be compromised easily. The simplest one is just guessing the password, also if someone gains access to user's email, then he/she can enter into a protected account by going through the forgot-password process. Also, a hacker may find out the password on a different platform that belongs to a user, and simply because the user uses the same password, he/she can gain access to the second account also.

As already mentioned in Section 1.1.4, MFA technologies may use four types of factors: factor someone knows (username, password, passphrase or PIN), you

have (token, OTP or encryption key), someone is (bio-metrics or the way the user behaves) and someone's context (location, time or IP address)[43].

Possession factors are three different types:

- Disconnected tokens - These have no connections to the client's device. It is typically hardware that generates the data for authentication [50].
- Connected tokens - These are devices that are physically connected to the personal computer. These devices that can be USB tokens, wireless tags, or card readers contain data itself [50].
- Software tokens - These tokens are stored on electronic devices such as smartphones or laptops and can be duplicated [50]. X.509 public-key certificate is usually used for this purpose [15][9].

A significant drawback of hardware tokens is that the user must carry it always. Hardware tokens are also hard to scale because every time a new user comes, a new physical device is needed. However, these drawbacks got resolved when smartphones emerged, which can allow the user to authenticate using access code to the device itself or sending OTP SMS to the phone. Security experts criticized sending SMS, and now big companies such as Google and Apple started using push notifications instead [47].

Context-based authentication adds the user's context, such as time, location, or IP address, when deciding whether authentication should be easier or harder [68]. Use of biometrics can be unsafe if the developer puts it on the server because if it is stolen, there is no way to issue a new bio-metric (fingerprint, for example). Regardless, biometrics can be made safer if the fingerprint or other biometric is saved on a secure device instead of a server [39]. In this case, if an attacker hacks into the server, there is nothing there. Behavioural biometrics can be utilized with continuous authentication [57], for example, monitoring how user types on a keyboard and authenticated continuously based on that can be a reliable way to identify who is typing. MFA also renders phishing very ineffective unless the hacker steals all of the factors and context of the user.

Bio-metrics also have disadvantages. If the technology for some reason can not recognize fingerprint, voice, or face, then there should be backup password to use [23], for example, having cast on the hand, growing beard, or having a cold would make identifying people based on bio-metrics challenging. Also, having bio-metrics as a way of identification may cause the user to feel uncomfortable because of privacy reasons. MFA provides a way to avoid sharing a password and defends from inside attacks in the company and third-party vendors.

2.6.2 Challenges

The simplest challenge that one might use is to ask the password or passphrase from the other person, but if a hacker is performing a man-in-the-middle attack, the password can be compromised easily. The second most straightforward challenge may be considered type when sender and receiver both have algorithms

based on which they are generating strings (adding character to the string, for example), but if the attacker finds out the previous string, it is not useful to log in, because the string is issued each time [40]. Another commonly implemented method of a challenge-response protocol is showing a distorted image - CAPTCHA, to check if a real person is performing an operation or not [66].

When sending data between two parties is needed, and the communication channel is unsafe, encryption has to be used [10][69]. Nevertheless, encryption still does not guarantee that eavesdropper can not read messages. Brute force and dictionary attacks can be used to decrypt such messages. A widely famous example happened during world war II when enigma code that was used by the Germans was cracked by Alan Turing with the brute force method using the Turing machine, that can be considered as a model of a general-purpose computer.

Another major topic for challenge-response authentication is using biometrics such as retina, fingerprint or face scanning as unique evidence. For example, a picture of a face with a passport or voice recording can be an effective way to prove identity. If the voice of the user is known to the sender of challenge, he/she can ask for pronouncing of some sentence or word from the receiver of the challenge.

3 Multi-Factor Authentication on Authcoin Protocol

The following chapter deals with applying risk assessment method to MFA in Authcoin protocol. First, levels of authentication security are presented to show MFA's advantage over single-factor authentication. Afterwards, MFA is presented in Authcoin's context, and the workflow of the authentication is depicted.

3.1 Introduction

The objective of Chapter 3 is to answer the research question RQ-1: How to secure the identity authentication process with MFA for the Authcoin protocol? - as presented in Chapter 1. To answer RQ-1 in an understandable way, the question is divided into thee subquestions:

- RQ-1.1 - What are the Security Levels of Authentication?
- RQ-1.2 - What is the Context where MFA can be Applied in Authcoin Protocol?
- RQ-1.3 - What are the Workflows of MFA?

Each sub-question has separate subsection correspondingly. Section 3.2 focuses on providing theoretical background by explaining safety levels of authentication in order to justify the selection of MFA method for Authcoin. Afterwards, in Section 3.3, the context of Authcoin is presented where MFA would be appropriate and where it is not needed. Section 3.4 illustrates the workflow of MFA in Authcoin protocol using a diagram. Subsequently, resulting diagram is discussed in Section 6.6 followed by the conclusion of this chapter in Section 6.7.

3.2 Multi-Factor Authentication As An Additional Security Layer

Currently, each country has its authentication assurance model, that does not allow to build trust between countries [64]. According to European Union website, usually, there is a scale, including 3 to 5 levels of assurance. Varghese shows that, too many levels can result in an additional cost to maintain authentication information, for example, issuing cards where passwords would be enough can be considered as an unnecessary expense. On the other hand, too few levels of assurance may not cover all business requirements and risks [64].

The Office of Management and Budget of USA describes four levels of authentication assurance (OMB 04-04). Each level represents the degree of trust that user who presented a credential is in fact that user [33].

Level	Description
Level 1	Little or no confidence exists in the asserted identity; usually self-asserted; essentially a persistent identifier
Level 2	Confidence exists that the asserted identity is accurate; used frequently for self service applications
Level 3	High confidence in the asserted identity's accuracy; used to access restricted data
Level 4	Very high confidence in the asserted identity's accuracy; used to access highly restricted data

Table 3: Authentication levels of assurance (OMB 04-04) (Source: [33])

NIST 800-63 Electronic Authentication Guidline presents requirements for each of authentication levels of assurance defined in Table 3, that is presented in below table:

Level	Identity proofing	Token (Secret)	Authentication Protection Mechanisms
1	No proofing required	Allows any type of token	No protection against offline attacks or eavesdroppers
2	Requires identity proofing	Allows single-factor authentication, such as passwords.	Online guessing, replay and eavesdropping attacks can be prevented
3	Requires stringent proofing	Allows MFA, typically using password or biometric factor used with a software/hardware/OTP token	Eavesdropping, online guessing, replay, impersonation and man-in-the-middle attacks are prevented
4	Requires in-person registration	Allows MFA with hardware cryptographic token	Online guessing, eavesdropping, impersonation, man-in-the-middle attack, and session hijacking attacks are prevented

Table 4: Technical Requirements of NIST 800-63 (Source: [33])

To clarify the meaning of certain terms, a man-in-the-middle attack is a wider term which also includes eavesdropping and replay attacks. Man-in-the-middle attacks are when small packets which are transmitted through the network between two parties, are captured by a malicious party.

Difference between offline and online attacks is that, during an offline attack, the attacker does not have to have communication with the system, and with an online attack, typically needs work on the system under attack.

Session hijacking is when computer session is stolen to authenticate a user against the remote server [49]. According to Nikiforakis et al., session hijacking is a form of impersonation.

Hardware cryptographic token is usually a smart card such as ID card, driver's license or credit card [29], and often is used with two-factor authentication [16]. For example, if hardware cryptographic token is used in combination of password, then hardware cryptographic token is useless without password. If the only password is compromised, it cannot be used without the physical token. According to De Cock et al., hardware cryptographic smart cards use algorithms such as RSA for secure data transmission.

As presented in Table 4, MFA resides on level three and four. Additionally, there are different security levels Using MFA. As presented by Kim and Hong, we can consider five level of security when using MFA:

Level	**Authentication method**
1	First level uses offline registered information such as bank account information, OTP and etc. At this level user has to provide something user has and knows. For example credit card information and password.
2	At this level an accredited certificate issued by a CA is used. CA identifies user with certificate issued by the government such as driver's license, passport and etc. At this level user has to provide something user has and knows. For example accredited certificate and it's password.
3	Level three adds another security measure to level 2 such as security card, security token and etc.
4	Level 4 adds hardware devices such as OTP for **something you have** factors
5	So far all the levels were 2-factor authentication types, but level 5 adds biometric information such as fingerprint, thus making authentication three factor. Aditionally to something user has and knows, level 5 adds **something user is** such as fingerprint or other biometric.

Table 5: User authentication level system (Source: [33])

As it is visible on Table 5, MFA also has different levels of security, that depends on specific application and business context. Analyze and decision about which type of user authentication is appropriate in Authcoin context is presented in subscetion 3.3

3.3 Authentication in Authcoin protocol

Authcoin relies on challenge-response mechanism for authentication [36]. So chosen challenge have to be the type, that helps one entity verify another participant. Also, if the goal is to fully automate VAR process, authentication factor cannot be biometric since it requires user interaction.

Token type	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Bio-Hard crypto token	X	X	X	X	X
Hardware crypto token	X	X	X	X	
One-time password device	X	X			
Software crypto token	X	X			
Passwords & PINs	X				

Table 6: Token types allowed at each assurance level (Source: [33])

Table 6 shows token types allowed at each assurance level that were presented on Table 5. Bio-hard crypto token uses biometric tokenization, which substitutes a stored biometric template with the token, that cannot be exploited and is non-sensitive. Hardware needed for such token is biometric readers, which can recognize a person based on a physiological or behavioural characteristic.

Bio-Hard crypto token is impossible to use with automated authentication, since without user it's impossible to provide biometrics. Other token types can be used with automated validation and authentication if necessary implementations are carried out on device or IoT machine.

Protect against	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Online guessing	X	X	X	X	X
Replay	X	X	X	X	X
Eavesdroppers		X	X	X	X
Verifier impersonation			X	X	X
Man-in-the-middle & PINs			X	X	X
Session hijacking & PINs				X	X
Signer impersonation & PINs					X

Table 7: Required Protections (Source: [33])

Table 7 further proves the fact that, using more factors of authentication, preferably biometrics is the most secure authentication type.

According to Kim and Hong, the user authentication method is chosen using the following steps:

1. Risk levels, authentication methods and transaction types are examined
2. Threats and vulnerabilities are analyzed
3. Risk assessment is performed to find the importance of threats
4. Table 5 is used to select authentication level system
5. Conduct test to ensure that risk has been decreased after applying user authentication
6. Regular risk assessments are conducted

Steps initialized for Authcoin context is as follows:

1. Transaction types of Digital certificates:
   - Create
   - Manage
   - Distribute
   - Store
   - Revocation
   - Use

   Risk Level: High
   User Authentication Methods: Challenge-Response Mechanism
   Additional Security Measures: Defence Against Sybil Nodes
2. The main threat for trust systems other than ones caused by the Internet's fundamental infrastructure is Sybil nodes.
3. Risk assessment:

Criteria	Description	Authcoin Descritpion
Service outline	Who are the customers? Data flow and etc	Trust network users, IoT machines
Transaction analysis	Analyze risk levels of transaction types	Challenge-response transaction type is vulnerable to man-in-the-middle and spoofing attacks
Transaction range	Verification of transaction types and range that require additional authentication	Automatic VAR
Promotions	Verification of provision when customer uses service to prepare for possible threat (transaction verification, password management and etc.)	User is responsible for keeping keys safe
Customer categorization	Verification of different customer types using different authentication methods	Human users, organizations and IoT machines In case of IoT machines and organizations, biometric authentication cannot be used
Influence on transactions	How application of MFA will influence customer service?	All customer categories will have increased trust in other entities

Table 8: Risk assessment criteria (Source: [33])

4. According to Table 5 and Table 8 level three authentication is the most appropriate in Authcoin context since it can be used in contexts where user might be a human or machine.

