Takhmasib Dadashev

POS TERMINAL NETWORK OUTSOURCING

Takhmasib Dadashev

POS terminal network outsourcing

Penki Kontinentai
Vilnius 2021

Editorial Board: *Žoržas Šarafanovičius (ASHBURN International), Kirill Ovsiannikov (BS/2).*

Translated by: *Yaroslav Radikevich*

ISBN 978-609-95007-5-1

Contents

Foreword 6

Introduction 8

General Information About the EFTPOS/POS Terminal 8

How EFTPOS/POS Terminal Networks Function 9

Accepting Payments Using QR Codes 13

Payment Systems 13

BIN and Its Role in Processing 19

Chapter 1. Acquiring Equipment: Its Past, Present and Future **21**

1.1. Common EFTPOS/POS Terminal Types 25

1.1.1. Integrated EFTPOS/POS Terminals with Self-Service Devices (Unattended POS) 26

1.1.2. Stand-Alone EFTPOS/POS Terminals 26

1.2. Android-Based EFTPOS/POS Terminals (Android POS) 27

1.3. Biometric EFTPOS/POS Terminals 29

1.4. Online Sales Registers 33

1.5. Overview of Devices from World's Leading Manufacturers 34

1.5.1. Equipment by Ingenico 35

1.5.2. Equipment by Verifone 41

1.5.3. Equipment by PAX Technology 44

1.6. Security of Acquiring Equipment 48

1.6.1. Hacker Attacks on EFTPOS/POS Terminal Networks 49

1.6.2. Hardware Security Modules (HSM) by Thales 53

1.7. The Future of Acquiring Equipment 56

Chapter 2. Aqcuiring System Software **58**

2.1. Payment Transaction and Its Types 59

2.2 Transaction Processing at the Processing Center 61

2.3. Transaction Routing in Complex Acquiring Ecosystems 65

2.4. Processing Center Software 67

2.4.1. The Universal BASE24-eps Solution by ACI Worldwide 67

2.4.2. WAY4 Solution by OpenWay Group 69

2.4.3. Tieto Card Suite Solution by Tieto 70

2.4.4. TranzWare Family of Products by Compass Plus 70

2.5. A Brief Overview of Software for Integrating Payments
in Acquiring Systems 71

2.6. Solutions for Managing the Fleet of Payment Terminals 73

**Chapter 3. TransLink.iQ Software and Hardware Complex
by ASHBURN International 77**

3.1. TransLink.iQ: a Comprehensive Solution for EFTPOS/POS
Terminal Network Administration and Transaction Routing 79

3.2. TransLink.iQ Manager: Basic Functionality and Transaction Routing 82

3.3. TransLink.iQ SmartPOS: EFTPOS/POS Terminal Application 89

3.4 . TransLink.iQ XConnect Communication Module 89

3.5. Report Generation Module TransLink.iQ Reporting 90

3.6. TransLink.iQ Insight: a Solution for Online Monitoring of the Technical
Condition and Activity of the Network of EFTPOS/POS Terminals 91

3.7. Round-the-Clock Call Reception Service Service Desk.iQ
and Its Main Tasks 93

3.7.1. Workflow in Service Desk.iQ 94

3.7.2. Service Desk.iQ System Modules 96

3.7.3. The Mobile Service Desk.iQ App 101

3.7.4. Web Service Desk.iQ Browser Solution 102

3.8. TSP-Services of ASHBURN International 103

Chapter 4. Outsourcing of Acquiring Networks – a Trend in Modern Banking 104

4.1. Why Do Banks Outsource Non-Banking Activities? 106

4.2. Recommendations of the European Banking Authority and the Basel Committee on Financial Supervision on Outsourcing 108

4.3. Outsourcing of Acquiring Networks: Risks or New Opportunities? 112

4.4. International Experience in Outsourcing Payment Infrastructures 113

4.5. Payment Innovations: What's Next? 115

Annex 119

Key International Security Standards for Card Operations and POS Systems 119

PCI DSS Standard 120

Payment Application Security Standard PA-DSS 123

PCI DSS Service Provider Certification Levels 127

VISA classification 127

MasterCard classification 127

Glossary 128

References 137

Foreword

Modern economic environment is defied by a multi-channel approach to customer service in many areas. This approach implies choosing a product or a service as well as processing its delivery and payment, commonly with the help of chat bots, biometric solutions and other innovative technologies. A modern smartphone becomes a payment terminal in itself with the payment functionality being integrated into merchant applications (integrated virtual bank card).

The company *ASHBURN International* (subsidiary of Penki Kontinentai Group, Lithuania) specializes in acquirer network outsourcing, payment terminal management and their integration with POS software.

The business approaches of *ASHBURN International* – SaaS (Software as a Service) and TaaS (Terminal as a Service) – are becoming a business strategy implemented by many international companies, including one of the market leaders – *Ingenico Group* [2, 5].

The software *TransLink.iQ* developed by *ASHBURN International* is designed for EFTPOS terminal management and transactions processing, as well as to perform transactional and technical monitoring of payment terminals in real time.

A key feature that distinguishes *TransLink.iQ* from its competitors is the new technological ability of switching the EFTPOS-terminal service from one acquiring network to another (see Chapter 3.1). In other words, *TransLink.iQ* transforms the EFTPOS terminal into a multi- acquiring device.

TransLink.iQ was created in compliance with international payment system requirements for different types of payment cards, including the contactless and virtual cards which have gained popularity in recent years.

With years of experience of ASHBURN International show that transitioning to a TSP (Terminal Service Provider) business model is possible only through the use of modern technological solutions for acquiring network management optimization, which allows, among other things, to provide merchants with the service of the so-called “constantly operational terminal”.

What is the reason behind the growing demand of the outsourcing model as means of ensuring efficient management of payment terminal networks and other equipment? Why do traditional market players and acquiring infrastructure owners resort to the services of third-party operators (*PSP-providers*) and allow them to access confidential customer information? The answer is not as obvious as it might seem.

To better understand this, let us explore the history of the phenomenon that is outsourcing. In general terms, outsourcing is the process of transferring certain non-primary business tasks to a third party in order to increase operational efficiency of the enterprise.

Henry Ford can be considered the pioneer in manufacturing outsourcing. At first, the head of the well-known automobile company sought to personally control all production stages. He soon faced exorbitant servicing costs of the multiple areas of the company's activities. Ford was one of the first to realize that no company can be self-sufficient, thus turning to independent companies for help.

This book discusses the EFTPOS terminal network and POS equipment outsourcing, TSP services for non-banking organizations on the basis of *TransLink.iQ* and *Service Desk.iQ,* technological products developed by *ASHBURN International* and *BS/2*. Our book was inspired by practical experience that these companies have collected since their establishment in 1993.

The outsourcing business is based on using integrated EFTPOS terminal fleet management tools and effective maintenance service. A company's competitiveness is directly related to how productive its routine operations are organized. If not for the productivity, why else should banks give up a part of their business operations to a third party at all?

Certain parts of the book that provide additional information (which is of no less importance) is highlighted with a colored background.

The book will be useful as a quick reference for those who work in the payment industry or are interested in implementing the latest payment solutions in their business.

The author expresses gratitude to the editorial board - the leading specialists of Penki Kontinentai Group. The numerous discussions and important comments have significantly helped to improve the book and expand its content.

The author expresses special thanks to Penki Kontinentai Group CEO Idrakas Dadašovas for the idea of this book and for the support provided in its preparation.

Introduction

The active popularization and greater availability of payment services are attracting an increasing number of people who find it more convenient to pay without using cash. Payment by card at points of sale has become rather commonplace. Behind something so ordinary is the work of thousands of industry professionals on the side of issuers, processing center acquirers and other market participants whose main task is to ensure smooth operation of the acquiring network and transaction security.

That is why for over 15 years the World Bank is promoting the development of global payment ecosystems as a key component of financial infrastructures of all countries and has provided various types of assistance to over 100 countries.

EFTPOS (electronic funds transfer at point of sale) is a technology based on the use of payment cards at points of sale that processes electronic money transfers.

General Information About the EFTPOS/POS Terminal

Due to payment system automatization most trade and service enterprises have special equipment installed at points of sale – that is the EFTPOS/POS terminal.

An EFTPOS/POS terminal is an electronic device (payment terminal) for card payment processing. It can process cards with chips, magnetic stripes, as well as contactless cards or other types of digital cards (in smartphones or other wearable devices).

These devices are not to be confused with POS systems (see Chapter 1) – cash register hardware-software systems that are installed at the cashier's workplace. However, in recent years a tendency is noticed for the business functions of the EFTPOS/POS terminal and the POS system to merge. This tendency stimulates the creation of a new type of device – online cash registers with card processing functionality.

EFTPOS technology emerged in the United States in 1981 and was quickly introduced in other developed countries. In Australia and New Zealand EFTPOS is also the trademark of the particular system used for such payments. These systems are generally country specific and not related.

Although technical capabilities and accessories of modern EFTPOS/POS terminals may vary, every device always includes: magnetic stripe and smart card readers, non-volatile memory, as well as ports for equipping a PIN keyboard, a printer, or connecting it to an electronic cash register or a computer.

How EFTPOS/POS Terminal Networks Function

Acquiring is the ability of trade and service enterprises to receive payments through payment cards. This notion is also understood as banking and technological client servicing, i.e., data transfer and processing. Acquiring enables an organization to provide its client with a payment method choice. It also helps minimize the costs associated with accepting and processing and depositing cash.

The *acquiring* procedure involves several parties:

The *Acquirer* is the organization responsible for transferring the payment to the merchant. Acquirers are subject to requirements of national and international regulators, including global payment systems (VISA, MasterCard, UnionPay, etc.). In addition, the acquirer ensures card payment acceptance technically (either directly or through outsource). In turn, the merchant pays commission to the acquirer for this service.

The *Issuer* is the organization that issues payment cards that are accepted by the acquiring equipment at points of sale. The issuer takes full responsibility for client crediting within the procedure of paying with a card.

The *Client* is the shopper, thus, the holder of the card issued by the issuer.

The *Acquiring network* is the acquiring equipment fleet installed at points of sale and in bank branches (including and not limited to self-service devices, ATMs, EFTPOS/POS terminals).

Large trade and service enterprises use point of sale systems that combine cash systems, payment terminals and various peripherals.

Let us review a payment process in a common trade or service enterprise in more detail:

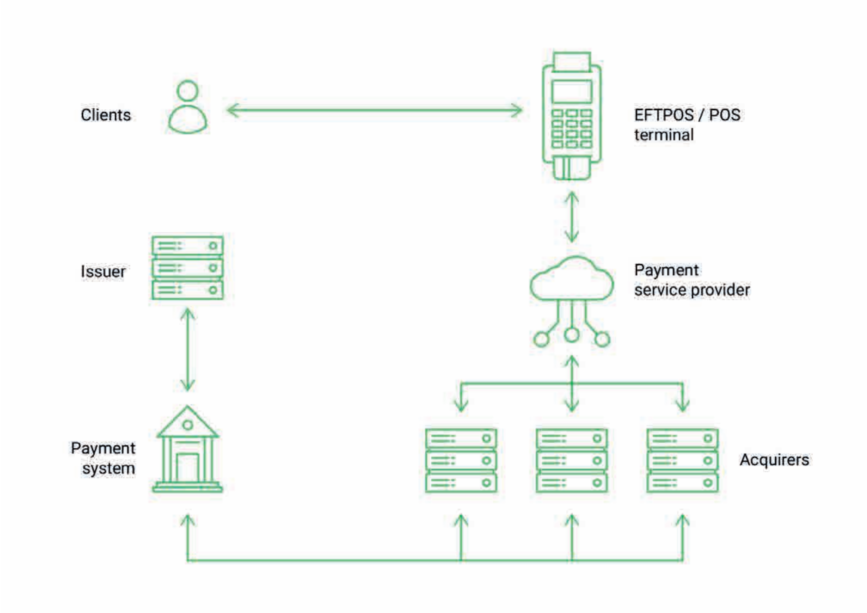


Fig. 1. The scheme of the payment process at a common trade or service company.

When paying at the checkout, the buyer uses the card based on the available method of data transfer (either contact or contactless) to the EFTPOS/POS terminal (through the magnetic stripe or an electronic chip). If necessary the buyer confirms the payment by entering the PIN code. The transaction data is sent through the acquiring infrastructure to the processing center where it is is processed and the payment confirmation is sent to the terminal. This confirmation allows the cashier to complete the purchase by issuing the product and the receipt.

POS systems facilitate these processes with the following conditions:

- *The bank must have a valid agreement with with the most common payment systems (VISA, MasterCard, Мир and others);*
- *The bank must have a trade acquiring agreement with the merchant;*
- *The buyer pays for the product or service using a payment card. Factually the merchant does not receive the amount at the time of transaction, but the product or service is provided. The provision of goods or services to the buyer is made in case of a successful authorization (i.e. by the bank or issuer confirming that the card is solvent).*

These operations are carried out by an authorized acquiring bank by installing payment terminals at merchant locations (in se of traditional merchant acquiring - EFTPOS/POS terminals). In addition, terminals built into online cash registers are now widely used.

