Axidian

WHITE PAPER

Axidian Access

Unified Authentication And User Access Control

Table of contents

Reliable authentication and centralized access management

Protection of access to corporate resources is one of the main tasks for a company cybersecurity service. Reliable user authentication and centralized access management are important elements of this task solution.

Selecting the authentication technology

The choice of reliable authentication technology is conditioned by several factors:

- Applicability - use scenarios might limit the range of available authentication technologies significantly. For example, if most of the use scenarios are remote ones, it is not feasible to use authentication devices that are to be connected to the workstation.
- Security is about the extent to which the authentication technology corresponds to the organization needs in the aspect of informational security. For instance, one-time passwords provide a protection level sufficient for most of the remote scenarios. However, the organization might have to use other technologies in order to comply with external requirements set by regulation authorities or industry standards.
- Usability - this is how comfortable are the users with applying one technology or another in their everyday working environment. For example, accessing the desktop using one-time passwords might not be comfortable, since one has to generate and enter a password multiple times per working day.
- Utilization value of an authentication technology is constituted by several factors: implementation costs, ability to use the current authentication device set, cost of ownership, the complexity of integration of the authentication technology to the target information systems.

Centralized access management

The employees have access to a wide range of information systems, managed by different administrator groups (Active Directory, databases, application systems). To manage such a type of access, a special centralized solution is required. The latter provides for the following:

- Collection of data on the information systems available to a user at one place;
- Implementation of uniform login mechanism - Single Sign-On;
- Definition of what authentication technologies should be used to login to each of the information systems;
- Restriction of access to information systems;
- Logging of employee access to information systems.

Centralization is achieved by using various integration technologies and protocols in the aspect of user authentication, depending on what exactly is supported by the target

system. There is no uniform integration mechanism due to a great variety of applications and technologies used by them. Therefore it is important that the access management system supports various mechanisms and protocols of integration to the target applications. This allows covering a maximum number of information systems.

Axidian Access

Axidian Access software suite is a platform for building up a centralized system for managing user access to the corporate information resources.

Axidian Access allows implementing strict and multi-factor authentication of users when accessing the information resources. The said technologies mitigate information security risks by supplementing or replacing password usage. Axidian Access supports various authentication methods. Due to that, it can easily be adapted to access scenarios required and therefore can offer optimal authentication technology to users in each case.

Besides various authentication technologies, Axidian Access utilizes a wide range of integration technologies that allow connecting the target application to the authentication system. The said technologies are implementation of Single Sign-On (Web and Enterprise SSO) approach, standard authentication protocols and agent modules. Axidian Access provides controlled access to information resources both within the company intranet and to services available externally (e.g., email, VDI, VPN and web portals). This approach makes it possible to build up a centralized access management system that encompasses all the target systems used, minimizes the number of user requests to help desk service, reduces infrastructure maintenance costs and enhances user efficiency.

Axidian Access platform

The platform is based on the essential modules that provide server infrastructure and management tools' functioning (see Figure 1). The said Axidian Access modules are:

Axidian Access authentication and management server. The server is the core of the system. It provides functioning of the whole of the system, performs user authentication and implements the solution business logic. The server is an ASP.Net application. It supports installation in cluster mode, and, therefore it provides for higher performance and fault tolerance level irrespective of the implementation scale.

Access Policies define access parameters for users, such as authentication technologies and available applications, as well as the scope of the rights of system operators and administrators.

Roles define the rights of operation in the Axidian Access management console. There are three roles in the system:

- Administrator - has full access to all functions and settings.
- Operator - has permission to work with the users.
- Inspector - has read access.

Rights via roles can be granted to the whole system or within individual policies.

Data storage. All the system data is stored in the uniform storage which can be addressed directly by the server only. Data storage and data transfer to/from a server are performed in encrypted form. The storage can be located in the Active Directory folder (scheme expansion is not required) or in a SQL database.

Events. All the events of settings change or access being granted are logged in the uniform log that is stored on the dedicated server. The log can be stored in Windows Event Log format or in Axidian Access proprietary format in SQL database. Besides, the syslog protocol can be used to send events to an external log server.

Management Console is implemented as a web application that can be used to view and to change system parameters or user settings, as well as to view the system log.

User Console makes it possible for users to register or modify their authentication data (smart cards, one-time password generators, fingerprints, etc.) as well as view the login history.

