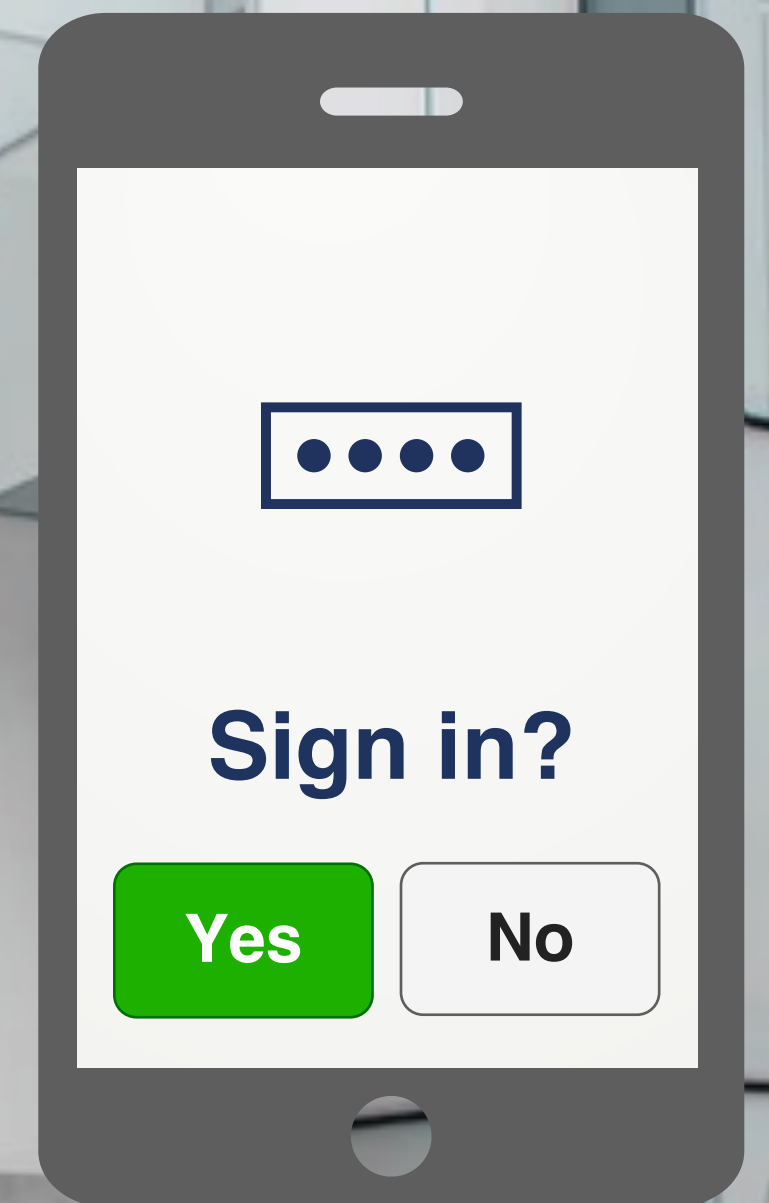
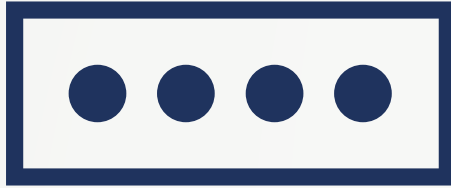


MULTIFACTOR

Simple. Reliable. Safe.

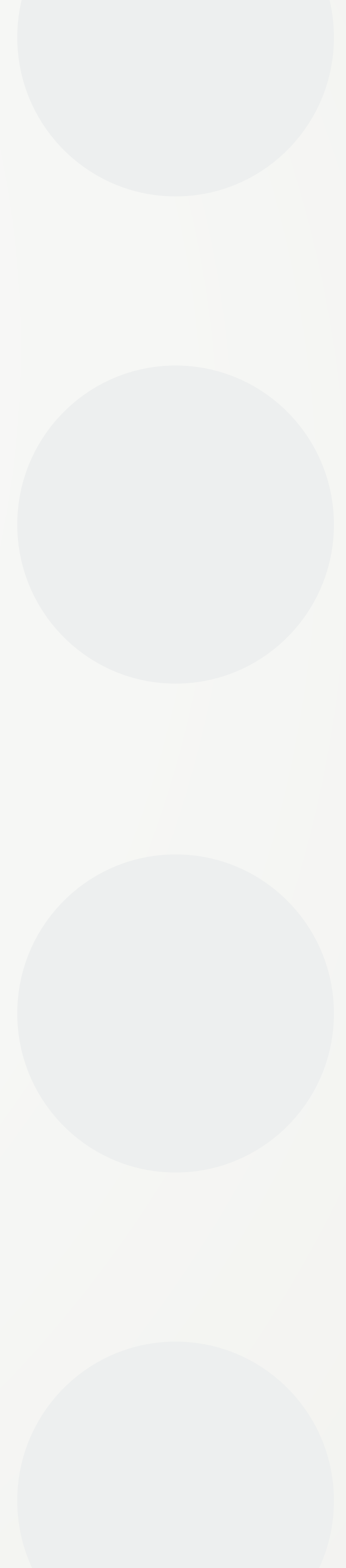
Multi-factor authentication (MFA)
Single Sign-On (SSO)





1. Market challenges

Remote access issues



Review

- **up to 18%** people in Kazakhstan work remotely¹
- **7th rank** in the world by the number of cyberattacks in 2023²
- **120%** increase in phishing attacks in the corporate sector³
- **x 3,5** growth in the number of information leaks in the world in 2022⁴
- **>223 mln** cyberattacks by foreign hackers recorded in Kazakstan in 2023 ⁶

As a result, companies are faced with:

- direct and indirect financial damage;
- reputational damage and loss of customers;
- theft of intellectual property and trade secrets;
- Regulatory sanctions for non-compliance with regulatory requirements.

\$1 mln

Average losses from cyber-attacks for medium and large companies in Kazakhstan⁵

¹ National Report “Labor Market of Kazakhstan: On the Way to Digital Reality” [2022](#).

² Kaspersky Lab research, [2023](#).

³ in Q1 2023 compared to Q1 2022. Kaspersky Lab research, [2023](#).

⁴ Infowatch analytical report, [2022](#).

⁵ Kaspersky Lab research, [2022](#).

⁶ Cyber Digest of the State Technical Service of Kazakhstan, [2023](#).

Challenges

1 Insecurity of remote connections

- Viruses, social engineering, phishing, and other attack vectors indicate that **passwords are insufficient for adequate protection**;
- Connections to corporate IT resources from compromised accounts;
- Unrevoked accesses when an employee is terminated.

The realization of a cyber risk is a matter of time if preventive measures are not taken to protect connections to corporate resources.