The *Acquiring network* of a specific aquiring bank is the collection of all devices at all merchants (i.e. shops, hotels, restaurants etc.) that have signed an agreement with the bank for trade acquiring services.

Most of the global acquiring services market is occupied by member banks of *VISA, MasterCard, UnionPay* and *JCB* payment systems (see below for more details). Beside those, *American Express* cards have wide popularity in the US and Russia is actively expanding the *Мир* payment system.

Alipay is a leading payment platform established in 2004 that is part of the *Alibaba Group*. In addition to being used internally by *Alibaba Group* to pay for the products it offers, over 460,000 other companies also use the payment system. *Alipay* cooperates with 65 financial institutions around the world, including *VISA* and *MasterCard* payment systems, as well as major global and regional banks. Currently, the number of users of the payment system exceeds 1.3 billion worldwide.

WeChat is an abundant communication system for text and voice messaging created by the Chinese company *Tencent* in 2011. The app is available on the *iPhone* as well as phones running on *Android*, *Windows* and other operating systems. By 2019, the number of active *WeChat* users exceeded 1.151 billion.

WeChat has its own payment system *WeChat Pay* that offers two payment methods: through the WeChat wallet and through a bank card linked to *WeChat*. These operations are carried out using a unique QR code assigned to each registered user in *WeChat*. The payment is made by scanning the QR code of the seller and / or the buyer, after which the password is entered and the money is transferred.

СБП (*Система быстрых платежей* (eng. Rapid payment system) of Bank of Russia) allows transferring funds with a recipient identifier (currently, by a phone number) even if the parties involved in the transaction have accounts in different credit institutions. In the future, *СБП* will allow making instant payments for goods and services, including government payments and will also process QR codes.

Another example is the global payments company is *Adyen*. It provides services to payment acceptance companies in e-commerce, mobile devices and points of sale. *Adyen* is one of Europe's largest fintech companies with a pan-European banking license to bypass banks and process cross-border payments directly for its merchant clients, including many of the world's leading e-commerce firms.

Adyen offers merchants online services to process electronic payments through a variety of payment methods, including card transactions and real-time bank transfers. The *Adyen* payment platform connects to payment systems around the world.

Internet acquiring should also be mentioned. It is the process of accepting payments using bank cards and *digital currency* via the Internet using a specially developed web interface. It can be applied in online stores and for paying for facilities or other bills.

Internet acquiring is characterized by the absence of direct contact between the seller and the buyer. Such a system is used for remote payments when a customer purchases a product or orders a service over the Internet. To make a purchase, one must enter card details and confirm the payment.

It is common to include cash withdrawal by a cardholder (via ATM or a specially-configured EFTPOS terminal) under acquiring as well.

Acquiring companies charge a commission (usually on a per-transaction basis; however, the commission may vary depending on bank tariff policies).

To pay one needs to introduce the card through the terminal and enter the payment details. The buyer confirms the payment in one way or another - and after confirming it, the buyer receives a paper or electronic check.

The terminal can be connected to the network in various ways, such as Wi-Fi, Ethernet, GPRS or Bluetooth. Note that the mobile connection option is preferable for enterprises where customers pay for goods and services not at a stationary cash register, but, say, for services such as taxi, delivery or street vending. Such a terminal can be equipped with a reader of various magnetic, chip and contactless cards. If this is the case, all information about the payment is displayed on a graphical screen. In addition, it is possible to accept payments by manually entering card data.

Accepting Payments Using QR Codes

Payment information can also be entered using a QR code (QR meaning *quick response*), which is a graphical set of small black squares on a white background. A client can decrypt a QR code using certain mobile apps installed on their mobile device by using the camera.

The QR code can be seen on receipts and settlement documents (for example, invoices for facilities). The counterparty (recipient of the service) only needs to scan it and pay through a specialized mobile banking application. This method significantly speeds up the settlement process, excluding the manual entry of details into the payment form.

QR codes are also used as a source of information to pay for goods and services (it is enough to have a smartphone with an application installed to pay using a QR code and having linked cards or accounts). QR codes are widely used in marketing and advertising, tourism, banking (payment of taxes, payment for services in retail outlets, etc.).

In general, QR codes are most common in Asia, Europe and the United States. Many innovative payment technologies are also created in developing countries where the introduction of mobile payments and low-cost fast-response technology are making digital payments the new norm. The research company *eMarketer* estimates that about 45% of China’s population used mobile payments in 2018, in comparison with 23% in the US and 15% in the UK. This is explained by the fact that QR codes are widely used for “alternative” payments in *Alipay* and *WeChat Pay*.

Recently QR payment technologies have been introduced in Russia as well: a pilot project for connection to the *СБП* (С*истема быстрых платежей*) was launched by the Bank of Russia in August of 2019.

Payment Systems

The term *payment system* describes the whole complex of rules, procedures and technical infrastructure that ensures the transfer of funds from one economic entity to another. Thanks to these systems settlements are made that exclude the use of cash when making domestic and international payments.

Although it is generally believed that money is transferred through payment systems, from a legal point of view, in most cases, it is debt that is transferred. Thus, the funds that a particular payment system owes to one of the clients becomes indebted to another client. When the first client transfers their money to the payment system the transaction amount is recorded, that is, the amount owed to the first client. The client can indicate through a special command that the payment system now owes the amount to the second client instead of the first. When the second client contacts the payment system, they have the opportunity to receive the monetary equivalent of such a debt.

VISA International Service Association is an example of this kind of international payment systems. The association currently includes two companies: *VISA Inc*. (headquartered in Foster City, USA) who own all trademark and technology rights, and *VISA Europe Services Inc*. (based in London, UK) operated by a number of European banks and is licensed by *VISA Inc*.

A unique technology called *3-D Secure* was developed for the *VISA* payment system in order to increase the degree of protection of users when they make online purchases. The authentication framework is based on three independent domains: card issuer, acquirer, and compatibility (with a payment system that supports the *3-D Secure* protocol).

Currently, the total turnover of *VISA* cards is $ 8.3 trillion. *VISA* cards are accepted for payment in over 53.9 million retail outlets in over 200 countries around the world. The organization plays a central role in the development of innovative payment products and technologies and is used by 15,500 financial institutions (as of March 31, 2019). As of December 31, 2018, there were over 3.4 billion *VISA* cards worldwide.

The basis of the payment system is the global processing network *VISANet*, which processes over 65,000 transactions per second.

It should be noted that *VISA* is not a bank, it does not issue payment cards, does not provide loans to card holders, nor does it set the commission amount or interest rates for its users. Uniting more than 21,000 banks all over the world, *VISA* plays the role of an intermediary, organizing settlements and ensuring technical interaction between system participants. It’s the members of the system who are responsible for card issuing and their acceptance.

Another international payment system is *MasterCard Worldwide* (also known as *MasterCard Inc.*). It is a transnational financial corporation uniting 22,000 financial institutions in 210 countries. The company is headquartered in Westchester County, New York, USA.

MasterCard was originally created in 1966 by a group of California banks under the name *Interbank / Master Charge* as a competitor to cards issued by *Bank of America*. In 1979 the organization was renamed *MasterCard*. In the early 1990s, *MasterCard* acquired the UK *Access Card* (but dropped the reference to *Access*). In 2002 *MasterCard International* merged with *Europay International S.A*. - another major association that was issuing cards under the name *Eurocard* for many years.

In 2006 *MasterCard International* was renamed *MasterCard Worldwide* and went public; prior to its first public offering, it was an organization jointly managed by over 25,000 financial institutions that issue branded cards.

MasterCard's main line of business is processing payments between acquiring banks that service points of sale, as well as issuing banks or credit cooperatives that use *MasterCard* debit and credit cards for payments.

MasterCard cards are most widespread in Europe and they are least popular in North America. It's the second most popular payment system with 16% of world's card holders using it.

One of the main business objectives of *MasterCard* is to ensure maximum payment security. To achieve this, MasterCard introduced such technologies as *SecureCode,* developed *GateKeeper 2.0*, offered the *Address Verification* and *Security Code Check* services

MasterCard cards use contactless payment technologies via *Google Pay, Apple Pay, Samsung Pay*, etc. Meanwhile, *Visa* cards rely on *Android Pay, Apple Pay, Samsung Pay* systems for this purpose.

There are no significant differences between these payment systems from the user standpoint, as the differences are mainly related to technological implementation, not the operational characteristics. When it comes to card differences, the card type makes a bigger difference than the service provider being *Visa* or *MasterCard*. The available limit amount, the presence of a personal manager, functionality, the currency conversion commission amount, and other characteristics depend on the type of card and the issuing bank.

JCB (*Japan Credit Bureau*) is the biggest payment system in Japan and is one of top 5 payment systems worldwide. It is headquartered in Tokyo. The system was created in 1961 and it currently ranks third by the number of card acceptance points. As of 2020, *JCB* has issued 130 million cards for clients in 23 countries.

UnionPay International (UPI) is an international payment system headquartered in Shanghai (PRC). It was established in 2002 on the initiative of the *State Council of the People's Republic of China* and the *People's Bank of China*. Over 200 financial institutions are its shareholders. *UPI* is a subsidiary of *China UnionPay* and is focused on expanding and supporting *UnionPay's* business outside of China. Having partnered with more than 2,300 financial institutions around the world, *UPI* provides payment and cash withdrawal services in 179 countries around the world. *UnionPay* cards are issued in more than 60 countries including Russia.

By joining efforts *Europay, MasterCard* and *VISA* have developed uniform requirements for card microprocessor manufacturing technology called *EMV* (*Europay* + *MasterCard* + *VISA*) to ensure security of payment acceptance on physical devices.

Founded in 1999, *EMVCo* is a global technical body that promotes universal interoperability and acceptance of secure payment transactions. It does so through the management and development of *EMV* specifications and associated testing processes.

Processing Center: Functioning and Main Tasks

The term *processing* is used in banking to describe the processing of information used when making payment transactions.

A *Processing center* is a legal entity or its structural unit that ensures technological interaction and information exchange between settlement participants.

From the standpoint of their activity processing centers, generally relate to the field of processing transactions that involve payment cards.

The *Head processing center* is a specialized computing center authorized by the payment system. In addition to processing, it is also responsible for routing requests / responses from other processing centers, maintaining databases of participants and interacting with other participants in the payment business according to the established regulations.

The head processing center maintains a payment system database (data on payment system members) in order to provide authorization requests for instances when the issuing bank does not maintain its own database. Otherwise, the processing center sends an authorization request to the issuing bank through the acquirer.

The processing center processes authorization requests and / or transaction protocols that record card payment and cash withdrawal data that is received from the acquirers. The center stores information about card holder limits and executes authorization requests in cases when the issuing bank is not available (is offline).

In other cases, the processing center forwards the received request to the issuing bank of the certified card and ensures that the response is sent to the acquiring bank. In addition, the processing center prepares and sends the final data for settlements between the banks participating in the payment system on the basis of daily transactions. It also generates and sends to the acquiring banks so-called *stop lists*.

Many banks that issue payment cards have their own card processing centers.

It should be noted that an international payment system always has an extensive network of regional processing centers.

There are several types of processing centers:

- *clearing centers of payment systems;*
- *processing centers of banks that connect to different payment systems;*
- *centers of specialized processing companies for banks that don't have processing centers of their own. Such companies provide outsourcing services of accessing the processing of payment systems*.

Clearing is a non-cash settlement procedure in which the clearing entity acts as an intermediary between the acquirer and the issuer, transmitting information about all realized debts that are to be paid by the acquirer and the amounts each entity owes it.

In other words, clearing is the process of non-cash settlements between parties for goods sold to each other, securities and services rendered, settled on the basis of the conditions of the payments balance.

Clearing is also used in banking in the implementation of mutual obligations, often implemented cyclically, with banks frequently involving *clearing centers* to perform these functions. If such is the case, clearing is treated as a form of non-cash bilateral or multilateral settlements in the payment system.

A *Clearing center* is an organization that deals with clearing, that is, non-cash payments. An organization of this type can function both between organizations within one country, and at the interstate level.

There are two types of clearing centers – *acquirer clearing centers* and *issuer clearing centers* – each having a different role.

Processing centers are most widespread in the following industries:

1. banking processing of payment cards:

- *card issuance, opening accounts and processing of payments of clients using bank cards;*
- *acquiring (EFTPOS/POS terminal maintenance and servicing, payment management of commercial companies);*

2. non-banking processing (electronic payment processing)

- routine payment operations (cellular service, Internet, digital TV, facilities etc.), and bank transfers*.*

Transaction information is received by the processing center.

In actuality mutual cash settlements are carried out on the basis of clearing data for a specific time frame, therefore, most of the payment systems are credit schemes. Meaning, when the receipt of money by the payment system parties is spaced out in time in relation to the flow of information.