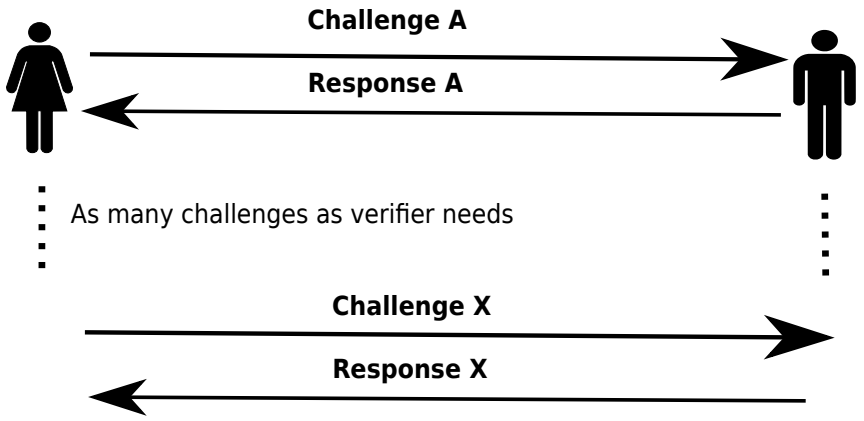
5. Testing requires users, IoT machines and organizations or their simulations, which is out of the scope of this thesis

6. If customer groups are changed or fundamental change will happen in Authcoin protocol the risk assessment and also steps for choosing an authentication method should be conducted again

3.4 Workflow of MFA in Authcoin protocol

In Authcoin protocol, there are two cases when authentication is used: Automatic VARs and standard authentication using challenge-response between two entities. In the presented diagram, it is assumed that verifier has no access to the digital representation of previous responses, so he/she cannot compare received response to anything. On this diagram verifier only can check received response on his/her own, without any infrastructure.

The workflow between two entities is represented on the diagram:



It depends on verifier to send an additional challenge or not, and to choose factors also since there are challenge types of local V&A, global V&A with and without additional information, the only verifier can decide if provided response was enough to authenticate someone. In the case of VAR, the only difference is that challenge is initiated by the system instead of the verifier.

3.5 Discussion

This chapter presented levels of security in authentication and steps to choose the user authentication method in Authcoin's context. Also, a simple workflow of MFA between entities where presented. Nevertheless, the risk assessment and steps provided for choosing user authentication are just guidelines to follow and not gives the guarantee that authentication is guaranteed to be safe. Safety measures against common hacking methods of internet infrastructure such as social engineering or spoofing still have to be conducted. Also, due to dependability on the context where Authcoin is used, the workflow of MFA is simplified since many variables might change, such as user, authentication factor, business and technical limitations.

3.6 Conclusion

3.6.1 Summary

Chapter 3 presented authentication levels of assurance and for each level by OMB 04-04, also described technical requirements for each level provided by NIST 800-63. Additionally, to further explain levels of authentication inside MFA, Table 5 was provided.

Furthermore, authentication token types that satisfy different levels of security were presented. Also, hacking methods that can penetrate through various levels of security were presented. The steps to choose user authentication methods were listed for general use and was initialized for Authcoin context, including risk assessment procedure. Finally, MFA workflow was presented in Authcoin protocol to understand better where it fits.

3.6.2 Research Questions

RQ-1.1 - What are the Security Levels of Authentication?

As presented in Table 3, there are four levels of security for authentication. They are ranging from self-asserted, no confidence level to a very high confidence level, which is used to access highly restricted data. According to these levels, we define our goals, that is to secure the authentication by achieving three or four levels of assurance.

As shown on Table 4 and Table 5 each of the levels has guidelines and requirements to fulfil. We can conclude that generally using MFA is the highest form of current security. Furthermore, if we combine biometrics with possession and knowledge factors, we can clearly improve security level compared to single-factor authentication.

RQ-1.2 - What is the Context where MFA can be Applied in Authcoin Protocol?

MFA is applicable for Authcoin users to create, manage, distribute, store, revoke and generally use their digital certificates. According to conducted risk assessment 8, we can conclude that level three authentication, which allows using MFA typically with biometric and password, is the most appropriate choice for Authcoin, since the user can be a human or machine and in-person registration might not always be possible for them.

Several considerations are that multi-factor authentication, if used with biometrics, cannot be used with fully automated VAR process if the goal is to avoid human interaction with the system fully. Also, if we are considering Authcoin in context of IoT devices, MFA can be used with different token types, such as OTP device or software token, as long as there are necessary implementations carried out on IoT device.

RQ-1.3 - What are the Workflows of MFA?

We concluded that the workflow of MFA could consist of several rounds of challenge-response messages between two Authcoin users, depending on the confidence of the verifier. Also, MFA can be used during the workflow of automatic VAR, when it is created randomly during the mining process of a new block on the blockchain and expresses the desire to verify the chosen user.

3.6.3 Future work and limitations

For future work, if Authcoin protocol will have any additional features added, the workflow of MFA should be instantiated in new contexts. Also, Risk-assessment should be done again to better assess the risks before choosing the

authentication factors for MFA.

The open issue for this chapter is the usage of biometric factors with IoT devices, whether the intervention of human users worth it for one-time authentication or how can or cannot MFA with biometric factors work with IoT devices.

4 Challenges For Authentication

In the following chapter, challenges are closely examined. First, the impact of risk-based authentication on challenges is presented. Depending on the context of the device used, different challenges are suggested. Afterwards, the ways of avoiding risks of biometrics are explained. Finally, customization of challenges are described, and the constraints are listed.

4.1 Introduction

The aim of Chapter 4 is to answer the research question RQ-2 - How to manage identity authentication for the Authcoin protocol? - this question is divided into three subquestions:

- RQ-2.1 - What Influence can Risk-Based Authentication have on Challenges?
- RQ-2.2 - What are the Ways to Mitigate the Risks of Biometric Authentication in Authcoin Protocol?
- RQ-2.3 - What level of Challenge Customization Should be Allowed from Users?

4.2 Challenges In Risk-based Authentication

Current portable technologies such as laptop and smartphones made it possible for everyone to access resources outside of network perimeter of work or home. Organizations can lose their credibility instantly, if their data is breached, or sensitive information about their workers is stolen. With the help of risk (or context)-based authentication, the system analyzes several variables before enabling login, such as device, IP address, biometrics, location and more [41]. Based on this information, the reliability of login attempt is measured, and depending on the level, login is complicated or simplified. Additionally, machine learning models can be utilized to learn about patterns of user login gradually, that can decrease the friction when possible and also increase the confidence of each context [41].

Challenge/response questions are used for different use cases in traditional centralized computing, such as password or PIN resets, or as a fallback in risk-based authentication when risk threshold is met and more challenging verification is required [53]. Challenges have to be carefully chosen to avoid sacrificing security and keep authentication convenient. There are some security consideration about challenge/responses authentication, for example, if the answer to a question can be searched on the internet or can be guessed, it can be easily compromised. Potential privacy issues are also another shortcoming of challenge/response questions because the user may not want to disclose answers to questions to other parties. Additionally, people tend to choose answers because of simplicity and familiarity, that eases hacker's job to guess it.

4.2.1 Context Attributes of Risk-Based Authentication

There are many attributes of user that might be considered as context: device (screen size, model number), physical environment (location, sound), network (IP) or behavioural (usage of a keyboard, mouse) attributes [68]. The context-aware system can be described as follows: "A system is context-aware if it uses context to provide relevant information or services to the user, where relevancy depends on the user's task" [67]. Analyze of each one of them for Authcoin protocol is needed:

Device environment - Spooren et al. analyzed mobile device fingerprinting and found that even though mobile device fingerprints are unique, it still does not constitute a suitable authentication mechanism. The author stated that most of the attributes such as screen dimensions, timezone, geolocation, fonts and etc. are highly predictable because they are either fully static or with a targeted attack, it is easy to simulate them. Contrary to mobile devices, Eckersley conducted an experiment that shows that web browser fingerprinting demonstrates more uniqueness of browser. This difference mainly due to the App Isolation model used by mobile phones and tablet operating systems. "Due to App Isolation model used by most mobile phone and tablet operating systems, installing new apps will, for example, not change the font list available in the phone's web browser" [61].

Physical environment - Mobile devices naturally has more chance of being stolen. However, Hintze et al. found that probability of robbery is highly dependent on country, city, district, time of the day and also social context, for example, it is less likely that theft will happen at home, but is more likely to happen in public transport or at work. If we could evaluate the risk of authentication numerically, then we can adjust the security level dynamically. At home, if the risk is low, maybe continuous gait recognition [46] can be used instead of explicit authentication, that identifies a person based on how they walk [26]. Hintze et al. continues by saying that, at night, in the criminal neighbourhood, maybe the second factor is needed like iris recognition, and probably some questionable actions like transferring money using mobile banking should be prohibited. To utilize this functionality, identifying high-risk locations are needed and GPS can not be considered as trustworthy since it drains battery life if used continuously and does not work indoors. Instead, GMS cell IDs and Wi-Fi MAC addresses should be used [26].

Network - According to Mostéfaoui and Brézillon, there are several technologies combined together to ensure the reliability of networks such as firewalls and encryption. Network-based security has flaws about the checks that it is able to perform because it does not operate on a high level of data abstraction and cannot understand the content of the traffic [26]. Mostéfaoui and Brézillon says that the network layer is only concerned about addresses, hosts and such network-related concepts. The author further continues that, IP can be used to find out the location of the user, but since there are many proxies used before reaching from one IP to another, it should not be used as the only source of truth. Moreover, it is merely cheaper to reconfigure the security infrastructure

at the application level, than on network-level [45].

Behavioural - Keystroke dynamics, speech patterns or gait recognition can be considered as behavioural attributes [67]. If fingerprint can be taken from ambient surroundings using sensors (audio, visual), then it is possible to identify if two IoT device is in the same trust network [41], but fingerprint cannot be used to identify user, without prior record of exact trust network fingerprint.

Before using any of the attributes, one should keep in mind the usability of attributes mentioned above heavily depends on the business case and should not be used as a single source of truth. Instead, they should be used in conjunction with other authentication mechanisms and some attributes such as IP, is better to use as a fallback if other primary authentication technologies are not available.

