SABIGLOBAL

TECHNICAL PAPER

SABIGLOBAL

SAFETY FIRST

SABI-net
Global Distributed Authentication Network
Based on Blockchain Technology

2018

CONTENTS

INTRODUCTION

Any development or application of innovations creates information, which is a key asset today. Both corporate and private information require protection.

We offer a global distributed blockchain authentication network called Sabi-net, which is based on the application of Sabi-auth (authentication module) technology. This solution will allow users registered in the network to receive various services that require authentication. Sabi-net is designed as an open system aimed at high availability, security and privacy.

1. PROJECT DESCRIPTION

Sabi-net is based on the use of Sabi-auth authentication modules built using SABI technology (system of adaptive biometric identification) and a decentralized blockchain network. A Sabi-auth module identifies and authenticaties the user and the blockchain network ensures reliable storage of user data.

To register with Sabi-net, the user should use a Sabi-auth device to connect to Sabi-net network and upload the information necessary for authentication in an encrypted form. The network will send the user's ID to the user.

The user can present his/her ID to a legal or physical person, and the latter one, in turn, can use a Sabi-auth module and the supplied software to authenticate the user.

Authentication can be performed as follows:

- In the presence of the user, when the person visits the service provider requiring authentication.

- Remotely, when authentication is performed via the Internet.

Authentication is carried out by a Sabi-auth module by means of provision of the user ID issued by the network. The presented ID is used to download the necessary information from the blockchain network (Sabi-net), after that the Sabi-auth module performs the authentication procedure. Data is exchanged via an encrypted channel.

No identity documents are required for registration and authentication, the information stored in the network does not disclose the identity of the user and is encrypted. Only authentication through Sabi-auth will confirm that the user is compliant with the presented identifier.

Advantages of using Sabi-net:

- Safe storage of user data required for secure authentication.

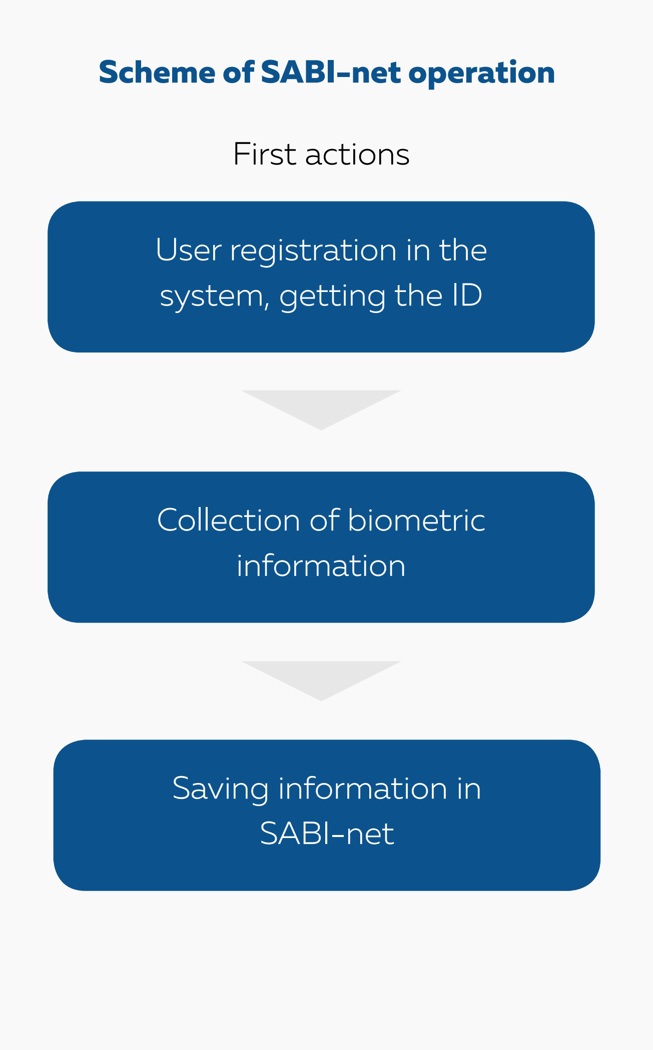
- User authentication by ID can be carried out anywhere in the world, where there is access to the Internet.

- Sabi-net network authenticates the user and does not disclose his/her identity.

- Joint operation of Sabi-auth and the blockchain network eliminates substitution of the user's authentication information and, as a consequence, makes it impossible for the attacker to act as the user with the desired ID.

- Impossibility to authenticate the user without his/her explicit consent.

In the future SABI project can replace all paper documents and identification markers and create a basis for free trade based on smart contracts using SABI authentication.



