

Axiadian CertiFlow

**Centralized Management of PKI,
Smart Cards and USB Tokens**

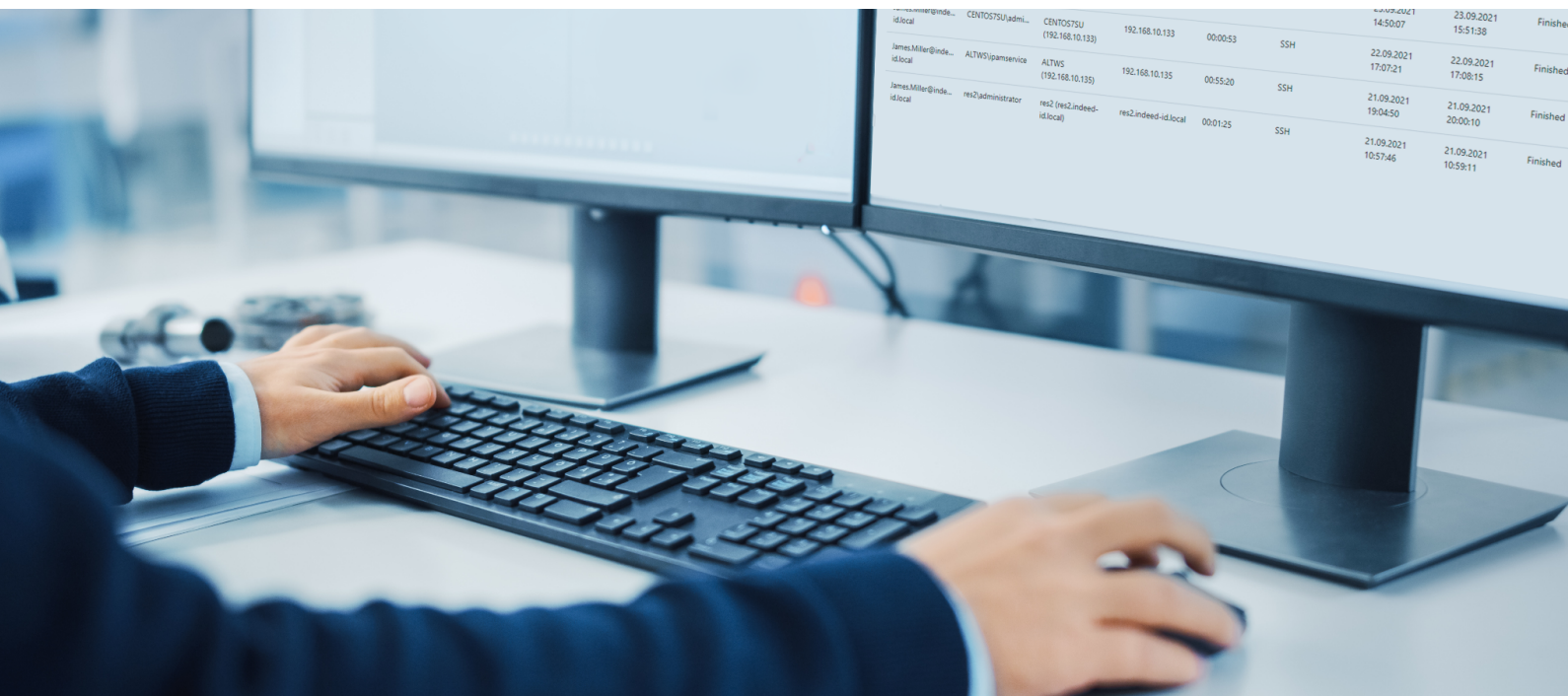


Table of contents

Table of contents	2
Effective Use of Public Key Infrastructure	3
Axidian CertiFlow	3
Labor Cost Optimization	
for Managing Certificates, Smart Cards and USB Tokens	4
Enhancing Overall Information Security	5
Axidian CertiFlow Architecture	7
Core Server Modules of Axidian CertiFlow	8
Management Console	8
User Self-Service Tools	8
API	8
Card Monitor	9
Event Log	9
Customizable Audit Logs	9
Internal Electronic Document Management Service	9
Integration Modules	10
Connectors to Certification Authorities	10
Connectors to User Directories	11
Connector to Data Storage	11
Connector to Event Audit Systems	11
Connector to Axidian Access	11
Client Components	11
Client Agent	11
Middleware for Working with USB tokens and smart cards	13
Client Tools for Unlocking USB tokens and smart cards	13
Smart Card Printer Interaction Module	13
Advantages of Axidian CertiFlow	14
Axidian CertiFlow technical characteristics	15
About Axidian	16
Our contacts	16

Effective Use of Public Key Infrastructure

Public Key Infrastructure (PKI) offers solutions to many information security challenges:

- Replacing outdated password-based authentication with strict two-factor authentication for access to operating systems and applications (VPN, VDI, etc.)
- Digital signing and encryption of email
- Using qualified electronic signatures to meet regulatory requirements and ensure legally significant document management
- Encrypting data: files, disks, and other storage media

However, managing PKI introduces a number of new tasks:

- Issuing user certificates according to their roles: ensuring that a user's smart card contains the certificates needed for their work, without providing unnecessary ones
- Managing smart card and USB token PIN codes: PIN complexity policies, regular changes
- Monitoring certificate validity periods and renewing them in a timely manner
- Tracking smart cards and USB tokens and assigning them to employees
- Unlocking blocked smart cards and USB tokens when a user forgets their PIN

The effective use of PKI is impossible without a quality solution to these tasks. For this purpose, specialized software known as a Card Management System (CMS) is used.

Axidian CertiFlow

The Axidian CertiFlow software suite is a centralized system for managing Public Key Infrastructure. Axidian CertiFlow provides full control over digital certificates, smart cards and USB tokens at all stages of their lifecycle and enables users to resolve issues related to the use of tokens without contacting administrators.

