UDC 004.057
https://doi.org/10.47533/2024.1606-146X.03

ZH. M. ALIMZHANOVA, N. J. TOIBEK*, A. K. ALI, N.M. NIYAZBEK, D. R. ASHIMZHANOVA, M. A. DUISENOVA

Al-Farabi Kazakh National University, Almaty, Kazakhstan

ANALYSIS OF MULTI-FACTOR AUTHENTICATION SOLUTIONS

This article analyzes open-source multi-factor authentication (MFA) solutions. Research on adapting the MFA solution is given, this research will help businesses to provide security in the implementation of remote work. This article discusses 5 open-source MFA solutions, functionality, advantages and disadvantages. For Small and Medium-sized Businesses (SMBs), using a multi-factor authentication (MFA) solution is an important element of security. MFA is an authentication method that requires several forms of authentication before a user can access a system or application. For SMBs, using MFA helps protect their business from cyberattacks, including phishing, network traffic interception and password cracking. In addition, the use of MFA helps to comply with regulations such as GDPR and HIPAA, which require companies to ensure data security.

In general, the use of MFA helps to protect important information and reduce the risks of security breaches, which can lead to financial losses, reputational problems and loss of customer confidence.

Key words: *MFA, 2FA, LDAP, AAA, RADIUS, authentication system authorization and event accounting, multi-factor authentication, open source solution.*

Introduction. This article focuses on the top 5 open-source MFA solutions. Technology is changing rapidly, so we will need to adapt open-source MFA solutions. Multi-factor authentication (MFA) is a method and technology that will be used to verify the identity of the user. At least two or more types of credential categories are required for users to be able to log in or perform a transaction. A successful combination of at least two independent accounting data is a requirement of the MFA method. It usually combines one of the following three categories of credentials:

What the user knows: the password or the passphrase?

What a person has: a security badge, a key fob or a SIM card?

What the user is: biometric data such as fingerprints, retina or iris, voice or facial recognition?

MFA requires a user to provide two or more verification factors in order to access a resource, such as an application or an online account. MFA requires one or more additional verification criteria in addition to username and password, which reduces the likelihood of a successful cyberattack. Publicly available code is considered "open source". In addition, open-source tools and solutions are more secure because the code can be checked and verified by anyone.

Experimental. Gluu Casa. Gluu Casa is an open-source, self-service multifactor authentication to enhance your digital identity. It's revolutionary. Casa provides a single control point for end users to view, log and delete MFA credentials. It also comes with hardware tokens, software tokens, commercial services (such as Duo), social media login, biometrics and mobile devices. It is also expandable. When any new authentication technologies be-

[*] E-mail корреспондирующего автора: nurtas.toibek@gmail.com

come available, you can download plugins to use in your organization with Casa [1].

Gluu Casa provides advanced multifactor authentication, such as adaptive authentication, location-based authentication, and trusted browser.

Benefits of Gluu Casa:

1. Deploying cloud technology

2. Casa is the right choice for you if you like Kubernetes or services like Amazon EKS, Google GKS or SUSE Rancher. Casa supports cloud deployments using standard tools such as Helm. It also supports several server databases, including LDAP, Couchbase, RDBMS, Amazon Aurora and Google Spanner.

3. Apply strong authentication

4. Only the right person on the right device can have access to the apps. By locking your front door, you can increase the security of your business. Casa offers the OpenID Connect API as an interface, as well as the standard JWT «id_token». It can also be used to enforce policy.

5. No more password resets

6. Even without contacting customer support or compromising account security, users can seamlessly register, manage, and delete passwordless credentials on all their devices. The organization's MFA is as reliable as the weakest working account recovery process!

Ory. Ory is the largest open-source MFA solution community in the world of cloud software application security. It will manage and authenticate users, set, and check permissions, protect your APIs, applications, data, and more. It has an ecosystem of services with clear boundaries that address authentication and authorization issues.

Advantages of Ory:

1. Solid protection

2. Ory offers strong protection against hacking attempts, such as keyloggers and brute force attacks. If an attacker manages to compromise credentials, this information will not be enough to gain access to the account.

3. Convenient user management

4. It provides seamless user management by providing identifiers, storing user information, customizing authentication methods, and using a headless API.