Each payment card settlement system imposes its own requirements on processing centers that process card transactions. As such, *VISA* and *MasterCard* require mandatory certification of the organization’s card hosts by payment systems. At the same time, all processing centers that carry out payments are required to function 24/7.

When shopping online, card information is requested and forwarded by specialized software. The software belongs to a separate entity that has a service agreement with the e-shop (no physical merchant is present), and the e-shop is not directly connected to a processing center of a payment system directly. To receive payments an e-shop therefore depends on an intermediary (a bank or a payment service provider). The intermediary. It is important that the intermediary has cooperation agreements with global payment systems such as *VISA* or *MasterCard*.

BIN and Its Role in Processing

BIN (*Bank Identification Number*) is a number that carries all information about the card issuer. Being part of any card number, the BIN is used to identify the bank within the payment system during authorization, processing and clearing.

BIN tables found in processing centers are constantly updated and are used for routing card operations of external issuers on processing center devices.

Every *BIN* digit has a particular meaning. For instance, the first digit identifies the payment system that services the card. For example, VISA – 4; MasterCard – 5, JCB International – 3, China UnionPay – 6.

Acquiring network outsourcing

www.ashburn.eu | mail@ashburn.eu

Chapter 1. Acquiring Equipment: Its Past, Present and Future

POS systems are software-hardware solutions for casher workflow automation on the basis of fiscal registrars. Typically, a POS system includes: a PC system unit, a fiscal recorder, a cashier's POS monitor, a cash drawer, a programmable keyboard, a card reader, a barcode reader and a customer display. These pieces of POS equipment integrated together conclude a complete *cashier workstation*.

The use of a POS systems for various business areas helps to optimize the operation of merchant workflow. Modern equipment greatly facilitates the work of the cashier, increasing the efficiency of routine problem solving when processing client requests.

In addition to accounting for goods and services payments, the POS system records and organizes sales data, generates reports, manages inventory, stores customer contact information, and much more. At the same time, choosing the right POS system is a difficult task due to many factors that either make it easier to manage a particular business, or, conversely, become an expensive obstacle. To simplify the selection of the optimal POS solution for a particular type of business, Reference [16] compiles more than 100 recommendations.

An integrated POS system can also be assembled individually based on business needs.

There's a joke saying that a POS system costs as much as a piece of gold of the same weight, but that isn't due to its business value, but due to its bulkiness and market price. However, the development of other technologies lead to the use of unexpensive devices such as tablets to be used for the task, so the joke may soon become irrelevant.

An EFTPOS/POS terminal can be part of a POS system. If such is the case, the payment terminal is used to accept and generate card transactions - and can be included in the POS system.

An EFTPOS/POS-terminal with the application installed in it must be certified in international payment systems; in turn, a cash register computer with its software is also subject to certification - but not in international payment systems, but in the relevant tax, metrological departments and local organizations where it will be used.

Nowadays, all that new systems need to function is a tablet or other mobile device based on Android or Windows operating systems. A modern tablet computer is not only much lighter, but also much cheaper than a conventional POS computer.

A *Retail PIN pad* is a subset of the EFTPOS/POS terminal for initiating transactions. It has reduced functionality, so it lacks a battery and a printer. It is intended for an integrated solution with POS software. Nonetheless, it is regarded as a payment terminal subject to all the principles of the payment industry (being certified, etc.). It simplifies checkout purchases by providing a convenient mode of cashless card payments, reduces errors and automates the process of serving customers.

Some models of these devices are equipped with front-facing cameras for alternative payment methods and biometric identification.

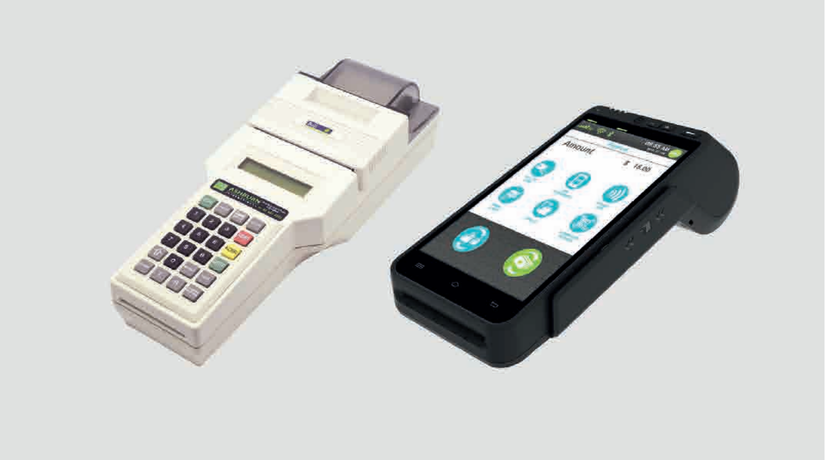


Fig. 2 One of the first examples of an EFTPOS/POS terminal (left) and a modern Android POS terminal (right).

Currently there are the following types of cash register POS systems [16]*:*

- cloud POS systems;
- locally-hosted POS systems;
- hybrid solutions.

Cloud POS systems offer mobility and convenience: they provide opportunities such as making sales calls, accepting orders and payments using a tablet or smartphone from any place where the merchant is situated. One can also access the back-office functions from any browser, allowing the user to view merchant sales metrics and generate relevant reports remotely. There is also no need to set up a local server to host the current production data, since the POS system supplier has already taken care of this.

Typically, there is a monthly fee for cloud POS software. It should be noted that such software is regularly updated, and the updates are included in the subscription price. Most companies include customer service as part of their subscription as well. Thus, a separate support contract for an additional monthly fee is not required.

The only potential downside to using cloud-based software is the requirement for constant availability of reliable Internet access. While many web systems have an offline mode that allows them to operate even during a connection outage, in case of intermittent problems with accessing or connecting to the Internet, one should consider a server-based solution.

Server-based (or *locally-hosted*) *POS systems* are installed on a dedicated server, rather than hosted in the cloud. Their main advantages are that, firstly, they do not require an Internet connection, and secondly, one can configure the system manually. On the other hand, the disadvantage of such systems is the need for technical support for your server, meaning that security and backup are up to you, and this type of system can end up costing you more than the cloud version. In addition to the extra hardware that you will have to purchase for your server, and the cost of its maintenance, you should also take into account the cost of the software. In addition, you will have to pay a monthly fee for support and maintenance, and buy annual updates.

Another important consideration is that you will most likely not be able to access your system remotely in real time. Therefore, in order to deal with back-office tasks (such as running reports and updating your product catalog or menu), your personal presence in the office is required.

Hybrid POS systems will be the most suitable option if you need the benefits of mobility and convenience of a cloud, and the stability of a server POS system. This type of POS system runs on a local server and creates backups of all the necessary data in the cloud, which allows you to access them remotely. If the Internet access is unstable, then you will also have no problems for your system. In terms of their cost, these systems are usually comparable to cloud-based POS systems with a monthly subscription fee. The disadvantages of a hybrid POS system are that, as in the case of server solutions, it is necessary to purchase additional equipment – the configuration of which may require more costs than just a cloud system. You may also need to manually back up the server – which is less convenient than using a cloud system that will do the job automatically.

The cash register system can be integrated with a payment card service device that allows you to read information from:

- the payment card chip (via the contact or contactless method), or
- magnetic stripe of the payment card.

These devices allow you to initiate a payment transaction and send it to the acquiring host. This solution also allows you to make payments using a smartphone or a wearable device that is linked to a payment card. Since 2020, all POS terminals operating with the MasterCard global payment system are required to support a contactless payment method.

The main advantages of non-cash payments include:

- *lack of physical interaction between the cashier and the buyer;*
- *reducing the time spent on the operation;*
- *minimizing the risks associated with entering an incorrect amount.*

In general, the basic scheme of interaction between the cash register software, acquiring software and the terminal itself is approximately as follows:

- *the cashier selects the type of operation and the amount in the cash register software;*
- *the cash register software generates a request and sends it to the card service device;*
- *the card is read on the device and the PIN code is entered if necessary;*
- *data is exchanged between the device software and the acquiring host;*
- *the cash register software receives a response from the device processing the card about the authorization result, after which the receipt is printed;*
- *if desired, this information is entered in the database of the cash register system.*

1.1. Common EFTPOS/POS Terminal Types

[20] assesses the efficiency and benefits of EFTPOS/POS terminals:

1. *Efficiency and reduction of labor costs. Through the use of EFTPOS/POS terminals, the amount of cash that a business will deal with is reduced; thus, the time spent on processing (validation, recalculation, packaging, and collection) of cash is reduced.*
2. *Reduces the risk of theft. Cash is much easier to steal, while EFTPOS payments go to the merchant's bank account, ensuring business transparency.*
3. *Service speed increases. Since most cards are contactless, this allows you to significantly speed up payments at service points.*
4. *Availability of all types of payments. This allows you to eliminate any friction when accepting payments, since you can make transactions exactly as the client expects (pay for the service using one or more payment cards or use a hybrid payment method).*

On the other hand, EFTPOS/POS terminals have a number of disadvantages:

1. *Payment card service fees. Such fees are considered a necessary evil when accepting card payments. For consumers to use their credit or debit cards to make purchases through EFTPOS/POS terminals, each transaction ultimately has to be paid for. These funds should cover the cost of renting and maintaining payment terminals and the costs of servicing the acquirer and payment systems.*
2. *Depending on the quality of the network connection. It is recommended to invest in reliable Internet access systems for electronic payments, as this is a critical factor for doing business.*

Depending on the interaction with the cash register software and other equipment, EFTPOS/POS terminals can be divided into two main categories:

- *integrated EFTPOS/POS terminals, and*
- *stand-alone EFTPOS/POS terminals.*

Sometimes *embedded EFTPOS terminals* used in vending machines or self-service devices are viewed as a separate category. They have a protected design for outdoor and indoor use.

1.1.1. Integrated EFTPOS/POS Terminals with Self-Service Devices (Unattended POS)

An important trend in the POS equipment industry is integrated (unattended i.e., maintenance-free) retail POS systems

According to the forecasts of a major participant in the payment processing market, *Global Payments*, the turnover of this industry is expected to grow to $13 billion by 2025 [15].

Integrated terminals (*PIN pads, PIN keyboards*) work only in conjunction with the cash register software. I.e., the terminal is integrated into the cash register software.

For mobile trading, there is a solution in the form of mPOS (mobile point of sale)- terminals. These are small, inexpensive devices that require additional hardware – a smartphone, tablet, or PC with the program installed. This type of POS terminal allows you to make a non-cash payment using a card. The main advantages are compactness, low cost and the ability to use a smartphone or tablet based on iOS or Android.

It should be noted that mPOS terminals, as a rule, do not provide for the possibility of printing a receipt.

1.1.2. Stand-Alone EFTPOS/POS Terminals

A *stand-alone EFTPOS/POS terminal* is a separate device that is not connected to the cash register software. In its functionality, it contains a reader of magnetic, chip and contactless cards, a digital PIN keyboard and a receipt printer. Therefore, an autonomous terminal is a completely self-sufficient device on which you can perform the entire range of necessary card operations.

Stand-alone terminals can work via Ethernet and GPRS, or they can be connected to a PC via USB or RS232 connectors for communication.

In turn, autonomous terminals can be divided into two groups: *stationary* and *portable*.

If a stationary terminal must be connected to the power grid, then a portable one is equipped with a built-in battery, which allows you to use it in a cafe, in a taxi, in a delivery service or at field trips. Any type of wireless communication can be used for these devices.

Also, with the help of a special application, the mPOS terminal can be connected to a smartphone – after which you can use a miniature card reader and an application installed in the smartphone to process and transmit requests to the processing center of the acquirer.

The device (reader) for reading payment cards is connected to a mobile device via a connector, most often a 3.5 mini jack, USB or Bluetooth connection, and is controlled via the bank's payment application. Such terminals are used, for example, when paying for taxi services or courier delivery.

In addition, SMART terminals of the *3-in-1* type are now gaining popularity in the form of a single device that performs the functions of the front-end of cash software, online fiscalization and payment functions of the EFTPOS/ POS terminal. They are not only very convenient for accepting non-cash payments, but also work as a full-fledged cash and fiscal equipment, sending data to the tax service, as well as printing fiscal receipts and card service receipts.

1.2. Android-Based EFTPOS/POS Terminals (Android POS)

Since an Android-based POS system (Android POS or APOS-system) works with any tablet device that has Android or Windows OS installed, there are many options for them.

It should be noted that the iPad platform is more preferable for most retail operators, and, since Apple develops both hardware and operating software, such devices are known for their user-friendly interface, stability and a high degree of security, since iOS is a closed platform, which makes it less attractive target for hackers – although it is not immune from malicious attacks (why it is important to constantly update your devices). Examples of iPad-based POS systems include Vend, TouchBistro, Lightspeed, Talech, and Revel. However, the iPad is more expensive than Android tablets.

