Axidian

WHITE PAPER

Axidian CertiFlow

Unified Management Of Public Key Infrastructure

Table of contents

Effective use of public key infrastructure **3**
- Axidian CertiFlow 3
  - Expenditure reductions 3
  - Improved security 4

Axidian CertiFlow composition **4**
- Basic modules 5
  - Axidian CertiFlow Server 5
  - Management Console 5
  - Self-Service tools 5
  - Card Monitor 6
  - API 6
  - Event Log 6
  - Axidian CertiFlow Policies 6
  - Custom Log 7
- Integration modules 7
  - Connectors to Certification Authorities 7
  - Connectors to User Directories 7
  - Middleware 7
  - Connector to Axidian Access 8
  - Connector to Smart Card Printer 8
- Additional Features 8
  - Client Agent 8
  - Axidian AirCard Enterprise 8

About Axidian **9**

Effective use of public key infrastructure

Public Key Infrastructure (PKI) offers a solution for many problems of information security:

- Replacement of obsolete password authentication by strict two-factor one for access to operating system and applications (VPN, VDI etc.);
- Digital signature and electronic correspondence encryption;
- Application of electronic signature to comply with regulatory requirements and to provide for legal document flow;
- Encryption of files, drives and other information.

However, the maintenance of public key infrastructure creates a number of new tasks:

- Issue user certificates according to their objectives: it is required to provide for necessary certificates on a user smart card. At the same time, excessive certificates should be avoided.
- Management of device user PIN codes: PIN complexity policies, change interval;
- Tracking of certificate validity terms and timely update of the former;
- Smart card and USB token accounting, assignment of those to employees;
- Unlocking of locked devices when a user forgot his or her PIN code.

Effective use of PKI is not possible unless the mentioned tasks are solved adequately. For this, special software of the Card Management System (CMS) is used.

Axidian CertiFlow Manager

Axidian CertiFlow is a CMS software which provides a centralized system for managing the public key infrastructure. Axidian CertiFlow allows for bringing the PKI usage processes into compliance with the needs of business units, IT department, security service and external regulatory authorities.

Expenditure reductions

Axidian CertiFlow is intended to reduce company expenditures for routine PKI maintenance operations:

- Certificate issuance. Axidian CertiFlow automatically generates the list of certificates to issue based on PKI usage policy mechanism. All users that fall within a single policy get an identical set of parameters and certificates. The operations of certificate request creation, certificate issue and writing those to security devices (smart card, USB token, TPM VSC or WHfB) are performed in automated mode.

- The Axidian CertiFlow contains a self-service cabinet for common users, implemented as a web application. With self-service, the users can issue and update certificates on their own, if this is allowed by the policy. This reduces the workload of the IT department.

- Axidian CertiFlow can send email notifications of certain system events to the Axidian CertiFlow system administrators and users: Say, administrator and/or user receives a notification of the certificate being about to expire. This allows for timely updates of the latter, thus avoiding downtime.

- Axidian CertiFlow also allows for unlocking locked smart card without addressing the administrator. Such unlocking can be performed either before or after user logon, as well as with or without explicit participation of the administrator.
- The Axidian CertiFlow provides a software interface (API) to integrate to third party systems. The integration expands the Axidian CertiFlow capabilities in the sphere of automation of certificate and security device usage processes. For example, Axidian CertiFlow can revoke the certificate of a dismissed employee upon an event from the Identity Management class system.
- Accounting of certificates issued by third parties. If the organisation uses certificates issued by third party certification authorities, the Axidian CertiFlow allows for adding those certificates to the database and provides for timely reminder to administrator and user of certificates being about to expire. This allows to avoid downtime when working with banks and trade platforms.

