System Requirements

Pecunia 7

Formblatt U 270 020222

Table of Contents

General Information

Pecunia 7 is a web-based application that is used via a browser and operated on the company's own infrastructure (on-premises).

The core system of Pecunia 7 is not hosted by ALVARA Digital Solutions GmbH. Operation is the sole responsibility of the customer, either on the customer's own infrastructure or through an external hosting service provider of their choice.

All hardware, servers, virtual environments, and the required operating systems, such as Windows operating systems for servers and workstations, Microsoft SQL Server, Apache, internet access, etc., referred to in this document must generally be procured, operated, and maintained at a technically sufficiently up-to-date level by the user.

The use of other operating systems, database servers, or a system configuration below the specified minimum requirements may lead to undesired side effects and errors. Please note that in such cases there is no entitlement to support and the warranty becomes void.

Supported Web Browsers

The Pecunia 7 application is a web application. For security, compatibility, and performance reasons, we always recommend using current browser versions.

The following browsers are supported:

- Chrome
- Firefox
- Edge

End Devices and Operating Systems

The application is optimized and approved for use on the following end devices:

- Desktop and notebook PCs
  - Operating systems: Windows 10 or higher, Linux
  - optimized display
- Tablet devices
  - Operating systems: iPadOS and Android, each in the current version

Use on smartphones is not approved due to the screen size and limited usability. Display and functional errors may occur when used on smartphones. Support is not provided for this use case.

Mobile Apps

Pecunia 7 is not provided as a native application (app) for Android or iOS. Access is exclusively via a supported web browser.

Serial Interfaces

When connecting counting machines with a serial interface, please note that FAT clients are required for this purpose. The use of built-in expansion cards with serial interfaces has not proven effective in practice. We recommend installing specific models of USB-to-serial converters.

Database Server

The following virtual servers are required for operation in the customer's own data center. We recommend the following reference values. In general, sizing depends on the size and performance requirements of the cash center. We recommend setting up the servers as virtual machines so that the systems remain scalable and resources can be added at any time.

- MS SQL databases: 4 vCPU, 32 GB vRAM, 250 GB, 650 GB for log and backup
- Application Server: 4vCPU, 16 GB vRAM, 80 GB

MS Windows Server as well as Linux can be used as the operating system.

At least SQL Server 2019 is required for the MS SQL Server.

Secure Access to Pecunia 7

Pecunia 7 is delivered from the server as a so-called “single-page app”. For secure and reliable operation of the web application on the intranet, we recommend the following measures. We recommend delivering the web application exclusively via HTTPS (HyperText Transfer Protocol Secure), even within the internal network (intranet).

HTTPS Encryption

Why HTTPS is important even on the intranet:

- Encryption: HTTPS protects data transmission against unauthorized access or manipulation.
- Trust: Avoids browser warnings about insecure connections.
- Future readiness: Many modern web functions require HTTPS.

A valid TLS/SSL certificate is required in order to use HTTPS. This certificate signals to the browser that the connection to the application is secure and trustworthy.

Although it is technically possible to use so-called self-signed certificates, we expressly recommend using publicly signed certificates, even on the intranet.

Benefits of Official Certificates

✅ No security warnings in browsers or applications.

✅ Automated renewal, e.g., with Let's Encrypt.

✅ Future-proof for later network extensions.

Disadvantages of Self-Signed Certificates

⚠️ Must be manually trusted on all devices.

⚠️ Increased maintenance effort and susceptibility to errors.

⚠️ Less scalable for larger numbers of users.

In a typical architecture, the web application does not run directly in public, but is delivered via a reverse proxy. This proxy not only forwards requests, but can also centrally handle certificate management.

Benefits of This Separation:

✅ Simplified HTTPS configuration: The certificate is integrated only in the reverse proxy, not in the application itself.

✅ Centralized management: For multiple internal services, a single certificate in the proxy is sufficient.