Labor Cost Optimization for Managing Certificates, Smart Cards and USB Tokens

Axidian CertiFlow reduces the labor costs associated with routine PKI maintenance operations:

Certificate Issuance

Axidian CertiFlow automatically generates a list of certificates for issuance based on PKI usage policy mechanisms. All users covered by the same policy receive an identical set of settings and certificates. Operations such as creating certificate requests, issuing certificates, and writing them to smart cards or USB tokens are performed automatically.

Automated Certificate and Token Management

The system ensures full autonomy of processes without the involvement of a Certification Authority operator. The automated process for managing certificates, smart cards and USB tokens includes mandatory assignment and monitoring of essential operations, such as:

- Registration of tokens in the Axidian CertiFlow system
- Assignment to users
- Issuance, renewal, and PIN change
- Clearing and initialization
- Blocking and revocation

User Access to Certificates, Smart Card and USB Token Management

Regular users of the system are provided with a convenient personal account in the form of a web application. The personal account allows delegating to users from different groups the authority to independently work with certificates, tokens and smart cards, helping to reduce the IT department's workload.

System Event Notifications

Administrators and users receive instant alerts about system events, enabling rapid incident response. Critical information is communicated to responsible parties in the shortest possible time. For example, Axidian CertiFlow will remind users when a certificate is about to expire, allowing timely renewal and avoiding work interruptions.

Integration with Third-Party Systems via API

Such integration enhances process automation capabilities for certificate and USB token usage and enables scenarios such as automatically suspending a user's personal certificates upon receiving a signal from an external system (e.g., in cases of vacation or business trips, loss, or damage to an access card).

Tracking Certificates Issued by Third-Party Organizations

If the organization uses certificates issued by external (non-proprietary) Certification Authorities, Axidian CertiFlow allows storing information about such certificates in the system database and promptly notifying both the administrator and the user about their upcoming expiration. This prevents downtime in work with banks and trading platforms and eliminates the need for manual certificate tracking.