2 Ineffective access control processes

High load on the IT support team due to onboarding and offboarding of users, organization of remote access, account maintenance, changing forgotten passwords and expired passwords.

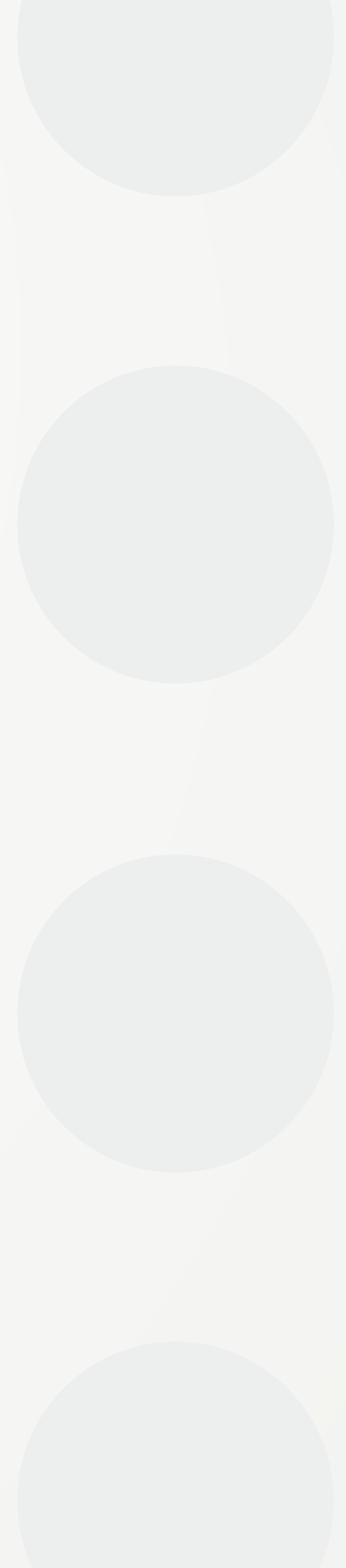
The result of business process downtime due to unresolved access problems is high financial and time costs.



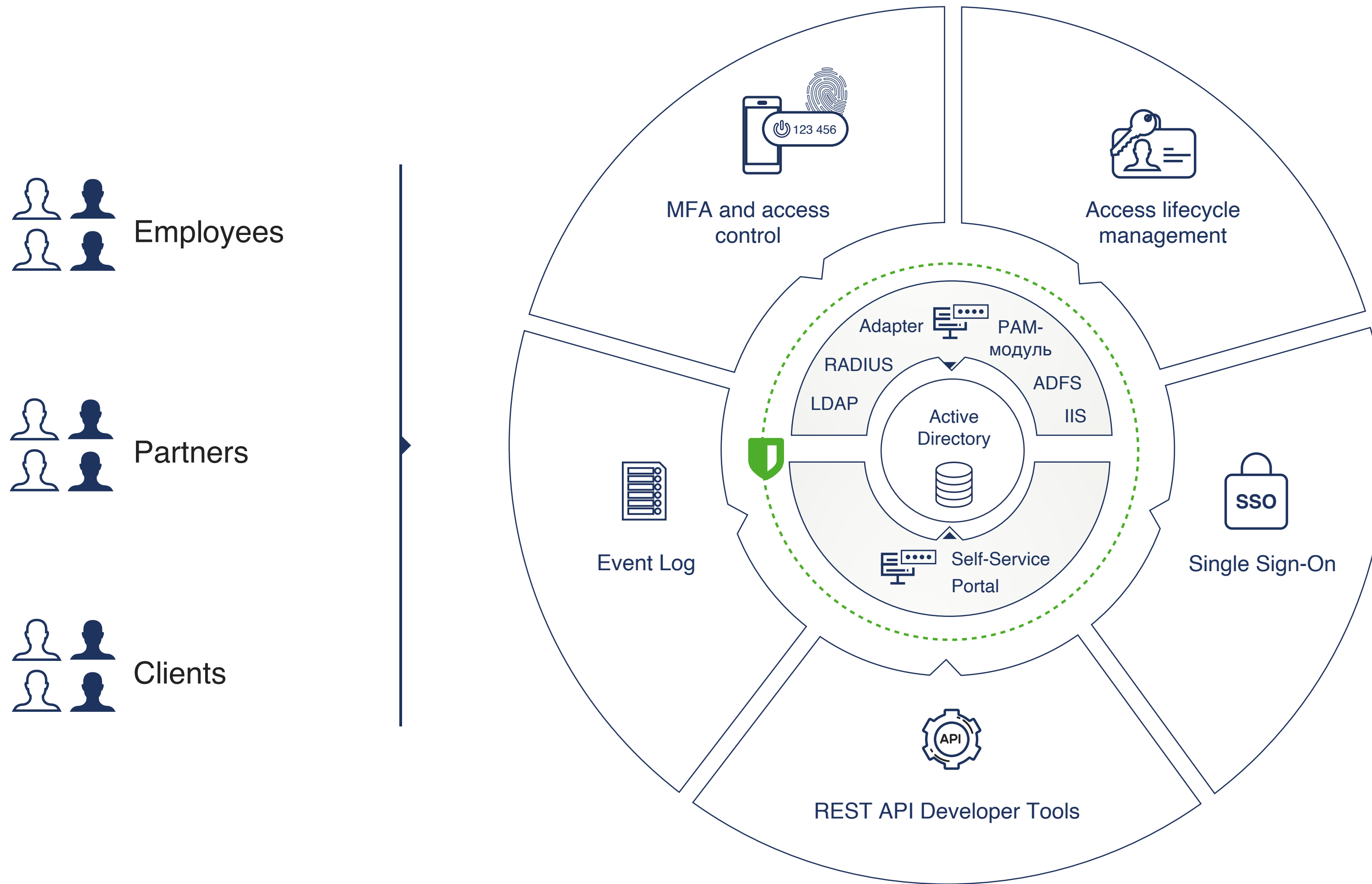


2. Solution

MULTIFACTOR product



MULTIFACTOR at a glance



- 1 **VPN**
[Cisco ASA](#), [Check Point](#),
[Fortigate](#), [OpenVPN](#), [Huawei](#),
[MiktoTik](#), [Windows VPN](#) etc.
- 2 **VDI**
[VMware](#), [Citrix](#),
[Remote Desktop](#) etc.
- 3 **Cloud applications, virtualization, web**
[SAML](#), [OIDC / Oauth](#),
[Outlook Web Access \(OWA\)](#) ,
[Huawei Cloud](#) etc.
- 4 **Linux infrastructure**
[SSH](#), [SUDO](#), [OpenVPN](#),
PAM etc.
- 5 **Windows infrastructure**
[Windows Logon](#), [VPN](#),
[RD Gateway](#), [NPS](#) etc.