4.2.2 Context as an Authentication Factor

In this section, we explain how context fingerprints can be represented, so it is encoded and maintains privacy in any environment. Also, the metrics to assess the distance of the behaviour context. This section is based on Giura et al. [22].

Firstly, let's define symbols. We are interested in user behaviour over period of $T = [t_0, t_1]$ and have set of recorded sessions $\{S_1(T), ..., S_n(T)\}$. Given user with behaviour $S(T^*) = S1(T^*), ..., Sn(T^*)$ during period T^*, we are interested if the same users behaviour during $S(T)$ has enough similarity with $S(T*)$. For this reason, we define two functions $\rho(S(T))$ and $\beta(S(T))$. ρ is representation of $S(T)$ that is enough to calculate the score and β is a similarity level between $S(T)$ and $S(T^*)$. So to sum it up, we need to check whether this comparison by Giura et al. is true:

$$|\beta(\rho(S(T)), \rho(S(T^*)))| < \varepsilon$$

where $\varepsilon > 0$. We should keep in mind that we do not need to store session record $S(T*)$ to compute this test, and instead only store $\rho(S(T*))$.

Generally, features should be the elements that can uniquely identify a user, for example, a set of IP addresses that device accessed. The easiest way to represent a set and to query it is hash set. According to Giura et al., we hash $S(t)$ values for each user together with generated nonce n_u.

$$\rho(S(T)) = H(f, n_u)|f\varepsilon S(T)$$

Where H is a cryptographic hash function For measuring the distance between hash sets S and S^* we can use **Jaccard distance**:

$$J(S, S^*) = \frac{|S \cup S^*| - |S \cap S^*|}{|S \cup S^*|}$$

The drawback of this formula is that same number of bits for each hash value of each feature in the set should be stored and also computation time is linear, which makes it problematic for scalability.

Giura et al. states that another method which we can use is the Standard Bloom filter, which is more space-efficient. A Bloom filter contains a bit array

of size m with all the bits set to 0 at first, and k hash functions with the range of $1, ..., m$. When an element is inserted in the Bloom filter, it is hashed by all k functions, and then all the zero bits are changed to ones in the bit array. In the case of one hash functions bit is already one, it will not be changed because of collision. During querying of an element, the element is hashed with all k hash functions, and then the bits are checked in a bit array, if all of them are one, then we can say that element was inserted in the Bloom filter with the probability of the **false positives** rate. Even if one element was zero in the bit array, then we know that element was not inserted, hence a Bloom filter has no false negatives.

The query returns **possibly in set** or **definitely not in set**, so it cannot have false negatives, also elements can not be removed but can be added in the set. Another feature of Bloom filter is that the more number of items increases, the higher is the chance of false positives [22].

Giura et al. explains that, using **Hamming Distance** we can calculate the difference between two Bloom filters:

$$H(B, B^*) = \sum_{i=1}^{m} B(i) \oplus B^*(i)$$

where B(i) is the bit from bit array at index i. Different from Jaccard distance, the computation time for the Hamming distance only depends on the Bloom filter size, it does not depend on the number of elements inserted in each Bloom filter. Because standard Bloom filters can be represented as binary strings, the distance can be calculated as a simple XOR operation.

Standard bloom filter insertion function is idempotent, meaning that it can not differentiate if the same element is inserted multiple times or only once. To solve this problem Giura et al. suggests using **Counting Bloom filter**, that can store the number of times the element was inserted. Counting Bloom filter uses an array of counter of bins, rather than a single bit for each array position. So there is a tradeoff between the information saved in the filter and storage-saving made by the Counting Bloom filter. Euclidian distance for Counting Bloom Distance would be:

$$E(CB, CB^*) = \sqrt{\sum_{i=1}^{m} (CB(i) - CB^*(i))^2}$$

where $CV(i)$ is the value kept in the i-th bin of bins array CB.

Regarding the privacy of the aforementioned methods, the hash set saves random strings because of nonce ρ and H as a random function (Random oracle model) [22]. As long as $n_U \neq n'_U$, we can say that H for different users are independently random, meaning it is not possible to determine if the same feature in both ρ for U and U'. However, we can reveal if the same feature was present for the same user in different time frames, moreover it is necessary to calculate Jaccard distance. Also, ρ reveals the number of features that were stored during T period for user U.

According to Giura et al., bloom filters are concise in the representation of information and hence, we gain all the privacy benefits. We store n bits of information, about set containing n number of features, where $n = |S(T*)|$ is the total of recorded features. An array of n bits has an entropy maximum of n, let us suppose that feature has an entropy of γ and all the features are independent. Then, after exposing Bloom Filter, the entropy would be $n(\gamma-1)$.

Giura et al. continues by saying that the privacy of Counting Bloom Filters is very similar to standard Bloom Filters. Suppose that ι is number of bits for each counter, then the entropy left after exposing counting array is $max0, n(\gamma - \iota)$. Theoretically, privacy provided by Counting Bloom Filters are dependent on the strength of the hash set representation, nevertheless, in practice, it is unlikely that an adversary can extract the entire hash set from the Counting Bloom Filter [22].

To sum this up, we examined three methods of storing sessions which in turn contains elements that help identify the users. Giura et al. states that the privacy is preserved more in Bloom filters than in Hash Sets, because of the lossy representation of information. The computational time of using Hash Sets for calculating Jaccard distance is linear, hence problematic for millions of users [22]. Giura et al. continues by saying that standard Bloom Filter is a space-efficient probabilistic data structure, and the computational time for Hamming Distance, which uses Standard Bloom Filter, is independent of the number of elements inserted in each Bloom filter and depends on the size of the Bloom filter only. In the case of Counting Bloom filter, computational time depends on the size of the bins array [22].

4.2.3 Changing Resource Owner

Since new user behaviour is not as easily detectable as changed device, Confidence function $C(s, t)$ would be necessary to assess current user sessions s at time t. It seems natural to value the confidence with an exponential decay with a half-life λ confidence when a new behaviour is recorded [61]. The threshold of confidence would be defined, and in case of exceeding it, we know that a new user is present.

4.3 Mitigating Risks of Biometric Authentication

The main goal of MFA is to increase the security of the authentication process, but there are still security considerations, and MFA should not be thought as perfectly safe. All of the biometrics can be compromised, and they are critically analyzed in this chapter.

Another consideration when using MFA is usability. Knowledge and possession factors have apparent usability disadvantages, remembering the password and carrying physical tokens accordingly. Concerning biometric recognition [30], studies [24][19] show that improved usability is major advantage of biometrics.

By definition, multi-factor authentication adds several factors to make authentication more challenging. This indeed hinders hackers from accessing the

protected resources, but it also adds discomfort for real users to use the application. Because of that inconvenience reason, Google recently revealed that less than 10 per cent of users are using the two-factor authentication, which they offer for free [1]. Also, workers who are relying on speed, such as hospital workers, can not use MFA. Theoretically, these problems can be solved using risk-based authentication, but because of implementation costs, it is not realistic in all cases.

4.3.1 Avoiding Problems of Biometrics

Biometric recognition systems, in essence, are pattern recognition systems. They record user characteristics using devices and then encode, store and compare these characteristics. Most of the biometric systems have two phases, enrollment and matching process [2]. It is essential to keep in mind that the efficiency of security systems does not only depend on technology and should be accomplished with people and technology working together [2]. According to Alaswad et al., the most used biometric technologies include hand geometry, iris recognition, retina recognition, signature recognition, facial recognition and fingerprint recognition. Alaswad et al. further continues by saying that attacks on biometrics can be grouped into four groups and analyzes them one by one: processing and transmission level attacks, input level attacks, back-end attacks, enrollment attacks.

Processing and transmission level attacks deserve attention because of many biometric systems transport data for processing. Encryption should be used before transporting, but not all systems use it because sometimes it is seen as a deployer-specific aspect of system design [2]. Anti-spoofing techniques, encryption of data, fallback techniques are essential aspects of biometric system security.

Regardless of how hard we try to secure the system, it still is not insured that nothing happens. So we have to have fallback mechanisms in place. Cancelable biometrics uses an algorithm to distort the recorded image and saves the data in this manner if the data is compromised, it is trivial to distort the image the second time [2]. This solution is not foolproof, and if the original image is not protected, then the whole technique loses credibility.

The main **Input Level attacks** are spoofing and bypassing, happening during the initial processing of the sample. Another input-level attack might be **overloading**. Overloading is an attempt to damage the input device by too many attempts [2]. In Authcoin context, if the authentication happens person to person than this is no significant threat, but if the authentication is machine to machine or person to machine, then it might need some protection mechanism in the system.

Back-end attacks are critical when protecting distributed biometric systems. The back-end is concerned with matching or making the decision and attacks targeted at modifying these decisions are severe. Attacking the template storage database is the most prominent attack on beck-end [2]. The possible modification of stored templates can result in false rejects or accepts. There

are many attack vectors once an attacker gains access to back-end: replay attack using a compromised template, hijacking identity and injection of attackers template. These attacks can be avoided by hashing and encryption of data [2].

The attacker also can change the matching subsystem in back-end and influence the decisions in this way. Defence against this attack is to use principles of building trusted systems and continuously check code integrity.

Similar to many back-end systems, denial of service attacks can be targeted to back-end biometric system, and traffic analysis can be used to stop this attack.

Next, Alaswad et al. talked about threats of **Enrollment attacks** include threats:

1. Enrollment with valid biometrics and changed identity.
2. Enrollment with false biometrics (using **gummy bear fingerprint**)
3. Enrollment with swapped biometrics
4. Enrollee and enrollment operator are both adverse, and any of the above listed can happen
5. External attacks to the enrollment station or other parts of the system: man-in-the-middle, replay, and spoofing. There are several countermeasures against these threats such as observing enrollment instead of unobserved self-enrollment, an additional manual check of identity, encrypted communications, and firewall on enrollment device.

Also, there are threats which are more related to identity proofing than enrollment:

1. Using forged documents
2. Impersonating legitimate users
3. Corrupt personnel

Additionally, to previously listed security measures, countermeasures against identity proofing include:

1. Separation of roles of personnel
2. Close inspection of documents
3. Confirm user during credential issuance to avoid manual modifications of personal data

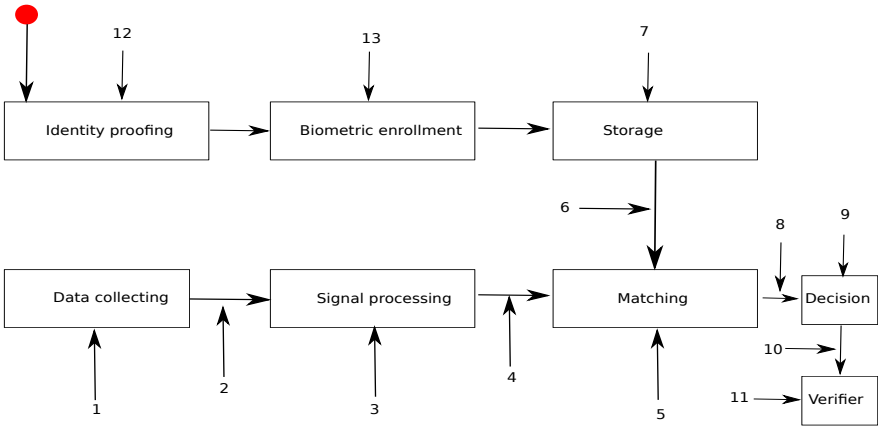


Figure 4: Attack points on biometric system (Source: [2])

4.4 Customization of Challenges

Without Risk-based authentication, the user chooses factors to use for authentication and also can customize the challenges if it is possible. In this case, choosing of factors depends on the user, and concerning the actual challenges, camera-, voice- and text-based authentications are the only types were the user can ask for significantly customized challenge.
Depending on the involved parties of authentication, the available challenges vary. Below are presented available challenges and their context, along with their usability considerations.