Unlocking Blocked Tokens Without Administrator Intervention

A blocked token or card can be unlocked either before or after the user logs into the operating system, with or without administrator involvement.

Enhancing Overall Information Security

With Axidian CertiFlow, organizations can improve their information security level through the following capabilities:

Centralized PIN Policy Enforcement

When issuing a USB token or smart card, PIN requirements are recorded on it – including complexity, rotation frequency, history depth, and other parameters, depending on the device model. Policies are stored and distributed centrally, so administrators do not need to set policies for each token/card individually.

Regular PIN Code Rotation

In Axidian CertiFlow, administrators can define a time period during which a user's PIN remains valid and initiate PIN changes for a group of smart cards and USB tokens. There is no need to manually track each token/card's PIN validity or individually notify users about required changes.

Additionally, the system can require the user to change the PIN upon first connection of the token / smart card to a workstation, if the hardware model supports this feature.

Tracking of USB Tokens and Smart Cards

Each USB token or smart card is assigned to a responsible employee. Certificate issuance or renewal on the token/card can only be performed by an administrator or the end user.

Timely Certificate Revocation for Dismissed Employees

To quickly block dismissed employees' access to corporate information resources, Axidian CertiFlow includes a specialized service that periodically checks the user directory and revokes certificates for users marked as dismissed.

Flexible Role-Based Access Control Model

Organizations can define custom security roles with configurable sets of permitted operations. This allows administrators to align Axidian CertiFlow's role model with the company's business processes.

Compliance with Zero Trust Policy

PKI provides the authentication, encryption, and integrity mechanisms required for a Zero Trust model, while Axidian CertiFlow tools allow for issuing, revoking, and replacing certificates in a reliable, scalable, and flexible manner.

Internal Electronic Document Management

Axidian CertiFlow eliminates risks associated with exchanging reporting documents via email and provides a secure internal EDM service for centralized management of documents related to certificate operations. Users can submit applications for an electronic signature certificate through their personal account, and employers can ensure compliance with regulations, including mandatory acknowledgment of certificate receipt by the employee.

The document search section enables verification of original document availability and tracking of unsigned documents, simplifying document control and helping avoid risks from missing critical files.