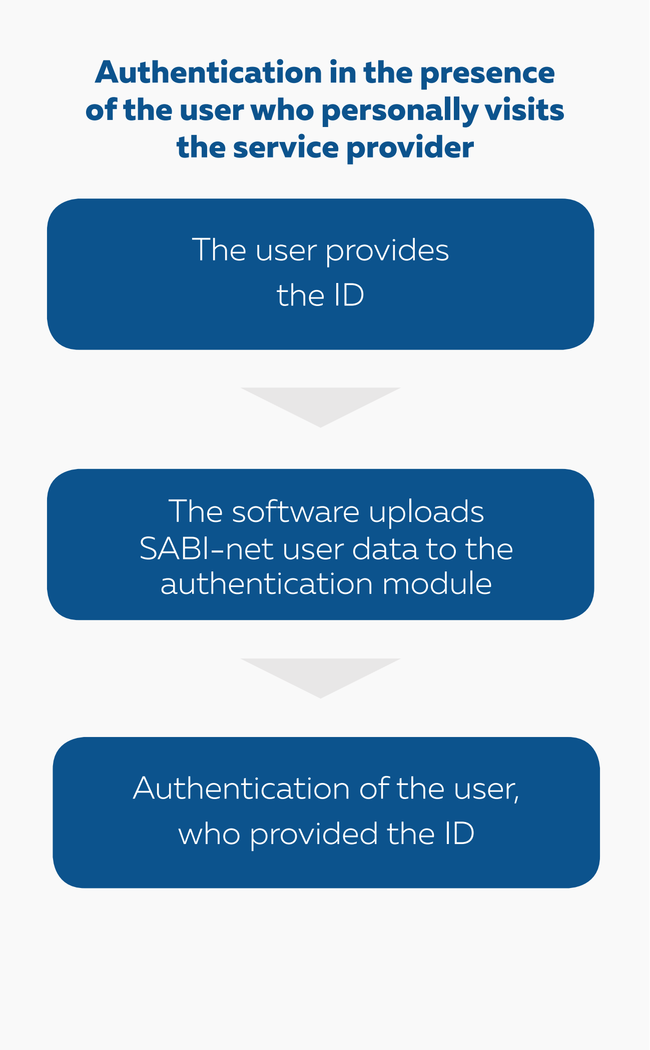
Scheme of SABI-net operation

First actions

User registration in the system, getting the ID

Collection of biometric information

Saving information in SABI-net



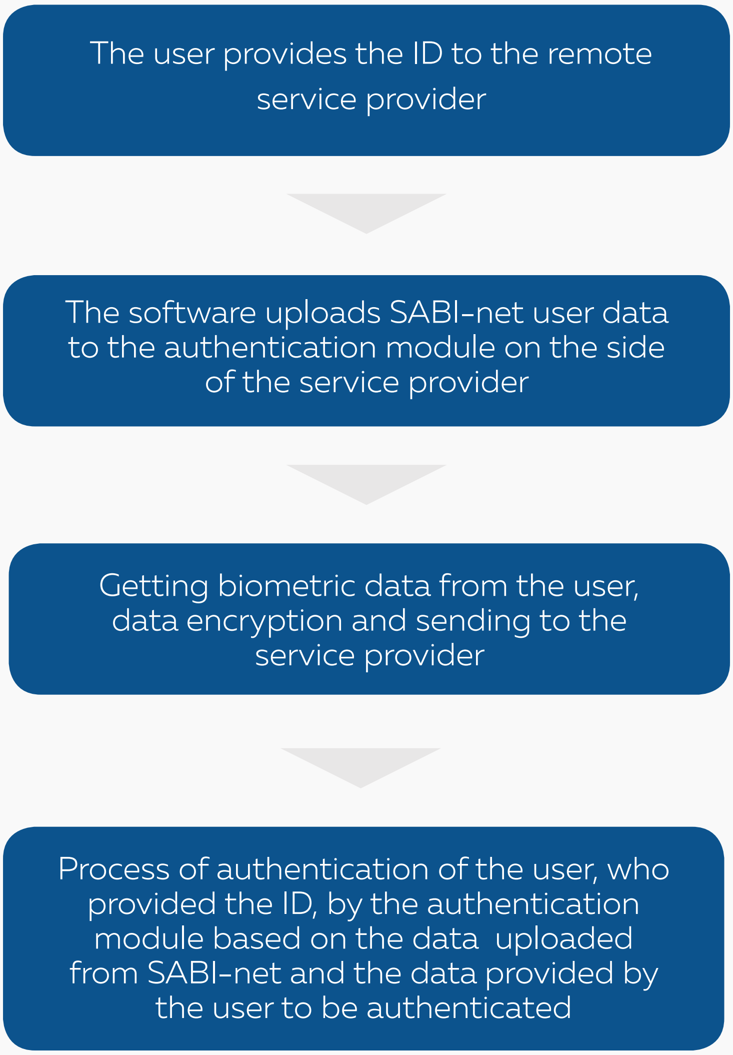
Authentication in the presence of the user who personally visits the service provider