On the other hand, Android, with more than 2.5 billion devices in use, is considered a more popular platform for consumers. Many developers may also prefer Android because it allows more customization than iOS. In addition, Android tablets are cheaper than iOS-based devices, since they are produced by different manufacturers – and the high level of competition in the market invariably leads to lower prices and a wider choice of models, when adding devices, or replacing faulty or lost-tablets. An example of an Android-based POS system is the all-in-one terminal from the US company *Toast* by the same name.

Currently, the market offers a variety of products from various manufacturers (such as *Samsung, Lenovo, LG, Acer, Dell*, etc.) that can be used with POS solutions based on Android. These devices cover the entire price spectrum, and each of them has its own unique set of advantages and disadvantages. There is also a wide range of mobile software solutions for sales management and other POS-related functions.

Mobile software solutions can also provide vital services, such as:

- *manage your inventory and notify you when you need to replenish your inventory;*
- *store customer data, including purchase history and other relevant information that can be used to improve direct marketing efforts and encourage new purchases in the future;*
- *provide sales reports to access key insights and trends, such as which products sell best, and when exactly;*
- *employee management features that can help you manage and track the amount of tips they earned, hours worked, etc.*

The Android POS system is easily scaled to meet these needs. For example, inventory management, data reporting, and other services may not be required at first; however, as your business grows and develops, these functions may become vital.

Some Android POS system providers offer different pricing plans: You can start with a low-cost “basic” plan, and when you need additional features or there are additional points of sale you can upgrade it.

With all the different functions and management capabilities, the APOS system is overflown with huge amounts of data. Leading companies are already aware of the importance of Big Data and use analytics to process large volumes of “raw” data in order to identify valuable and effective business ideas. These insights can help businesses get to know their customers better, make targeted decisions, and ultimately generate more revenue. For example, customer data allows a company to learn about the purchasing behavior of an individual customer or an entire group of customers.

Due to the fact that the market offers ergonomic devices with large screens based on Android with EFTPOS/POS terminal functionality, it becomes possible to combine cash software, as well as fiscal and payment functions in one device.

Such terminals are exceptionally user-friendly, as they are focused on merchant needs for accepting payments both behind the counter and in the field of mobility (especially in the transport and hospitality sectors). They combine the Android user interface with *Ingenico* solutions in the field of secure payments. So, they support all payment methods for goods and services, including alternative ones - and offer merchants a full set of services through Android business applications.

1.3. Biometric EFTPOS/POS Terminals

Financial services biometrics is widely used in biometric systems to help with cash flow. This technology covers biometric payment cards, POS systems and payment systems, transaction processing and other payment technologies, as well as mobile wallet applications and money transfer systems.

The results of a survey conducted by the *VISA* payment system in 2017 among 1,000 Americans to study the awareness and perception of biometric authentication, show that consumers still show a great interest in biometric technologies that make their lives easier [34]. Fingerprint recognition technologies are of the greatest interest, but 39% of respondents are interested in eyeball scanning technologies, and another 36% are interested in face recognition.

The main advantages of using biometric authentication for payments include not having the need to remember passwords and PINs (50%) and creating a sense of greater security than with passwords and PINs (46%). In addition, consumers believe that using biometric technologies is faster (61%) and easier (70%) than entering passwords.

Biometric authentication technologies have gained popularity in the retail industry largely due to their efficiency in meeting the requirements of retail outlets. For retailers this means, in particular, the ability to ensure biometric security in their work without resorting to investments in individual developments. According to a study by *Juniper Research*, by 2023, confirmation of the authenticity of transactions when paying for goods via a mobile device in stores and for remote mobile payments will be carried out through biometrics

– and the total turnover of all “biometric” transactions can reach $2 trillion per year. If we compare this forecast with the data for 2018 ($124 billion), the growth will be very significant — over 1600% [32].

It is noteworthy that the growing popularity of biometric payment terminals is observed in the markets of developing countries (such as India or China) - despite the fact that the total volume of transactions with confirmation of biometrics in these countries by 2024 is estimated at $254 million (compared to $84 million in 2019) [35].

Back in March 2020, China introduced new standards for applications that collect biometric data, including for facial recognition systems. Chinese researchers and developers decided to carefully study the capabilities of facial recognition technology after several scandals broke out in 2019, including data leaks and the *Zao* application for creating *DeepFakes*. The term *DeepFake* refers to a method of synthesizing a human image based on artificial intelligence. This method is used to combine and overlay existing images on a video. As a result, China has updated guidelines on biometric data collection and consent requirements.

Initially, the personal data security standards, which came into force in 2018, were China’s response to the European *GDPR* (**General Data Protection Regulation**) specifications.

The latest updates to the law, which came into force on October 1, 2020, provide that users must give active consent to the collection of biometric data using a pop-up window, a hint, or other means. Service providers should also inform users about the purpose, method and the scope of data collection, as well as offer other information for review. In addition, the updated standards recommend that companies store biometric information separately from personally identifiable information, and offer several clarifications on data processing, including third-party access [33].

For example, *Fujitsu* and *PulseWallet* have already developed an innovative POS terminal that uses biometric technologies to provide all users with the highest level of security. Its main innovation was the *PalmSecure* biometric identification technology. Once registered, users can make payments without resorting to payment cards – they just touch the terminal with the palm of their hand [19].

Another example: the national identity service planned in Singapore will replace passwords and physical data with biometric data for a number of processes and transactions [23]. Biometric facial verification will be implemented to replace passwords and identity cards. Banks and government agencies are expected to introduce kiosks where Singaporeans aged 15 and over will be able to scan their faces for instant verification, and seniors and citizens of other countries will be able to scan biometric indicators of faces using a special *SingPass Mobile* application. It is expected that the new face identification service will counteract spoofing (spoofing – “substitution”; in the context of network security, spoofing attack is a situation in which a person or program disguises itself as another by falsifying data). As of 2018, the *SingPass* mobile app supports biometric fingerprint and face data for use throughout Singapore. At the same time, the country’s authorities announced plans to use facial recognition technology as part of the *National Digital Identity system (NDI)*. The same system should allow fingerprints and voice recognition technology.

Banks can use these technologies to make online transactions with a high degree of risk (for example, money transfers in excess of $10 thousand). Another potential area of application of biometric technologies includes the identification of visitors to commercial buildings, hotels, etc. According to representatives of the Smart Nation and Digital Government Office (SNDGO) of Singapore, the authorities of the country intend to retain ownership and control over all biometric data, and users will still be able to choose between biometric and traditional verification methods (including passwords). Meanwhile, strict data management and protection protocols will be provided.

As an example of a device that successfully uses biometric technologies, we can mention the portable biometric POS-terminal of the new generation *Move/2500B*, released in 2018 by *Ingenico*. It is distinguished by a high level of payment security along with the advantages of fingerprint authentication. Note that the device is aimed at those customers who do not have their own bank accounts; it takes into account local specifics (for example, fingerprint authentication is relevant for POS terminals in India, and in Mexico, all banks are required to verify the identity of each applicant for a loan). At the same time, the terminal can compare fingerprints with a sample stored in the database in a fraction of a second. Compliance with *PCI-v5* and *TQC* standards makes the *Move/2500B* a highly secure and extremely cost-effective portable POS system that supports all payment methods based on national identification programs.

ASHBURN INTERNATIONAL

Penki Kontinentai GROUP

ingenico GROUP

Online sales register for retail enterprise

Comprehensive solution managed by TransLink.iQ

www.ashburn.eu | mail@ashburn.eu

1.4. Online Sales Registers

An online sales register is a device designed to automate cash transactions and financial accounting.

An offline online sales register is a type of online sales register that is able to operate without connecting to the power grid, i.e., from a battery (the battery life depends on the model). There are Wi-Fi, as well as and Bluetooth mobile internet modules available. Such devices successfully replace calculators and sales logs; they are especially convenient in the conditions of off-site and street trade. With the help of the online sales register, you can calculate the funds in the cash register, the number of services rendered, the sum of the average receipt and the total revenue. In addition, such a device records the daily work results of each employee, shows the opening and closing time of the shift, and so on.

A mobile online sales register is a device that allows you to perform all the necessary cash transactions without being tied to a specific location. It is characterized by compact dimensions and low weight. It includes a built-in printer for printing the receipt. Despite the fact that the print speed rarely exceeds 100 mm / s, this is enough to complete the tasks. An important advantage is the built-in battery for autonomous operation.

Online cash registers with fiscal execution allow you to use two devices at once (a cash register and an EFTPOS/POS terminal) on one device. They can be presented in both stationary and mobile versions. Such devices allow integration with the main commodity accounting systems.

Online sales register for an online store is equipment for selling goods (or services) on the Internet that has a large number of interfaces and modules (3G, Wi-Fi, BT, USB, etc.). These are used for sending fiscal data to the fiscal data operator (FDO), as well as software updates, integration with popular CMS systems (*WordPress*, *Joomla*, *1С-Битрикс*) and various peripherals. There are models with a built-in thermal printer (check printing speed from 45 to 300 mm / sec, tape width from 44 to 80 mm), which allows you to print fiscal data, including a QR code, on paper or send an electronic check to the phone (in the form of SMS) or e-mail of the buyer.

Acquiring online cash registers are an integral part of the cash register equipment and are a 2-in-1 device: an EFTPOS/ POS terminal and an online cash register.

Currently, an increasing number of customers who are considering acquiring online cash registers, opt for smart terminals with acquiring based on Android, because banks provide their support, and installed applications provide maximum convenience, as for a regular smartphone.

1.5. Overview of Devices from World's Leading Manufacturers

Most of the global EFTPOS/POS terminal market is divided between the two largest players, *Ingenico Group* and *Verifone*, who occupy approximately 80% of its volume. Most banks use equipment from these manufacturers when providing trade acquiring service. Another company, *PAX Technology*, occupies the third position. Their terminals are much less common at the checkout counters of stores. Below we will discuss EFTPOS/POS devices from these three manufacturers and developers of advanced payment solutions.

Ingenico Group is a French company that specializes in providing equipment and technologies related to secure electronic transactions. The traditional business is based on the production of EFTPOS/POS payment terminals, but also includes complete payment software and related services, as well as software for merchants. For more than 40 years, *Ingenico Group* has been leading the payment industry in the field of seamless payments, providing its customers with reliable and secure solutions to expand the possibilities of commerce using all channels, including the Internet and on mobile devices. In March 2020, the French fintech company *Worldline* acquired *Ingenico Group* for $8.6 billion in cash and stock, creating the world's fourth-largest payments company by revenue.

Verifone is a multinational US corporation specializing in technologies for electronic payment transactions and point-of-sale value-added services. It is engaged in the production and sale of merchant-managed and consumer-oriented payment systems, including self-service payment systems for the public sector, financial, oil and medical industries, retail and hospitality. The company's products include EFTPOS/POS devices for electronic payments that use proprietary operating systems, security and encryption software, and certified payment software. The equipment produced by the company is capable of processing various types of payments, including signature and PIN-based credit and debit cards, contactless / RIFD cards, smart cards, prepaid gift cards, etc.

In 2018, *Verifone* was acquired by *Francisco Partners* for $3.4 billion.

PAX Technology is a Chinese company. It is focused on developing solutions for the international payment business. It was established in 2001. In 2002, it was selected as a supplier of EFTPOS/POS terminals for China *UnionPay Merchant Services*, in 2004 – for the *Bank of China* and the *Chinese Bank of Communications*. Today, 40 million PAX terminals are used in more than 110 countries around the world. The company operates in various markets through a network of representative offices and partners. Most of the *PAX* products are bank POS payment terminals and peripherals. *PAX* is also engaged in the development and maintenance of software for servicing the terminal network and solutions for conducting Internet payments. The company ranks 7th globally for the supply of payment terminals (according to the *Nielsen Report*) and is the only supplier of EMV solutions in the Chinese market. In 2016, *PAX* announced a strategic partnership with *Samsung* to implement the *Samsung Pay* payment method in *PAX* payment terminals. In the same year, the first smart terminal based on the Android OS – *PAX A920* – was presented at *TRUSTECH*.

1.5.1. Equipment by *Ingenico*

Compact and easy to use, Ingenico desktop terminals work equally quickly and safely with various payment options in small stores as they do in large banks as well as in supermarkets with many cash desks.

Ingenico's consumer-focused, universal payment solutions are easy to install and support. They provide all the connectivity options (USB, RS232, Ethernet, 3G/GPRS, optional Wi-Fi and Bluetooth).

Ingenico's EFTPOS/POS terminals can simultaneously work with multiple applications, which eliminates the need to install additional POS devices on a single cashier's workstation. Maintaining performance regardless of the number of running applications is achieved through the use of a two-processor scheme, one of which is fully responsible for the operation of applications, and the other for processing and encrypting transactions. Large screens with an extended user interface of all Ingenico devices allow you to use them in a web browser mode when working in advanced payment structures with a large number of additional applications, including non-payment ones.