✓ Sign-on protection

✓ Easy integration

✓ Coverage of all IT infrastructure



MULTIFACTOR solution

CAPEX
0 ₹

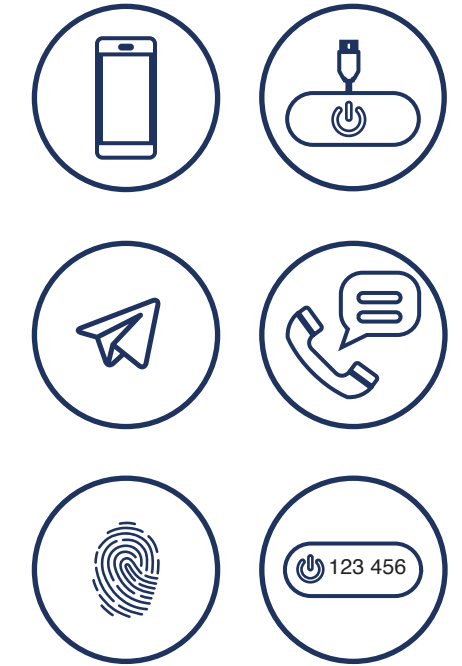
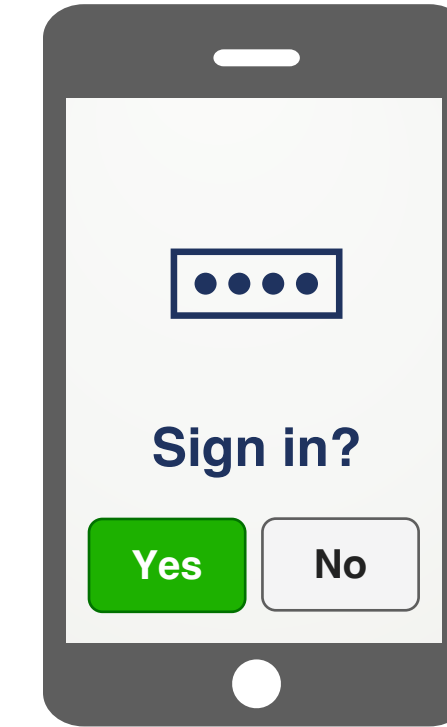
No implementation and IT infrastructure costs.

from **2 hours** for integration

Fast integration and commissioning.
Rapid onboarding.

up to
99 %

Reducing the risks of unauthorized access without creating new ones.



 **MFA and access control**


- Secure access to infrastructure;
- Prevent account hijacking, data breaches and network attacks;
- Protect VPN and VDI connections;
- Protect cloud SAML applications;
- Protect Windows and Linux infrastructure.

 **Self-service portal**


- User Self-Onboarding;
- Self-configuration of 2FA;
- Solving access problems without IT support (including changing expired passwords)

 **Single sign-on and access control**

- Eliminates account multiplication in cloud systems;
- Single account provider for access to your applications;
- Simplifies hiring and firing of employees for IT.

 **Security**
An extra layer of protection on top of your basic IT authentication methods.

 **Reduced support costs**
Simplifying the resolution of access problems.

 **Continuity of processes**
Intuitive UX, increasing employee productivity.

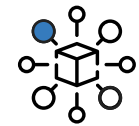


Why MULTIFACTOR?



High accessibility

Uptime 99.98% of the time.
A solution proven by real customer integrations.



Fault tolerance

A Multifactor cloud failure will not affect the operation of your business. In the worst case scenario, the infrastructure reverts to the previous level of access, without the use of a second factor.



Performance

MULTIFACTOR cloud – 1800 tps
RADIUS Adapter – 120 tps¹



Infrastructure security

The Multifactor cloud is located in PS Cloud Services' data centers in Almaty with multi-level physical protection, redundant internet channels and power supplies.



Scalability

No limits on the number of users and IT resources.



Zero CAPEX

SaaS solution for any business.



Easy user adaptation

Intuitive and simple process to connect users to multi-factor authentication.
Possibility of automatic connection.



Simplifying the user experience

Multifactor allows you to simplify password policies. Combined with SSO capabilities..



Customize any process

Ability to add any necessary business logic.



ByPass mode

Allows groups or individual users to log in without a second factor.

SLA



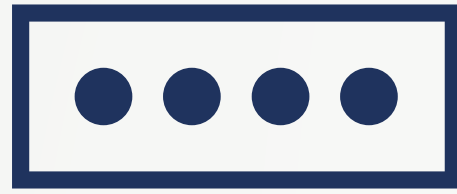
Uptime
99.98%



Tech support
7x24x1H

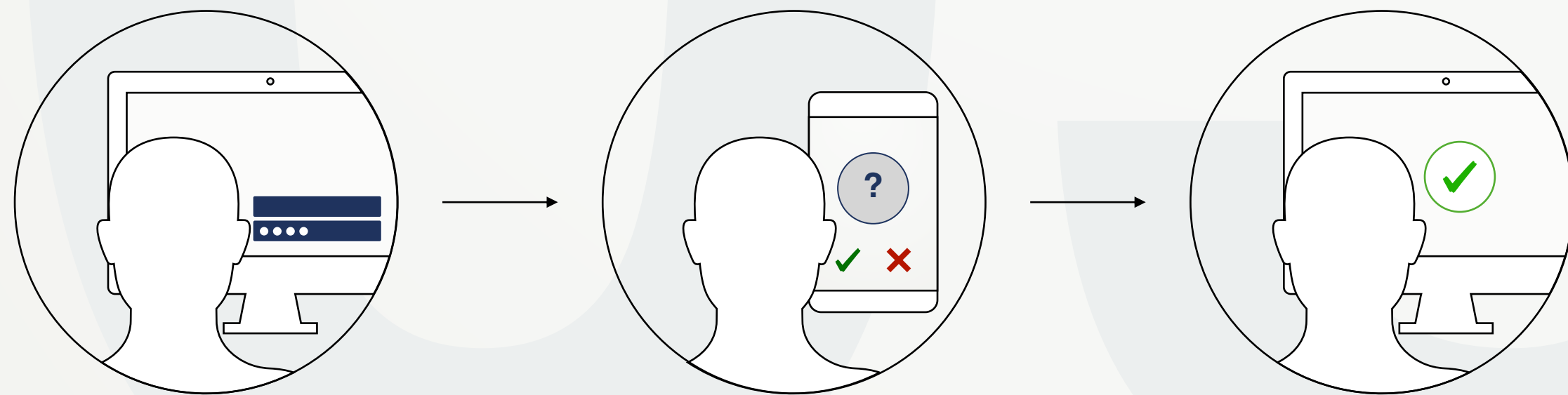
¹ Horizontal scaling if necessary





3. Technology overview

Multi-factor authentication (MFA)

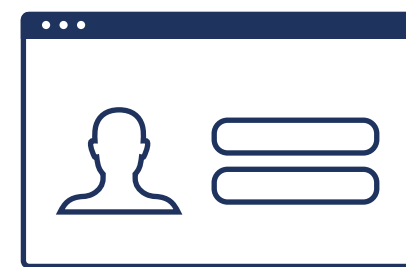


Multi-factor authentication (MFA)

Users can prove their identity by what they know (the primary authentication method, usually login and password); by what they have (e.g., hardware or software token); or by who they are (biometrics). The last two are possible ways to verify the second factor.