5. Fully flexible

6. It is flexible enough in terms of authentication, authorization, access control and delegation to meet the changing needs of your business [2].

ForgeRock. ForgeRock is an open-source identity solution provider that offers MFA capabilities. It is a digital identity platform designed for any cloud environment that gives users the freedom to perform identification and access activities themselves. This solution improves user interaction and productivity while delivering results without compromising cybersecurity threats. This solution can reduce organizational costs by providing the right level of access to all systems and users at the right time, allowing users to control their profile, password and privacy settings.

Benefits of ForgeRock:

1. Implementation of a wide range of authentication measures

2. Various authentication measures, such as secure multi-factor authentication (MFA) or two-factor authentication (2FA) methods, are implemented by ForgeRock Access Management.

Solutions range from simple, password-free options to social media login, to the most secure biometrics and NIST 800-63 assurance level requirements.

3. One platform, any cloud

4. ForgeRock offers a variety of flexible options, such as on-premises, cloud or hybrid deployments. It also provides a variety of DevOps tools so that developers don't have to spend the effort of creating their own tools to move configurations between environments [3].

5. API Security to protect against malicious activity.

6. Cybercriminals are also targeting unsecured APIs. Its Identity Gateway is used to monitor API traffic, limit traffic volume, and detect anomalies to keep services running and protect against hacks and distributed denial of service (DDoS) attacks.

PrivacyIDEA. PrivacyIDEA is an open-source solution that provides a wide range of different authentication technologies, including MFA. It comes with a powerful and flexible policy structure that allows you to tailor PrivacyIDEA to your needs. Unique event handler modules allow you to build PrivacyIDEA into existing workflows or create new workflows that best fit your scenario. It also works well with others and integrates with identity and authentication solutions such as FreeRADIUS, simpleSAML, Keycloak or Shibboleth. This flexibility may be the reason why organizations such as the World Wide Web Consortium and companies such as Axiad use PrivacyIDEA [4].

Benefits of PrivacyIDEA:

1. Cloud Protection

2. PrivacyIDEA offers various flexible options, such as on-premises, cloud, or hybrid deployment. It protects your organization's data by preventing the wrong users from accessing it. Only the right person can provide access to the right device.

3. Accelerate the payback time

4. PrivacyIDEA supports several geographic regions around the world. Increase speed and simplify your organization's response to global service needs with automated deployment. This will reduce the complexities associated with geographic compliance. To achieve performance and operational goals for development, testing, or production, you can customize, and scale deployments as needed. It even has regional configuration options to help you comply with geographic or regulatory restrictions.

5. Ease of use and operation [5]

6. PrivacyIDEA realizes that the initial purchase costs are only part of the total cost of implementing the solution. So, they designed the deployment architecture for scalability and ease of maintenance. Upgrades shouldn't stop you in your tracks and require operating budgets far more than your initial investment. No questions should arise, technical specialists are always available and guarantee a timely response.

Authentik. Authentik is an open-source identity solution provider that offers MFA capabilities. Particular attention is paid to flexibility and versatility. Even in an existing environment, you can use authentik to add support for new protocols, implement logging/ recovery, etc. in your application to avoid problems with it and more.

It has some useful features, such as a proxy you can use in a cluster to add authentication to services, or things like monitoring panels without a password (Longhorn, etc.) [6].

Benefits of Authentik:

1. Suitable for changing business needs

2. Authentik is highly flexible, which means you can easily adapt to the changing needs of your business. It can be configured for all users, including employees, customers, and partners. This eliminates the need for multiple passwords, simplifies the login process and improves user interaction.

3. Enhances security – Authentic's open-source multifactor authentication is the most effective security tool for protecting local and public cloud data.

4. Easy to use – Authentic has simplified the authentication process by providing easy access control [7].

Result and discussion. After a brief review, let's delve into the architecture of one of them, more specifically about PrivacyIDEA.