EFTPOS/POS terminals and PIN pads by Ingenico are equipped with contactless readers by default. All Ingenico terminals are equipped with an impressive set of tools for wired and wireless connections, which allows customers to use various communication channels, while remaining in touch with the bank's host. At the same time, the configuration of the terminals provides a flexible choice of connection methods, saving the user's funds.

In 2014, Ingenico Group released its own Telium Tetra operating system with support for applications written in HTML5, and then launched an integrated POS solution that combines the Telium Tetra terminal and any modern tablet.

With a broad geographical reach with a presence in 125 countries, Ingenico can process over 300 types of payments, including – in addition to traditional credit and debit cards – the EMV standard, contactless (or NFC) technologies, e-wallets and payment solutions using QR codes.

In 2016, the APOS portable device based on Android was released with a 5.5" touch screen, front and rear cameras. It supports all types of payment (EMV chip & PIN, magnetic stripe, contactless / NFC interface). The secure, PCI 4.1-certified APOS terminal reliably protects cardholder data while remaining open to business applications developed in accordance to web standards.

Ingenico bank PIN pads provide fast and secure transactions. They have high performance, intuitive architecture and easy access to applications. Thanks to this device, you can save about 40 minutes of the cashier's working time during the work day at an average and high traffic point of sale. For example, by connecting the iPP220 PIN pad of the PCI v4 version to the desktop terminal of the Desk series, retail enterprises receive a complete and multi-faceted solution with the acceptance of contactless payments.

In 2018, Ingenico announced the release of the Move/2500B portable terminal. This biometric EFTPOS/POS terminal is aimed at the demographic of those without bank accounts in developing countries.

Retail PIN pads are the most well-known family of EFTPOS/POS payment equipment. Some models are equipped with front-facing cameras, which makes them suitable for accepting alternative payment methods and biometric identification, and touch displays are convenient for buyers. Ingenico's embedded solutions are tailored to the needs of the self-service industry and are designed for a variety of self-service payment scenarios, including round-the-clock payments at gas stations, ticket purchases, parking payments, sales of goods at vending machines and self-service kiosks, etc.

In turn, the iWB Bio series of wireless terminals provides freedom of action in acquiring, processing and verifying biometric data, allowing for secure biometric transactions, if necessary. Designed to simplify user identification and authentication, the shock-resistant iWB Bio series terminals facilitate the implementation of biometric controls in a wide range of payments, government benefit programs, and micro-loans. Scanning a fingerprint and comparing it to a template on a smart card chip takes less than one second, and biometric templates can be stored in a terminal or a remote database or used to customize magnetic or smart cards.

Let's look in more detail at the new generation Land/3000 PIN pad (Fig. 3), created on the Telium Tetra platform specifically for retail enterprises, and providing:

- *acceptance of traditional and alternative types of payments thanks to an additional camera;*
- *easy integration into trading systems;*
- *possibility of modernization thanks to replaceable modules;*
- *enhanced payment security with PCI PTS 5.x certification.*

When developing the *Lane/3000*, the requirements of local regulators were initially taken into account. The integrated plug-in modules used in *Lane/3000* comply with the latest PCI DSS security standards and minimize the cost of maintaining the current state of the terminals. This PIN pad implements modern encryption algorithms in combination with physical protection (cable disconnection sensor, Kensington lock). *Lane/3000* supports EMV chip & PIN, EMV chip & sign, magnetic stripe transactions, and accepts contactless card payments, NFC gadgets, e-wallets, and alternative payment methods. The terminal is easily integrated into the trading environment of any store [36]. Automatic remote diagnostics of the terminal is available, which provides proactive support for the device.

The terminal is offered in two versions: the "non-modular" model is focused exclusively on processing EMV payments at multi-line cash desks. The "modular" model includes additional high-tech features such as a camera, Wi-Fi and Bluetooth, that can be updated on site. With two options, businesses can choose whether they want to focus on the main payment method or offer more flexibility by allowing a range of other innovative payment and connection options. The terminal can work with more than 2500 payment applications, allowing you to accept more than 300 payment methods.

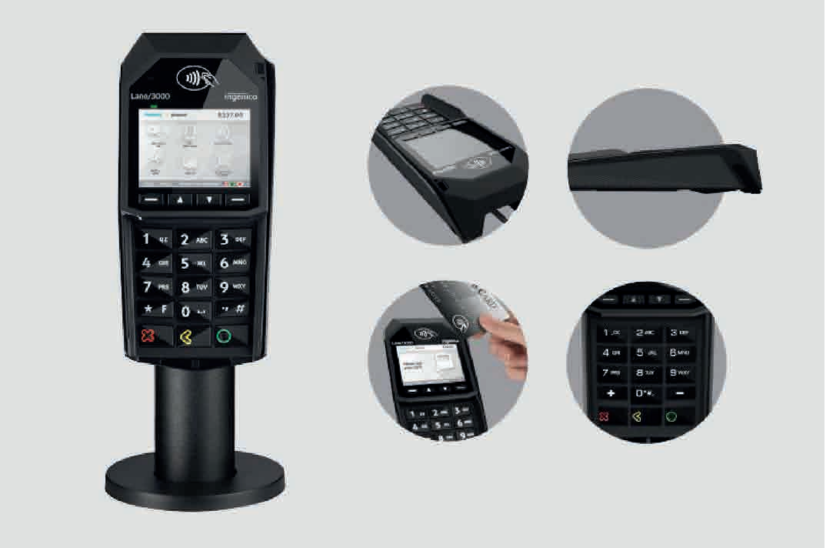


Fig. 3. The new generation Ingenico Lane/3000 PIN pad for retail.

The *Lane/3000* model is certified and fully complies with the latest global and regional PCI standards. It operates on the basis of the *Telium Tetra* OS, which uses the latest cryptographic software and peer-to-peer encryption technology to protect data. Due to the fact that these terminals are attached to each lane, they are equipped with anti-theft systems, such as Kensington lock locks in order to increase physical security. By supporting interconnected solutions, *Lane/3000* works in unison with *Ingenico* service platforms, enabling retailers to access business services such as back-office reporting.

Designed for mobility, the *Move/3500* terminal uses a wide range of *Ingenico* payment applications to support EMV chip & PIN reading, contactless cards and NFC wallets, allowing for a large dedicated activation area. The *Move/3500* is notable for a large screen, easy handling, as well as reliability and optimized battery life.

Ingenico's Smart POS terminals and payment modules cover all transaction points, whether automatic, multi-channel, in-store, on-street, or mobile. They meet the latest security standards and support any non-cash payment methods.

The line of Electronic Cash Register POS (ECR) based on *Android* offered by Ingenico, is designed to fulfill the current tasks of merchants in accepting payments behind the counter and in the field of mobility, especially in the transport and hospitality sectors. Smart POS terminals support all payment methods, including alternative ones, and offer sellers a full set of business services through Android business applications.

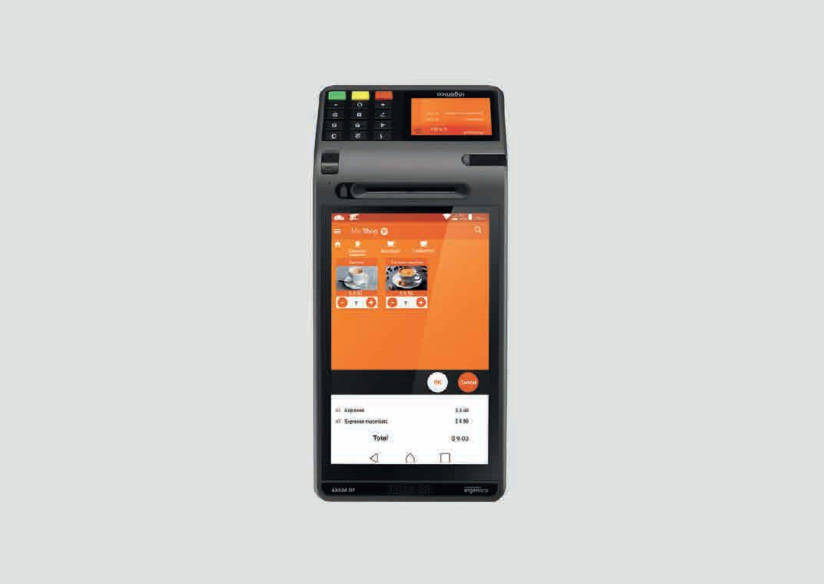


Fig. 4. AXIUM D7 POS platform running Android and the Telium Tetra operating system by Ingenico.

For example, the *AXIUM D7* is a convenient device for a scalable transition from payment to electronic checkout. The rich business ecosystem of *AXIUM D7* combines *Ingenico's* latest solutions in secure payments and store management. It allows you to browse the web and use a variety of Android apps.

The *AXIUM D7*:

- *assists merchants with expanded store functionality, inventory and personnel management, electronic accounting, and supporting peripherals;*
- *connects stores to a scalable Cloud Services Center platform offering POS, business, and analytics services;*
- *supports all payment methods including alternative ones, such as QR codes or multi-channel;*
- *includes a physical keyboard and an audio kit designed for accessibility purposes for merchants with physical disabilities;*
- *includes a large 7-inch HD tablet interface with an extended viewing angle.*

The *Ingenico Desk 3500* smart EFTPOS/POS terminal (Ethernet, GPRS/3G) allows you to use next-generation *Telium* applications and make NFC payments. The model is suitable for reading magnetic, chip, contact and contactless payment cards (*VISA, MasterCard, American Express, China UnionPay*). It has a color 2.8" display (320×240 px) with backlight. Dimensions: 168 x 83 x 40 mm. Weight: 325 g.

Ingenico's mPOS-class miniaturized payment devices allow you to accept magnetic, chip & PIN, and contactless payments in mobile commerce and services. When combined with a fiscal printer and an iOS or Android smartphone or tablet, *Ingenico's* mobile solutions form a fully functional mobile cash register system, regardless of the business location.

APOS A8 is a mobile and compact universal point of sale that fits in the palm of your hand. The *APOS A8* model is the most integrated solution for various retail outlets, fully providing the seller with control over the operation of the enterprise.

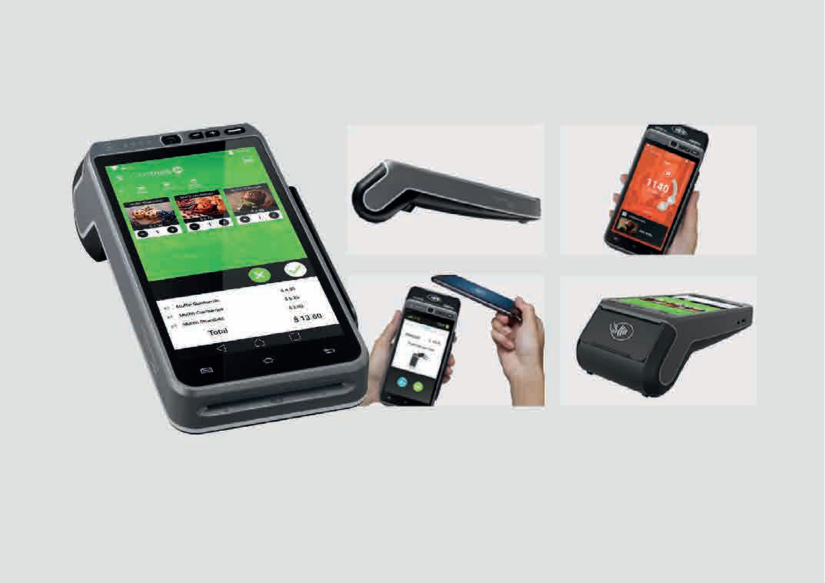


Fig. 5. The compact universal mobile device APOS A8 running Android, combining a payment terminal, cash register, printer and barcode scanner.

APOS A8 is a set of intelligent EFTPOS/POS terminal products using the platform's network solutions. Not only does it support all major types of communication (4G, 3G, 2G), but it also ensures the smooth operation of the Android 5.X OS. The model is equipped with a 5.5-inch 720P high-resolution screen, an integrated magnetic stripe card, a thermal printer, a camera, a 1D/2D barcode scanning module and other functional modules. At the same time, it provides full support for bank cards, NFC, scanning and other payment methods.

The business-oriented user interface of the *APOS A8* with a clear contactless zone, a large 5.5-inch touch screen and powerful processing capabilities speeds up the checkout process. *APOS A8* complies with international payment security certificates, such as PCI-PTS 5. x, providing a secure payment acceptance service, and supports both traditional and alternative payment methods (for example, using a QR code).

Supporting wireless connectivity with a full range of options (4G, 3G, GPRS, and Wi-Fi), the *APOS A8* offers broad flexibility in touch points while optimizing communication costs.

The capabilities of the *APOS A8* cloud services are compatible with the *Ingenico* suite of services, which includes fleet management for payment application updates, as well as commercial business services, such as business analytics.