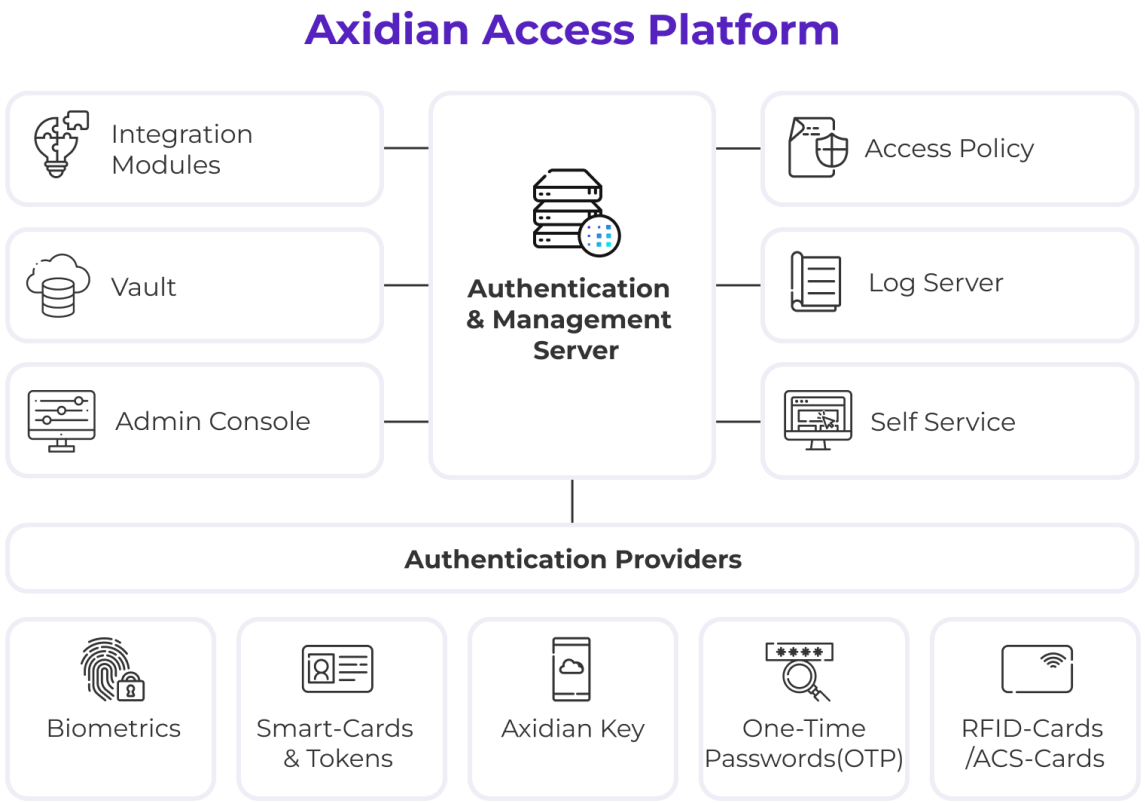

Figure 1. Axidian Access platform

Authentication Providers give Axidian Access an opportunity to work with user authentication technologies. An authentication provider implements a unified interface for the system to perform the required operations of a certain authentication technology: getting the authentication data to store and verify, as well as data verification. Axidian Access supports the following authentication technologies:

- Cryptographic smart cards and USB tokens, such as eToken, IDBridge etc.
- Proximity RFID cards (used as pass in ACS) of EM-Marin, HID iClass, HID Proximity, Mifare format.

- Hardware and software tokens for one-time password generation using OATH TOTP and HOTP protocols.
- One-time codes sent via SMS or E-mail.
- Biometrics: fingerprint, hand vein pattern, 3D face image.
- Out-of-band authentication using a mobile application and push notifications based on the Axidian Key product. Axidian Key mobile apps are available for iOS and Android operating systems. With the use of the application, a user confirms login operations into information systems. The login details are displayed on the smartphone screen where the user can check which system he/she logs into. Besides, Axidian Key supports the generation of one-time passwords with the TOTP algorithm.

The technologies can be combined to a single authentication method, thus implementing the multi-factor authentication (MFA).

Integration modules

Each of the integration modules is designed to solve a certain task of access protection and user authentication in specific applications. Any of the said modules can be used separately from other ones. The integration modules are designed for operation in combination with other modules. With that said, you can create any configurations of an authentication system, adapting it to the current needs and information system structure of the enterprise.