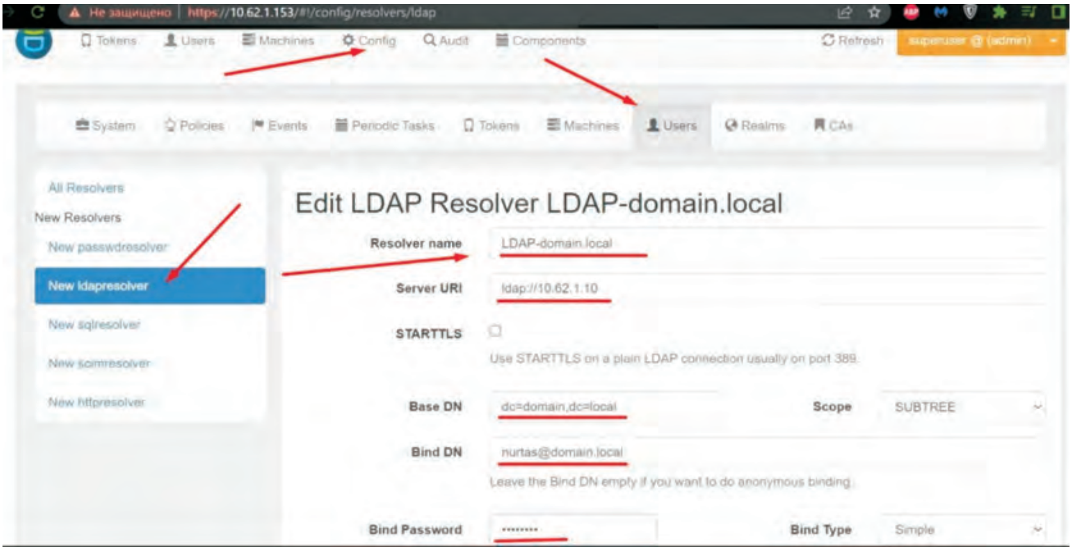
PrivacyIDEA is a system used to manage devices for two-factor authentication. Using PrivacyIDEA, you can enhance your existing applications, such as local login, VPN, remote access, SSH connections, access to websites or web portals, with a second factor during authentication. This increases the security of your existing applications. Originally OTP tokens, but other means of authentication such as SSH keys have been added. Other concepts emerge, such as machine processing or certificate registration. PrivacyIDEA is a web application written in Python based on the flask micro framework. You can use any wsgi web server to run PrivacyIDEA. For example, it could be Apache, Nginx or even werkzeug. The device or item used for authentication is still called a "token. All information about tokens is stored in an SQL database, and you can choose which database you want to use. PrivacyIDEA uses SQLAlchemy to map the database to internal objects. So, you can choose to run PrivacyIDEA with SQLite, MySQL, PostgreSQL, Oracle, DB2 or another database [8].

PrivacyIDEA provides a clean REST API. Administrators can use the web interface or the command line client to manage the authentication devices. Users can log into the web interface to manage their own tokens. Authentication is done through API or certain plugins for FreeRADIUS, SimpleSAMLphp, Wordpress, Contao, Dokuwiki ... either provide default protocols such as RADIUS or SAML or integrate directly into applications. Because of this flexibility, there are also many ways to install and configure PrivacyIDEA.

As already mentioned PrivacyIDEA can be integrated with a Directory Domain, using the LDAP protocol, so it can add users directly from AD(Active Directory). Figure 1 shows an example of adding an LDAP Resolver. LDAP is used here, but you can also use a secure version of LDAPS. Then you have to import the certificates. Here you need a user account with read privilege for domain users. At the bottom you can select an entire domain or filter them by group.

Figure 1 shows all the available authentication methods, and here we usually use TOTP and HOTP methods in production. The most used method is TOTP, which calculates OTP (One Time Password) based on time. And it changes by default every 60 seconds. This method is now considered relatively safe.

PrivacyIDEA has a module FreeRADIUS, and with it he can integrate different network devices and NAD (Network Access Device). Figure 2 shows adding the RADIUS client to FreeRADIUS. Only after adding PrivacyIDEA will work with it, it's like adding to trusted devices.



