Requirements

Data Preparation and Key Management Subsystem Main Technical Requirements

03.49.30

15.06.2020

Contents

Warnings and information are marked as follows:

Warnings about potentially hazardous situations or actions.

Messages with information about important features, additional options, or the best use of certain system functions.

1. Architecture of Data Preparation and Key Management Subsystem

Architecture of the data preparation and key management subsystem is shown in Fig. 1.

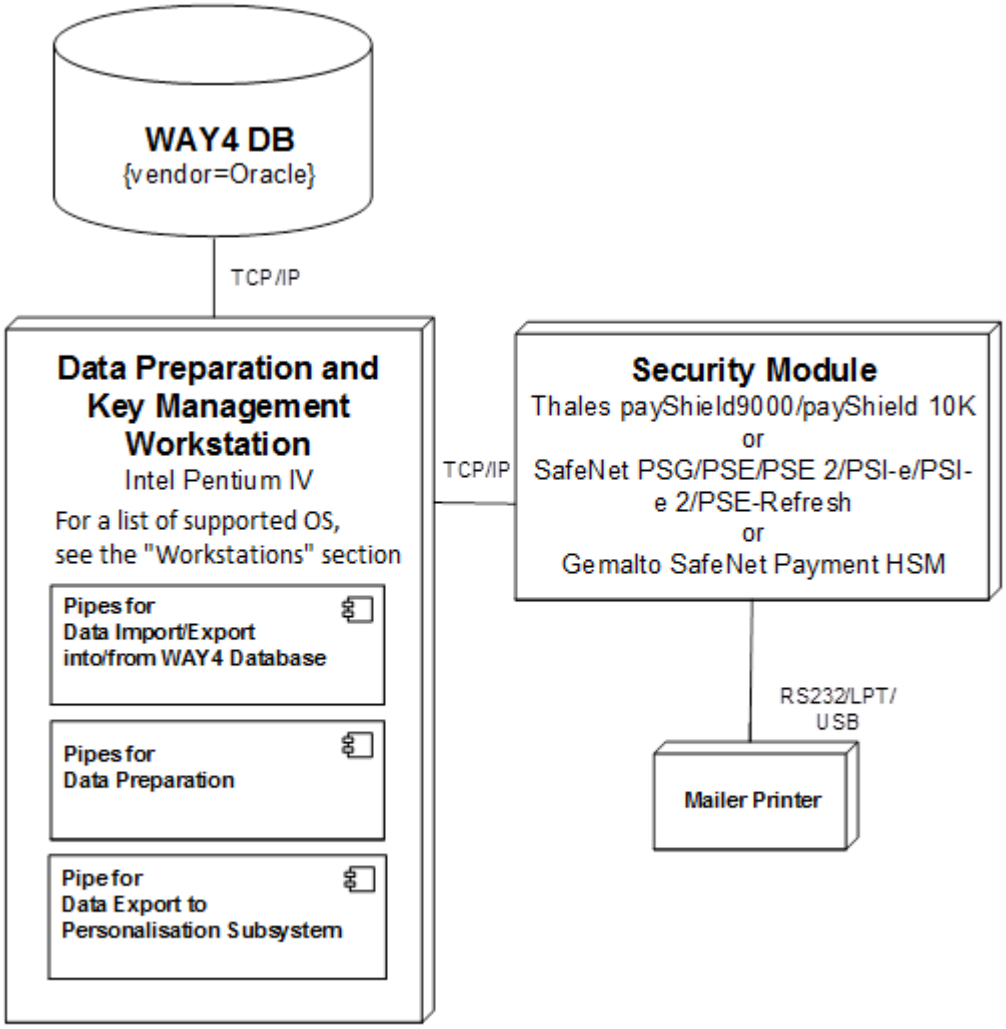

Fig. 1. Architecture of the data preparation and key management subsystem

2. Hardware Requirements

These are general requirements. They may be more precisely defined in the course of analysis performed while implementing the WAY4 system or while upgrading servers. The requirements assume the standard configuration required for issuing 100,000 cards.