The user provides the ID

The software uploads SABI-net user data to the authentication module

Authentication of the user, who provided the ID

Remote authentication



The user provides the ID to the remote service provider

The software uploads SABI-net user data to the authentication module on the side of the service provider

Getting biometric data from the user, data encryption and sending to the service provider

Process of authentication of the user, who provided the ID, by the authentication module based on the data uploaded from SABI-net and the data provided by the user to be authenticated

2. SABI-AUTH TECHNOLOGY

Sabi-auth technology carries out the process of user identification and authentication. The technology is implemented in the form of a built-in or external module and software for its maintenance. Sabi-auth authentication module identifies and authenticates the user by a unique patented algorithm. The biometric technology is used as the basis for the authentication procedure. It is based on the analysis of the electromagnetic field of the SHF and EHF bands reflected from the user. The combined radiation of frequencies in the SHF and EHF bands can deeply penetrate into the tissues of the human body. Radiation is used as a sounding signal with respect to the proposed authentication system. Part of the sounding signal reflected from the cell structures of the body after treatment by a unique patented algorithm carries within itself information about rhythmic electrophysiological and molecular processes taking place in the bioobject. So, the reflected signal contains features of body structure and functioning and represents its unique electromagnetic profile.

The authentication module is trained to recognize users and store the information that is necessary for authentication. Developers of systems that require user authentication can embed the module in those systems or connect it via external interfaces. Communication with the module at the program level occurs through an encrypted communication channel.

The system software that is working with the module receives the event of user authentication and its identifier, which is saved by the system during module training, and after that the system software solves the problem of user authorization. The authentication module can work in a continuous mode, periodically monitoring the presence of the authenticated user in close distance to the module and reporting the results to the system software. The authentication process requires the module and the user, for whom the module was trained. Authentication technology SABI-auth eliminates any possibility to bypass the authentication procedure by counterfeiting the electromagnetic response, and the encrypted channel for module communication with the system software eliminates any possibility of compromising the module in the chain of the system authorization process.

3. WHY BLOCKCHAIN?

The company faced the task to create an authentication system that would have the following characteristics:

- **Decentralization –** no servers for data storage belonging to anyone, immunity to the intervention of states and corporations.

- **Data storage security –** the user must be sure that attackers will not have access to his/her data, will not alter or use it against his/her will.

- **Secure authentication processes –** authentication processes must be safe for the user, since his/her identity cannot be disclosed.

- **System openness –** transparency of all processes occurring in the system for all participants, system architecture openness for studying, no hidden functions that undermine the participants' confidence in the system and in each other.

- **High availability –** these networks cannot depend on equipment failures, changes in network loads, etc.

- **Safe data transfer –** secure data exchange in the system.

- **Reliable data storage –** retention of all user data and no data loss due to software or hardware failures.

- **User security –** reliable protection of the user's identity and his/her data, users' total control over their data.

- **Security of the service provider –** permissions to access the services must be granted to the right users.

The use of a blockchain network jointly with encryption algorithms and Sabi-auth modules allows solving these problems.

Let us consider the advantages of using blockchain technology in more detail:

- The use of a decentralized blockchain network to store user identification data will help avoid bringing pressure by corporations and the state, as well as prevent potential attempts aimed at nationalization and the use of the technology for lucrative purposes.

- Data recorded in a blockchain cannot be changed, the network guarantees impossibility to alter data. Additional encryption of stored information ensures protection from unauthorized access. Data is encrypted with the user's key, and no system part can use it without the user's knowledge.

- A blockchain network is transparent, accessible and irreversible, so anyone can check their data at any time to get sure that it is unaltered. Users can get sure that their data stored in the network is not used, which is extremely important for any authentication system.

- A blockchain network is distinguished by high availability and fault-tolerance, because data is stored on multiple nodes and there is no single point of failure.

The use of a blockchain network in Sabi-net project ensures openness, decentralization, safe and reliable data storage.

The project team decided to implement the project on NEM blockchain platform.

4. WHY NEM BLOCKCHAIN PLATFORM?

Fast processing of transactions and scalability.

According to the developers, the speed in a private network can reach 4,000 transactions per second and more, which guarantees high availability and extendability. Now Ethereum Blockchain can process up to 15 transactions per second. It is possible to increase this figure up to hundreds of transactions per second in NEM Blockchain, and a possibility to increase the number of transactions up to thousands of transactions per second using NEM Catapult has already been tested. New NEM 2.0 called "Catapult" was released at Consensus 2018.