Edit LDAP Resolver LDAP-domain.local

Resolver name: LDAP-domain.local

Server URI: ldap://10.62.1.10

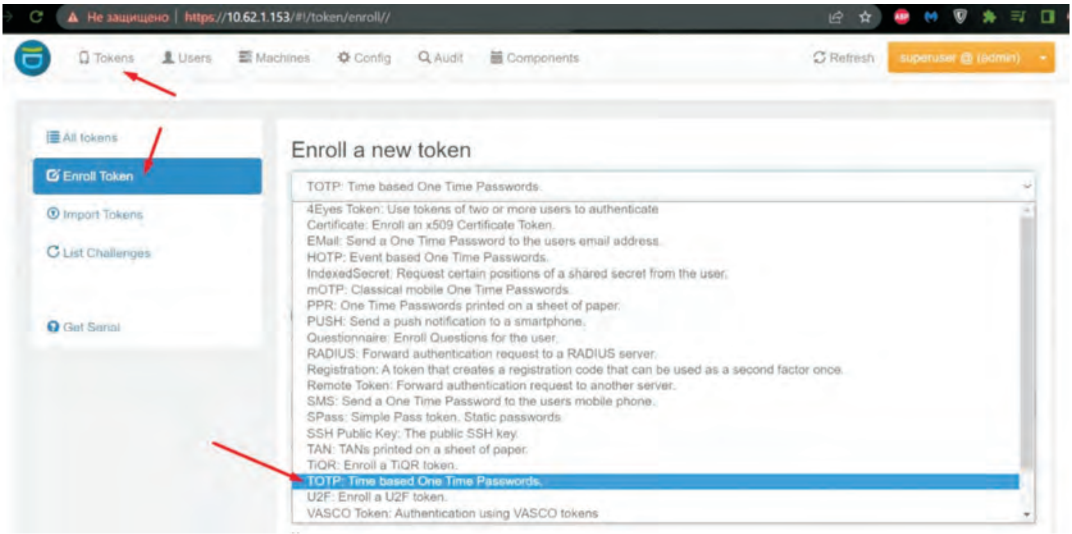
STARTTLS □
Use STARTTLS on a plain LDAP connection usually on port 389.

Base DN: dc=domain,dc=local   Scope: SUBTREE

Bind DN: nurtas@domain.local
Leave the Bind DN empty if you want to do anonymous binding.