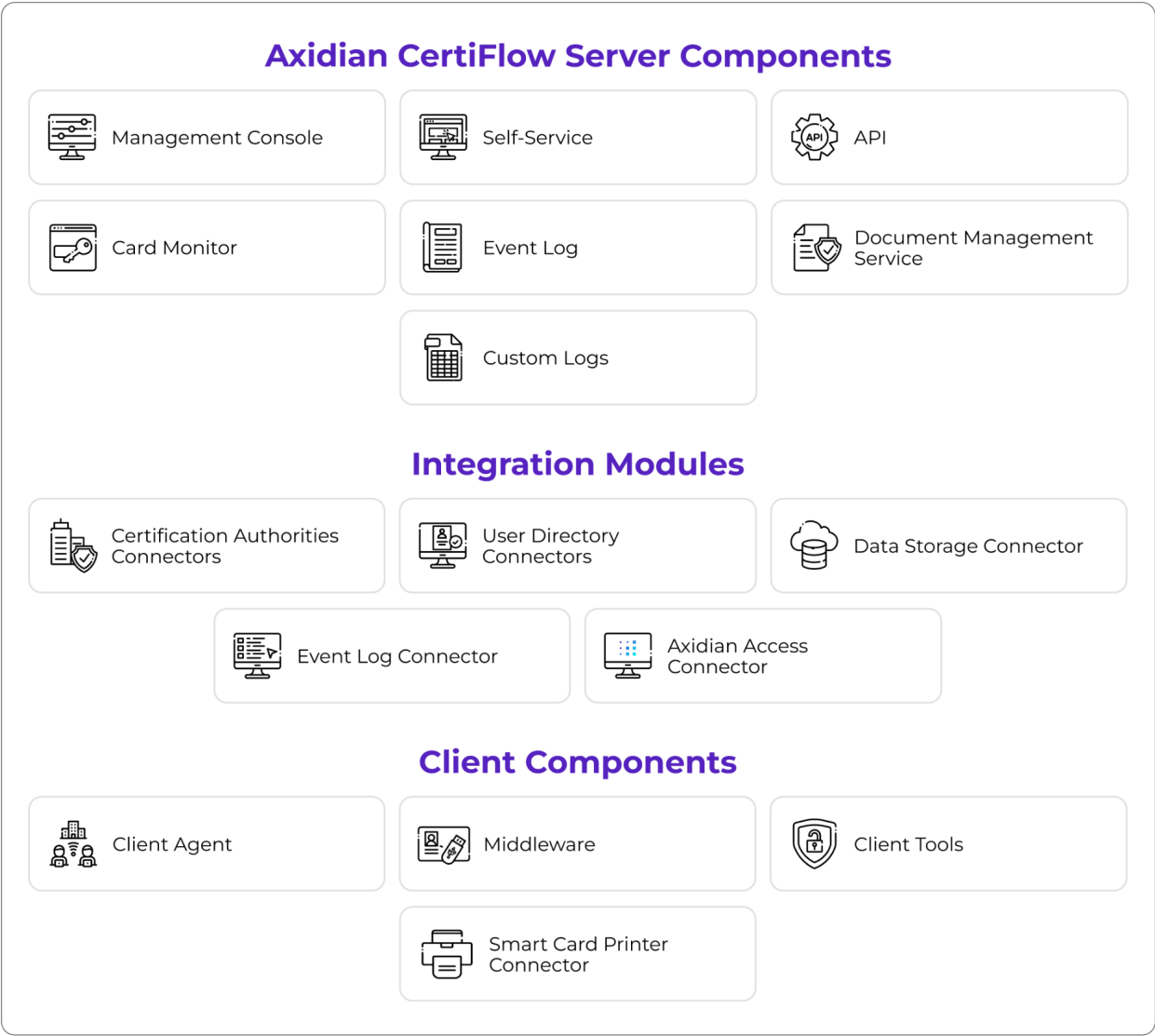
Monitoring of USB Token Usage on User PCs

With Axidian CertiFlow, companies can track which USB tokens or smart cards are connected to organizational PCs and who is connecting them. An administrator can assign a USB token / smart card to a specific user or PC. If the token/card is connected during an illegitimate user session or to an unauthorized PC, Axidian CertiFlow detects the violation and informs the administrator and/or blocks the user session and the token/card.

Axidian CertiFlow Architecture

The architecture of Axidian CertiFlow is built on a modular principle. Each module implements a specific set of functions to address a particular task. Depending on the company’s business needs, all modules or only selected ones can be installed.

Axidian CertiFlow consists of the following functional and software modules:



Axidian CertiFlow Architecture

Core Server Modules of Axidian CertiFlow

The server is the central component of the Axidian CertiFlow infrastructure, connecting all system modules. It enables centralized management of security policies, users, USB tokens, certificates, and documents. The server also performs USB token unlocking operations and event logging.

Management Console

The management console is a web application that provides administrators and operators with an interface for performing all PKI maintenance operations. System parameters can be distributed centrally via policies. These policies control certificate issuance, PIN codes, permitted self-service operations, and more.

In the management console, administrators can:

- Register and issue tokens and smart cards
- Search for certificates linked to a token/card and a user
- View audit logs
- Configure the role-based access model
- Monitor token and smart card usage through client agents
- Manage user documents

User Self-Service Tools

The self-service portal is a web application that allows users to independently manage their certificates, USB tokens and smart cards: issuing, revoking, renewing, changing PIN codes, and more. The set of available operations is determined by the administrator.