It ensured faster operation of NEM and added aggregated transactions and multi-level personal accounts. There are also two new features that have never been implemented by other blockchain networks.

Network security and reliability.

Eigentrust++ algorithm implemented in NEM in conjunction with POI (Proof-of-importance) algorithm ensures network stable operation and protects it from unfair and malevolent nodes. Immunity to classical attacks (attack 51%, etc.) and centralization of control, no energy-consuming mining.

Ease of development.

Application developers interact with NEM blockchain via Gateway API. Like most decentralized blockchain networks, NEM network is protected by a global node system that is used by API Gateway platform. All NEM functions are available through REST API, which allows developers to focus on the implementation of the business logic and apply the programming language used by the team instead of the specific "smart contract" language. The process of development of a decentralized application based on NEM blends seamlessly into existing development teams. Unlike Etherium smart contracts, the code ensuring the business logic can interact not only with the blockchain, but also with any other resources, which significantly increases development flexibility.

Designed for real applications.

Currently NEM seems to be a good choice for the development of applications considering current business requirements. Its security features and development tools allow companies to focus on real problems of project development and implementation rather than on technical difficulties associated with blockchain technology peculiarities.

One of the key features of NEM is Smart Asset System. This is the basis for NEM uniqueness, which allows to customize blockchain network operation using simple API calls.

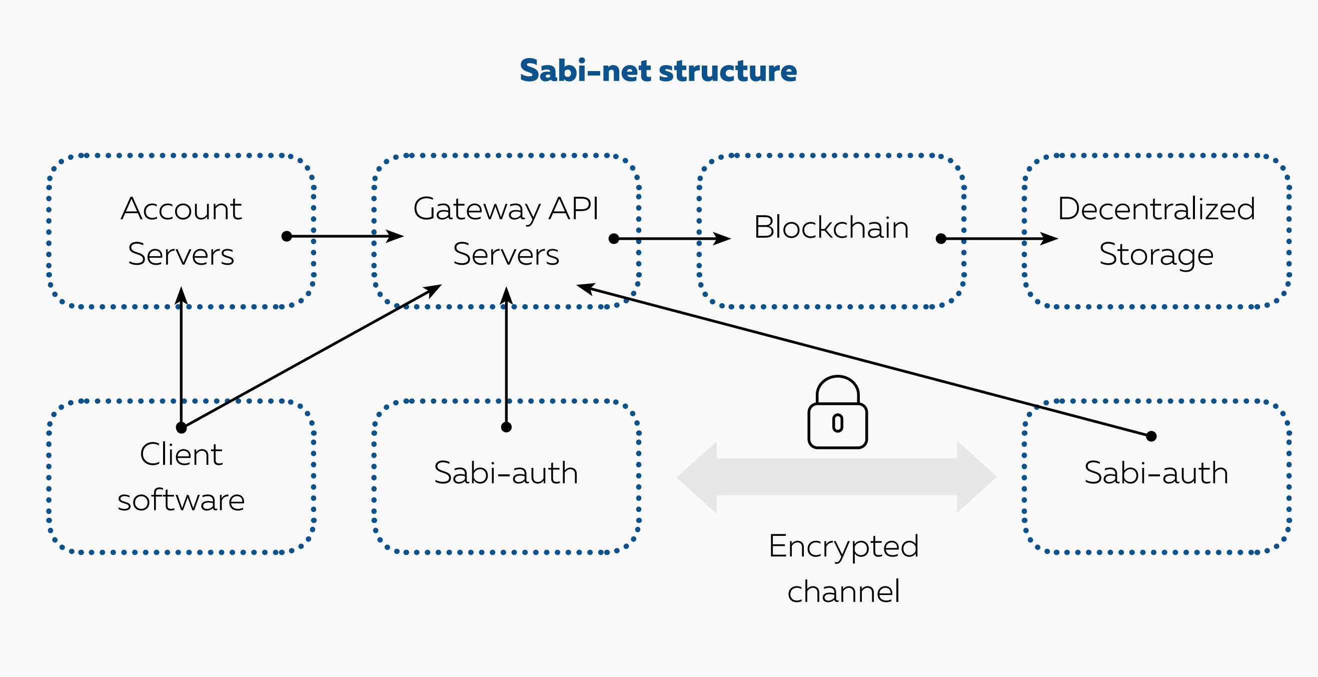
Possibility to deploy a private blockchain in the corporate network

The system allows companies to configure and differentiate their corporate blockchain networks. NEM private network provides additional advantages related to network security, privacy and operating speed. An application based on a private NEM network can be run on internal servers, and the nodes used in the blockchain shall be predetermined by the user. After Catapult launching it will be possible to seamlessly connect the private and public networks, which will significantly expand capabilities of applications based on NEM, and in particular, integration of Sabi-net corporate solutions with Sabi-net global network.