1 First factor

What the user knows:



Login and password



2 Second factor

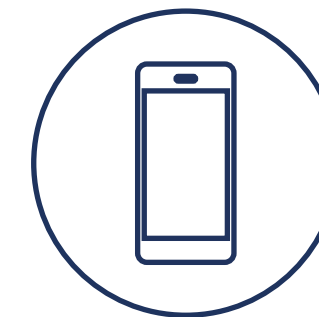
What the user owns or who the user is:



Telegram



Phone call



Mobile app



SMS



Token
(OTP, FIDO¹, U2F¹)



Biometrics¹



3 Access







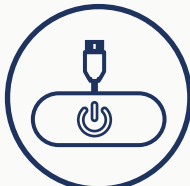

Access granted.

¹FIDO, U2F tokens and biometrics are not available in configurations with NAS firewalls (Checkpoint, Cisco, Mikrotik, etc.) and VDI.



Supported authentication methods

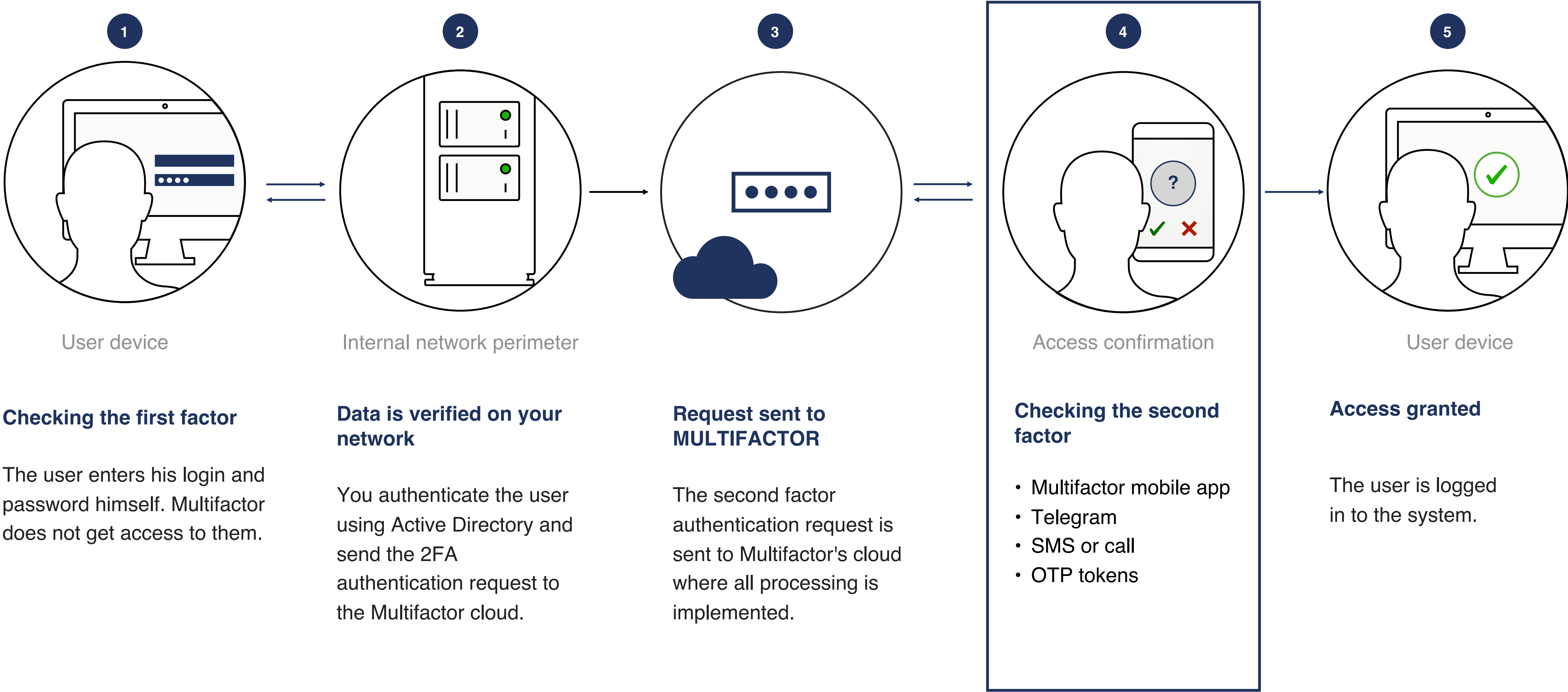
The table below summarizes the 6 main second factor validation methods supported by Multifactor depending on the usage scenario.

	VPN and VDI	Linux infrastructure	Windows infrastructure	Cloud apps (SAML)	API (Web)
 MULTIFACTOR mobile app	✓	✓	✓	✓	✓
 Telegram bot MULTIFACTOR	✓	✓	✓	✓	✓
 SMS or phone call	✓	✓	✓	✓	✓
 OTP tokens (hardware or software)	✓	✓	✓	✓	✓
 U2F / FIDO tokens				✓	✓
 Biometrics				✓	✓