In their personal account, users have access to a list of their tokens and certificates, as well as a section for internal electronic document exchange with the administrator.

API

The Axidian CertiFlow Application Programming Interface (API) is used to manage users' tokens, smart cards and certificates from external systems, such as Identity Management (IDM) solutions.

The API provides functions to perform operations such as:

- Revoking, suspending, or resuming user certificates (for example, in cases of termination, vacation, or job change)
- Searching for USB tokens and smart using filters

Card Monitor

The Card Monitor service monitors the use of smart cards and USB tokens and performs the following operations:

- Revoking and withdrawing tokens and cards from users whose accounts have been deleted from the Axidian CertiFlow user directory
- Revoking temporary media whose validity period has expired
- Disabling devices and suspending certificates of users whose accounts have been deactivated in the user directory
- Deleting accounts from the Axidian CertiFlow directory when they have been disabled in the user directory
- Setting the status of certificates stored on a USB token or smart card (expiring/expired)
- Updating the contents of a token or smart card
- Logging the “Prolonged loss of connection with agent” event in the system log
- Removing agents that have been inactive for a configurable period of time
- Sending email notifications to system administrators and users:
 - Certificate expiration
 - Approval/rejection of token/card issuance or replacement
 - Approval/rejection of certificate renewal
 - Changes to the Axidian CertiFlow policy applicable to a user
 - Changes to user attributes in the resource directory

Event Log

The log records all events related to the lifecycle of USB tokens and smart cards, agent activity, Card Monitor operations, and changes to system parameters. In the management console, administrators can view the event log and generate reports based on various criteria.

Customizable Audit Logs

Audit logs contain data on USB tokens, smart cards and certificates, their owners, and the systems in which these media/certificates are used. The set of fields in the logs is configurable by the Axidian CertiFlow administrator.

Entries in the audit log are added automatically during issuance, replacement, withdrawal, or renewal of tokens and cards. Fields can also be filled in manually or using a reference directory.

Internal Electronic Document Management Service

With Axidian CertiFlow’s internal EDM service, administrators and users can exchange documents that support certificate management processes. These include copies of a user’s personal documents, applications for certificate issuance or revocation, printed certificate forms, and other reporting documents.

A user can request an electronic signature certificate via their personal account. The administrator checks whether the document complies with the organization's regulations, and the document is sent to the Certification Authority (CA). The CA operator verifies the submitted information and issues a certificate on the USB token or smart card.

Additionally, the document search section allows verification of original document availability and tracking of unsigned documents.

Integration Modules

Connectors to Certification Authorities

Axidian CertiFlow includes specialized connectors for integration with Certification Authorities (CAs). Using these connectors, Axidian CertiFlow can perform the following operations:

- Retrieve certificate templates
- Create and send certificate requests
- Approve certificate requests
- Issue certificates
- Suspend and revoke certificates
- Check certificate status

Axidian CertiFlow supports integration with the following Certification Authorities and electronic signature services:

- Microsoft Enterprise CA
- CAmelot

Connectors to User Directories

Axidian CertiFlow retrieves user information from a directory. Supported directory types include:

- LDAP directories (Microsoft Active Directory, FreeIPA)
- Internal user directories stored in Microsoft SQL or PostgreSQL databases

Connector to Data Storage

Axidian CertiFlow works with Microsoft SQL and PostgreSQL databases. The database is created manually, and scripts included in the Axidian CertiFlow distribution are used to populate it.

Connector to Event Audit Systems

Axidian CertiFlow can log events to:

- Local databases
- Windows Event Log
- MS SQL
- PostgreSQL
- Syslog servers (for SIEM system integration)

Centralized log storage reduces the labor costs of manual auditing, simplifies incident detection and investigation, and helps meet regulatory compliance requirements.