5. SABI-NET PLATFORM ARCHITECTURE

The algorithm and architecture of SABI-net is implemented using own developments and functionality provided as an open source application.

Client software will be implemented for PCs and mobile devices.



Client software is implemented for PCs and mobile devices and ensures registration with Sabi-net, user data management, acceptance and rejection of authentication requests, and Sabi-auth module control.

The user works with his/her data through the server of user accounts (account server), which provides all the necessary functionality through REST API. API Gateway server provides a high-level REST API for the interaction with NEM blockchain network, which is used by the account server, client software, and Sabi-auth authentication modules.

As the load grows, additional server personal accounts and API Gateway are put into operation, between which the load is distributed.

Decentralized data storage ensures storage of encrypted data of the client necessary for his/her authentication using SABI technology. Only metadata and the file hash are stored in the blockchain network. The need to use a decentralized file storage comes in responce to the need to provide the user with a possibility to delete his/her data from the system, as well as improve the reliability of storage.

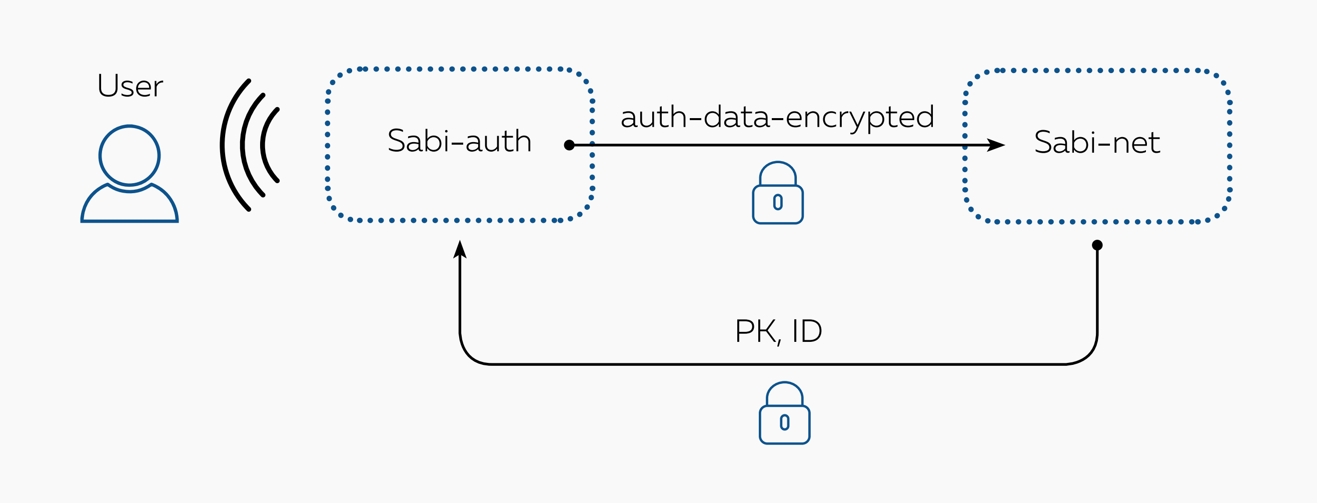
The diagram shows two Sabi-auth modules that establish communication in the process of authentication and interact with the blockchain network.

Sabi-net provides for two authentication options: remote and local.

Sabi-net block presupposes a blockchain and decentralized file storage on the schemes below.

5.1. USER REGISTRATION

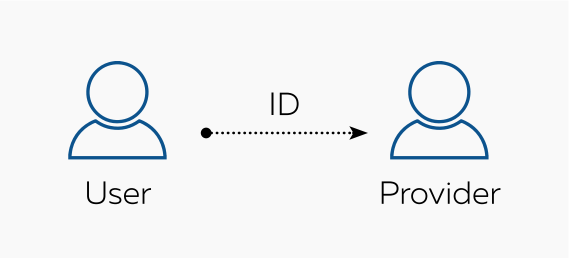
By registering with Sabi-net the user downloads neural network data from Sabi-auth module trained to authenticate the user encrypted with his/her private key (PK).