Bind Password: ••••••••   Bind Type: Simple

Figure 1 – Adding remote users



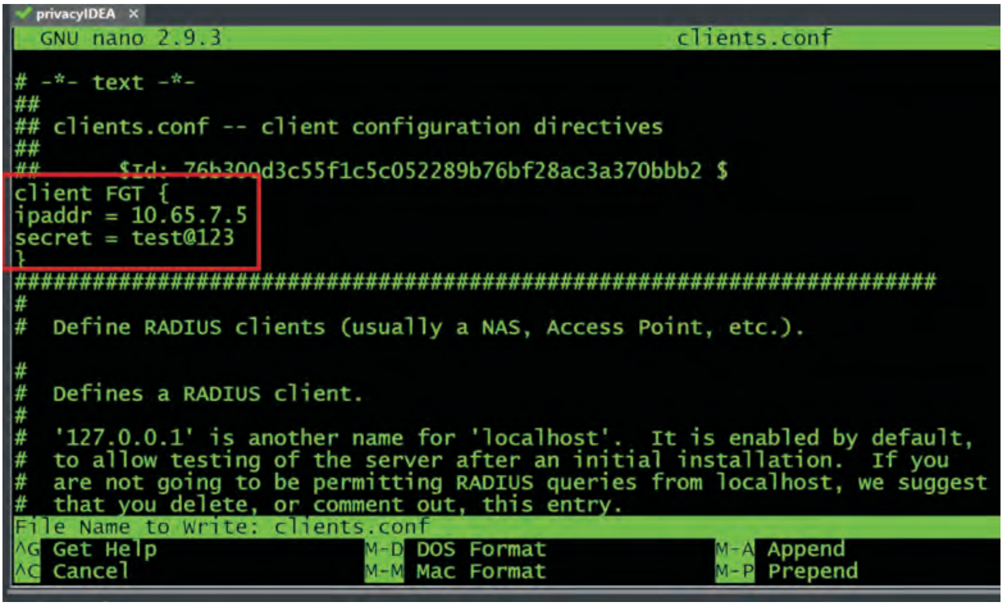
Enroll a new token

TOTP: Time based One Time Passwords

4Eyes Token: Use tokens of two or more users to authenticate
Certificate: Enroll an x509 Certificate Token.
EMail: Send a One Time Password to the users email address.
HOTP: Event based One Time Passwords.
IndexedSecret: Request certain positions of a shared secret from the user.
mOTP: Classical mobile One Time Passwords.
PPR: One Time Passwords printed on a sheet of paper.
PUSH: Send a push notification to a smartphone.
Questionnaire: Enroll Questions for the user.
RADIUS: Forward authentication request to a RADIUS server.
Registration: A token that creates a registration code that can be used as a second factor once.
Remote Token: Forward authentication request to another server.
SMS: Send a One Time Password to the users mobile phone.
SPass: Simple Pass token. Static passwords.
SSH Public Key: The public SSH key.
TAN: TANs printed on a sheet of paper.
TiQR: Enroll a TiQR token.
TOTP: Time based One Time Passwords.
U2F: Enroll a U2F token.
VASCO Token: Authentication using VASCO tokens

Figure 2 – Available methods in PrivacyIDEA

As an example of a RADIUS client, we took the next generation firewall (NGFW) FortiGate, and Figure 3 shows adding the RADIUS server FreeRADIUS to the FortiGate. FortiGate can further use this RADIUS server in the Remote Access VPN settings or in policies, etc.



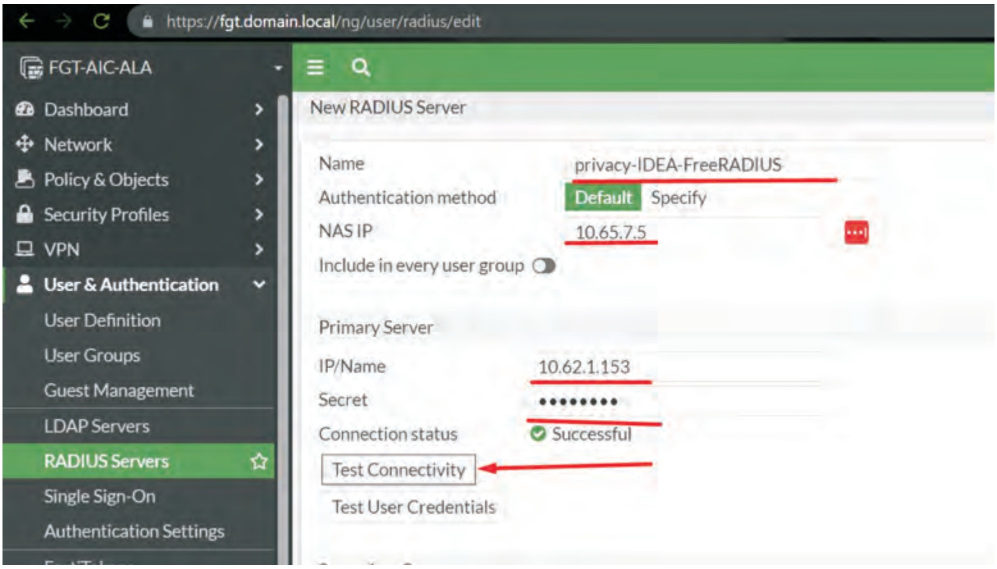
```
  GNU nano 2.9.3                                 clients.conf

# -*- text -*-
##
## clients.conf -- client configuration directives
##
##              $Id: 76b300d3c55f1c5c052289b76bf28ac3a370bbb2 $
client FGT {
ipaddr = 10.65.7.5
secret = test@123
}
#######################################################################
#
#  Define RADIUS clients (usually a NAS, Access Point, etc.).

#
#  Defines a RADIUS client.
#
#  '127.0.0.1' is another name for 'localhost'.  It is enabled by default,
#  to allow testing of the server after an initial installation.  If you
#  are not going to be permitting RADIUS queries from localhost, we suggest
#  that you delete, or comment out, this entry.
File Name to Write: clients.conf
^G Get Help                 M-D DOS Format              M-A Append
^C Cancel                   M-M Mac Format              M-P Prepend
```

Figure 3 – Adding a RADIUS client

After adding a RADIUS server, you can use various built-in utilities to test the connection between the RADIUS server and the client. In Figure 4 you can see that the connection status is set, but in the bottom field shows incorrect credentials. It shows this way because after the first authentication login and password, our RADIUS server asks for a second factor for this user, because multifactor authentication is already configured for this user.