Connector to Axidian Access

The connector to the Axidian Access access management system automatically registers a USB token or smart card issued in Axidian CertiFlow in the Axidian Access database. This enables the user to immediately use their smart card or USB token not only for digital signature operations but also for accessing application information systems via Axidian Access Enterprise SSO.

Client Components

Client Agent

The Axidian CertiFlow Client Agent (hereafter – the agent) is designed for remote management, status monitoring, and usage control of users' personal USB tokens or smart cards. The agent is installed on user workstations together with Axidian CertiFlow Middleware.

The agent performs the following operations:

- Sends information to the Axidian CertiFlow server about the USB tokens and smart cards in use – indicating which PC the tokens and smart cards are currently connected to and which user is working on that PC
- Locks the Windows session or the USB token/smart card if usage rules are violated. For example, a token or card can be bound to a specific user account or PC; if the current user or PC does not match the assigned ones, the agent can lock the user session or the token/card.
- Resets/unlocks the user PIN of a token/card with a change request from the administrator
- Locks USB tokens and smart cards at the administrator's request

- Automatically registers USB tokens and smart cards in Axidian CertiFlow when connected to a PC and changes the PIN at the administrator's request
- Changes the user PIN on the token/smart card upon first connection (if the hardware supports this) or after a configurable period of time
- Automatically assigns a token/smart card to a user when connected to a PC
- Automatically issues USB tokens and smart cards assigned to a user or empty ones
- Updates certificates on USB tokens and smart cards
- Deletes information from USB tokens and smart cards
- Simultaneously performs wiping or initialization of USB tokens and smart cards and revokes them from the user
- Changes the administrator PIN on USB tokens and smart cards
- Logs the status of USB tokens and smart cards connected to a PC, recording the following events in the system log:
 - Presence of USB tokens or smart cards with a blocked user or administrator PIN
 - Attempts to enter incorrect user or administrator PINs
 - Connection of unregistered USB tokens or smart cards to a workstation

Thanks to the agent's functionality, administrators can audit the use of smart cards and tokens, as well as remotely perform operations with USB tokens and smart cards on a user's PC. The agent also helps prevent unauthorized use of USB tokens and smart cards.

Middleware for Working with USB tokens and smart cards

Axidian CertiFlow Middleware is a client component of Axidian CertiFlow installed on administrator and user workstations. Middleware performs operations that require direct access to the USB token or smart card, including:

- Setting and resetting PIN codes
- Key generation
- Certificate writing
- Initialization and other related tasks

Axidian CertiFlow supports working with the following USB tokens and smart cards:

- ACOS5-64
- ePass 2003
- ePasslet Suite, JCOP
- SafeNet eToken, IDPrime
- HID Crescendo
- ID-One Cosmo
- TikTok CARD V2/V3
- TPM Virtual Smart Card (VSC), Windows Hello for Business (WHfB)
- YubiKey 5 Series

Client Tools for Unlocking USB tokens and smart cards

Axidian CertiFlow Client Tools is a client component required to unlock devices used for authentication in the Windows OS in both online and offline modes, as well as to unlock devices not used for Windows login.

Smart Card Printer Interaction Module

The smart card printer interaction module significantly reduces the time needed to personalize and issue a large number of smart cards to employees. In a single batch operation, Axidian CertiFlow issues certificates, writes them to smart cards, and personalizes the cards by printing employee data on them.

Advantages of Axidian CertiFlow

Flexibility and Scalability

- Modular architecture for easy integration into existing infrastructure
- Simple expansion of platform functionality

Automation of PKI Infrastructure Management Processes

- Execution of operations with USB tokens and smart cards: registration in the system, user assignment, issuance, renewal, PIN change, wiping and initialization, blocking, and revocation
- Tracking the validity of certificates from integrated CAs as well as third-party certificates issued outside Axidian CertiFlow
- Managing certificates issued by different CAs in a unified system
- Remote unlocking of USB tokens and smart cards without physical access