4.4.1 Authentication Against Organizations

If the organization have a back-end system in place to check the received hashed biometrics as explained in 4.2.2 or other credentials, then authentication can be done. Using hashed biometrics is a private challenge in Authcoin context, because non-involved parties cannot check the actual biometric, but can see if the authentication was successful or not.

4.4.2 Person to Person Challenges

When the authentication happens between two people, who do not have any back-end technologies in place to use against hashed biometrics or other sent credentials, they can only use the type of challenges which they can identify. Examples are face recognition with and without identification documents, voice recognition and text-based challenges.

As explained by Leiding et al. [36] there are three types of challenges between two persons:
1. Local V&A with additional information, when two entities have a channel to communicate and also have old information about each other
2. Global V&A with additional information, when two entities do not know each other's personal information but can communicate
3. Global V&A without additional information, when two entities do not have each other's personal information and neither can communicate. In this case, Authcoin only allows validation, not authentication.

4.4.3 Machine to Person Challenges

If IoT machine tries to get permission on something and it needs to authenticate itself against the person, then this type of authentication can be used in Authcoin protocol. This type of authentication is quite limited because there is a limited amount of credentials that person can authenticate without having any technology or system at hand. One example of this type of Authentication can be if IoT device sends its serial number and the permission that it tries to get to the person, and the person declines or accepts it.

4.4.4 Machine to Machine Challenges

For successful authentication, IoT machines have to have the back-end necessary to authenticate based on received credentials, that can be many things depending on the IoT machine: OTP, recorded audio [41], captured image, using risk-based authentication or combination of any of them.

4.5 Discussion

One has to keep in mind that challenges analyzed in this chapter (such as biometrics) are not meant to be used in isolation, and the analysis is based on the precondition that several challenges are combined for Authentication. Concerning attacking vectors, besides the listed threats, all of the dangers which information technology systems fundamentally have, such as man-in-the-middle or DDos, also applies to the challenges explained in this chapter. Specifically, it is impossible to defend from all kinds of social engineering attacks, since it is limited only by attackers creativity.

4.6 Conclusion

4.6.1 Summary

The main goal of Chapter 4 was to specify how challenges are managed in Authcoin protocol. We analyzed how risk-based authentication can change the challenges based on context information, what kind of contexts can influence the challenge choosing process, how the context is stored and compared to another context, and how changing of the device or changing the owner of the resource

can happen in the Authcoin protocol. Then we presented attack vectors of Biometric authentication since as explained in 3.3, it is a preferable factor during MFA.
Finally, different challenge combinations of the participant in the authentication process were analyzed, and examples were given how authentication might happen between them.

4.6.2 Research Questions

RQ-2.1 - What Influence can Risk-Based Authentication have on Challenges?
We concluded that with risk-based authentication, we could automate the authentication using the context, that might be based on device-related, physical, network-related and behavioural attributes. Risk-based authentication has the goal to authenticate the user based on his/her context, and only if a certain threshold of confidence is not achieved, then activate authentications which usually requires user interaction.
By examining three methods of storing sessions for identifying users, we concluded that when privacy is prioritized, Bloom filters should be used rather than Hash Sets.
RQ-2.2 - What are the Ways to Mitigate the Risks of Biometric Authentication in Authcoin Protocol?
By identifying attack points on the biometric system, we concluded that defence mechanisms such as anti-spoofing techniques, encryption of data, fallback techniques and also identifying questionable behaviours could be used to mitigate risks for the listed attack vectors. Also, traffic analysis can be used to identify denial of service attacks.
There are several attack vectors on biometric authentication such as input level attacks, processing and transmission of data attacks, back-end and enrollment level attacks.
RQ-2.3 - What level of Challenge Customization Should be Allowed from Users?
By depicting the types of combinations of use cases between human person and machine, we concluded that depending on used factors of authentication, challenges could be customized with a different degree. The most customizable challenge type being a biometric factor when used between two persons. Also, machine sometimes can customize the challenge for a person, for example, using CAPTCHA.

4.6.3 Future work and limitations

The open issue about mitigating risks is that none of the prevention mechanism is always successful in doing its job, and security should not be taken as granted when using any of the listed risk mitigation techniques.

5 Application of Multi-Factor Authentication on Authcoin Protocol

The following chapter deals with the application of MFA in a real-life scenario. In Section 5.2 the most seamless factors and challenges are chosen for implementing the person-to-person use case of Authcoin protocol. Section 7 presents an implemented solution that uses factors chosen previously. Finally, issues and considerations of implementing MFA are presented in Section 5.4.

5.1 Introduction

The objective of Chapter 5 is to answer the research question RQ-3: How to implement MFA for the Authcoin protocol? - as underlined in Chapter 1. To answer this question step by step, it is divided into three subquestions:

- RQ-3.1 - What combination of challenges is the most seamless for two-factor authentication?
- RQ-3.2 - What are the use cases of MFA in person to person authentication?
- RQ-3.3 - What problems arise during implementation?

Each sub-question is answered in a separate section. Section 5.2 answers subquestion RQ-3.1, by focusing on finding a seamless way to use two-factor authentication. Subsequently, by answering RQ-3.2, Section 7 demonstrates the use case of implemented two-factor authentication of the Authcoin protocol. Afterwards, Section 5.4 answers RQ-3.3 by providing lessons and issues concerning the implementation of two-factor authentication of the Authcoin protocol. Finally, the section 6.6 discusses additional considerations followed by conclusion in Section 6.7.

5.2 Usability of MFA

In chapter 3, we showed that MFA, preferably using biometrics, is the most secure authentication type. In Subsection 5.2, we investigate what kind of biometrics are the most usable.

According to Maple and Norrington, biometric authentication is divided in two areas:

- Physiological - What someone is. For example, fingerprint or other physiological characteristics of human.
- Behavioural - What someone does. For example, Gait recognition or other display of action from a human.

Some biometrics gradually were discredited through the years, for example, Alphonse Bertillion's Anthropometric technique (1878) of physiognomic body

and head measurements considered as different measurements of the same individual that was inconsistent, so it changed over time. However, his **speaking likeness** method of describing a person with facial and physical characteristics is used worldwide.

Biometric	**Global**	**Japan**
Fingerpint	43.6%	57.4%
Face	19.0%	3.2%
Hand Geometry	8.8%	-
Middleware	11.5%	-
Iris	7.1%	3.8%
Voice	4.4%	-
Signature	1.7%	-
Multiple Biometrics	4.0%	-
Vein	-	25.4%

Table 9: Biometric market by technology. Global data (2006), Japan data (2005) Source: [37]

The ISO has developed a definition of usability and practicality, helping of which, we can assess the biometric schemes.

Usability: "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use"[20].

Practicality: "The extent to which a product can be used by an organisation to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [37].

Maple and Norrington also states that authentication is not goal intrinsically, and is a means to an end because people go to work for work and not to authenticate themselves.

Each biometric has a different characteristic of effort, uniqueness and intrusiveness. As shown in Table 9 intrusiveness is almost inversely proportional with uniqueness.

Biometric	**Intrusive**	**Effort**	**Unique**
Ideal	20	20	20
Retina	2	3	16
Fingerprint	7	9	14
Iris	7	10	12
Facial	8	16	11
Hand	11	6	9
Voice	20	11	7
Signature	16	15	5
Keystroke	18	12	4

Table 10: Biometrics and Usability Source: [37]

International data shows that around 10% of the world's population has disabilities [37], which gives us a strong argument for designing workplaces for the variability of human capabilities. People with visual disabilities might not be able to see the scanner at all, or someone with arthritis or cerebral palsy can find fingerprint scanning challenging [37].

Our recommendation is to before implementing biometric schemes, engineers should consider how people with different characteristics or disabilities interact with equipment. Maple and Norrington states that people with different level of perception can perceive equipment differently, and cognitive abilities might be a problem if instructions are challenging. In conclusion, the equipment should be tested with possible users before designing biometric system.

As seen in Table 10 facial recognition is the most effortless biometric to use. In Authcoin context, in case of a person to person authentication, we use facial recognition in combination with knowledge factor. Because of easily accessible smartphones, facial recognition technologies are available for almost every smartphone user.

5.3 Demonstration of Authentication

The easiest way to demonstrate MFA on Authcoin is to implement its use case - two-factor authentication using inherence and knowledge factors between two persons. This demonstrates how the MFA can be used in example scenario between two persons, but as explained in Section 4.4 it is not limited to person to person.

5.3.1 Authentication Scenario

In this Subsection, two users are sending challenges and responses to each other that finishes with successful authentication.

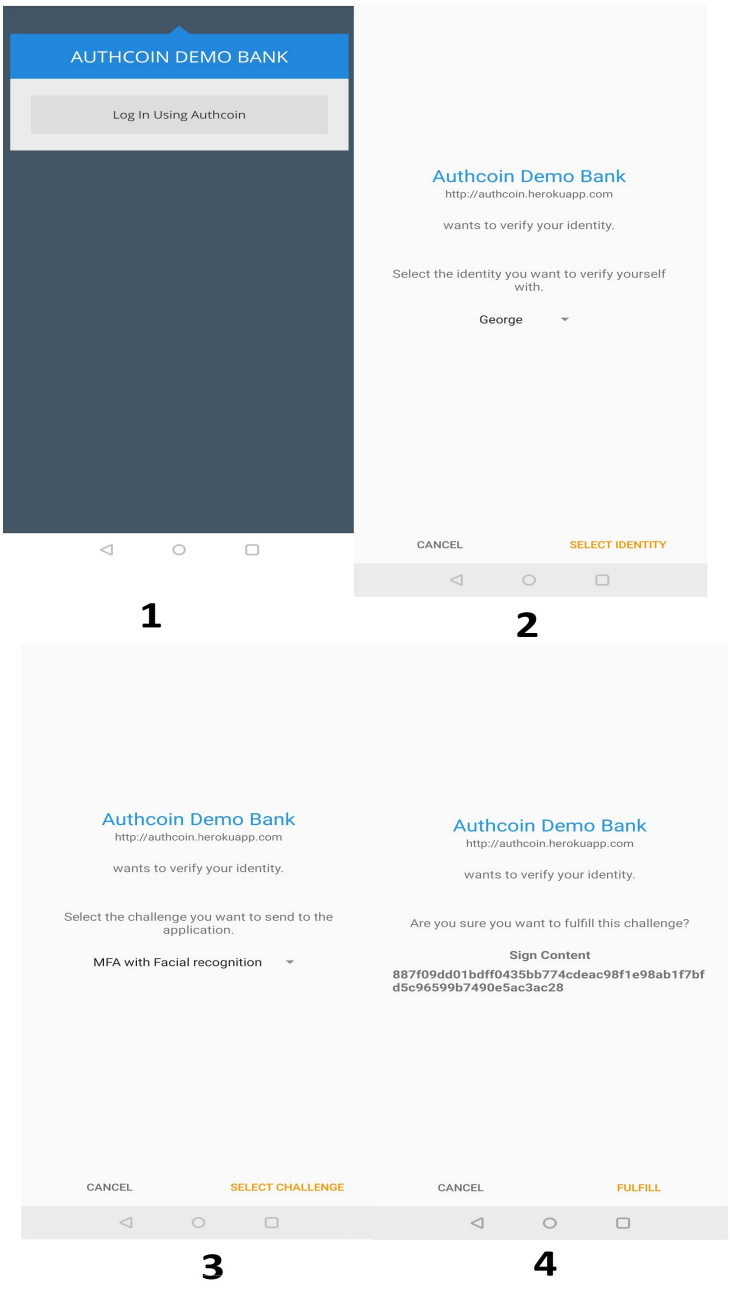


Figure 5: Steps 1, 2, 3 and 4 of Authentication scenario

In this demonstration, we have two parties: Bank and client. Authentication starts on the bank website by clicking **Log in Using Authcoin** button (Figure 5 - Step 1). Next, the Authcoin android application opens