The Axidian Access includes the following modules for integration with target information systems:

Figure 2. Axidian Access integration modules

Axidian Access Windows Logon

Axidian Access Windows Logon provides an opportunity to login to Windows using the strong authentication technologies within the Microsoft Active Directory environment. To do so, the Windows Logon agent is installed onto user workplaces. The agent installer is implemented as a standard MSI (Microsoft Windows Installer) package. This allows performing bulk installation and update of the system using various tools, such as Active Directory group policies, Microsoft System Center Configuration Manager (SCCM) etc.

To integrate to the Windows operating system, a standard Credentials Provider mechanism is used to implement a custom user authentication interface. The said technology allows third-party developers to integrate their own authentication technologies using Windows interface. It is also possible to execute Windows logon using Axidian Access technologies and authenticate a user within OS bounds using Axidian Access, e.g., when attempting to access the domain resources, web applications etc.

The Windows Logon supports all the authentication technologies available within Axidian Access (smart cards, RFID cards, OTP, biometrics etc.).

Off-line mode

To enhance operational resilience, Windows Logon can create local cache on a user PC. This cache contains the user authentication data and can be used when server infrastructure cannot be connected to (off-line mode), for instance, due to connection failure or while on a business trip. The local cache lifetime can be limited to a certain number of days or a specific date. The cache is created only for the users, explicitly allowed by the Axidian Access administrator. To protect local data, the Windows Data Protection API technology is used.

Employee substitution mode

Axidian Access Windows Logon supports an employee substitution mode. To activate it, the administrator should assign a substitute to a certain user. In this mode, a substitute can logon to the operating system as the substituted user, but using his or her own authentication data (card, fingerprint etc.). The system log shall contain the information about the substitute user being logged on, not the substituted one. The mode might be of use when it is required to perform some action as soon as possible (say, to send an annual report) on behalf of the currently unavailable user (who is ill, is on leave etc.). A substitution period can be limited by calendar dates.

Automatic user identification (kiosk mode)

This mode is characterized by that one workplace is used by many employees. Therefore, switching between their working sessions should be performed promptly. For maximum comfort, it is recommended to use proximity (RFID) cards or PKI smart cards. In this case, the access scenario shall look like as follows:

1. For identification users do not need to indicate a username, they only need to

submit a smart card. To do so, a kiosk is equipped with a smart card reader.
2. The system may require the presence of a card on the reader for the whole work time on the PC. When the card is removed from the smart card reader, the current session may be blocked or terminated.
3. When a new smart card is put on the reader, the current session can either end or switch to a session of a new employee.
4. Biometric authentication can be added to the card as additional protection of access (for example, contactless biometrics using a palm pattern).

Management of Active Directory user passwords

Axidian Access does not substitute the standard Active Directory authentication system but automates the process of user password management. In such configuration, the password authentication becomes an internal mechanism used at software level only. Axidian Access administrator can configure the system so that at the moment of registering the first authenticator, the user password is automatically changed to a random value that neither the user nor the system administrator are informed of. Thus, access to the domain becomes possible with Windows Logon technology only. Later on, the user password is automatically changed either upon operating system prompt or according to the schedule set.

Axidian Access RDP Windows Logon

Axidian Access RDP Windows Logon module is used to implement the two-factor authentication for remote connections via RDP protocol. In this case, the first factor is the domain password, and the second one is a one-time password (OTP) or confirmation of logon via Axidian Key mobile application. The said OTP can be either generated on the user side with smartphone application or OTP token or sent to the user via SMS or Email.

The RDP Windows Logon is to be installed onto the end terminal server where the user logs in remotely. There is no need to install any components onto the user PC. A configuration with Remote Desktop Gateway is supported as well.

Axidian Access Enterprise Single Sign-On (Enterprise SSO)

Axidian Access Enterprise Single Sign-On (Axidian ESSO) implements a single sign-on approach for legacy applications that do not support SSO mechanisms. The system provides for centralized storage of user passwords to applications that require credentials and pastes those in automatically when the application requests to do so. The Enterprise SSO technology can be used with any application types (Windows, Java, Web, .Net), irrespective of the architecture - be it single-tiered, two-tiered, three-tiered, thick client or terminal applications.

The Enterprise SSO relieves the employees from memorizing the passwords and keeping those in secret, entering them with a keyboard and changing the passwords manually in accordance with password security policies.

For this, an Enterprise SSO agent is installed onto the user workstation. The said agent monitors applications launched and intercepts authentication forms when they appear on the screen. The agent also contains extensions for popular web browsers (Internet

Explorer, Google Chrome, Mozilla Firefox) that allow working with web applications as well.