1.5.2. Equipment by Verifone

Currently, *Verifone*‘s area of responsibility covers 150 countries, with 29 million of its devices delivered to their markets.

The *Verifone Carbon* line of devices, designed to develop trading, are intelligent business engines for a connected environment. It is a complete solution with a developed ecosystem for running a successful business.

To support the mobile business, the *Carbon 8* features a removable thermal printer for on-the-go printing, while a long-lasting battery with a capacity of 7680 mAh provides ease of mobile use, even supporting inventory management and price checking.

Carbon 10 has a simple setup and provides tools for convenient business management. Thanks to the flexibility of both desktop and portable use of the equipment, it is possible to serve consumers wherever and however they prefer, and at the same time safely accept payments of the latest types.

The integrated design of *Carbon* includes two screens for interaction between the seller and the buyer. It works as a full-featured desktop and as a portable POS device with flexible connectivity for reliable operation.

The device allows you to apply alternative payment options, such as gift coupons, loyalty cards, launch targeted ads and promotions. The tablet's display measures 10.1" (1280 × 800), and the terminal's is 5" (854 × 480). Payment acceptance options: EMV / MSR / NFC / CTLS.

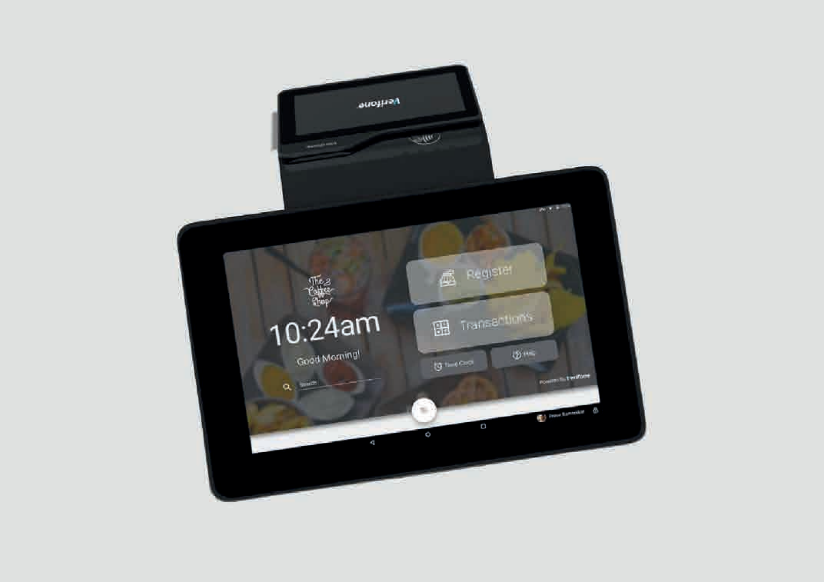


Fig. 6. Verifone's Carbon 10 end-to-end solution.

The device also has a front 2-megapixel camera for 1D barcode scanning and a rear 5-megapixel camera for 1D and 2D barcode scanning.

For a long time, payment terminals were considered just a means of accepting popular types of electronic payments. However, now the process of paying for a purchase is clearly evolving, and innovative products and services have begun to play a key role here.

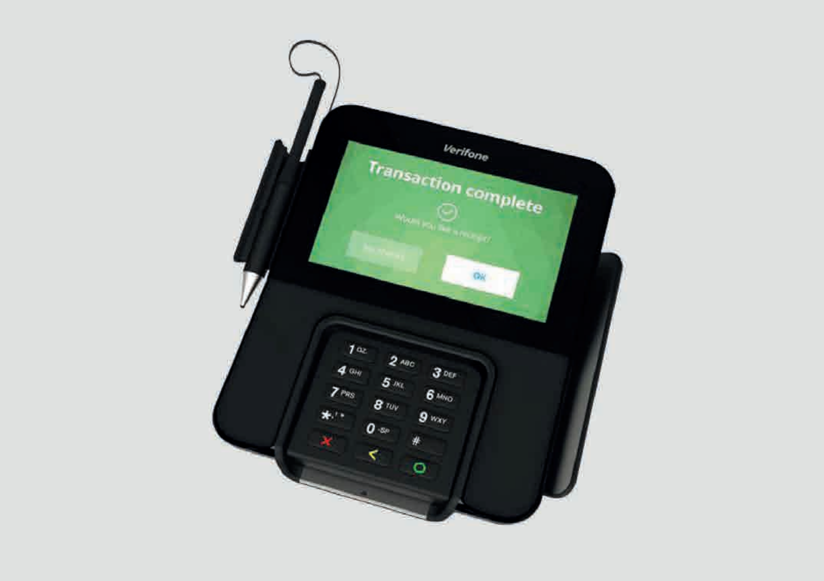


Fig. 7. Multi-channel EFTPOS/POS device Verifone M400 of the ENGAGE line with advanced features for commerce and payer personalization.

Verifone's line of *ENGAGE* devices for e-commerce provides interaction with the consumer in a dialog mode using a wide range of different business applications (including non-financial ones). For example, retailers can simultaneously accept electronic payments and conduct customer surveys. The open and flexible *Linux*-based operating system used in *ENGAGE* terminals allows you to create applications that, based on the accumulated customer information and transaction data, can create personalized offers for a specific target audience, including individual loyalty programs, gift cards and coupons [24].

We will briefly focus on the terminals that have already become widespread in the market. Among them, there are both stand-alone and integrated terminals. As such, for example, *Verifone Vx670, Verifone Vx675, Verifone Vx 680, Verifone Vx520* are standalone. *Verifone Vx520* is a desktop, stationary payment terminal with an external remote keyboard *PP1000 SE* for entering the PIN code. The device allows you to accept all currently known credit and debit cards, including contactless ones. The *Verifone Vx675* terminal is designed for mobile portable acquiring. The device works with all known payment systems and plastic cards – and *Verifone Vx680* meets the needs of small businesses (cafes, bars, etc.), where it is possible to configure a Wi-Fi network. The model features a large color display and a stylish design.

In turn, the *Verifone* line of integrated terminals includes *Verifone Vx805, Verifone Vx810, Verifone Vx820. Verifone Vx810* is a reliable terminal, but it has no CTLS. In contrast, the *Verifone Vx820* has CTLS with a color display.

Also of note are the *UX* series terminals – payment card terminals for round-the-clock operation (both outdoors and indoors) for paying for various goods and services in self-service mode (ticket sales, gas stations, vending and parking machines, etc.).

1.5.3. Equipment by PAX Technology

According to *PAX*, Android-based terminals have become the most popular products with a total sales volume of more than 300,000 units for 2019. These include mobile SmartPOS terminals for outbound trade and small retail outlets, SmartECR payment modules, and SmartKiosk self-service kiosks.

The “classic” EFTPOS/POS terminals produced by *PAX* are the most popular, cost-effective and fully certified solutions on the market - and the Linux-based *Prolin* OS platform provides a simplified approach to software application development that allows you to easily deploy new services and specialized business applications at an extra cost.

Today, you need to offer more than just a payment terminal. Therefore, it is necessary to benefit from the full range of features of the new generation of payment devices, as well as the market of sales-oriented business applications and POS devices based on Android, in order to maximize their full potential.

The model worth noting from the series of the latest mobile EFTPOS/POS terminals is the *S920*. The device is characterized by maximum productivity and is the ideal solution for both outdoor payments and as an additional payment device when placing orders with a busy work schedule. The *S920* comes with a built-in printer and a variety of connection options. Due to its compact size, as well as its speed and convenience for customers, the *S920* is very popular in premium retail and hospitality. The *S920* features an HD color touch screen and a bright backlit keyboard and is praised for its payment processing speed and extended battery life.

Key characteristics of S920:

- *2G (GPRS), 3G (WCDMA), 4G, WiFi, Bluetooth;*
- *Contactless NFC, chip & PIN, magnetic stripe;*

- *3,5" TFT QVGA display;*
- *Security: PCI PTS 4.x SRED;*
- *Open and flexible Prolin OS.*

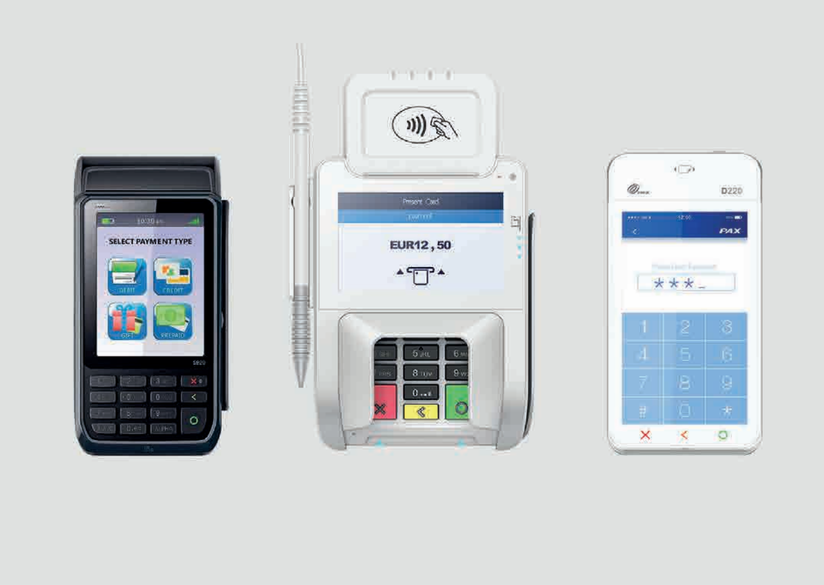


Fig 8. Classic and mobile EFTPOS/POS terminal line by PAX.

The *Q30* is a next-generation integrated smart PIN pad that comes with the latest industry certifications, including the PCI PTS 5.x certificate, allowing multi-specialty retailers to connect to any type of cash register, self-service kiosks, or terminals. The *Q30* features a high-resolution capacitive touch screen.

Key characteristics of *Q30:*

- *Ethernet, Wi Fi, Bluetooth;*
- *Contactless NFC, chip & PIN, magnetic stripe;*
- *4" TFT WVGA display;*
- *Security: PCI PTS 5.x SRED*
- *Prolin OS.*

With the *Q30*, merchants around the world can accept any type of payment, including traditional cards, QR code, mobile wallets, and NFC payments, via

Apple Pay, Samsung Pay, Wechat Pay, and Alipay.

The *Q30* model comes in compliance with the latest industry certifications, including PCI PTS 5.x certification and the contactless payment feature. It operates under the *Linux* OS.

The S300 EFTPOS/POS-terminal is a simple payment terminal for multi-channel merchants, which combines the convenience of retail payments with high security requirements for transactions based on contactless electronic signature, magnetic stripe and chip & PIN. In terms of reliability and security, the S300 is comparable to its more modern equivalent (the Q30 terminal). The model is equipped with a 32-bit ARM11 processor and a large amount of memory for increased multimedia performance.

Other technical characteristics of S300:

- Optional local network *(LAN Ethernet);*
- Contactless NFC;
- *3,5" TFT QVGA touch display;*
- Security: *PCI PTS 4.x SRED;*
- *OS Prolin.*

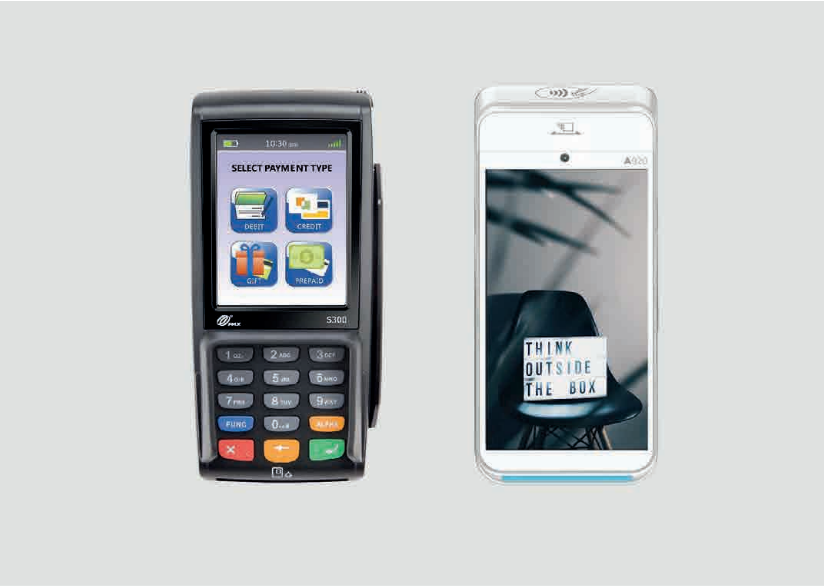


Fig 9. Payment PIN pad S300 (left) and mobile terminal Android SmartPOS A920 (right).