Improved security

Axidian CertiFlow increases the overall information security level of a company due to the following:

- Centralized PIN code policies. When a security device is issued, it has PIN requirements written to it: complexity, change interval, history depth etc. The available parameters depend on the device model. The policies are stored and distributed centrally. The administrators do not need to configure policies for every single smart card.
- Security device accounting. Each device - smart card or USB token - is assigned to an employee responsible for it. Only the Axidian CertiFlow administrator or the device owner can issue or update certificates for the device.
- Timely revocation of dismissed employees' certificates. In order to disallow access of dismissed employees to corporate resources promptly, the Axidian CertiFlow contains a special service that checks the user directory through at defined intervals and revokes certificates of users marked as dismissed.
- Flexible configuration of privileges Axidian CertiFlow allows companies to define their own security roles with a configurable list of allowed operations. It makes it possible for administrators to bring the Axidian CertiFlow role model into compliance with the company business processes.
- Control of security device usage at users' PCs. Axidian CertiFlow allows for tracking of what security devices are connected to company computers and by whom. Administrator can assign a certain security device to a certain user or PC. If the system discovers a discrepancy (say, a smart card is connected within a session of another user or to a disallowed PC), then the security device might be locked.

Axidian CertiFlow composition

The Axidian CertiFlow architecture is based on the modular concept. Each of the modules implements a certain set of functions to solve a certain task. You can install all modules or select only the required ones. It depends on the company's business needs. Axidian

CertiFlow consists of the following software and functional modules:

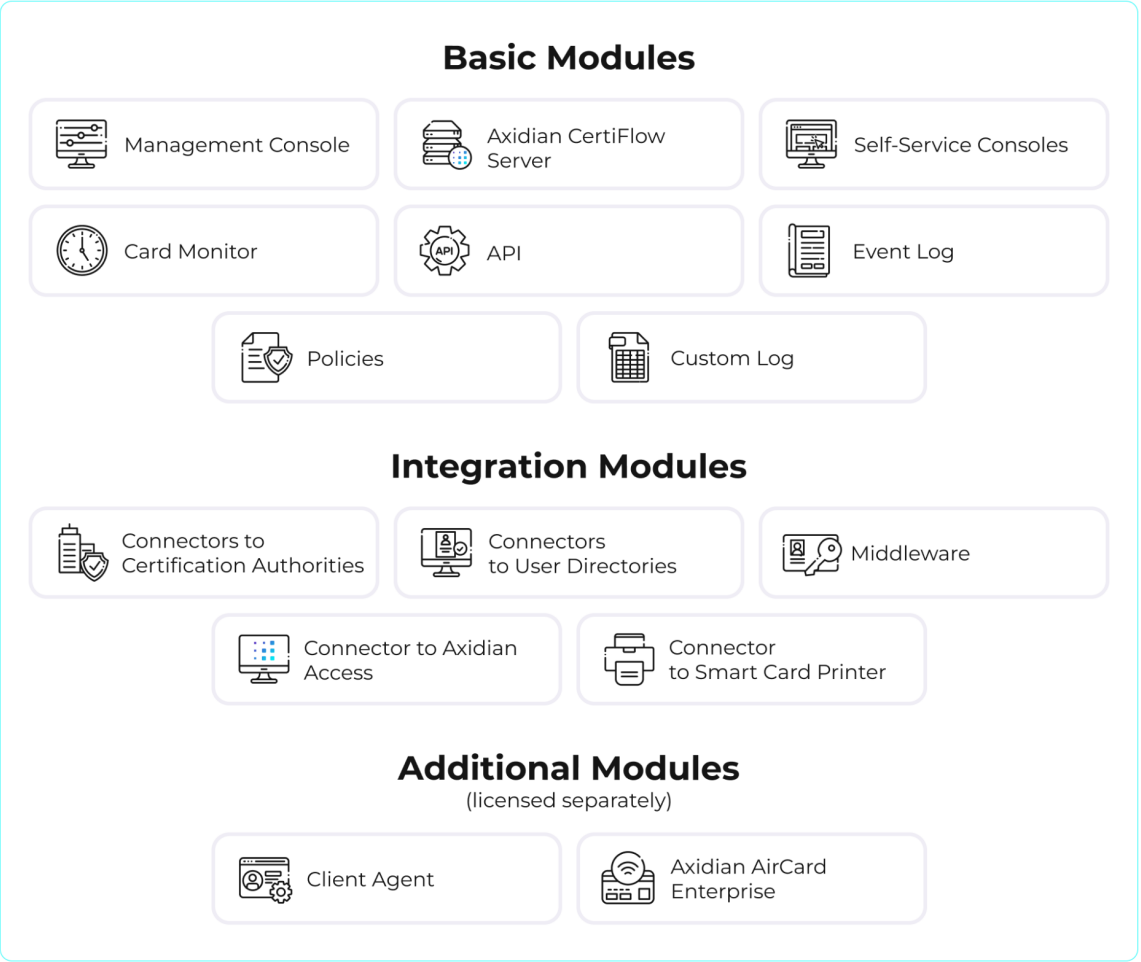

Figure 1. Axidian CertiFlow composition

Basic modules

Axidian CertiFlow Server

The server is the main component of Axidian CertiFlow infrastructure that links all the system modules together. It is an ASP.Net application, operating on Internet Information Services (IIS) server. The Axidian CertiFlow server provides centralized management of system users, card repository and security policies. The server also provides card unblocking operations, as well as event logging.

Management Console

The Management console is implemented as a web application that provides administrators and operators with an interface to perform all PKI maintenance operations: edit security device and certificate usage policies, perform registration and issue of devices, view logs and device storage, configure role model, and card usage control via client agents.

Self-Service tools

Self-Service tools include:

- Self service - a web application that is available to system users. This application allows users to perform operations with certificates and security devices on the user's own: issue, revocation, update, PIN code change, etc. The set of available operations is defined by the system administrator.
- Credential Provider is a module installed to a PC. It allows for unlocking of security devices at user workplace in online or offline mode without logging in to the operating system.

Card Monitor

The Card Monitor service is intended for operations of controlling smart card and USB token usage. The service performs the following operations:

- Revocation of security device and certificates of dismissed employees
- Revocation of expired temporary smart card
- Deactivation (optional) of devices and revocation of certificates for the users, whose Active Directory accounts are disabled
- Removing accounts (optional) from the Axidian CertiFlow user directory whose Active Directory accounts have been disabled
- Status setting for certificates stored on security device (about to expire/expired)
- Update of security device contents
- Agent inactivity timeout event registration in the system log
- Sending of email notifications to the system administrators and users:
    - User certificate expiration
    - Security device issue approval / rejection
    - Approval or rejection of renewal for certificates
    - Approval or rejection of security device replacement
    - Changing user attributes in the user directory
    - Change of Axidian CertiFlow policy applying to user

API

Axidian CertiFlow API is used to manage security devices and certificates of users from external systems, such as Identity Management (IDM). API provides for functionality required for the following scenarios:

- Automatic assignment of PKI usage policy to a user (what certificates are to be issued, what operations with security devices are available to the user, etc.)
- Automatic revocation, suspension and reactivation of user certificates (say, in case of dismissal, leave or change of position).

Event Log

The log registers all the events associated with smart card life cycle, operation of agents and Card Monitor service, as well as system parameters' modification. The log can be viewed in the Axidian CertiFlow administrator console. Reports can also be generated in the console.

Axidian CertiFlow Policies

Axidian CertiFlow Policies define the behavior of the system and allow to centrally distribute the work settings. Policies contain data such as the list of certificates to issue, PIN policies, allowed self-service operations, and more.

Custom Log

The custom logs contain data about devices, certificates and their owners. The set of required fields is configured by the administrator in the Configuration Tab.

Log entries are automatically logged when issuing, replacing, withdrawal or updating smart cards in the Axidian CertiFlow Management Console or Self-Service.

Integration modules

Connectors to Certification Authorities

The Axidian CertiFlow has special connectors to communicate with certification authorities (CA). Axidian CertiFlow performs the following operations using these connectors:

- Receiving certificate templates
- Creation and sending of certificate requests
- Certificate request approval
- Certificate issue
- Certificate suspension and revocation
- Certificate status checking

Axidian CertiFlow supports Microsoft CA and CAmelot - Cryptovision as certification authorities and digital signature service.