Enterprise SSO integration to target systems

The Enterprise SSO can be configured for an application without interfering with neither server nor client parts of the application in question. Support of a new application stipulates for the creation of a special template in xml format written in the internal Axidian Access Enterprise SSO script language. The language allows defining the application forms to be handled and how these are to be handled. The Enterprise SSO reaction might be: additional strong authentication of a user, filling in the fields with authentication data (say, username and password), clicking the required control elements (for instance, “Login” button), recording of the event to the log etc.

Change of password in a target application

Most of the information systems support the capability to require the password to be changed right upon the first login to the system or upon the expiration of password validity period in order to minimize security risks. The Enterprise SSO processes the situation and allows for an automatic block of user access to the password change window (transparently for user), generation of new password value, fill in the “new value” and “confirmation” fields and click OK button. The Enterprise SSO agent saves new password value in Axidian Access database after the system notifies that the password has been changed successfully, From now on, neither the user, nor the administrator knows the new password value, and, consequently, cannot log in to the target system without Enterprise SSO.

The situation of password change can only be processed if the application ESSO template supports the window type in question.

Support of the terminal environment

Axidian Access Enterprise SSO is adapted for operation in a terminal environment in order to relieve the employees from using their passwords explicitly when an application is used within a terminal session. For this, the Enterprise SSO must be installed onto the terminal server.

In some situations, an employee might have to perform an additional authentication procedure, for instance, to access some critical applications. If the technology involves using an external equipment, connected to the employee’s PC (say, fingerprint scanner), then communication is established between the Enterprise SSO agent on the terminal server and the said equipment. Enterprise SSO communicates using Microsoft RDP or Citrix ICA protocol. This means that no additional software needs to be installed on the employee’s PC, except for the driver and run-time libraries required for the authentication equipment.

Axidian Access SAML Identity Provider

Axidian Access SAML Identity Provider (SAML IDP) module is used to implement the multi-factor authentication and single sign-on access to web applications (web single

sign-on, WebSSO). The SAML 2.0 (Security Assertion Markup Language) open international standard is used for integration to target solutions. This provides for compatibility with a wide range of commercial systems. SAML relieves a user from memorizing quite a number of authentication data. In other words, only one set of credentials is required to access all the integrated systems. The authentication itself is performed centrally on the SAML Identity Provider (IDP) side. Axidian Access SAML IDP is implemented as a web application and is deployed in the customer infrastructure. Being attempted to access, the target application redirects a user to IDP page for authentication. If authenticated successfully, the user is redirected back to the target application with “authenticated” token, and the user session is then started.

Integration via SAML protocol is done on the server side. Therefore, the MFA and WebSSO approach can be used with any device that has a browser: PC, smartphone or tablet PC.

Axidian Access SAML IDP supports any combinations of the following user authentication technologies: domain password, OATH TOTP and HOTP one-time passwords, one-time codes sent via SMS or EMail, out-of-band authentication with Axidian Key mobile application.

The WebSSO and MFA bounds might contain both corporate on-premise applications with SAML support (say, SAP, Citrix etc. solutions, and cloud services, such as Office 365, Salesforce, Slack, G Suite (former Google Apps) and many others.

Axidian Access ADFS Extension

Web applications based on the Internet Information Services (IIS) server can be integrated to the Axidian Access software suite using ADFS mechanism and Axidian Access ADFS Extension component. The latter implements a provider of multi-factor authentication for Microsoft ADFS server, thus adding the second factor to the access gaining process. This approach makes it possible to integrate into target applications without modifying those. When logging in to an application, the user is redirected to the ADFS authentication page, where the second authentication factor is requested from him or her via Axidian Access ADFS Extension. If successful, the user is redirected back to the target application.

The ADFS is supported by Microsoft web applications, such as Outlook Web Access, Sharepoint, Skype for Business etc.

Axidian Access ADFS Extension supports the following variants of the second authentication factor: OATH TOTP and HOTP one-time passwords, one-time codes sent via SMS and EMail, out-of-band authentication with Axidian Key mobile application.

Axidian Access IIS Extension

We developed a special Axidian Access IIS Extension integration module for authentication in the web applications that use Internet Information Services (IIS) and do not support ADFS mechanism. The module is installed onto the web server where the target application is deployed. The module provides for two-factor authentication without interfering with the application code. The said module intercepts the authentication procedure and after supplying the username and password, the user is redirected to a

separate page to authenticate himself or herself with a one-time password.