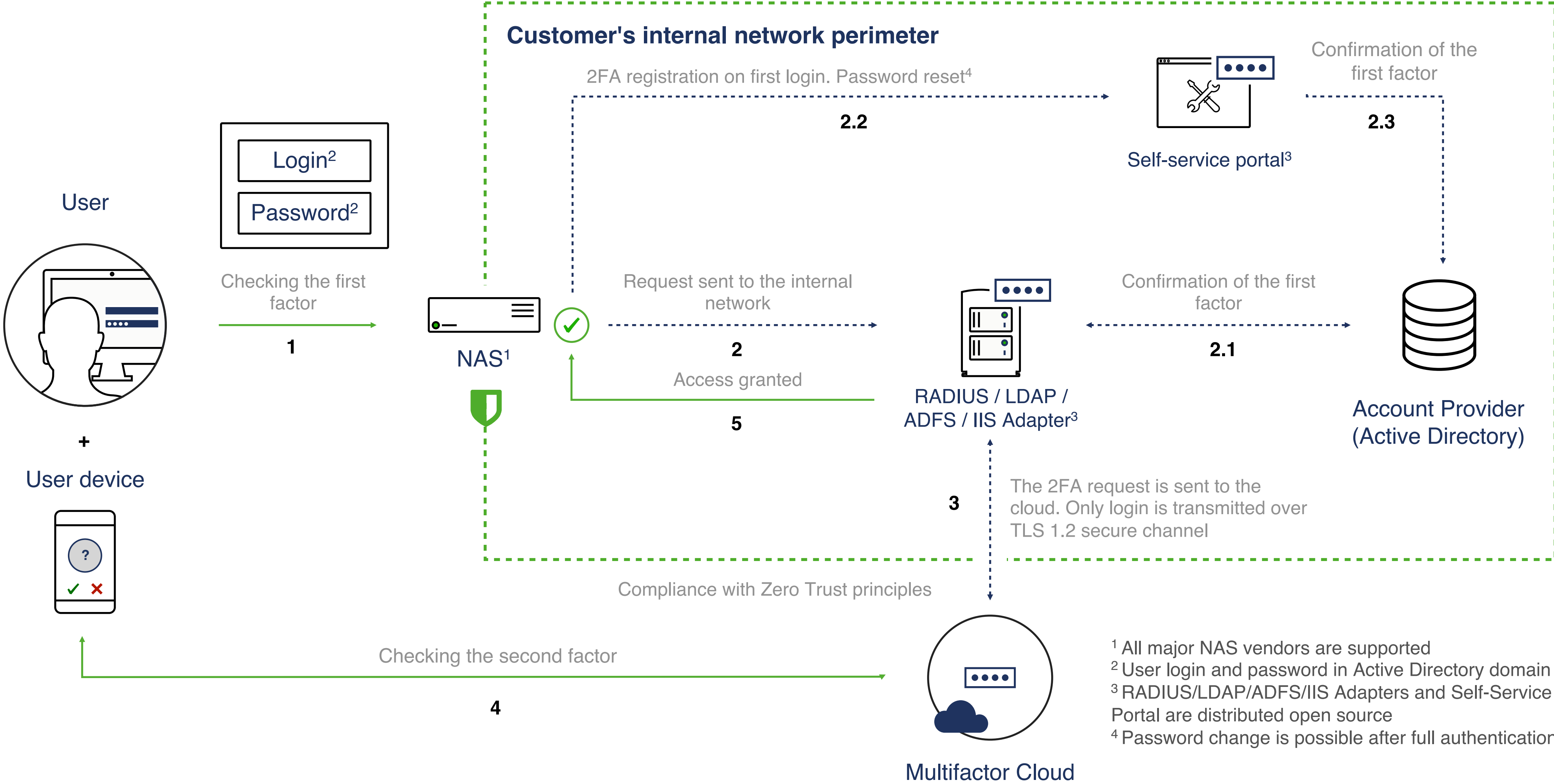


MULTIFACTOR does not access your credentials

The software operates on top of the main authentication method and never processes or stores your users' passwords.



High-level solution scheme



Composition of the solution

1 On-Premise components

1. Self-Service Portal

Extension for Active Directory

- Self-registration of the second authentication factor in Multifactor Cloud by the employee;
- Password change in the corporate Active Directory domain with mandatory verification of the current password and confirmation by the second factor in Multifactor Cloud;
- The component is [open source for Windows and Linux](#).

Minimal system requirements:
1 core CPU, 2Gb RAM, Windows Server 2012 or higher

2. RADIUS, LDAP, ADFS, IIS Adapters

Adapter for Active Directory

- Receiving employee authentication requests in CheckPoint VPN, RDP and Citrix via RADIUS protocol;
- Verification of the first authentication factor (login and password) in AD or NPS domain;
- Verification of the second authentication factor in Multifactor Cloud;
- The components are [open source for Windows and Linux](#).

Minimal system requirements:
4 core CPU, 4Gb RAM, Windows Server 2012 or higher

2 MULTIFACTOR cloud

multifactor.kz

Securely hosted in a reliable data center PS.KZ

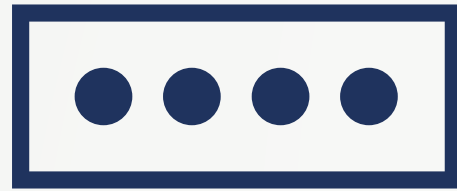
- Confirm and sign user authentication requests with a second factor;
- A personal IT account for your organization to manage and control employee access to resources with 2FA;
- Event log;
- API and developer tools.

SLA

Uptime **99.98%**

Tech support **7x24x1H**

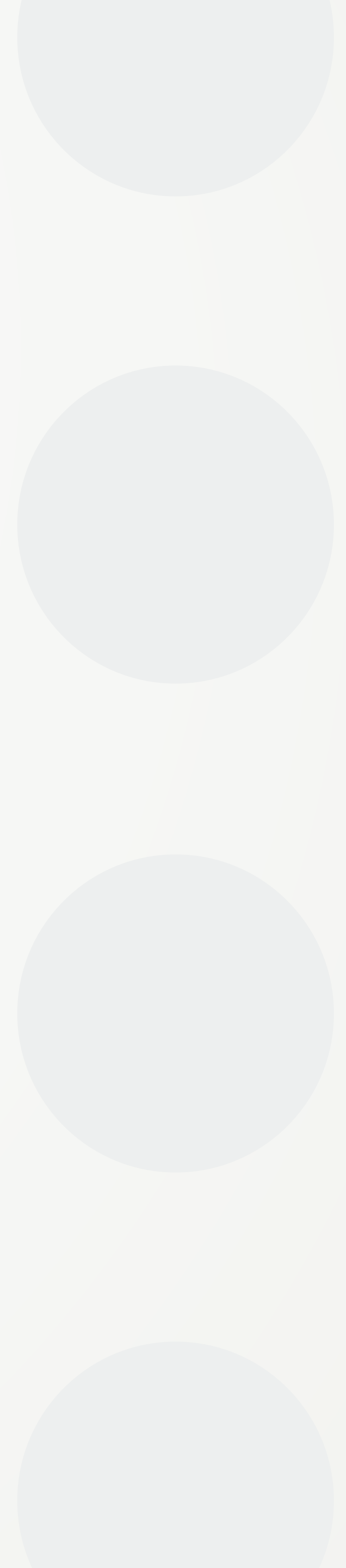





4. Technology review


Single Sign-on (SSO)

04




SSO MULTIFACTOR - simplifying access control to enterprise applications and the second factor


 **Reducing costs**
A single account provider makes it easy to manage all users in an organization by granting access based on job title.