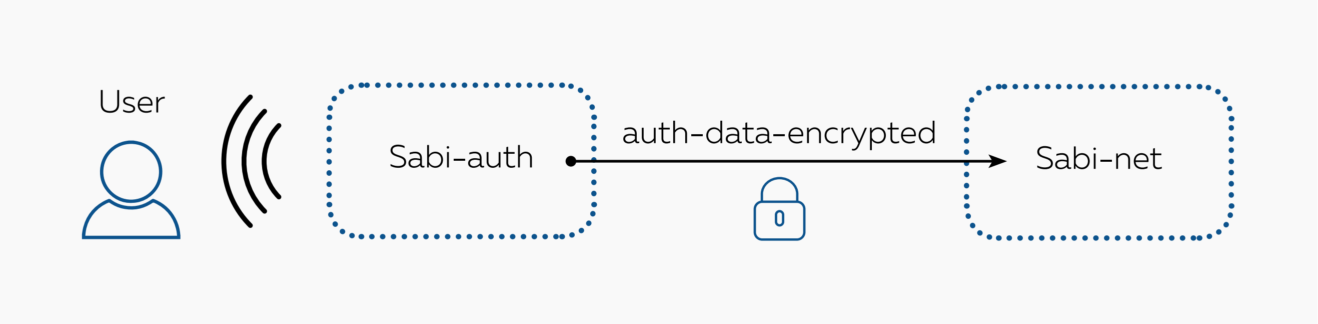
The encrypted image of the neural network (auth-data-encrypted) is placed in the decentralized file storage, the hash sum of unencrypted data and the link to the file in the file storage are stored in the blockchain. The user receives the ID, which can be presented where sabi authentication is required.

5.2. REMOTE AUTHENTICATION

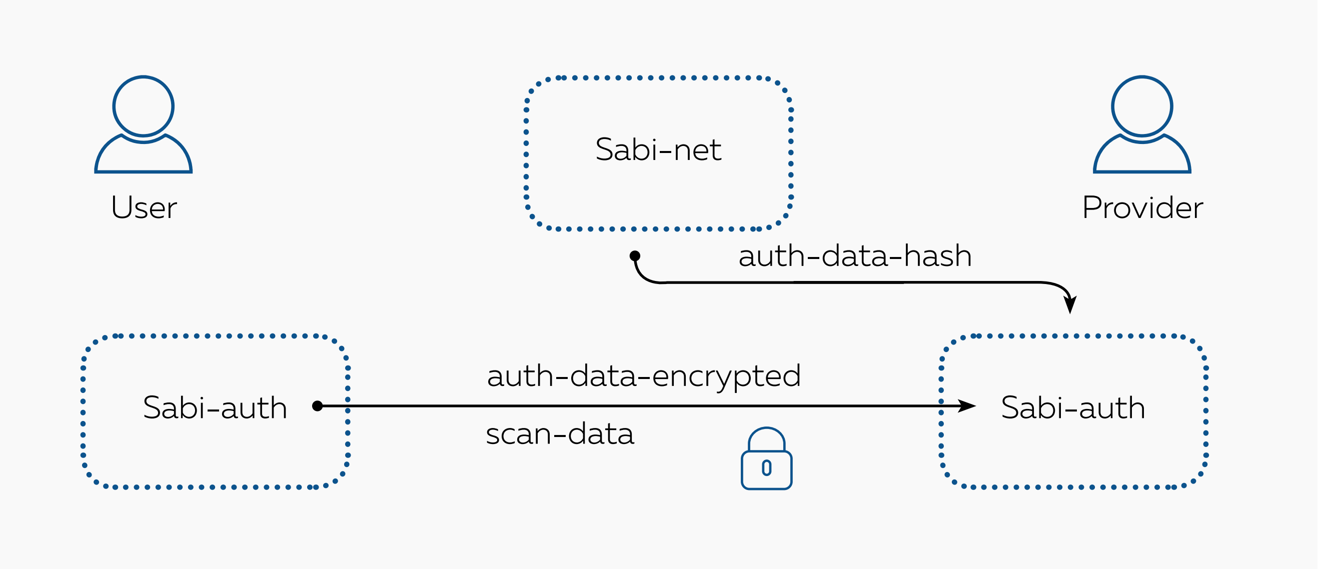
The user contacts the service provider and provides his/her ID to Sabi-net. In response the authentication module of the service provider and the user establish a connection and exchange session encryption keys. After that data is exchanged via an encrypted channel.



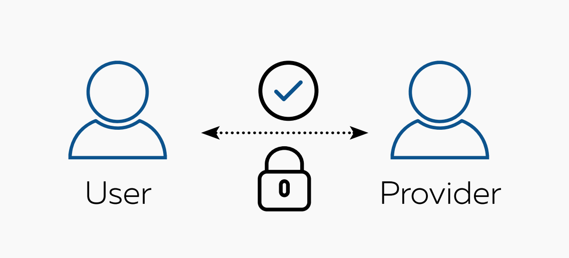
The user's device scans him/her, loads the neural network from Sabi-net and decrypts it with the user's private key.