It is necessary to note the unified application platform *PAXSTORE* – this is the key competitive difference between *PAX Technology* and other payment solution providers. For example, in the *PAXSTORE*, users can buy and download applications and drivers necessary for configuring and administering *PAX* terminals, automating business, implementing loyalty plans, integrating with product accounting systems, and so on.

The A series payment terminals offered by *PAX* don't just look like high-end smartphones. The PayDroid OS embedded in them allows you to access marketing and analytical applications through the *PAXSTORE* app store. The *Android SmartPOS A920* mobile terminal accepts traditional and alternative payment methods, including contactless NFC, QR code scanning, mobile and wallet payments, chip & PIN, Swipe. The *A920* is equipped with a large high-definition screen and a fast thermal printer, as well as a lithium-ion battery for continuous operation throughout the day and two cameras with fast autofocus for 1D / 2D barcode recognition. It can be successfully used in such areas as food transportation, retail and transport.

Let's list a number of key features of the *A920*:

- *PayDroid OS running on Android 7.1;*
- *Cortex A7 processor;*
- *5" capacitive touch screen IPS WXGA with 720x1280 resolution;*
- *4G + WiFi + Bluetooth 4.0;*
- *Built-in GPS;*
- *Contactless NFC;*
- *2 cameras (5-megapixel rear + 0.3-megapixel front);*
- *5250MAH battery;*
- *Security according to PCI PTS 5.x SRED;*
- *Optional docking station and optional accessories can also be provided.*

The PAX SK800 is an all-in-one intelligent self-service kiosk. It can be installed in super and hypermarkets, chain restaurants, gas stations, train and bus stations, etc.

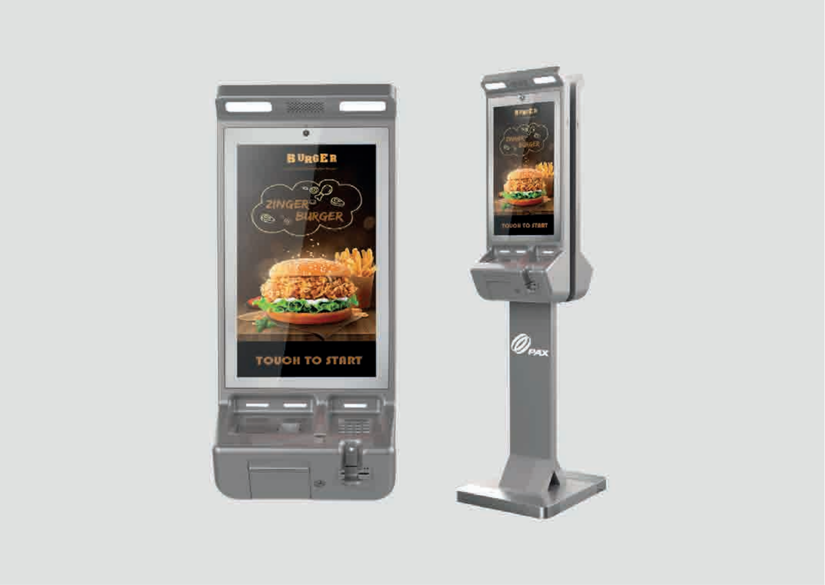


Fig. 10. Interactive self-service kiosk PAX SK800.

The *PAX SK800* model running *PayDroid* OS (based on Android 6.0) is distinguished by: a quad-core Cortex A-17 processor, 2 GB of RAM, and 16 GB of permanent memory; it has universal payment acceptance capabilities, a face recognition module, a 23.8" vandal-proof touch display and a built-in thermal printer. Connectivity options include Wi-Fi, 4G / 5G.

Currently, the *PAXSTORE* ecosystem unites over fifteen hundred developers, one hundred and fifty trading platforms in more than 80 countries of the world and 1 million terminals.

1.6. Security of Acquiring Equipment

Currently, any purchase initiates a very complex automated and highly integrated process, which involves not only merchants, but also acquirers, issuers, payment systems, and possibly many other market participants. Unlike in previous years, when this community was a relatively small club of organizations operating in isolation, the situation is now noticeably more complicated.

The emergence of new technologies and gadgets (such as smartphones and digital wallets), changes in customer habits, the requirement for individuals to accept card payments, and the growing interest in peer-to-peer payments have all led to fierce competition in the industry as organizations struggle to maintain their market position. Now, the entire existing payment ecosystem is just a component of the broader commercial landscape in which the fight against fraud and strife for ensuring data privacy is unfolding. This ecosystem is already an important part of a comprehensive information security infrastructure.

1.6.1. Hacker Attacks on EFTPOS/POS Terminal Networks

Usually, a POS system consists of: a PC system unit, a fiscal registrar, a cashier's POS monitor, a cash drawer, a programmable keyboard, a barcode reader, a buyer's display, as well as an EFTPOS/POS terminal, either stand-alone or integrated with the POS system.

To carry out a hacker attack on such a POS system, one can run a special program, so-called "malware", at the time of data transfer for payment processing. One such malware (called *AlinaPOS*) was available in the "Darknet" (underground forum) for only $6000.

The largest leak of personal data in the United States occurred in 2007 in an attack on the department store corporation *TJX*. The hackers obtained information of 94 million credit card holders. During another incident on October 15, 2014, a large American retail chain *Kmart*, which has more than 1,000 discounters in the United States, was attacked by hackers. According to the representative of the chain, the attackers managed to introduce malware into the retailer's payment system, allowing them to obtain the credit and debit card data of 40 million customers.

These are no random hacker attacks on retail chains in the United States. In 2015, the company *Home Depot*, which sells home improvement tools and equipment, also fell victim of hackers. The criminals managed to steal data of 56 million bank cards of the company's customers.

In September 2018, specialists of the *IBM X-Force IRIS* division discovered a malicious campaign aimed at EFTPOS/POS terminals in Europe and the United States. All these attacks were organized by the hacker group *FIN6*, who specialized on stealing payment card databases for their subsequent sale on underground forums.

The *FIN6* group first became known in 2016, when hackers attacked the POS systems of retailers and healthcare companies. Overall, they managed to steal the data of more than 10 million payment cards, which were then put up for sale in one of the underground markets [28].

To be specific, the criminals used the *Grabnew* backdoor to collect credentials, and a number of publicly available tools, as well as the *Trinity* malware (aka *FrameworkPOS*) to extract information from the memory of EFTPOS/POS terminals. The data was then compressed into a ZIP archive and sent to a server controlled by hackers.

During the new campaign, hackers from *FIN6* acted in a similar way, but in addition to Grab new and Trinity, they used a framework

Metasploit and the WMIC (Windows Management Instrumentation Command) program for automating remote execution of PowerShell scripts and commands. According to experts, the tools used by hackers are quite simple and available on the Internet. However, the main interest is the ability of attackers to surreptitiously bypass the system security tools.

During the new campaign, hackers from *FIN6* acted in a similar way, but in addition to *Grabnew* and *Trinity*, they used the *Metasploit* framework and the *WMIC* (Windows Management Instrumentation Command) software for automating remote execution of *PowerShell* scripts and commands. According to experts, the tools used by hackers are quite simple and available on the Internet. However, the main interest is the ability of attackers to surreptitiously bypass the system security tools.

FIN6 obfuscates *PowerShell* commands using base64 encoding and the gzip utility, generates random service names in the Windows event log, and dynamically generates file names on disk. In addition, the grouping uses certain PowerShell parameters to bypass antivirus programs and creates a winhlp.dat file to mask a malicious PowerShell script designed to inject FrameworkPOS into the lsass.exe process.

Attacks on POS systems have had serious consequences for large retail companies. The detection of two different types of malware on *ElasticSearch* servers suggests that similar incidents will be repeated [29].

Experts from *Kromtech Security* outlined their findings in a post in the *MacKeeper*. It was claimed, in particular, that two different types of malware – *JackPOS* and *AlinaPOS* – infected more than 4 thousand computers of *ElasticSearch* (known only to members of the technical community as a replicated “search engine” with open source code based on the *Apache Lucene* software license).

After initially detecting the malware during a routine scan, *Kromtech Security* researchers reported that more than a quarter of all *ElasticSearch* samples were exposed to files associated with hidden command and control servers. Much more worrisome is the fact that almost all (except for 1% of the *ElasticSearch* systems that were considered) are hosted by *Amazon Web Services*, one of the most popular cloud computing providers.

Meanwhile, the threat from various types of malware can be rather serious. Analysis of two strains showed that they have been reemerging as recently as last year, and in some cases the systems were infected more than once.

The use of *AlinaPOS* and *JackPOS* in *ElasticSearch* means that threat agents could destroy important information, gain full administrator rights, and perform remote code execution. The servers in question were very vulnerable due to a lack of password security or technology for authenticating user sessions. As a result, different types of malware can remain active in the entire group of systems, even if they were detected on individual servers.

Among the many “red flags”, some file names refer to the malware *AlinaPOS* and *JackPOS*. These are typical POS malware that tries to steal credit card details using various methods. They first became widespread in 2012, but are still in use today – and are available for sale online. [31]

When *Kromtech Security* researchers began to look for updates to this type of malware and the status of files that are distributed on “unsuspecting” servers, it turned out that there are new and updated versions of these malicious programs that any attacker can currently buy.

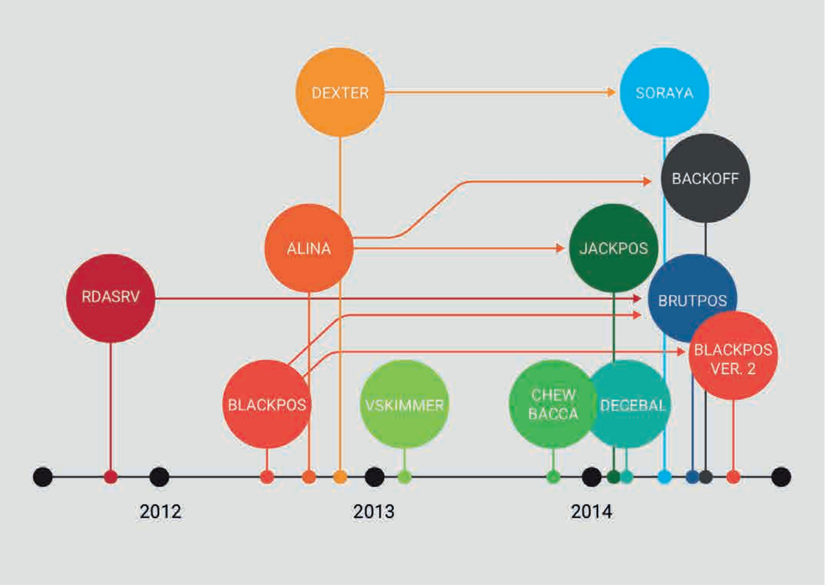


Fig. 11. The growth dynamics of the spread of POS malware and their relation to updates [31].

Back in January 2014, the US FBI published the *Recent Cyber Intrusion Events Directed Towards Retail Firms* report which described spyware parsers installed by hackers on EFTPOS/POS terminals [27].

Although the hacker attack on the Target retail chain in late 2013 affected only residents of the United States, it became widely known around the world. During the incident, more than 40 million bank cards and the data of more than 70 million customers of the company were compromised — in just a month, the attackers obtained more than 11 GB of confidential information [18].

Hackers focused their attention on cash registers and EFTPOS/POS terminals. As it turned out, these terminals were infected with malware that intercepted the necessary information.

How exactly did this happen? The thing is that even before getting to the servers of the payment system, card data is being encrypted, which makes its interception almost meaningless. However, on the way to the server the information is decrypted at a certain point to the form of a simple text (for a very short period of time) and it settles in the RAM of the cash register or the computer linked to it. At this very moment, a special malware program comes into operation, whose task is to "scrape" all the decrypted data from RAM and extract the required information from them: card numbers, names, addresses, secret codes, etc. Such programs, the so-called *RAM-scrapers* make up a separate malware category and have been known for a long time.

In the case of Target, hackers used a *RAM-scraper* called *BlackPOS* and infected all EFTPOS/POS terminals with it at once. As it seems, the task was performed in a centralized manner, because otherwise they would have had to install the malware on each terminal manually.

Researchers from *Seculert* confirmed this version by finding traces of infection of one of the computers in the internal network with the *BlackPOS* malware, which, with a sufficient level of knowledge could be obtained on the black market. Of course, *BlackPOS* is not the only POS malware: after all, in addition to *Target*, two other major retailers were attacked with similar malware.

It is also worth noting the first report of *FinCERT* (Financial Sector Computer Emergency Response Team of the Bank of Russia), which notes the growing interest of attackers in stealing payment card data using EFTPOS/POS-terminals.

According to *FinCERT*, since the end of 2015, certain "modified" EFTPOS/POS terminals which are able to store card data with a PIN code and transmit it remotely, are being are offered for sale. The main geographical distribution of such devices is the United States; however, there are cases of their detection in Europe. Usually, the attackers "work" in close cooperation with the merchant employees, who have full access to the EFTPOS/POS terminal and (in some cases) to the client's payment card.