✅ Application remains unchanged: No changes or configuration within the application are required.

✅ Better separation of responsibilities: IT can operate the proxy and certificate while the application remains isolated.

Use of a Reverse Proxy

The reverse proxy listens on port 443 (HTTPS) and can also hold the certificate if required. It decrypts the HTTPS connection and forwards requests internally in unencrypted form to the application, for example on port 3000. Pecunia 7 runs by default on a configurable port (here 3000) and expects internal HTTP requests. A reverse proxy is required for normal web access via port 80 (HTTP) or port 443 (HTTPS).

Product Variants

Apache HTTP Server

- ✅ Flexible due to its module structure, e.g., mod_proxy.
- ✅ Well suited if already in use.
- ⚠️ Slightly more heavyweight than NGINX.

NGINX

- ✅ High performance, widely used.
- ✅ Good HTTPS support, including Let's Encrypt.
- ⚠️ Configuration is file-based and may initially appear technical.

Caddy

- ✅ Automatic HTTPS setup with Let's Encrypt.
- ✅ Very simple configuration.
- ⚠️ Not yet as widely used – smaller community.
- ⚠️ Some features require a commercial license.

As an example, the implementation with Apache and mod_proxy as well as certificates from Let's Encrypt is shown below.

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
  ServerName   pecunia.intranet.cloud
  ServerAlias  pecunia.intranet.cloud

  ProxyPreserveHost On
  ProxyPass        / http://localhost:3000/
  ProxyPassReverse / http://localhost:3000/

Include /etc/letsencrypt/options-ssl-apache.conf
SSLCertificateFile /etc/letsencrypt/live/intranet.cloud/cert1.pem
SSLCertificateKeyFile /etc/letsencrypt/live/intranet.cloud/privkey1.pem
SSLCertificateChainFile /etc/letsencrypt/live/intranet.cloud/chain1.pem