2.1 Database Server

System architecture

Unix platform compatible with Oracle Database

Processor

2 or more

RAM capacity

2 GB or more

Magnetic disk capacity

Two 20 GB or more internal disks, hardware- or software-programmable RAID1

Backup capacity

Any that ensures regular backup of volumes corresponding to the size of the disk subsystem

Software capability

The hardware must be certified for Oracle Database and the Unix platform

Local area network

At least 100 Mbit Ethernet

Other equipment

DVD/CD-ROM drive

Quantity

1 set of equipment

2.2 Encryption Hardware

To perform cryptographic operations while preparing data for smartcard personalisation, a hardware encryption device must be installed in the system.

The data preparation and key management subsystem supports two types of encryption devices:

- Thales PayShield 9000 or payShield 10k;
- SafeNet PSG/PSE/PSE 2/PSI-e/PSI-e 2/PSE-Refresh

2.2.1 Thales (payShield) Encryption Hardware

2.2.1.1 System architecture

Thales payShield 9000 or payShield 10k with TCP/IP network adapter.

2.2.1.2 Software Environment

To produce EMV cards on payShield 9000 one of two configurations can be used:

1. For Smart Card Issuer Firmware version 1119-09xx, the following licenses are required:
   - HSM9-PAC301 Standard Base Package;
   - HSM9-LIC002 RSA license;
   - HSM9-LIC509 Russian CIF custom software for payShield 9000.

2. Starting from WAY4 Cards version 03.38.30, Thales payShield 9000 with basic firmware (HSM9-LIC001 Base Firmware, version 2.2a or later) and set of licenses is supported:
   - HSM9-LIC002 RSA License;
   - HSM9-LIC011 Magnetic Stripe Contactless Card Data Preparation License;
   - HSM9-LIC016 EMV based Card Data Preparation License;
   - HSM9-LIC024 Magnetic Stripe Issuing;
   - HSM9-LIC027 PIN and Key Printing License.

To produce EMV cards on Thales payShield 10k, a Premium license package and 1.0c firmware is required.

2.2.1.3 Quantity

2 (main and backup)

2.2.2 SafeNet (ProtectServer) Encryption Hardware

2.2.2.1 System architecture

Control module for PSG/PSE (OWSeM) version 4.17.075 or later (for devices with one COM port - PSI-e/PSE-Refresh, version 4.17.079 or later).

Any of the following devices may be used as a hardware platform:

- SafeNet ProtectServer Gold (PSG)
- SafeNet ProtectServer External (PSE)
- SafeNet PSE-Refresh (with one COM port) in the mode for manual entry of LMK without the use of a smart card
- SafeNet PSI-e (with one COM port) in the mode for manual entry of LMK without the use of a smart card
- SafeNet PSE 2 in the mode for manual entry of LMK without the use of a smart card

- SafeNet PSI-e 2 in the mode for manual entry of LMK without the use of a smart card

2.2.2.2 Software Environment

Firmware is encryption device software. The following Firmware versions may be used:

- v.2.04.xx
- v.3.00.xx

> ⚠ The use of Firmware versions v.2.06.xx/ v.2.07.xx is prohibited due to a fatal error in operation with the printer port.

The following Cryptoki (ProtectToolkit C (Runtime)) versions may be used:

- for internal (PCI) devices: v.3.28 to v.4.00
- for external devices – not used

DOM (Disk-On-Memory) Image is software for a server that includes an encryption device. The following DOM Image versions may be used:

- for internal (PCI) devices– not used
- for external devices: v.2.00

2.2.2.3 Quantity

2 (main and backup)

2.2.3 Gemalto (LUNA EFT 2) Encryption Hardware

2.2.3.1 System architecture

Gemalto LUNA EFT 2 with TCP/IP network adapter.

2.2.3.2 Software Environment

To produce VISA PayWave and Mastercard PayPass EMV cards on Gemalto LUNA EFT 2, firmware version 6.10.5 is required with SafeNet Luna EFT Payment HSM 2.2.0 software installed.