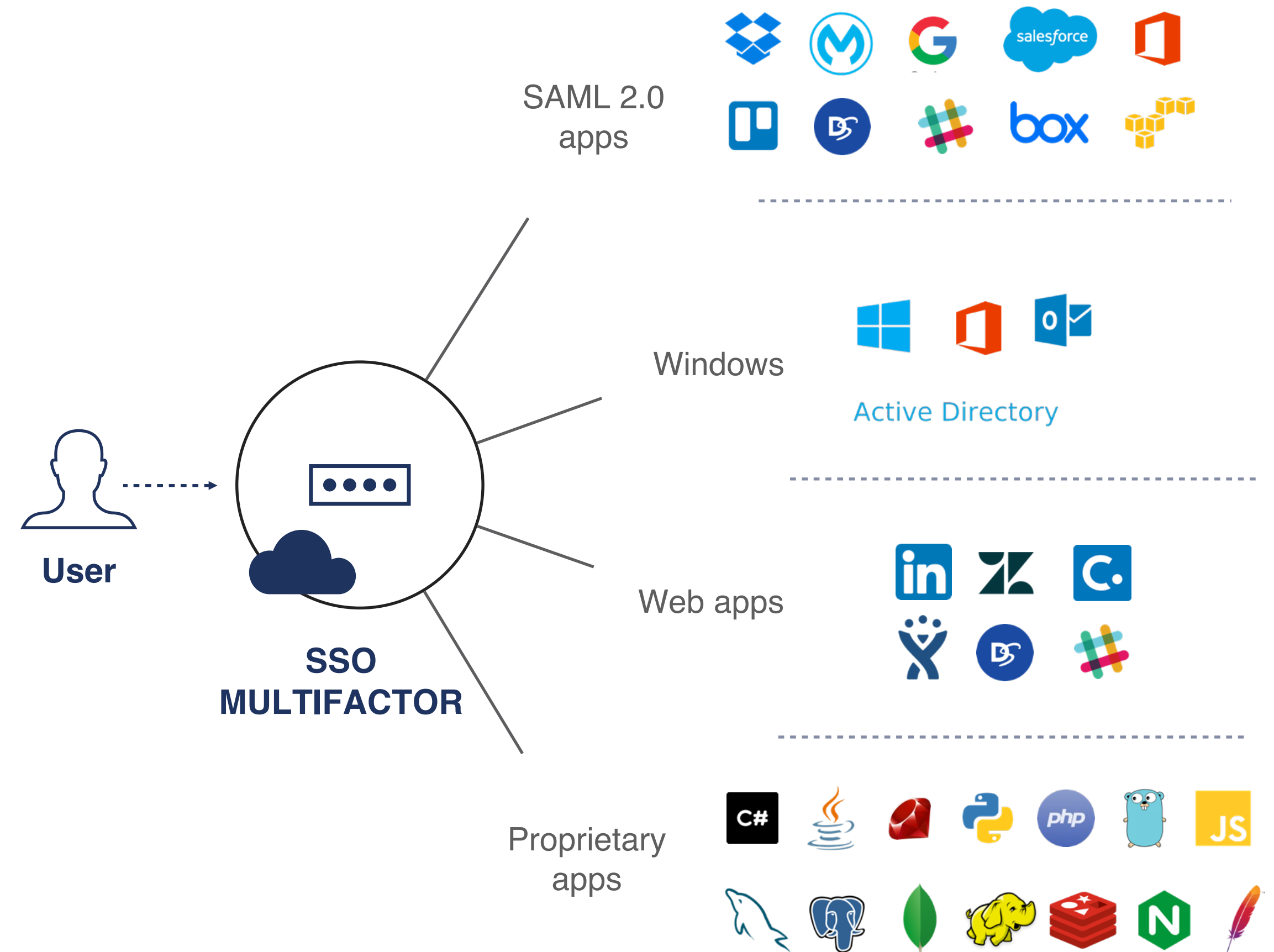
 **Improved user experience**
No need to memorize multiple passwords and accounts. Ability to change passwords in all services in a couple of clicks

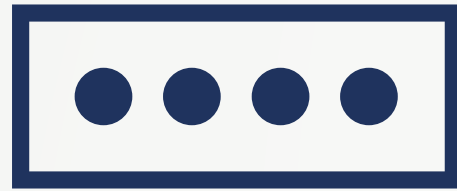
 **Better compliance with safety requirements**
Introducing the second factor into all systems, regardless of their capabilities.

 **Customizable password policies**
Password policies depend on the account provider, not a third-party system.

 **Increased productivity**
Simplified control of user access. Easily manage the movement of an organization's human resources.

 **Simplified connectivity**
It takes less time to integrate a new application into the company's infrastructure.





5. 2FA users enrollment

Registration of the second factor by system users

3 modes of 2FA enrollment

1 Automatic registration

● User experience

● Easy to integrate

● User enrollment speed

Automatic registration of SMS as the second access factor (synchronization of phone numbers with ActiveDirectory).

2 Self-service registration

✓ 1) Dialog with user ([see more](#))

● User experience

● Easy to integrate

● User enrollment speed

The technology allows the second factor to be configured in a dialog with the user directly in the VPN/VDI client or in Multifactor's API/SAML interface on the first connection.

✓ 2) Self-Service Portal ([see more](#))

● User experience

● Easy to integrate

● User enrollment speed

The portal allows you to configure the second factor in self-service mode. In this scenario, you need to prepare and distribute instructions to users.