for client and asks to choose the identity which they want to verify themselves with - Step 2. On the third step, client chooses the authentication method which is MFA using Signing content & Facial recognition, and on the Step 4 the MFA starts with Sign content challenge (Figure 5).

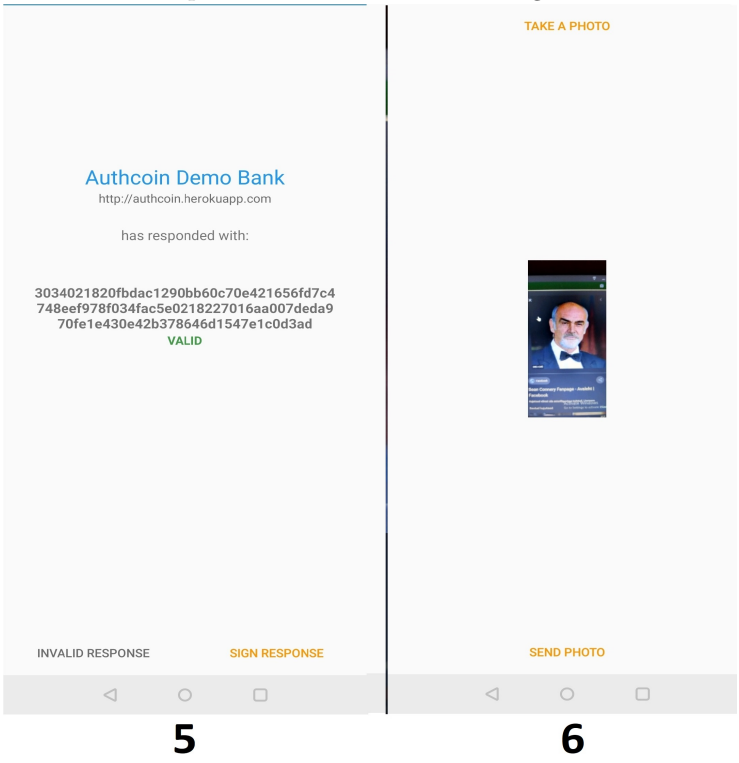


Figure 6: Steps 5 and 6 of Authentication scenario

After receiving the response from the bank, the client signs the reponse to finish the authentication of the first factor, and then authentication for Facial recognition starts Figure 6.

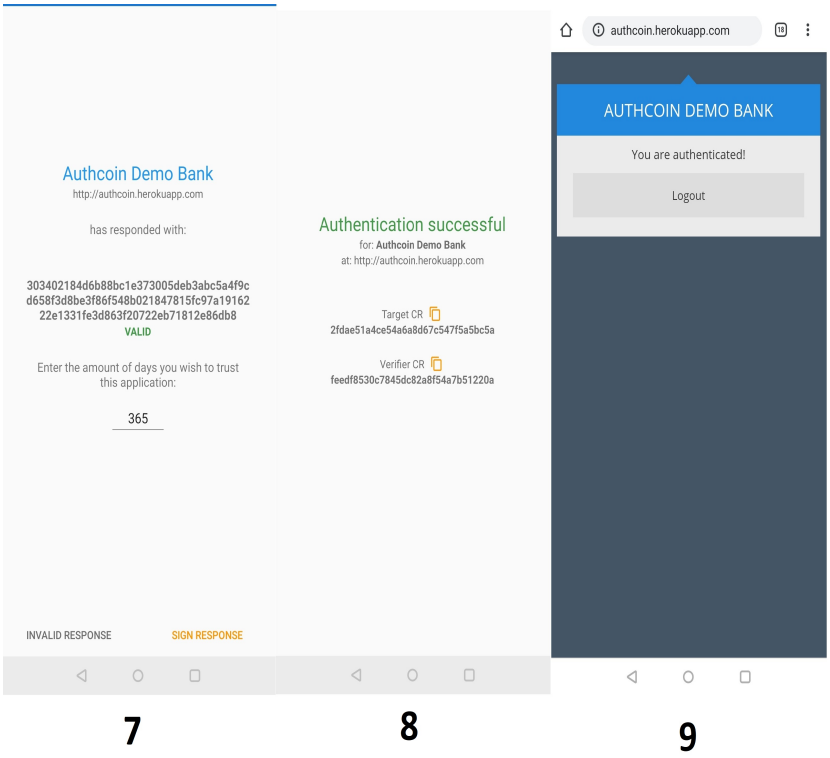


Figure 7: Steps 7, 8 and 9 of Authentication scenario

After taking picture, the client sends it to bank Figure 7. Finally, after accepting your picture, the bank responds it's own picture which is sent as bytes, and if the client accepts it, then he/she signs it. In this way, MFA finishes and the client writes the number of days to trust the application. The android application returns challenge record of target and verifier also, the bank displays successful authentication.

5.4 Lessons Learned from the Implementation of Multi-Factor Authentication in Authcoin Protocol

Implementing two-factor authentication presented some challenges. In this subsection, we present all the issues related to the technical part and also give recommendations to business-oriented readers.
The biggest lesson learned during implementation is to always have documentation of software as a required step of the system. Documentation should be the consideration of the technical- and business-oriented people alike. Non-documented software increases the time for not only to add features to software but also to simply run the already implemented one because of required configurations that are always part of non-primitive software systems.

Also, when starting the implementation of software, it is needed to make it as extendable as possible. Because if the goal is to build the system step by step, then changing the structure of the system becomes challenging. Either system should be planned to have all of the authentication features from the start, or if it is impossible, then implementation of the system should be started in a way that allows easy integration of new features.

5.5 Discussion

As a result of implementing MFA with Authcoin, some limitations apply to resulting software artifact. The responses of the bank are simulated, it always responds successfully. In the ideal case, the bank should display the picture that was sent from Android application, approve or reject it, and then, in turn, take a picture to send it to Android client.

5.6 Conclusion

5.6.1 Summary

Facial recognition paired with signing of content is implemented in order to demonstrate MFA on Authcoin protocol. The implemented software is presented and described. As a first step, the usability of MFA and additional considerations were explained. Table 10 presents different features of biometrics, and as a most effortless way of biometric authentication, facial recognition was chosen for implementation.

5.6.2 Research Questions

RQ-3.1 - What combination of challenges is the most seamless for two-factor authentication?
From Table 10, we concluded that since facial recognition is the most effortless biometric to use, we should implement it with MFA on Authcoin as one factor. Current use of smartphones makes the combination of knowledge factor and biometric such as facial recognition, the most seamless combination for MFA.
Another conclusion is that since 10% of the world's population has a disability, the developers of the MFA system should consider and support them. Our chosen facial recognition is effortless, but people with different disabilities may still find using it difficult.
RQ-3.2 - What are the use cases of MFA in person to person authentication?
Our implementation helped us conclude that when there are two persons authenticating each other, successful MFA can happen while posting one unique VAE id for all of them challenge-responses. Same VAE id means that both factors of authentication took place as a single unit.
RQ-3.3 - What problems arise during implementation?
The implementation helped us conclude that missing documentation of the software, make it hard to understand the already existing system, which in turn

makes hard to implement MFA. Also, the structure of software was not set up to have MFA added but was created to add another single-factor authentication challenge types.

5.6.3 Future work and limitations

A possible subject of future work can be implementing missing features of Authcoin protocol in software system or add different biometrics of authentication other than facial recognition. Also, implementing currently simulated bank's side, so it becomes closer to reality. Concerning the implementation of Authcoin protocol itself, currently, it is not secure enough since it is only for demonstration.

6 Evaluation

The following chapter evaluates the results of previous chapters. Chapters 3 and Chapter 4 require formative approach [65] for evaluation because of exploratory nature of the research, and Chapter 5 needs summative approach [65] of evaluation because it produced the artifact. Section 6.2 evaluates the security and usability features of MFA introduced in Chapter 3. Subsequently, Section 6.3 evaluates the feasibility of risk-based authentication and usage of biometric factors presented in Chapter 4. Section 6.4 focuses on evaluation of proof-of-concept produced in Chapter 5. Lastly, this chapter presents related work in Section 6.5 and ends with discussion and conclusion in Section 6.6 and Section 6.7, accordingly

6.1 Introduction

Based on the design science research methodology explained in Chapter 1, this chapter performs an evaluation of artifacts created in this thesis.

According to Shenton [59], there are criteria which determine the trustworthiness of evaluations: transferability, credibility, dependability and confirmability. The author further explains each of them: transferability ensures that findings apply to other scenarios, whereas credibility is concerned with the validity of findings. Dependability of the evaluation in the context of qualitative research is concerned that the processes of the study are reported in detail so that future researchers can reiterate the work. Confirmability means that the source of the results is informants and not the preferences of the researcher.

6.2 MFA Evaluation

Due to the exploratory nature of the Chapter 3, simulations or technical characteristics are not applicable. Our main goal is to evaluate the answer to our first main research question and also provide guidance for business-related readers about cost-benefit, resource utilization and social action:

RQ-1: How to Secure the Identity Authentication Process with MFA for the Authcoin Protocol?

Also, we will evaluate efficiency, uncertainty and also reduce the risks of our proposed concept. MFA's major risk is user-oriented, rather than technical, so the evaluation should involve social aspects of MFA. Therefore, Human Risk & Effectiveness strategy is chosen for evaluation.

Concerning evaluation criteria, because of formative content of Chapter 3, chosen criteria are: Cost-benefit, resource utilisation and social action.