2.2.3.3 Quantity

2 (main and backup)

2.2.4 Additional hardware

RS-232-C (DTE)-compatible terminal. Data transfer rate from 300 bits per second (upgradable to 115200 bits per second).

The terminal must be not able to save information for subsequent output.

- Cable to connect the terminal to the encryption device, according to the vendor's specification.
- Terminal compatible with RS-232-C (DTE). Data transfer rate from 300 bps (with the ability to increase to 115200 bps).

Number of terminals: 1

For SafeNet PSG/PSE: ASCII PIN mailer printer with serial RS-232-C (DCE) interface (not parallel). Data transfer rate from 300 to 38400 bits per second.

For Thales payShield 9000 or Thales payShield 10K,a PIN mailer printer with a USB interface can be used. It is possible to use printers with a serial RS-232 (DCE/DTE) or parallel LPT interface through a USB-COM, USB-LPT adapter.

An impact printer (e.g. matrix or character output) or a special laser printer for PIN mailers must be used.

The printer must be able to print without a typing ribbon to keep secret information contained in PIN mailers. Sprocket paper must be advanced by a sprocket roller mechanism (not a friction one) to justify text lines and columns.

Cable to connect the terminal to the encryption device, according to the vendor's specification (for printers with a serial interface - taking into account the complete RS-232 specification).

For Gemalto LUNA EFT 2,a PIN mailer printer with a USB/ Serial interface can be used, which meets the technical requirements of the cryptographic device manufacturer.

Number of printers: 1

> ⚠ The capabilities of a particular hardware model must be clarified with its vendor.

2.3 Operator's Workstation

System architecture

Personal computer with Intel PC Pentium IV processor or higher

1 GB or more RAM

20 GB or more hard disk

Monitor with resolution no lower than 1024x768

Keyboard, mouse

Ethernet network interface

Quantity

2 (the number of workstations depends on the number of used personnel).

For the data preparation and card production subsystem, it is recommended to use a dedicated workstation.

3. Software Requirements

3.1 Database Server (Software Requirements)

Unix operating system (depending on hardware platform).

Oracle Database Standard Edition or Oracle Database Enterprise Edition.

Supported versions of Oracle Database:

- Oracle 12c 12.1.0.2 with mandatory installation of the latest PSU (Patch Set Update) and patch 21068213 (ORA-04043).
- Oracle 12c 12.2.0.1 with mandatory installation of the latest RU (Release Updates), patches 27539876 and 24850493 (Doc ID 2463589.1).
- Oracle 18c with mandatory installation of the latest RU.
- Oracle 19c with mandatory installation of the latest RU.

Backup software.

3.2 Workstations

The following Microsoft Windows versions are supported:

- Windows 7.
- Windows 8.
- Windows 8.1.
- Windows 10.
- Windows Server 2008 R2.
- Windows Server 2012 and Windows Server 2012 R2.
- Windows Server 2016.
- Windows Server 2019.

For the data preparation and card production subsystem, it is recommended to use a dedicated workstation on which other processes are not run: neither WAY4 processes nor processes requiring a large number of input/output operations and/or computing resources (including with the use of virtual machines).

It is recommended to increase the memory of the java machine for the workstation to 1024 MB. Contact WAY4 Customer Support for instructions on configuring memory.

In addition, it is recommended to use standard WAY4 directories (<OWS_HOME>, <OWS_WORK> and <OWS_TEMP>), located on the local machine; it is also recommended to put the <OWS_WORK> and <OWS_TEMP> on an SSD. Use of network disks is not recommended.

Oracle JDK (the required version and installation description, see the document "Oracle Java Commercial Updates for WAY4 ™").

Oracle Client for the corresponding Windows operating system version, including ODBC Driver.

Supported versions of Oracle Client: 12.1, 12.2, 18.3 and 19.3 (for Oracle Database 12c 12.2, Oracle Database 18c and Oracle Database 19c).