Then this data (auth-data-decrypted and scan-data) is sent to the service provider's device, which reads the neural network hash (auth-data-hash) from Sabi-net by the user's ID and compares it with the neural network data hash received from the user. In case hash sums mismatch, the authentication process is completed, and the user does not certify his/her ID.

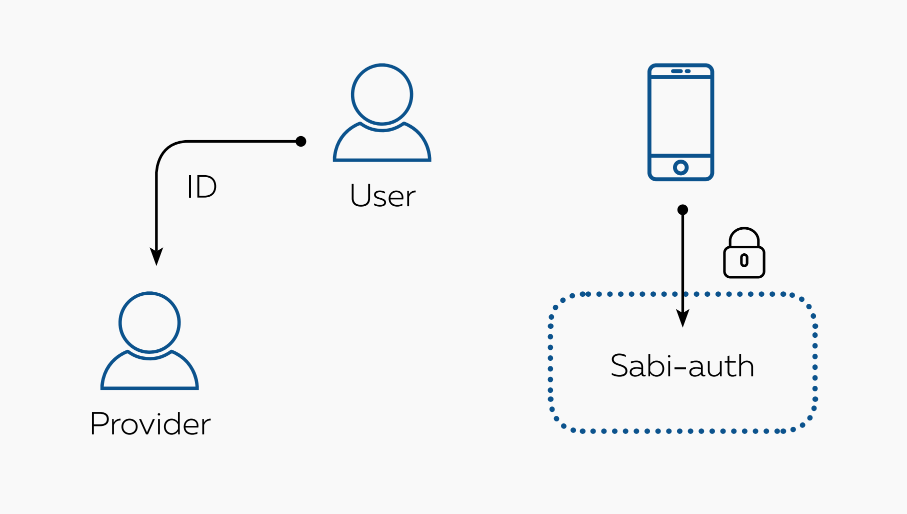


Then the service provider's Sabi-auth module performs user authentication based on the received data, after which the data received from the user is erased from memory, and the communication channel between the modules is closed. If continuous authentication is required, the user's scan data will be sent to the service provider's device at specified intervals (the communication channel between the authentication modules will not be closed). If the user leaves the area covered by his/her authentication device, the device will send a signal to stop working, in response to which the service provider may terminate authorization in the protected system to which the user has access.

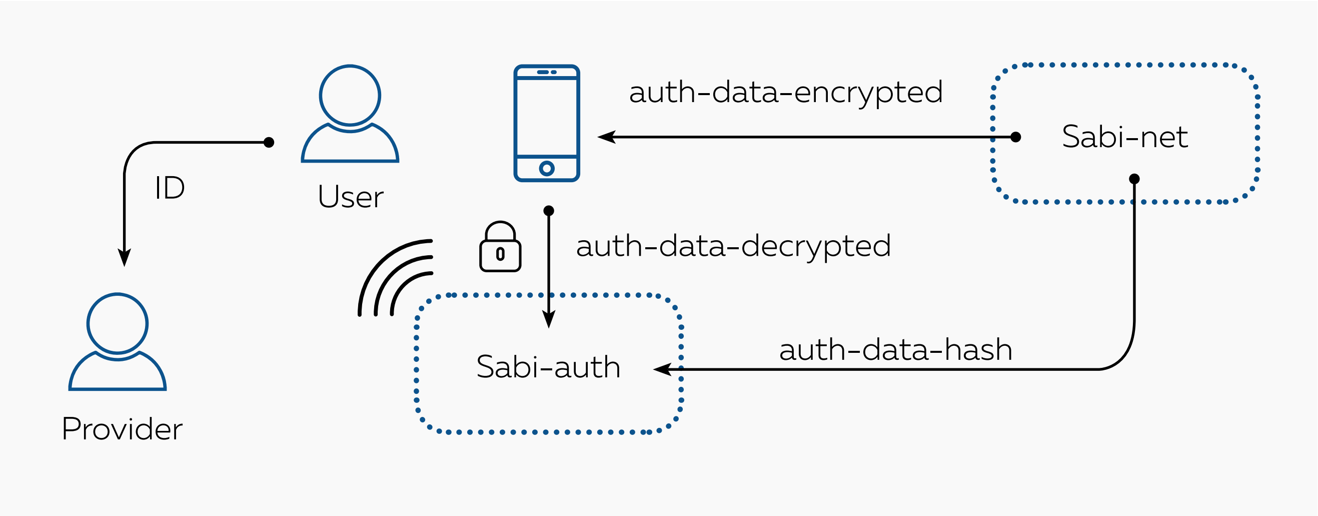


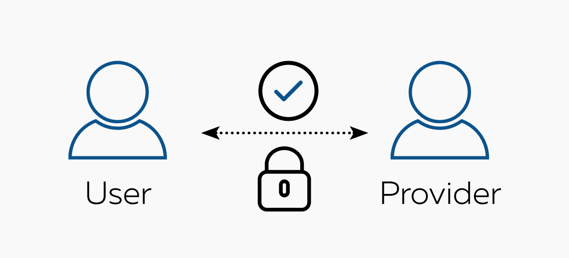
5.3. AUTHENTICATION IN THE PRESENCE OF THE USER

The user personally visits the service provider and provides his/her ID.