6.2.1 Secure Identity with MFA

Presented four levels of authentication gives us the starting point to decide what kind of authentication we need. Depending on business requirements, the

needed level can be chosen, which in turn will be needed to follow guidelines to satisfy the technical requirements of different levels.

The main limitation to using MFA with Authcoin is that, if Authcoin is used with machines, authentication part of VAE, usually can not be fulfilled by machine. The essence of biometric is that human interaction is needed, which in turn constraints authentication of the machine against a person or another machine when the biometric factor is used. Usage of Authcoin with IoT devices are out of the scope of this work, but generally, every different type of challenge type needs different implementation on IoT device to generate or accept the token. If we assume that token types are not a problem for neither participant party, the MFA can be used to authenticate user, when he/she tried to create, manage, distribute, store, revoke or use a digital certificate to authenticate themselves in environments such as a bank.

The workflow of MFA in Authcoin consists of several challenge-response cycles between two users. Also, MFA can be initiated by VAR and hence, machine to person MFA can take place in such a manner.

6.2.2 Cost-benefit

According to Altinkemer and Wang, the expected loss, when the system fails, is the value that the provider has to compensate to customers, and also the lawsuits and penalty costs. This compensation increases with the level of the provided information by users. In a single-factor authentication system, according to Altinkemer and Wang, the cost of the failed system would be:

$$C_n = F_n(t)(V_n + L_n)$$

Where n represents a component of authentication system. V is the potential value that lost customers could create, and L is the cost of lawsuits and penalties.

Altinkemer and Wang continued by explaining about four components of using biometric authentication and also provided the formula for it: When a company decides to use biometric authentication, cost consists of four components. First it the implementation costs (c). The second is the net change of customers base (net_bio), which is measured by the net value which new customers can possibly bring. When new system is installed, the company may lose some existing customers due to inconvenience created by new system, which equals to market share (m) times percentage of lost customers. On the other hand, the company may attract some new customers because of possible safer authentication, that is measured as a potential market share $(1 - m)$ times certain percentage. The last two components are the expected loss after the system fails and loss of customers if the system in fact fails.

$$C_{bio} = c_{bio} + V_{net\_bio} + F_{bio}(t; \bar{s})(V_{bio} + L_{bio})$$

V_bio equals the new market share after the net change of customer base multiplied on a certain percentage. L_bio is a sum of weights of each components: $w\_bio1 + w\_bio2$

If the company decides to pair biometric with factor of authentication that was used during single-factor authentication, then Altinkemer and Wang provided a different formula for it: Expected costs and losses would consist of four components:

$$C_{nbio} = c_{nbio} + V_{net\_nbio} + F_{nbio}(t; \bar{s})(V_{nbio} + L_{nbio})$$

where *net_nbio* is the net change of customers potential value when the company adopts the new system.

6.2.3 Resource Utilisation

Altinkemer and Wang argues that only decreasing of the probability of system failure might not be enough reason to justify spendings for the new authentication system. To be specific, implementation costs should balance the reduced losses and the net change of customer value [4]. The study says that sometimes if the implementation costs are high, it is still preferable to implement a new system if it can reduce the losses and gain new customers at the same time.

If the number of privacy-sensitive customers is too small, the implementation cannot be justified by improved security, and on the other hand percentage of privacy-sensitive customers should not be too high [4]. The study finds that it might seem unnatural but if most of the customers are privacy-sensitive, then the provider might lose the majority of the customers if the system fails.

If the convenience is the main reason for implementing new authentication system, then the provider should consider needs of new potential customers, instead of existing ones, otherwise thinking about privacy issues are redundant since the main goal would not be achieved [4].

Altinkemer and Wang adds that from the governments side, to make the system more preferable, they can lower the penalties and payments to customers, in case the system fails. Also, regulators can increase penalties and payments to customers if the provider keeps the old authentication system. In this way, the government can force then provider to start using the new system.

In conclusion, it is not necessary to choose between single- and multi-factor authentication systems and depending on customers preferences, provider can implement different authentication systems to better fit the customers needs [4].

6.2.4 Social Action

Altinkemer and Wang explains that when we want to change the level of authentication system, it can imply that the user needs to provide more personally identifiable information. The concern about privacy may stop potential users from using authentication system, which in turn impacts company's decision about choosing authentication system. Therefore, privacy should be considered when choosing authentication system [4].

Altinkemer and Wang emphasises that loss increases as the level of the provided information. The study adds that, when the company needs to collect

new information because of a new system, assuming other things equal, the new system is less desired.

6.3 Challenges Evaluation

For Chapter 4, our goal is to evaluate ethics, uncertainty and reduce risks and also evaluate the answer to the main research question:

RQ-2: How to Manage Identity Authentication for the Authcoin Protocol?

Since biometric authentication, getting the context of user and also allowing users to customize challenges are all social related and privacy-critical topics, chosen strategy for evaluation is Human Risk & Effectiveness strategy [6].

Chosen evaluation criteria are User Satisfaction, Social action and Resource utilisation.

6.3.1 Manage Identity Authentication in Authcoin

Risk-based authentication can be thought as the intersection between all the other factors of authentication such as biometric, knowledge-based or possession-based. It can be used in Authcoin context by machines and by users alike. Additional implementation costs will be needed for risk-based authentication, and contextual data about unsafe and safe environments will be needed, but the resulting product will significantly simplify the authentication process.

Biometric authentication, similar to other factors, has several points where it can be compromised. The system should try to cover as much as possible to mitigate risks in such places: When inputting the biometrics, transmission the data or when a new user is registered. Risk mitigation techniques such as traffic analysis, encryption of data or fallback techniques reduce risks, but it is not a full guarantee of a secure system.

Challenge customization can happen in within the range of challenge tokens which allow it, such as audio or facial recognition, where one user can ask another user to record audio or take a picture with a specific demand. Machines can only demand customized challenges as much as they have implementations to support them and identify such response.

6.3.2 User Satisfaction

According to El-Abed et al., interviewed respondents thought that biometric authentication is more trustworthy than secret-based solutions against fraud. The robustness of the face recognition system against hackers is considered as a major factor affecting their concerns about privacy issues [19]. El-Abed et al. claims that only the performance of the biometric system is not enough reason to consider it more preferable than another biometric system with less performance. The author continues by saying that robustness of a system against hackers should always be seen as another important factor when designing a system, involving biometrics.

Risk-based authentication balances using the context of user and factor that needs user's proactive action for authentication [19]. The study by El-Abed et al. says that not needing to do anything for authentication can be considered as the most seamless way to identify person, but the main pitfall is to avoid giving away context information to a hacker. The main goal for Risk-based authentication system should be to correctly identify dangerous situations and act accordingly [19].

6.3.3 Social Action

By definition, the least social action from users is needed during risk-based authentication, assuming that context is not considered dangerous. Since risk-based authentication may involve biometric factor as a trustworthy way of verification, we must also consider their social action.

Biometrics require more action from a user than secret-based authentication methods. An additional consideration for biometrics are people with limited capabilities, also, people's appearance, voice or other factors are not always constant.

6.3.4 Resource Utilisation

If the biometric factors are used between two persons, and the identification happens directly between them, then needed resources like system for matching biometrics, are not needed.

If the usage of Authcoin is planned between parties when one or both participants are machines, then additional implementation of systems for matching the biometrics are needed.

6.4 Proof-of-concept implementation

6.4.1 Implementation

Our goal is to evaluate the answer to one of the main research questions:

RQ-3: How to Implement MFA for the Authcoin Protocol?

Current use of smartphones makes a combination of knowledge and biometric factors the most seamless two-factor authentication type. Several other biometrics can be thought of as a replacement for facial recognition such as audio recognition or fingerprint, but a key point to remember is that easiness of usage depends on the business case and user base.

The easiest way to show the use case of MFA is the person to person authentication. We showed how MFA with biometrics could be used between phone and simulated bank.

Problems of implementation include missing documentation, since the Authcoin system alone is already complicated system to understand, and if there is the additional factor of authentication to add, then it becomes hard if the developer does not understand already existing system.

6.4.2 Use Case evaluation

While Section 6.2 and Section 6.3 evaluate Authcoin with regards to challenges and general multi-factor authentication, the applicability and feasibility of MFA in information system has not been covered yet. To do so, the proof-of-concept of multi-factor authentication based on Qtum blockchain [14] was created and is available on Github (see Appendix A). As a note, the implementation of Authcoin protocol was started already, and this thesis adds MFA implementation to it. In order to evaluate the prototype in a common authentication scenario, we use android application and spring project to initiate and fulfil the challenges for identification.

When sending bytes as a challenge to another party, the price which is paid in QTUM's was approximately 8 unit. Transferability of implemented software is applied to all establishments or parties which has a human representative, in case if the machine is a sender or verifier, then the system needs additional implementations.

Confirmability of the results of authentication is provided by the blockchain naturally. Anyone knowing the address of the contract can go to the explorer of QTUM, and see the list of transactions.

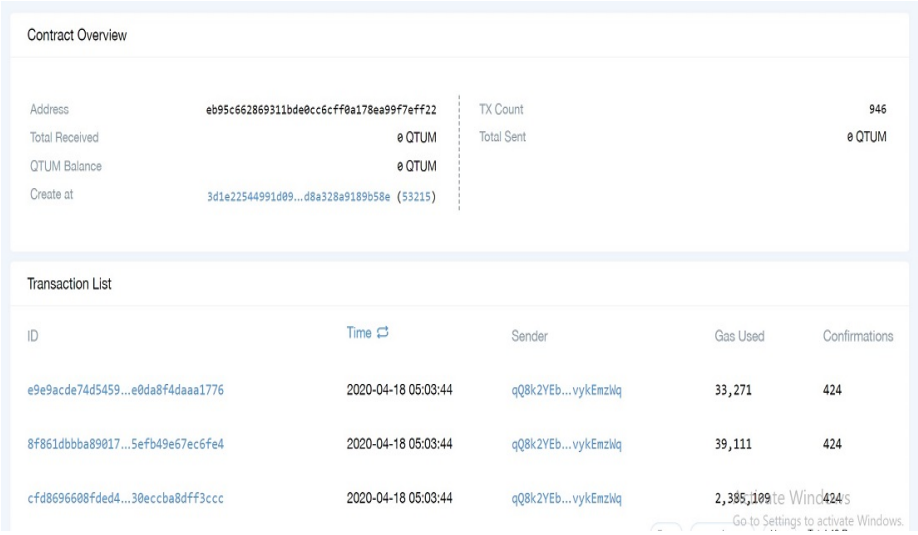


Figure 8: Transaction list

It is also possible to to query Validation And Authentication entry (VAE) using qtum command line interface, as it is explained in Authcoin truffle project documentation (see Appendix A).
Another way to confirm that two challenges belong to the same VAE is through the android application. On the challenges page, there is a list of challenges, and they display the VAE byte array when it is clicked. We can identify challenges which have the same VAE:

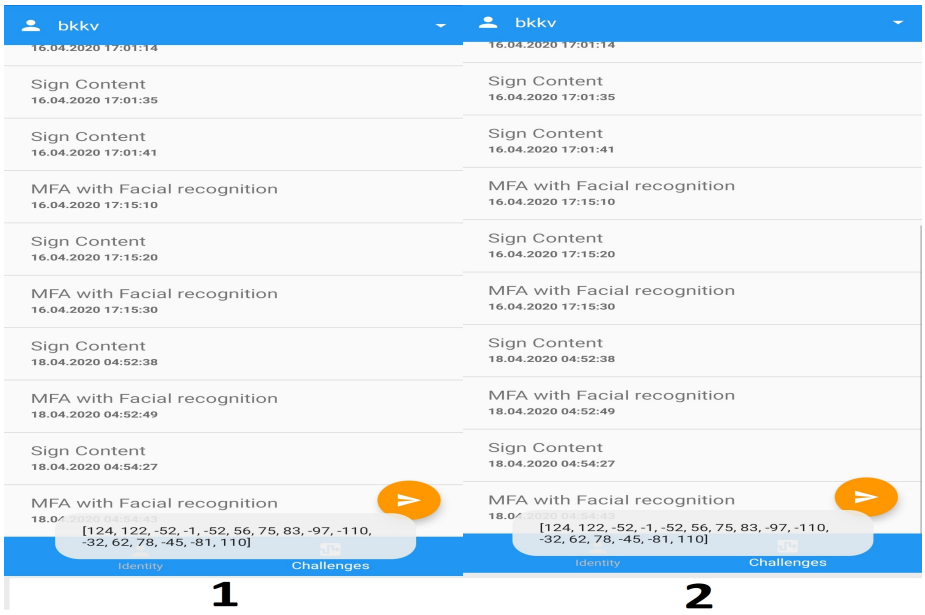


Figure 9: MFA: same VAE IDs for two challeges

As it is displayed, when clicking two different challenges (last two challenges in the list), the displayed VAE was the same. Hence we can be sure they are posted to the blockchain with the same VAE ID, and show in this way that multi-factor authentication took place.

6.5 Related work

Code coverage and unit testing is common practice in software engineering to test the system [62] [55]. So tested software can give us more trustworthy insight then untested one.

Rise of blockchain technology promoted research on PKI solutions that utilize blockchain as an alternative to CA [5][60][12]. These research also touch the privacy of the data on the blockchain and proposed techniques such as smart contract obfuscation, public key address translation, which generates different public keys for different transactions, and tumbling used in Bitcoin. Tumbling transfers coins between different wallets of a network, in a way that obscures the trail to the original source of the fund.

However, MFA (including risk-based authentication) with customizable challenges, has not been researched in the context of blockchain-based authentication protocol such as Authcoin.

6.6 Discussion

In this Section, we discuss conducted a controlled experiment using our implementation. As mentioned previously, our case is just one example of many MFA cases that can be implemented on the Authcoin protocol, so our controlled experiment only was limited to the testing client to bank interaction.
Multi-factor authentication, in conjunction with the trust-based decentralized system, was not implemented so far. Moinet et al. autonomous Wireless Sensor Networks in a simulated environment. Different from Moinet et al., we added MFA for authentication instead of using standard single-factor authentication. Risk-based authentication has never been researched in the context of blockchain-based trust networks also. Hintze et al. only considered risk-based authentication related to the location of the user, but our work gave a more broad view of how risk-based authentication can be a balance between single-factor authentication and MFA in context of the blockchain-based trust network. Witte et al. presented how a support-vector machine model can be used to train a risk-based mobile biometric system to gradually learn about unsafe environments. For our context, using machine learning models for improving risk-based authentication is out of the scope of this thesis.

6.7 Conclusion

Even though our controlled experiment demonstrates MFA on the Authcoin protocol, there are many unfinished implementations such as additional optimizations and security checks. Additionally, a different combination of factors in MFA can change the requirements of authentication. For example, if fingerprints are used for authentication, then verifier party can not do it just by looking at the fingerprint, he/she needs a way to compare it to the old record of the fingerprint.

7 Conclusion and future work

The following chapter summarizes this thesis and answers the research questions depicted in Chapter 1. Section 7.1 presents general conclusion of the thesis. Subsequently, Section 7.2 answers each research questions independently. Afterwards, the limitations of this thesis are presented in Section 7.3, followed by Section future work in Section 7.4

7.1 Conclusion

This thesis proposes MFA as a safer way than single-factor authentication to authenticate people on the Authcoin protocol. MFA is presented as a safer alternative to single-factor authentication. Authentication levels of assurance and their requirements were presented to specify the advantage of using MFA. Furthermore, the user authentication level system using MFA was presented, to define what level of security is achieved with different factors using MFA. Common attacking vectors for each level of security was depicted, that need considering before choosing some authentication method.

The steps for choosing a user authentication method were listed for general use and subsequently was initialized for Authcoin context. Based on Risk assessment procedure, we decided to use level three assurance level from Table 4. Finally, MFA workflow was presented to display how can it be used in a real life scenario.

We analyzed the influence of risk-based authentication on challenges and how it can be connected to MFA based on context information. Also, explained several ways to save context information to later compare another context and identify the possible unsafe situation. We presented attacking vectors on biometric authentication, so we can mitigate the risks. For customizing challenges, different types of users of Authcoin protocol was presented since not all the challenges apply to each one of them.

We presented usability considerations of Biometrics and chose inherence and knowledge factor for use case demonstration. Table 10 showed different characteristics of biometrics authentication types, and facial recognition was chosen as the most effortless challenge type. After implementation, the use case of successful implementation was presented, and lessons learned during implementation were shared.

7.2 Answering the research questions

The main research question for this thesis is: **How to apply MFA with customizable challenges to Authcoin protocol?** As depicted in Chapter 1 it was divided into three sub-questions, and the following sections provide answers to each one of them.

7.2.1 RQ-1: How to Secure the Identity Authentication Process with MFA for the Authcoin Protocol?

Based on presented user authentication level system on Table 3 and required protection against threats on Table 4, we concluded that more factor of authentication preferably with biometrics is safer than any single-factor authentication.

MFA can be used with Authcoin to create, manage, distribute, store, revoke and generally used the digital certificate. Based on Risk assessment 8, we concluded that level 3 on Table 4 is the best option for Authcoin protocol since it allows MFA with biometric and stringent in-person registration is not needed for users.

We also found that in Authcoin MFA, rounds of challenge-response messages happen between two users as many times as possible.

7.2.2 RQ-2: How to Manage Identity Authentication for the Authcoin Protocol?

We showed that for identity authentication challenges may change with the help of risk-based authentication. Our finding is that with the help of Risk-based authentication, Authcoin can authenticate the users automatically without interaction from the user, as long as the biometric factor is not used. If a certain threshold of risk is met, then risk-based authentication can require MFA. Hence, a balance between automated authentication and MFA can be made. We also showed how to compare and save context in the system so we can compare it to another context later.

We found that using defence techniques such as anti-spoofing, encryption of data, identifying questionable behaviour, and traffic analysis can help us mitigate risks of biometric authentication. We showed points where biometric authentication can be compromised in Figure 4.4.

Concerning customization of challenges, we concluded that person to person authentication is mostly used when customization takes place. Challenges can be customized as long as the privacy of a person is not compromised.

7.2.3 RQ-3: How to Implement MFA for the Authcoin Protocol?

We presented different biometrics and its usability properties. We concluded that all the biometric system should consider people with different abilities. Based on Table 10, we found that facial recognition is the most effortless biometric to use, so we decided to implement it with MFA.

We showed that successful authentication could take place between two users and challenge-response is posted on the blockchain with the same VAE id, meaning that more than one challenge-response round took place under the same session.

After implementation, we learned that it is essential to have documentation of an already built system on which we want to implement MFA, and also beforehand to plan necessarily to avoid restructuring the whole system.

7.3 Limitations

Several limitations apply to different parts of this thesis. First, MFA is not a safety guarantee, and it should be used with still great caution, it only lessens the chance of hacking, but does not completely exclude it. Most of the security issues come from the social part of the system - human. Even biometrics can be forged or avoided. Even though it is complicated, the context of Risk-based authentication can be faked if it consists of stealable characteristics.

Responder to challenge also has to consider the information which she/he gives, for example, if intentions of other person are not clear, probably passport or other sensitive information should not be shared.

Concerning automatic VAR, MFA with biometrics cannot be used with automated VAR process since users interaction will be needed. Also, to use Authcoin MFA with IoT devices, necessary implementations should be done on the side of the machine to receive the challenge and response accordingly.

Regarding implementation, our use case is only one example of all the other scenarios where Authcoin can be used. This implementation only proves the concept, but it can change the factors, challenges, users and context of usage.

7.4 Future work

Throughout this thesis, there have been issues that still require further research. We slightly touched private challenge types that preserve the privacy of data, but in real-life scenarios, it is needed, so it needs further investigation. There are concepts such as zero-knowledge proof, which can be used for providing privacy in Authcoin protocol, but it was out of the scope of this thesis. Additionally, there are more and more authentication types introduced in today's world, so in the case of emerging new biometric or another factor, research might be needed to validate it in the Authcoin protocol.

Also, this thesis was mentioning private and public key pairs as the central resource for which authentication was taking place. However, the Authcoin protocol is not limited to a private/public key pair and can authenticate users to access any resource.

Another open issue for future research is the usage of machine learning models for improving risk-based authentication. Since risk-based authentication compares old, existing contexts to user's current context, machine learning models can be used to improve information about previously used contexts.

Furthermore, in the implementation, we only consider a person to person interaction since it is easy to test, but in real life, there can be different use cases which can include users such as organization, ministry, government or machine. Hence, many combinations can happen, and it needs further research.

References

[1] Google engineers claim that less than 10 percent of users use two-factor authentication on gmail.

[2] Abdulmonam Omar Alaswad, Ahlal H Montaser, and Fawzia Elhashmi Mohamad. Vulnerabilities of biometric authentication threats and countermeasures. *International Journal of Information & Computation Technology*, 4(10):947–58, 2014.

[3] Jan Philipp Albrecht. How the gdpr will change the world. *Eur. Data Prot. L. Rev.*, 2:287, 2016.

[4] Kemal Altinkemer and Tawei Wang. Cost and benefit analysis of authentication systems. *Decision Support Systems*, 51(3):394–404, 2011.

[5] LM Axon and Michael Goldsmith. Pb-pki: A privacy-aware blockchain-based pki. 2016.

[6] Richard Baskerville. Feds: a framework for evaluation in design science research. *European Journal of Information Systems*, 2014 Forthcoming: 1–13, 11 2014. doi: 10.1057/ejis.2014.36.

[7] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. Passwords and the evolution of imperfect authentication. *Communications of the ACM*, 58(7):78–87, 2015.

[8] Vitalik Buterin et al. Ethereum: A next-generation smart contract and decentralized application platform. *URL https://github.com/ethereum/wiki/wiki/% 5BEnglish% 5D-White-Paper*, 7, 2014.

[9] D. Chadwick, A. Otenko, and E. Ball. Role-based access control with x.509 attribute certificates. *IEEE Internet Computing*, 7(2):62–69, March 2003. doi: 10.1109/MIC.2003.1189190.