When using a 64bit operating system:

- The 32bit version of Oracle Client must be installed; otherwise it will be impossible to use ODBC.
- The ODBC source in a 64bit operating system is configured by running C:/Windows/SysWOW64/odbcad32.exe (32bit version of ODBC Administrator tool), and not from the Control Panel.

On the "Workarounds" tab in the Oracle ODBC Data Source configuration, it is necessary to set the flag in the "Bind TIMESTAMP as DATE" field. Otherwise, some SQL requests executed from DB Manager and including date conditions may be executed slowly.

4. Personnel Requirements

Below, please find the requirements to personnel who are intended to work with the WAY4 system. The requirements set by OpenWay for the period of installation, testing and certification of the system you will find in the final section of this document.

4.1 Client Personnel Requirements

For WAY4 installed at a bank or a processing centre to function properly, a certain minimum number of personnel with certain skills and practical qualifications are required.

Clients decide how many and how skilled people they need depending on the amount of work they are supposed to do, that is, the volumes of issuing and acquiring. However, it is strongly recommended that the below described employees be engaged in operating the WAY4 system.

The following guidelines should be followed while selecting personnel to work with the WAY4 system:

- Employees operating theWAY4 system must be appropriately educated and have the necessary practical experience.
- All personnel engaged in operating the WAY4 system must be trained, tested and certified before being admitted to actual operations.
- The moral qualities and psychological profile of each employee should be meticulously analysed in order to prevent possible fraud.
- It is advisable that all personnel members speak English fluently. It is also required that all supervisory personnel, managers and staff members engaged in settling accounts and disputes have good English writing skills.
- The comprehensive training and certification of security personnel, accountants and software, hardware and telecommunications engineers are absolutely necessary.

4.1.1 Cards Operations, Manager

Number

1

Department

Information Technologies Department

Skills

Management, marketing, Information technologies, accounting basics

English

Fluent spoken English and good writing skills

Special training

OpenWay training in operating the WAY4 system, international payment systems' trainings

Certification

OpenWay certification recommended

4.1.2 Cards and PIN Mailers Issuing, Engineer

Number

2

Department

Information Technologies Department

Skills

Information technologies, card business basics

English

Fluent spoken English

Special training

Plastic cards and PIN-mailers issuing, security policies

Certification

OpenWay certification recommended

4.1.3 Security Officer

Number

1-3

Department

Information Technologies Department

Skills

Information technologies, data security, personnel management

English

Fluent spoken English

Special training

Plastic card technologies, VISA and MasterCard security policies, encryption software operation, card fraud information awareness

Certification

OpenWay certification recommended

4.1.4 Database Administrator

Number

1

Department

Information Technologies Department

Skills

ORACLE-certified database administrator

English

No special requirements

Special training

Mid-level training with ORACLE required

Certification

ORACLE certification advisable

4.2 Personnel Requirements for Installation Period

The following bank staff members responsible for installing the WAY4 system must be available during the whole period of installation and testing:

- ORACLE Database Administrator - The entire period
- Security Officers in possession of the mechanical and electronic keys and encryption equipment documentation, trained in cryptographic device operation - When required

5. Environmental Requirements

The following is the list of requirements concerning the WAY4 system operational conditions.

5.1 Working Conditions

The following guidelines must be observed when preparing premises for installing the WAY4 system:

- The installation area must be sufficient for the unobstructed movement of equipment and personnel and access to all equipment units.
- All rooms on the premises must be located close to each other for the ease of communication and safety.
- When security limitations are introduced for certain parts of the premises, security guidelines set by international payment systems must be strictly observed.
- All parts of the premises must be air-conditioned in order to avoid equipment overheating and assure comfortable working conditions.
- Electronic locks must be used for all the parts of the premises. The rooms where equipment for card production and servers are installed require special security locks.
- Every room on the premises must have the necessary furniture.

5.2 Environmental Requirements for Installation Period

By the time the WAY4 system is installed, every requirement as to the working environment must be met with regard to the conditions necessary for the functioning of OpenWay personnel taking part in the installation.

The computer networks must be fully configured by the time the installation of the WAY4 system begins.