3 Manual enrolment

● User experience

● Easy to integrate

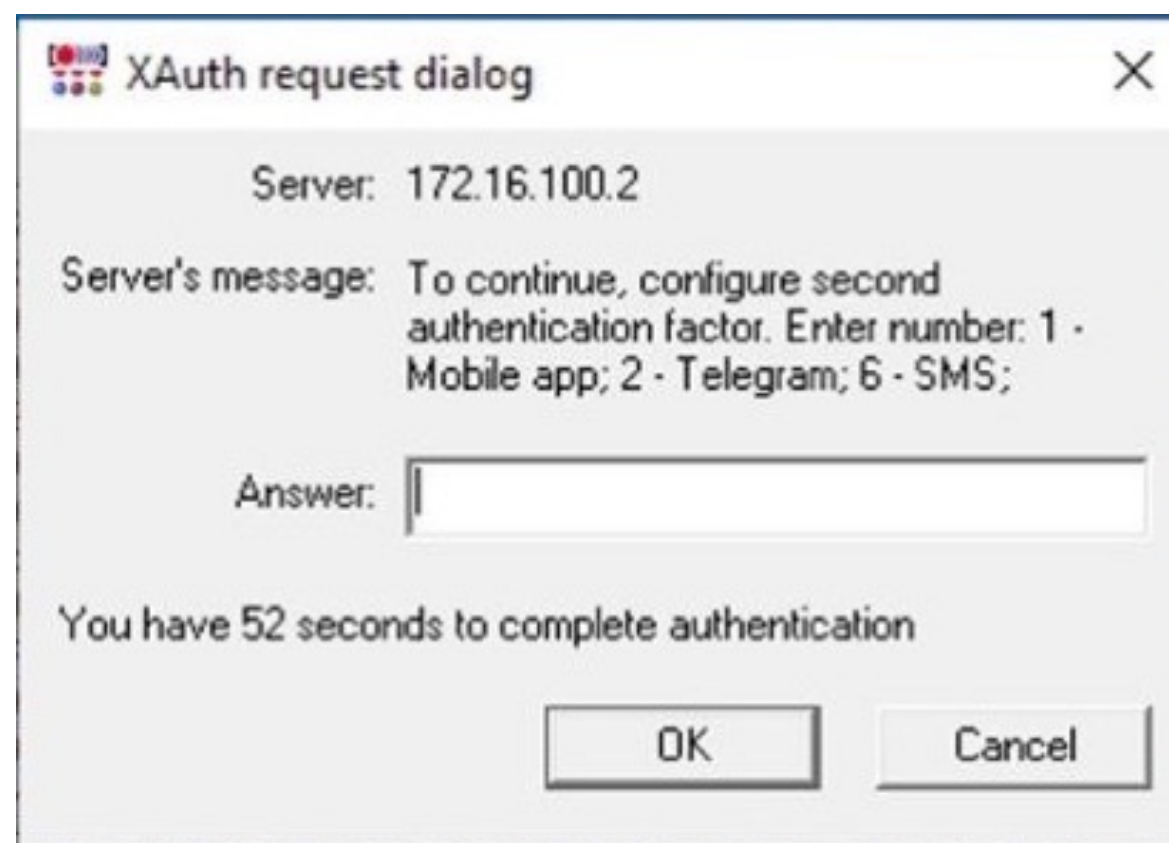
● User enrollment speed

Administrators manually add or import users and send out registration links to email.



Example 1: Registering 2FA in user dialog mode

1 Factor selection



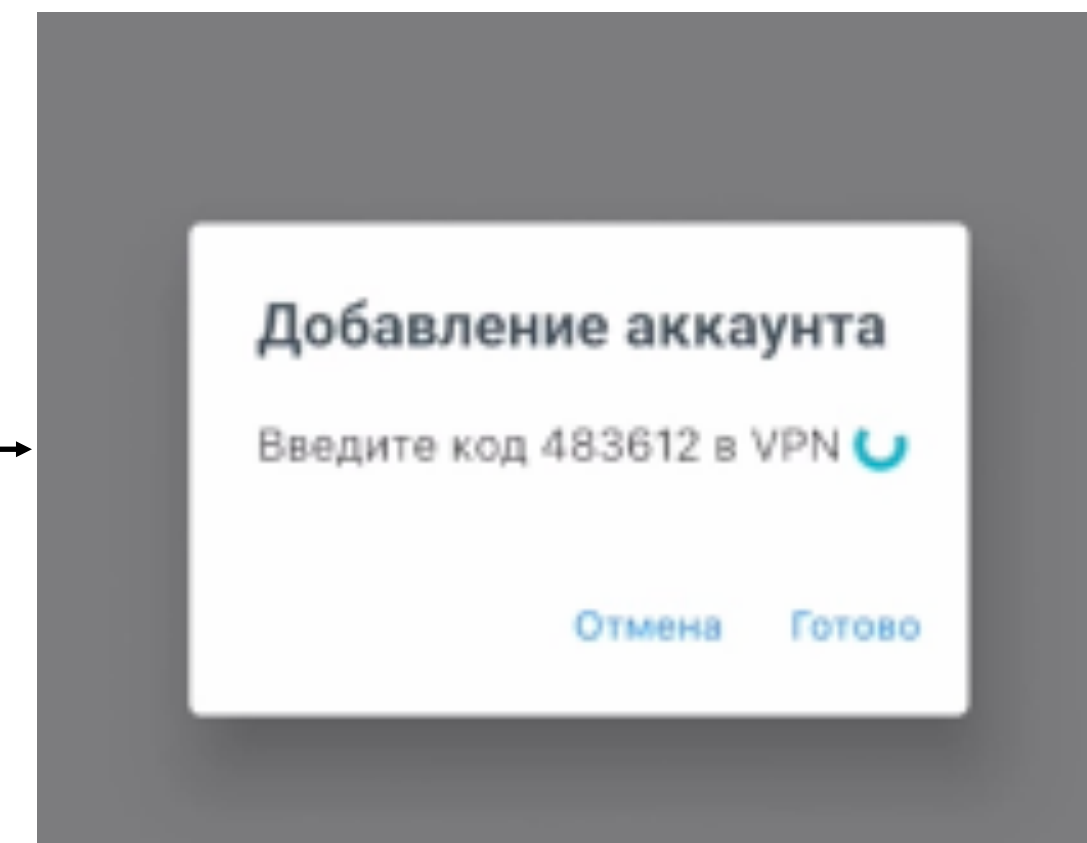
The user selects a convenient two-factor authentication method from a preconfigured list¹ by entering the corresponding digit.

2 Binding factor



The client sends the user a code that they need to enter in the Multifactor app or Telegram bot.

3 Proof of ownership



The user confirms ownership of the factor by entering a code from Telegram, the Multifactor mobile app, or SMS back into the client.

4 Done!

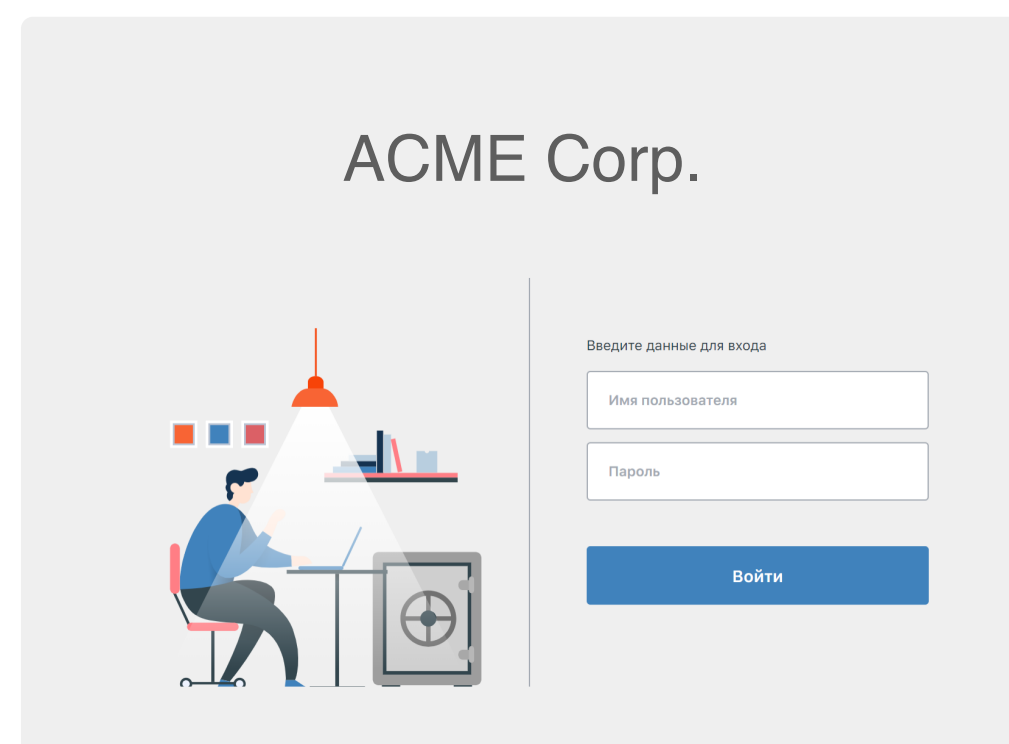


Registration of the second factor is completed. The log-on is additionally protected by the second factor.