[10] Don Coppersmith. The data encryption standard (des) and its strength against attacks. *IBM journal of research and development*, 38(3):243–250, 1994.

[11] Federal Financial Institutions Examination Council. Authentication in an internet banking environment. *Retrieved June*, 28:2006, 2005.

[12] Ben Cresitello-Dittmar. Application of the blockchain for authentication and verification of identity. *Independent Paper*, 2016.

[13] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al. Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2 (6-10):71, 2016.

[14] Patrick Dai, Neil Mahi, Jordan Earls, and Alex Norta. Smart-contract value-transfer protocols on a distributed mobile application platform. *URL: https://qtum. org/uploads/files/cf6d69348ca50dd985b60425ccf282f3. pdf*, page 10, 2017.

[15] Duncan de Borde. Selecting a two-factor authentication system. *Network Security*, 2007(7):17–20, 2007.

[16] Danny De Cock, Karel Wouters, Dries Schellekens, Dave Singelee, and Bart Preneel. Threat modelling for security tokens in web applications. In *Communications and multimedia security*, pages 183–193. Springer, 2005.

[17] Peter J. Denning. A new social contract for research. *Commun. ACM*, 40 (2):132–134, February 1997. ISSN 0001-0782. doi: 10.1145/253671.253755. URL `https://doi.org/10.1145/253671.253755`.

[18] Peter Eckersley. How unique is your web browser? In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 1–18. Springer, 2010.

[19] Mohamad El-Abed, Romain Giot, Baptiste Hemery, and Christophe Rosenberger. A study of users' acceptance and satisfaction of biometric systems. In *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, pages 170–178. IEEE, 2010.

[20] ISO—The International Organization for Standardization. Iso/ts 20282-2: 2013 (en). usability of consumer products and products for public use—part 2: Summative test method, 2013.

[21] Conner Fromknecht, Dragos Velicanu, and Sophia Yakoubov. Certcoin: A namecoin based decentralized authentication system 6.857 class project. *Unpublished class project*, 2014.

[22] Paul Giura, Ilona Murynets, Roger Piqueras Jover, and Yevgeniy Vahlis. Is it really you? user identification via adaptive behavior fingerprinting. In *Proceedings of the 4th ACM conference on Data and application security and privacy*, pages 333–344, 2014.

[23] Larry Hamid. Biometric technology: not a password replacement, but a complement. *Biometric Technology Today*, 2015(6):7–10, 2015.

[24] Rosa R Heckle, Andrew S Patrick, and Ant Ozok. Perception and acceptance of fingerprint biometric technology. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, pages 153–154, 2007.

[25] Alan Hevner, Alan R, Salvatore March, Salvatore T, Park, Jinsoo Park, Ram, and Sudha. Design science in information systems research. *Management Information Systems Quarterly*, 28:75–, 03 2004.

[26] Daniel Hintze, Eckhard Koch, Sebastian Scholz, and René Mayrhofer. Location-based risk assessment for mobile authentication. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, pages 85–88, 2016.

[27] Lance J Hoffman, Kim Lawson-Jenkins, and Jeremy Blum. Trust beyond security: an expanded trust model. *Communications of the ACM*, 49(7): 95–101, 2006.

[28] Marco Iansiti and Karim R Lakhani. The truth about blockchain. *Harvard Business Review*, 95(1):118–127, 2017.

[29] Anil Jain, Lin Hong, and Sharath Pankanti. Biometric identification. *Communications of the ACM*, 43(2):90–98, 2000.

[30] Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1):4–20, 2004.

[31] Kurt Jensen. An introduction to the theoretical aspects of coloured petri nets. In *Workshop/School/Symposium of the REX Project (Research and Education in Concurrent Systems)*, pages 230–272. Springer, 1993.

[32] Stevo Jokić. Analysis and security of crypto currency wallets. *ZBORNIK RADOVA UNIVERZITETA SINERGIJA*, 19(4).

[33] Jae-Jung Kim and Seng-Phil Hong. A method of risk assessment for multi-factor authentication. *Journal of Information Processing Systems*, 7(1): 187–198, 2011.

[34] Benjamin Leiding. *Securing the Authcoin Protocol Using Security Risk-oriented Patterns*. PhD thesis, 03 2017.

[35] Benjamin Leiding and Andreas Dähn. Dead letters to alice - reachability of e-mail addresses in the pgp web of trust, 2016.

[36] Benjamin Leiding, Clemens H. Cap, Thomas Mundt, and Samaneh Rashidibajgan. Authcoin: Validation and authentication in decentralized networks, 2016.

[37] Carsten Maple and Peter Norrington. The usability and practicality of biometric authentication in the workplace. In *First International Conference on Availability, Reliability and Security (ARES'06)*, pages 7–pp. IEEE, 2006.

[38] Salvatore March and Gerald Smith. Design and natural science research on information technology. *Decision Support Systems*, 15:251–266, 12 1995. doi: 10.1016/0167-9236(94)00041-2.

[39] Václav Matyáš and Zdeněk Říha. Biometric authentication—security and usability. In *Advanced Communications and Multimedia Security*, pages 227–239. Springer, 2002.

[40] A Melnikov. Salted challenge response http authentication mechanism. Technical report, Experimental RFC 7804, 2016.

[41] Markus Miettinen, Thien Duc Nguyen, Ahmad-Reza Sadeghi, and N Asokan. Revisiting context-based authentication in iot. In *Proceedings of the 55th Annual Design Automation Conference*, pages 1–6, 2018.

[42] C. Mitchell. Limitations of challenge-response entity authentication. *Electronics Letters*, 25(17):1195–1196, Aug 1989. doi: 10.1049/el:19890801.

[43] M. M. Mohammed and M. Elsadig. A multi-layer of multi factors authentication model for online banking services. In *2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE)*, pages 220–224, Aug 2013. doi: 10.1109/ICCEEE.2013.6633936.

[44] Axel Moinet, Benoît Darties, and Jean-Luc Baril. Blockchain based trust & authentication for decentralized sensor networks, 2017.

[45] Ghita Kouadri Mostéfaoui and Patrick Brézillon. A generic framework for context-based distributed authorizations. In *International and Interdisciplinary Conference on Modeling and Using Context*, pages 204–217. Springer, 2003.

[46] Muhammad Muaaz and René Mayrhofer. Orientation independent cell phone based gait authentication. In *Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia*, pages 161–164, 2014.

[47] Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin, and Jean-Pierre Seifert. Sms-based one-time passwords: attacks and defense. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 150–159. Springer, 2013.

[48] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. *none*, 2008.

[49] Nick Nikiforakis, Wannes Meert, Yves Younan, Martin Johns, and Wouter Joosen. Sessionshield: Lightweight protection against session hijacking. In *International Symposium on Engineering Secure Software and Systems*, pages 87–100. Springer, 2011.

[50] Ekwonwune Emmanuel Nwabueze, Iwuoha Obioha, Oju Onuoha, et al. Enhancing multi-factor authentication in modern computing. *Communications and Network*, 6(03):172, 2017.

[51] Ken Peffers, Tuure Tuunanen, Marcus Rothenberger, and Samir Chatterjee. A design science research methodology for information systems research. *J. Manage. Inf. Syst.*, 24(3):45–77, December 2007. ISSN 0742-1222. doi: 10.2753/MIS0742-1222240302. URL `http://dx.doi.org/10.2753/MIS0742-1222240302`.

[52] Gareth Peters, Efstathios Panayi, and Ariane Chapelle. Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective. *SSRN Electronic Journal*, 09 2015. doi: 10.2139/ssrn.2646618.

[53] Ariel Rabkin. Personal knowledge questions for fallback authentication: Security questions in the era of facebook. In *Proceedings of the 4th symposium on Usable privacy and security*, pages 13–23, 2008.

[54] Tim Ring. Spoofing: are the hackers beating biometrics? *Biometric Technology Today*, 2015(7):5–9, 2015.

[55] Per Runeson. A survey of unit testing practices. *IEEE software*, 23(4): 22–29, 2006.

[56] Alireza Pirayesh Sabzevar and Angelos Stavrou. Universal multi-factor authentication using graphical passwords. In *2008 IEEE International Conference on Signal Image Technology and Internet Based Systems*, pages 625–632. IEEE, 2008.

[57] Hataichanok Saevanee, Nathan L Clarke, and Steven M Furnell. Multimodal behavioural biometric authentication for mobile devices. In *IFIP International Information Security Conference*, pages 465–474. Springer, 2012.

[58] Louise I Shelley. Organized crime, terrorism and cybercrime. *Security sector reform: Institutions, society and good governance*, pages 303–312, 2003.

[59] Andrew K Shenton. Strategies for ensuring trustworthiness in qualitative research projects. *Education for information*, 22(2):63–75, 2004.

[60] P Sivakumar and Kunwar Singh. Privacy based decentralized public key infrastructure (pki) implementation using smart contract in blockchain. *technical report*.

[61] Jan Spooren, Davy Preuveneers, and Wouter Joosen. Mobile device fingerprinting considered harmful for risk-based authentication. In *Proceedings of the Eighth European Workshop on System Security*, pages 1–6, 2015.

[62] Mustafa M Tikir and Jeffrey K Hollingsworth. Efficient instrumentation for code coverage testing. *ACM SIGSOFT Software Engineering Notes*, 27 (4):86–96, 2002.

[63] Dennis Tsichritzis. *The Dynamics of Innovation*, page 259–265. Copernicus, USA, 1997. ISBN 0387949321.

[64] Aniyan Varghese. Authentication levels - status. URL `https://ec.europa.eu/information_society/activities/ict_psp/documents/authen_level_status.pdf`.

[65] John Venable, Jan Pries-Heje, and Richard Baskerville. Feds: a framework for evaluation in design science research. *European journal of information systems*, 25(1):77–89, 2016.

[66] Luis Von Ahn, Manuel Blum, Nicholas J Hopper, and John Langford. Captcha: Using hard ai problems for security. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 294–311. Springer, 2003.

[67] Heiko Witte, Christian Rathgeb, and Christoph Busch. Context-aware mobile biometric authentication based on support vector machines. In *2013 Fourth International Conference on Emerging Security Technologies*, pages 29–32. IEEE, 2013.

[68] Jeffrey Xiong, John Xiong, and Christophe Claramunt. A spatial entropy-based approach to improve mobile risk-based authentication. In *Proceedings of the 1st ACM SIGSPATIAL international workshop on privacy in geographic information collection and analysis*, pages 1–9, 2014.

[69] Xin Zhou and Xiaofei Tang. Research and implementation of rsa algorithm for encryption and decryption. In *Proceedings of 2011 6th International Forum on Strategic Technology*, volume 2, pages 1118–1121. IEEE, 2011.

A Appendix

Projects necessary to run the implemented software(With MFA):
- Demo Server - Bank
- Android Application - Client
- Truffle Project - Smart Contracts

Projects before MFA was implemented:
- Demo Server - Bank
- Android Application - Client
- Truffle Project - Smart Contracts