</VirtualHost>
</IfModule>
```

The specific technical implementation, e.g., selection and installation of the reverse proxy and automation of the certificate infrastructure, is the responsibility of the customer. If required, we will be happy to advise on the selection of suitable solutions.

Monitoring

It is strongly recommended that the availability of the Pecunia 7 service and any required additional services be monitored in a monitoring platform, such as Nagios.

Pecunia Count Service

Workstations connected to counting machines require the Pecunia Count Service (PCS). The Count Service is provided as a Windows installation package.

The following operating systems are supported:

- Windows 10
- Windows 11

If counting machines with serial interfaces are used, FAT clients are required as workstation computers. The use of built-in expansion cards with serial interfaces has not proven effective in practice. We recommend using USB-to-serial converter models with an FTDI chipset.

For further information, please refer to the separate instructions for the Pecunia Count Service.

Supported Peripheral Devices

Counting Machines

Machine-specific serial connection cables or LAN connections are required to connect a counting machine to a workstation. The user is responsible for providing the connection cables. Pecunia 7 includes a library of counting machine drivers.

The following banknote and coin counting machines are supported:

Banknote Counting Machines

Manufacturer	**Device Name**	**Version**
Cummins Allison	JetScan	1.2.0
G & D	Numeron	1.2.0
Glory	GFR-220	1.2.0
	GFS-220	1.3.1
	UW-F	1.2.0
Hitachi	iHunter 110	1.2.0
Newton	3 / 4 / V / F(+)	1.2.0
Hyundai	MIB9	1.2.0
South Automation	*K6*	*Version planned*

Banknote Counting Machines (Large-Scale Counting Technology)

Manufacturer	**Device Name**	
G & D	BPS M5 / M7 / C4 / C5	1.2.0

Coin Counting Machines

Manufacturer	**Device Name**	
ScanCoin / Suzohapp	ICP-Active 9 / SC4000	1.2.0
	SC4000	1.2.0
	Contovit S2 / Conto / Sorto / Vit / Fax / Rex	1.2.0
	DTC1	*Version planned*
Cummins Allison	*JetSort*	*Version planned*

South Automation	*Evosort H9*	*Version planned*
NGZ Cash Automation	*NGZ Q12*	*1.2.0*
Procoin	*PRC 420*	*Version planned*

If you have any questions regarding the approval of additional counting machines, please contact our support team.

Video Systems

The network in which the video system is integrated must be reachable from the counting workstation. Data is transmitted via UDP tickets.

The following video systems are supported:

- Geutebrück GCore
- MAKU
- TimeLine video systems

Keyboard Scanners

To make it easier to capture Safebag or seal numbers in Pecunia 7, a keyboard scanner may be used. Procurement is the responsibility of the customer.

The following scanners are recommendations from ALVARA Digital Solutions GmbH:

Manufacturer	Model
Datalogic	Gryphon I GM410X
	Gryphon I GM4102 (wireless)
	Gryphon I GD4132 (wired)

Android-Based Scanners

For the use of the Pecunia 7 products

- MobiTour
- MobiTick

the following hardware is approved in combination with the specified Android version of the operating system.

Scanner	**Android Version**
Datalogic Memor 10	from 8.x
Datalogic Memor 11	from 11.x
Panasonic FZ-N1	from 8.x
Zebra TC 26	from 10.x
Zebra TC 27 / 57x / 77 / 78	from 11.x
Chainway C66	from 11.x

If you have any questions regarding the approval of additional hardware, please contact our support team.

Mobitour/Mobitick

Operation of Mobitour/Mobitick requires an externally accessible HTTPS-based URL, which must be configured externally in the firewall and can also access the Mobile Backend Service via the reverse proxy.

Printers

A4 Printers

All DIN A4 printers with Windows drivers can be connected to Pecunia 7. The printers can either be connected locally to the workstation or set up as network printers.

Label Printers

All label printers with Windows drivers are supported and can be used with Pecunia 7.

Mobile Printers

The scanner apps support the Bixolon SPPR200 and the Zebra ZQ210.

Communication / ICC-Connector

The ICC-Connector acts as the interface between the ALVARA ICC web portal and Pecunia 7 and runs as a central Windows service on the server.

Data is exchanged in both directions. An HTTP/HTTPS connection is used for communication between the ICC-Connector and ICC.

The required access data, including the security key for each cash-in-transit provider, is assigned and provided by ALVARA Digital Solutions GmbH.

Additional requirements:

- Internet access with the following firewall approvals:

IP Address Range	**Port(s)**
87.234.35.1/29 85.239.114.216/30	TCP/80, TCP/443
87.234.35.1/29 85.239.114.216/30	TCP/2680, TCP/8080, TCP/8088

- Active connection to the IP addresses:
    - Customer test environment:
        - 87.234.35.1 255.255.255.248
        - DNS kundentest.alvara.de

- Production environment:
  - 85.239.114.216 255.255.255.252
  - DNS icc.alvara.de / DNS: as-app.alvara.de

– For all DNS entries, please note that all IP addresses of the target network may be delivered via DNS round robin. Therefore, the complete networks must always be approved.
– Proxy server: none or HTTP (SOCKS is not supported)

License Model

For the Pecunia 7 product, one license is required per cash center; this means that the product can be used on any number of workstations within one cash center.

For counting workstations, one license is required per workstation; this means that the product may only be used on the contractually agreed number of workstations.

Licenses for the use of the apps can be purchased per device. Billing is carried out monthly per app used.

The customer of ALVARA Digital Solutions GmbH is responsible for purchasing and maintaining an MS SQL license.

In addition, the customer of ALVARA Digital Solutions GmbH does not incur any further costs for the purchase and maintenance of third-party systems used by Pecunia 7.

Remote Maintenance

To facilitate support, ALVARA Digital Solutions GmbH may provide remote maintenance via TeamViewer access.

Remote maintenance is carried out using the current released version of the TeamViewer application.