New RADIUS Server

Name privacy-IDEA-FreeRADIUS

Authentication method Default Specify

NAS IP 10.65.7.5

Include in every user group

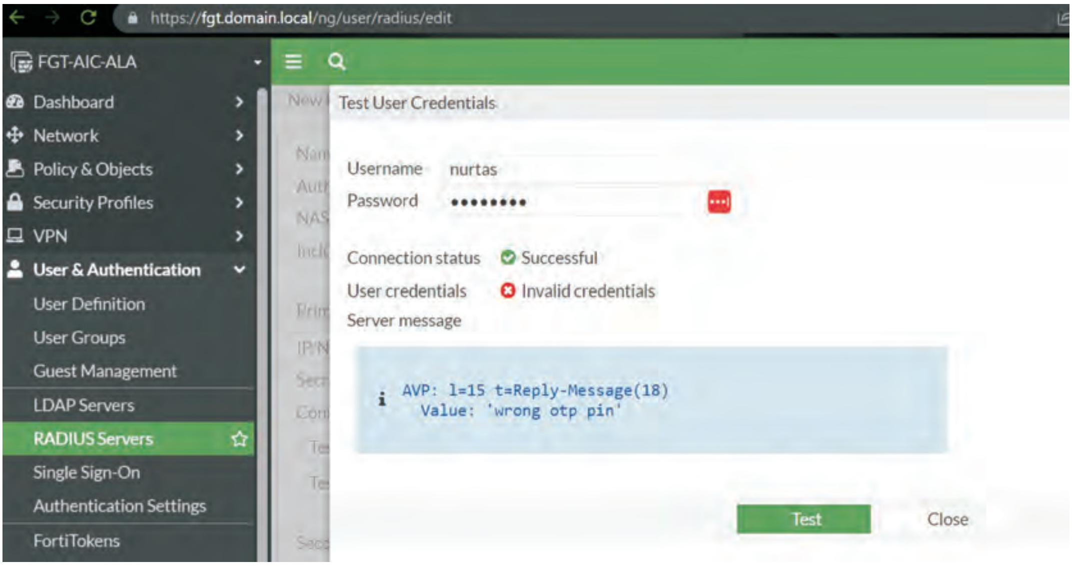
Primary Server

IP/Name 10.62.1.153

Secret ••••••••

Connection status ✓ Successful

Figure 4 – Adding a RADIUS server



Test User Credentials

Username nurtas
Password ••••••••

Connection status ✓ Successful
User credentials ✗ Invalid credentials
Server message

```
AVP: l=15 t=Reply-Message(18)
  Value: 'wrong otp pin'
```

Figure 5 – Checking communication with the AAA server

Therefore, the answer is incorrect OTP is normal, because, it is a graphical utility only allows you to send the first factor login and password (Figure 5).

Conclusions. This article analyzed several open-source multifactor authentication solutions to evaluate their advantages and disadvantages. It was found that each of the considered methods has its strengths and weaknesses, as well as certain limitations that may reduce its effectiveness in certain conditions. The use of multifactor authentication generally improves system security and recommend choosing the most appropriate and effective methods based on specific requirements and needs. Thus, the article provides valuable information for developers and information security professionals who are interested in using open multi-factor authentication solutions to improve the security of their applications and systems. All the open-source MFA solutions mentioned above are the most popular MFA solutions available on the market and are widely used.

REFERENCES

1 Ussatova O. Nyssanbayeva S. Generators of one-time two-factor authentication passwords // Informatyka, Automatyka, Pomiary w Gospodarcei Ochronie Środowiska. – Poland, 2019. – № 2. – Pp. 60-64.

2 Srivastava A. Open-Source Identity Management Patterns and Practices Using OpenAM 10.x. – 2013. – Pp. 101-106.

3 VPN vulerabilty and Risk Report, 2021. – Holger Schulze

4 Howlett T., Stiennon R. Open-Source Security Tools: Practical Guide to Security Applications. – Holger Schulze, 2004. – Pp. 87-95.

5 Morris S. FreeOTP Authentication Server, 2018. - Pp. 60-64.

6 Mind H. Mitigating social engineering in second factor authentication / H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, N. Memon // Computers & Security, 2017. – Vol. 65. – Pp. 14-28. doi: 10.1016/j.cose.2016.09.009

7 Harini, N. 2CAuth: A New Two Factor Authentication Scheme Using QR-Code / N. Harini, T. R. Padmanabhan // International Journal of Engineering and Technology, 2013. – Vol. 5, Issue 2. – Pp. 1087-1094.