¹ Telegram, SMS, MULTIFACTOR App in case of VPN and VDI connection protection.

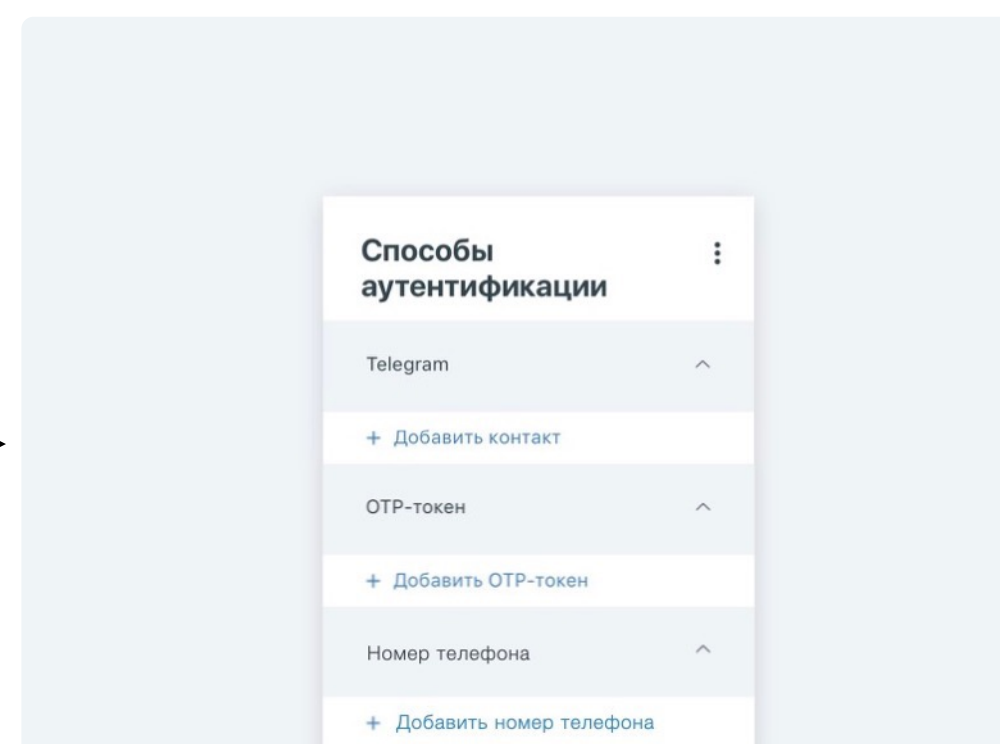
Example 2: Registering 2FA on a self-service portal

1 First connection



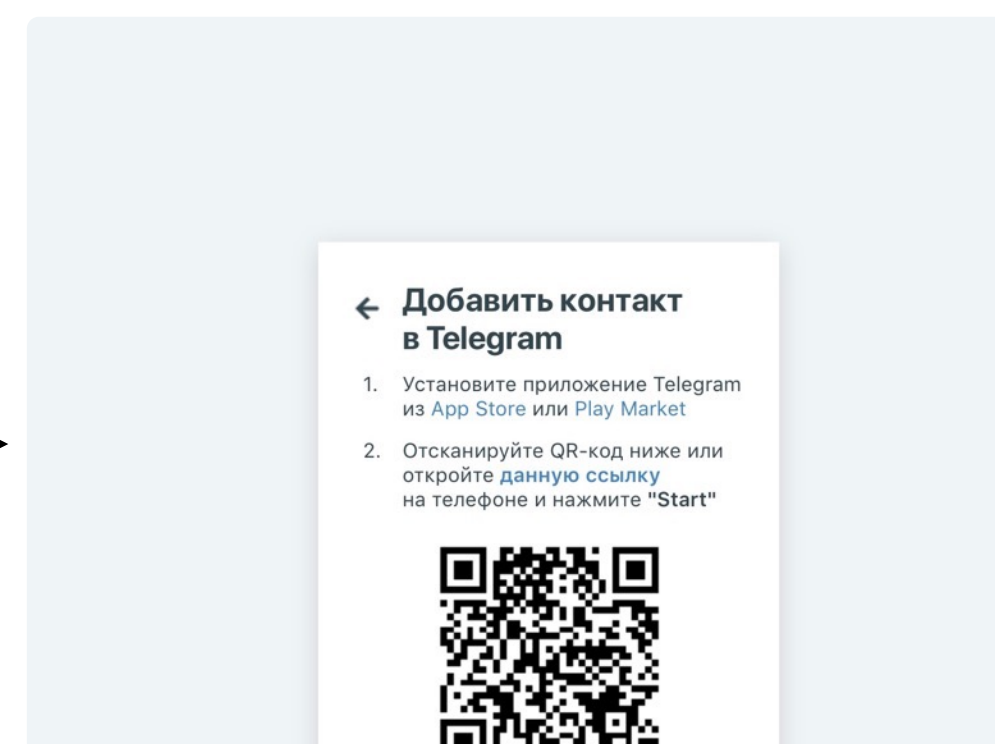
The user is authenticated on the Self-Service Portal (Active Directory credentials).

2 Factor selection



The user selects a convenient two-factor authentication method from a preconfigured list¹.

3 Proof of ownership



The user confirms possession of the factor.

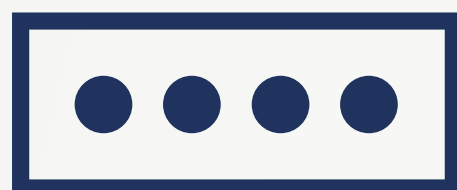
4 Done!



Registration of the second factor is completed. The log-on is additionally protected by the second factor.

¹ Telegram, SMS, phone call, MULTIFACTOR App or OTP tokens (hardware or software) in case of securing VPN and VDI connections.

² For example, in case of confirmed loss of the second factor or objective impossibility to use the second factor.



Contact us, let's discuss your case in detail!



sales@multifactor.kz



+7 747 610 43 40



<https://multifactor.pro/>
Multifactor Kazakhstan LLP