Operational Cost Reduction

- Integration with third-party systems via API and remote management of USB tokens and smart cards
- User self-service for certificates, tokens and smart cards through a personal account
- Centralized management of documents supporting certificate-related processes via the internal electronic document management (EDM) service, including the ability for both users and administrators to electronically sign documents
- Reduced workload for the support department

Enhanced Information Security

- Full audit of operations
- Instant blocking and revocation of USB tokens and smart cards in case of loss or employee termination
- Centralized enforcement of PIN code policies and regular PIN updates
- Flexible role-based access control model
- Automatic enforcement of information security policies

Technical Support

- Comprehensive assistance at all stages of software implementation and operation
- Help with Axidian CertiFlow infrastructure planning, installation, configuration, and troubleshooting during operation

Axidian CertiFlow technical characteristics

Target operating systems	Windows 2008 and later versions Debian 9-11 Ubuntu 18.04 LTS - 20.04 LTS Red Hat Enterprise Linux 8-9
DBMS and storage systems	Microsoft SQL PostgreSQL
User directories	Active Directory
Certification authorities	Microsoft Enterprise CA CAmelot
CA operations	Obtain certificate templates Create and send out certificate requests Approve certificate requests Issue certificates Suspend and revoke certificates Check certificate status Create and update CA user data
Integration with infrastructure components	MFA SIEM (syslog) API Mail (SMTP) Smart card printers IdM solutions
Fault tolerance	Support for all scenarios including hierarchical management, distributed deployment, and fault-tolerant installation
Tokens	Removable hardware tokens Microsoft Windows NT Registry Trusted Platform Module (TPM) Microsoft Windows Hello for Business Axidian AirCard Enterprise
Removable hardware tokens	eToken (SafeNet) ESMART (SafeNetISBC) Yubikey (Yubico) ID Prime (Gemalto) ePass (Feitian)

About Axidian

Axidian delivers identity and access management solutions designed to enhance cyber resilience for organizations worldwide. With a strong presence in over 25 countries, Axidian has delivered more than 800 projects in access management (IAM), privileged access management (PAM), public key infrastructure (PKI) management, and identity threat detection and response (ITDR) solutions across various sectors.

If you have any questions about our products or need additional information, please visit axidian.com.

Our contacts

-  axidian.com
-  sales-europe@axidian.com
-  sales-mena@axidian.com
-  sales-asia@axidian.com
-  www.linkedin.com/company/axidian



**VOTRE PARTENAIRE
TECHNOLOGIQUE**
**POUR DES INFRASTRUCTURES IT
SÉCURISÉES ET PERFORMANTES**



EXPERTISE
Des solutions adaptées
à chaque environnement



CONFIANCE
Un partenaire fiable
à vos côtés



PERFORMANCE
Des infrastructures
sécurisées et évolutives



SUPPORT
Un accompagnement
technique de qualité



**WIRELESS
RADIO**
Connectivité sans fil
haute performance



**RÉSEAUX &
SÉCURITÉ IT**
Des réseaux fiables
et sécurisés



**VIRTUALISATION
CLOUD**
Des solutions Cloud
flexibles et évolutives



CYBERSECURITY
Protéger vos données
et vos systèmes



**VIDÉO
PROTECTION**
Solutions de vidéosurveillance
intelligentes



**HCI STORAGE
SAUVEGARDE**
Stockage, sauvegarde
et haute disponibilité



SOLUTIONS IT



CYBERSÉCURITÉ



CLOUD



INFRASTRUCTURE RÉSEAU



STOCKAGE



PROTECTION



**Département
Commercial**



Vous accompagne



HAFS NETWORKS WCA



+225 07 89 82 56 49 / +225 07 59 05 85 82



sales-ci@hafs-networks.com



HAFS NETWORKS FRANCE



+33 (0)7 49 92 62 57 / +33(0)9 73 89 20 39



sales@hafs-networks.com

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