Connectors to User Directories

Axidian CertiFlow receives information about users from external directory. Microsoft Active Directory user database can be used as user directory

Middleware

Axidian CertiFlow Middleware is the client side software installed to administrator and user workstations. Middleware provides for execution of operations that require access to security devices: set and reset of PIN code, key pair generation, writing of certificates, initialization etc. Axidian CertiFlow supports the following security devices:

- ACOS5-64, by ACS
- ePass 2003, by Feitian
- ePasslet Suite, JCOP, by Cryptovision
- eToken, ID Prime, by Thales
- HID Crescendo, by HID
- ID-One Cosmo, by Bit4id
- Axidian AirKey Enterprise Virtual Smart Card
- TicTok CARD V2/V3, by CRYPTAS
- TPM Virtual Smart Card (VSC), Windows Hello for Business (WHfB), Windows

Registry, by Microsoft
- YubiKey 5 Series, by Yubico

Connector to Axidian Access

The connector to Axidian Access automatically registers the smart card issued in Axidian CertiFlow in the Axidian Access database. After that the user can immediately use the smart card or USB token not only for digital signature operations, but also to access the informational systems using Axidian Access Enterprise SSO.

Connector to Smart Card Printer

Connector to special smart card printers allows for significant reduction of time spent on personalization and issue of large numbers of smart cards for employees. The Axidian CertiFlow makes it possible to issue the certificates and write them to smart cards, as well as personalize the cards by printing the card owner data on the card within a single operation.

Additional Features

Client Agent

The client agent is installed onto user PCs and is used to control usage of smart cards, USB tokens and certificates on workplaces. The agent performs the following operations:

- Sends the data on the security device used to the Axidian CertiFlow server - what PC the token or smart card is connected to and who exactly is working on the PC.
- Locks Windows session or security device, if usage rules are violated. E.g., a smart card might be assigned to a user account or PC. If the user or PC does not correspond to the preset one, the agent might lock the smart card.
- Reset/unlock the user's PIN code with its change on the requirement of the administrator.
- Smart card lock upon the administrator request
- Update of certificates on the smart card.
- Monitoring the statuses of connected devices to the workstation.
- Deleting data from the security device.

Thus, the agent allows the administrators to audit smart card and token usage, as well as to perform operations with security devices remotely on a user PC. The agent also can prevent unauthorised use of the smart card.

Axidian AirCard Enterprise

Axidian AirCard Enterprise is the software implementation of a smart card, that lets a user to perform the same operations as the hardware smart card does:

- digital signing of documents;
- data encryption and decryption;
- two-factor user authentication (operating system logon is also supported);

- operations according PKCS#11 standards;
- provision of access in Single Sign-On mode.

Axidian AirCard Enterprise simulates hardware smart card behavior completely. For the operational system of the PC and for target applications the user works with, the Axidian AirCard Enterprise is indistinguishable from a traditional smart card. The Axidian AirCard Enterprise operation is based on correspondence to standard protocols, interfaces and mechanisms of PKI infrastructure. The private keys are not sent to the user PC but stored in the database of Axidian AirCard Enterprise server in encrypted form. Cryptographic operations are performed at the server within system processes of Axidian AirCard Enterprise server. To provide for security, the communication channels between user PC and the server are encrypted using asymmetric encryption algorithms. The encryption protocol is TLS. Only the result of cryptographic operation is sent to the user PC (public key, signed or decrypted data).

The Axidian AirCard Enterprise has the following advantages as software implementation of smart card:

No hardware components. Plastic smart cards or USB tokens can be broken, lost or left behind. They also require periodic replacement. Virtual smart cards have none of the mentioned disadvantages.

Execution of cryptographic operations at server.
The private key is not stored at the client side. Therefore it cannot be compromised by malware or intruders.

Full control of usage by informational security specialists. All operations of issue, revocation and connection of virtual smart card to a user PC are logged in the system log. Informational security specialists can stop usage of Axidian AirCard Enterprise smart card by revoking the card remotely and deleting the private keys.

Remote delivery of smart card to a user. Virtual smart cards are delivered to a user PC remotely without his or her participation. A user does not have to obtain the card in person from the system operator. The Axidian AirCard Enterprise appears in the operating system of the user PC as soon as the operator issues it at his/her workplace.

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.