A single-factor authentication mode is supported as well. The mode is useful for Exchange ActiveSync (EAS) application, as it allows to exclude the domain password from the authentication scheme. A separate password is used to access EAS in this case. In fact, it is a so-called application password, used for EAS only. This password is to be entered into a mobile client for access to corporate email.

IIS Extension can be used with any web application based on IIS, such as Outlook Web Access, RD, Exchange Active Sync etc.

Axidian Access NPS RADIUS Extension

Axidian Access NPS RADIUS Extension is an expansion module for Microsoft Network Policy Server (NPS). This module allows implementing two-factor authentication for RADIUS-compatible services and web applications. The following is required for this:

- To deploy an NPS server in the enterprise network. The server is to provide for authentication via RADIUS protocol using the Active Directory user data.
- To configure the target application to user authentication via RADIUS protocol at the NPS server.
- To install Axidian Access NPS RADIUS Extension module onto the NPS server. The module is to process the authentication requests and prompt the users for the second authentication factor.

Authentication on the second factor is performed at the Axidian Access server. The result is sent to the target application via the NPS server.

Axidian Access NPS RADIUS Extension supports the following variants of the second authentication factor: OATH TOTP and HOTP one-time passwords, one-time codes sent via SMS and EMail, out-of-band authentication with Axidian Key mobile application.

Authentication via RADIUS protocol can be used with many VPN and VDI solutions, for example, in software products from Cisco, Citrix, Check Point, VMWare, C-Terra companies.

Axidian Access API

Axidian Access API is a software interface of REST API format to integrate to third-party systems and applications. The API can be used for two purposes:

- Implementation of two-factor authentication. If the target application does not support any of the authentication standards, then the two-factor authentication can be added to it by integrating Axidian Access API calls to the application. This approach can be used with one's own custom application or an ordered application that can be customized.
- Integration to incident systems. Such integration allows implementing additional scenarios of user account data process automation or user access control. Integration to identity management (IDM) systems or ACS systems might serve as an example of such scenarios.

Integration with Identity Management systems

The integration allows for creating and filling in the user access profile for Axidian Access Enterprise SSO module automatically. A connector to an IDM system allows for automatic synchronization of user account data in Enterprise SSO database. The credentials are created using IDM connectors to target systems and are immediately stored in Axidian Access Enterprise SSO subsystem, relieving the employee from memorizing the passwords and entering them manually. The integration has the following benefits:

- The company information security level increases due to complete automation of user password lifecycle: passwords are created, entered and changed automatically, without user or administrator intervention.
- The procedures are shortened to the minimum for granting and gaining access by employees. A user gains password-free access to all the necessary systems immediately after registering a new user (e.g., in the HR system) and automatic synchronization.

Scheme of Axidian Access Enterprise SSO integration to IDM

Let us see the operation principle closely using an example of hiring a new employee and authentication with a USB token to access the Desktop. The whole of the process can be roughly subdivided into five major steps.

1. An HR employee registers a new employee record in the HR system.
2. The new employee data appears in the IDM database via the connector to the HR system.
3. Based on that, the IDM performs synchronization, thus creating accounts for the user in all the applications required for the employee position or business role. For this, special IDM connectors are used.
4. The same principle is used for implementation of a connector to Axidian Access Enterprise SSO system. The said connector creates the employee access profile in the Enterprise SSO database by copying the user account data at the final stage of the process.
5. When done, the employee has all he or she needs for performing the duties. After the access to a desktop is obtained, Axidian Access Enterprise SSO agent provides for transparent access to all the applications required for the user by automatically filling in the application login forms.

Integration with ACS

Integration with ACS (physical Access Control Systems) allows Axidian Access to take the employee location at the moment of authentication into account. This makes the following scenarios possible, for example:

- Access is granted only if the employee is within the building perimeter (say, entering via entrance checkpoint #1, #2 or #3;
- Access is granted in the specific room only (say, in the room #5, no matter how the employee got there);
- Access is granted only from a PC in a specific zone (e.g., from any PC on the third floor).

About Axidian

Axidian is a global IT security vendor with a corporate center located in Dubai, UAE, and branches in Lithuania and Singapore. We provide authentication, comprehensive access management, privileged access management (PAM), public key infrastructure (PKI) management and identity threat detection and response solutions.

Axidian is where security finds its Axis.

If you have any questions about our products or interested in more detailed information on those, please visit axidian.com.