Then the service provider's Sabi-auth module establishes a connection with the software on the user's smartphone, where neural network data is received, decrypted and sent to the service provider's device via an encrypted channel. After that the service provider's Sabi-auth device authenticates the user by means of scanning.

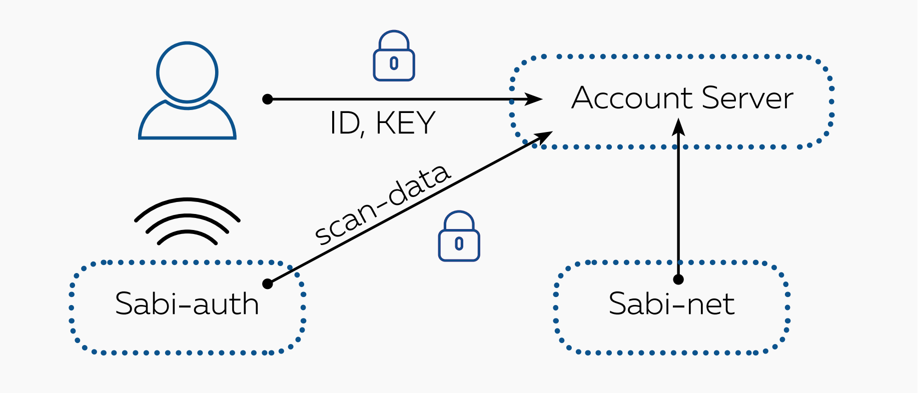


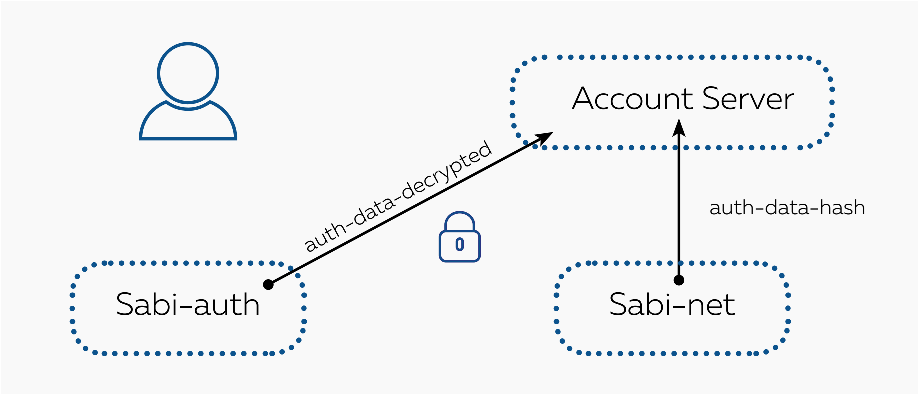


The user can refuse to provide his/her data to the service provider by blocking or ignoring the request in the software.

5.4. DELETION AND UPDATING OF AUTHENTICATION DATA

The user can replace the saved neural network in Sabi-net or delete it. For this purpose he/she shall log in to his/her account through the account server and pass authentication by entering the key.





Then there is the second stage of logging in using sabi-auth technology - the data saved in sabi-net is used. Sabi-auth module downloads and decrypts the user's neural network from sabi-net and sends it to the server.

Sabi-auth authentication in this case is carried out programmatically on the server, where the user's scan data is transmitted via an encrypted channel. If the user enters the correct key, but fails to comply with the imprint stored in sabi-net, he/she will not be allowed to change the data in the personal account. An attacker who could steal the user's secret key will not be able to change data in Sabi-net.

CONCLUSION

The use of SABI technology in combination with NEM blockchain and Sabiglobal software and hardware solutions allows to create a convenient and secure online platform that provides a unique biometric authentication service anywhere in the world.

SABIGLOBAL

Contact us

sabiglobal.io

support@sabiglobal.io | partners@sabiglobal.io | contact@sabiglobal.io

https://www.linkedin.com/company/sabiglobal/
https://t.me/joinchat/AAAAAEiN8fcDuKkGVzk0uQ