8 D'Mello, D.P. An Alternative Approach in Generation and Possession of Backup Codes in MultiFactor Authentication Scheme [Text] / D. P. D'Mello // BIJIT - BVICAM's International Journal of Information Technology, 2015. – Vol. 7, Issue 2. – Pp. 883–885.

Ж. М. АЛИМЖАНОВА, Н. Ж. ТОЙБЕК, А. К. АЛИ, Н. М. НИЯЗБЕК, Д. Р. АШИМЖАНОВА, М. А. ДУЙСЕНОВА

әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
e-mail: nurtas.toibek@gmail.com

КӨП ФАКТОРЛЫ АУЕНТИФИКАЦИЯ ШЕШІМДЕРІН ТАЛДАУ

Мақала ашық бастапқы коды бар Multi-factor authentication (MFA) шешімдерін талдауға арналған. MFA шешімін бейімдеу бойынша зерттеулер келтірілген, бұл зерттеулер кәсіпорындарға қашықтан жұмыс істеу кезінде қауіпсіздікті қамтамасыз етуге көмектеседі. Бұл мақалада 5 ашық бастапқы MFA шешімдері, функционалдығы, артықшылықтары мен кемшіліктері қарастырылады. Шағын және орта бизнес үшін Small and medium-sized Businesses (SMB) көп факторлы аутентификация шешімін (MFA) пайдалану қауіпсіздіктің маңызды элементі болып табылады. MFA – пайдаланушы жүйеге немесе қолданбаға кірмес бұрын аутентификацияның бірнеше түрін қажет ететін аутентификация әдісі. SMB үшін MFA пайдалану олардың бизнесін фишинг, желілік трафикті ұстау және құпия сөздерді бұзу сияқты кибершабуылдардан қорғауға көмектеседі. Сонымен қатар, MFA-ны пайдалану GDPR және HIPAA реттеулерінің сәйкес келуіне көмектеседі, бұл өз кезегінде компаниялардан деректердің қауіпсіздігін қамтамасыз етуді талап етеді.

Жалпы, MFA қолдану маңызды ақпаратты қорғауға және қауіпсіздікті бұзу қаупін азайтуға көмектеседі. Бұл қаржылық шығындарға, беделді мәселелерге және клиенттердің сенімін жоғалтуға әкелуі мүмкін.

Түйін сөздер: *MFA, 2FA, LDAP, AAA, RADIUS, оқиғаларды аутентификациялау және есепке алу жүйесі, көп факторлы аутентификация, ашық бастапқы шешім.*

Ж. М. АЛИМЖАНОВА, Н. Ж. ТОЙБЕК, А. К. АЛИ, Н. М. НИЯЗБЕК, Д. Р. АШИМЖАНОВА, М. А. ДУЙСЕНОВА

Казахский национальный университет им. аль-Фараби, Алматы, Казахстан
e-mail: nurtas.toibek@gmail.com

АНАЛИЗ РЕШЕНИЙ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Статья посвящена анализу решениям Multi-factor authentication (MFA) с открытым исходным кодом. Приведены исследования по адаптированию решений MFA, данные исследования помогут предприятиям обеспечивать безопасность при реализации удаленной работы. В статье рассматриваются 5 решений MFA с открытым исходным кодом, функциональность, преимущества и недостатки. Для малых и средних бизнесов Small and Medium-sized Businesses (SMB) использование *решения многофакторной аутентификации (MFA) является важным элементом безопасности. MFA — это метод аутентификации, который требует нескольких форм проверки подлинности, прежде чем пользователь сможет получить доступ к системе или приложению. Для SMB использование MFA помогает защитить их бизнес от кибератак, включая фишинг, перехват сетевого трафика и взлом паролей. Кроме того, использование MFA помогает соответствовать регулированиям, таким как GDPR и HIPAA, которые требуют от компаний обеспечения безопасности данных.*

В целом, использование MFA помогает защитить важную информацию и снизить риски нарушения безопасности, что может привести к финансовым потерям, репутационным проблемам и потере доверия клиентов.

Ключевые слова: *MFA, 2FA, LDAP, AAA, RADIUS, система аутентификации авторизации и учета событий, многофакторная аутентификация, решение с открытым исходным кодом.*