FinCERT also discusses the emergence of malware designed to infect cash terminals running on *Windows*. The simplest malware of this kind is capable to intercept data entered from the keyboard (keylogger), remote control and receive data from the RAM of the EFTPOS / PO terminal. Meanwhile, the main modules (with the exception of the software launcher) are not detected by anti-virus protection. There is also a version of the malware that allows one to send stolen data, instead of storing it in the device's memory [63].

1.6.2. Hardware Security Modules (HSM) by Thales

For more than 30 years, payment hardware security modules by *Thales* have been used in various business fields. The company's products provide guaranteed data security and reliability in any environment, while maintaining the efficiency of the business.

The recently-published report by *Thales* [46] is based on results of an online survey conducted by the research company *IDC* among 1,200 managers, as well as employees responsible or influencing IT departments and data protection in a particular organization (industry, healthcare, financial services, retail, government structures in nine countries, including the United States, Germany, India, Japan, and the United Kingdom) in November 2018. The survey covered a wide range of organizations, most of which had between 500 and 10,000 employees.

One of the main conclusions of the report is that no one is really protected. Even the most advanced companies become victims of leaks; and the higher the level of complexity of the business, the more likely problems are to occur. 64% of those who spend more than 10% of their IT budget on security confirmed that they have experienced leaks at least once, 34% among them – in the current year. Respondents claim paying about equal attention to the security of the network (36%), applications (30%) and data (34%).

Respondents noted a wide range of data security issues related to mobile payment technologies. In addition to fraudsters (who are slightly leading the list of problems), they pointed to the disclosure of identity information, weaknesses in authentication protocols, and the potential for disclosure of payment card information. In their opinion, the main methods of solving the problems of mobile payments include the use of strong encryption (31% of respondents), multi-factor authentication (30%) and strict password requirements (30%).

Conclusion: it is necessary to use tools that will allow you to manage security even in the most difficult situations; the tools should cover both traditional on-premises and modern cloud technologies, helping to manage encryption and tokenization, which provide better protection in today's insecure environment.

Let us note that payments made using cards in the EFTPOS terminal via the Internet or mobile application include various elements of confidential account data. Although important components of the cardholder's data (the main PAN card number, the cardholder's name, and the card expiration date) are listed on the payment card itself, their fraudulent interception can give attackers information that can be used for illegal actions.

It is important to emphasize two different aspects of ensuring end-to-end protection of a payment transaction. The first relates to the security of the payment system infrastructure; in particular, to the interaction between participants as the transaction moves from the point of payment to its target point – where it is either confirmed or rejected by the issuer or payment operator. The tasks of the payment infrastructure in this part include, first of all, preventing the possibility of compromising cryptographic keys shared by all participants, ensuring only authorized access to the hardware security modules (HSM) of trusted applications and personnel, as well as reducing the time spent by the HSM in an inactive state to a minimum.

The second aspect concerns the permanent protection of data, including the periods when the HSM is in an inactive state, which is relevant for most participants in any payment transactions (issuers, merchants, buyers, payment operators, payment gateways and payment networks). In this regard, the tasks of data protection in the conditions of non-operational equipment are primarily related to providing reliable protection against fraudulent influence on any data allowed for storage in accordance with the PCI DSS standard.

The payment industry uses three main technologies to protect cardholder data in a complex of infrastructure solutions and storage solutions: *point-to-point encryption (P2PE), data encryption in an inactive state, and tokenization*.

Thales payShield HSM hardware modules are a vital component in improving security, and the P2PE (Point to Point Encryption) standard is widely used to protect vulnerable areas in the payment infrastructure (see Annex).

Traditional POS systems are increasingly using the P2PE standard in order to avoid vulnerabilities associated with data transmission using a magnetic stripe and a card chip in the clear. Thus, the use of P2PE implies data encryption already at the capture point (i.e. in the EFTPOS/POS terminal), after which this data is maintained in an encrypted state in the POS system and can only be decrypted at the payment gateway or the acquirer's host using HSM.

Hardware security modules (such as *Thales payShield*) are a vital component in improving security and reducing the risk of key compromise, through the use of reliable hardware key generation, distribution and management technologies within the implementation of the PCI P2PE standard. *Thales payShield* HSM meet the most stringent PCI key management requirements, implementing this in a simple and cost-effective way, and also facilitate secure PIN processing in accordance with the requirements of the PCI security standard, using the standard PIN management features available in the HSM.

PayShield hardware protection modules are used in the global payment ecosystem by issuers, service providers and purchasers, processors and payment systems [17]. They play a fundamental role in ensuring the issuance of credentials, user authentication, card authentication, and the protection of sensitive data for personal and remote digital payments. At the same time, the cryptographic needs of all major payment applications for contact and contactless chips, mobile secure elements, and host card emulation applications are supported in accordance with evolving security standards from organizations, including EMVCo and PCI SSC, as part of broader security audit compliance requirements.

1.7. The Future of Acquiring Equipment

Mobile POS have broad prospects for the future: not only do they perform the same functions as conventional POS systems, but they do much more. Therefore, by integrating various functions into your POS machine, it is possible to create a successful business management toolkit. In addition, the small, portable design of the tablet-based POS system provides greater flexibility and a higher quality of interaction between the seller and the customer.

The modern world dictates new conditions for making payments. The payment function itself is no longer a commodity. No one talks about it as a separate product anymore. The combined multi-channel approach to customer service comes to the fore. It includes the selection of a product (or service), the delivery process, the payment process, which is accelerated by the introduction of chat and voice bots acting as consultants, as well as face recognition solutions. Today, an ordinary phone is becoming a payment terminal, where the payment function is integrated into the business applications of retail enterprises.

For example, during the *Ingenico Payment Summit 2020* forum (Barcelona, Spain), the company's latest developments in the EFTPOS/POS terminal industry were presented. Thanks to the introduction of special software, *Android* devices have been turned into multifunctional terminals that are interconnected with business applications and can perform, for example, the role of cash registers. *ASHBURN International* has already developed such solutions and is implementing them in various countries around the world [5].

ASHBURN INTERNATIONAL

Penki Kontinentai GROUP

ingenico GROUP

Smart POS for your business

Android-based Mobile POS terminals

www.ashburn.eu | mail@ashburn.eu

Chapter 2. Aqcuiring System Software

Thanks to the introduction of new POS technologies, the adaptation of enterprises of all types to the *cashless society* is facilitated. At the same time, POS system software and hardware suppliers are becoming important supporters of moving towards cashless payments, enabling companies of all shapes and sizes to accept not only payment cards, but also mobile, digital and other contactless cards.

A question arises – which features of the software for POS systems are in demand by these companies? After all, POS systems have hundreds of different functions depending on the specifics of the business: there may be situations when you need a full arsenal of functions, or it will be enough to limit yourself to only a part of them. When searching for software for POS systems, you should think about what features you need to have, and which of them would be nice to have, and which, in all likelihood, will never be needed.

In addition to the basic cash register functions that are included in each POS solution, you should carefully study the following six key feature sets before choosing a system. It should be noted that the set of specific functions may vary depending on the system [16].

Supporting mobile applications. The best POS systems have applications that are installed on Android tablets and iPads, and sometimes even on smartphones, turning these devices into mobile FTPOS / POS terminals so they can be used as mobile cash registers for accepting orders and serving customers anywhere in the store or restaurant. In addition, you can easily attach such a tablet to the stand and, by adding a number of peripherals (such as a cash drawer and a receipt printer), create a cash register on the counter. Although a number of POS systems can be used with both Android tablets and iPads, some of them are specific only to a particular platform.

Inventory management. Do you need alerts on low inventory levels or automatic reordering of items? If you have a retail business, estimate the number of item IDs (SKUs); some apps only support a limited number of them. Also, consider whether you need vendor and purchase order management tools. In addition, if you need advanced inventory management functions, and they are not available, will the system you are purchasing be able to integrate with the inventory software?

Customer data management and loyalty programs. You should consider if you need customer email addresses for your mailing list. What about phone numbers and addresses for the delivery of the goods? Or do you need a system with a built-in CRM (Customer Relationship Management) application that allows you to create customer profiles with detailed purchase histories, add notes, such as birthdays and personal tastes of customers? Should the purchased POS system include a loyalty program?

Personnel management. If your employees will use a POS system, then you need to control the data and functions that they will be able to access. For example, you can allow store managers to process refunds, or allow all cashiers to do so. Do you prefer role-based permissions or do you want to set them individually for user profiles? Also, do you need to set up arrival and departure hours so that your employees can enter and exit using the POS system? If you already use time and attendance software, will it be integrated with the POS system?

Making reports. Although all POS systems are capable of generating reports, their list, number, specific types, and settings vary from system to system. Will you need sales data within an hour so that you can serve your business more effectively? Do you need a list of the best-selling and least-requested items in order to improve your existing product range? Do you need the system to automatically send you certain reports by email? Do you need real-time reports that you can access using the mobile app?

Integration features. The software in most POS systems can be integrated with various external systems. For example, the POS system can be connected to the merchant's back-office accounting program. This will save time on exporting sales data from the POS system and manually uploading it to the accounting program. Do you need a POS system that integrates with accounting software such as accounting, payroll, e-commerce platforms, and email marketing services?

2.1. Payment Transaction and Its Types

A *transaction* (Latin *transactio* – agreement, contract) in the general sense — a deal involving the exchange of data with subsequent adjustments to the system. This term is increasingly used in banking when it comes to the movement of funds in the process of purchase and sale.

The result of the transaction is a change in the amount of funds in the owner's bank account (settlement, card or other).

In this context a transaction may mean:

- *cash withdrawal at an ATM;*
- *payment by card in the store or in any other merchant (this is the most common case). Such a transaction (card transaction) begins from the moment the cardholder pays for the product or service. In the card industry, a transaction is not a transfer of funds, but primarily information about the payer and recipient of the payment, the amount of the payment, the participants of this operation, etc. In other words, in the card industry, a transaction is a set of data generated by the service point and the payer's card to record the transaction being made;*
- *money transfer between accounts;*
- *other operations.*

If the transaction is approved by the banking institution and executed, the transaction is considered successfully completed – and each such operation is necessarily recorded in the database.

The result of a bank transaction is always one of the following actions:

- *approval followed by payment processing;*
- *refusal (denial).*

In the practice of credit institutions, there are several main types of transactions:

- *a bank transaction is the ability to perform any operations related to the transfer of money between customer accounts;*
- *other types of transactions (for example, a special type of transaction is possible in ATMs: withdrawal or deposit of cash; transactions in smart safes, information kiosks, payment terminals – all these devices are the points of generating the corresponding transactions).*

Note that in card transactions, the crediting of money to the account or the debiting of funds from the account is spaced out in time.

According to the method of implementation, the following forms of execution of card transactions are distinguished:

- *online transactions;*
- *offline transactions.*

These two forms of transactions differ in the following matter: in an online transaction, authorization of the availability of funds in the cardholder's account at the bank or processing center of the issuer is performed online, i.e. directly at the time of the transaction itself. On the contrary, in an offline transaction, such an operation is not performed and the decision is made at the level of communication between the terminal and the card or the payer's ID without contacting the acquiring bank and subsequent verification measures. This procedure applies to card accounts where the balance available for spending on the card is reserved in advance by the bank, and the data on the payment amount and card details remain in the memory of the POS-terminal.

If the limits set on the card and in the terminal match, the transaction passes, and the withdrawal of funds from the card is approved. For this purpose, the process of closing the day is provided: after connecting the terminal to the communication channel, the transaction data available in the terminal is transmitted to the host of the processing center.

Transaction statuses include: authorization at the beginning, then approval, and then closing of the day (final confirmation of receipt and accounting of all transactions made by the processing center) within one financial day.

The *response code* (decoding of the actionCode) is a digital designation of the result that the user's access to the system led to.

Here is a list of the most common reasons for the failure of the transaction. Each of the options listed below corresponds to a specific response code [37]:

- *the card is blocked;*
- *insufficient balance;*
- *card restrictions (for example, on making international or online payments);*
- *incorrectly entered PIN code;*
- *suspected fraud (detection methods vary from card stop lists to analysis of devices and payment behavior);*
- *technical reasons;*
- *error in the recipient's account number or other bank details.*

2.2 Transaction Processing at the Processing Center

The process of purchasing by payment card is a complex multi-sided procedure in which the buyer and the merchant are located between the following chain: processing center, self-payment system, card issuing bank, acquiring bank, as well as the bank where the funds are received.

Information and technological interaction between settlement participants in this chain is provided by the processing center. As we have already noted in the Introduction that there are different types of processing centers: payment system clearing centers, processing centers of banks that connect to different payment systems, as well as centers of special processing companies that connect banks that do not have their own processing centers (such companies outsource services for access to payment system processing).

A *payment gateway* is a service that accepts authorization requests from points of sale of goods and services and routes them to different acquiring banks according to the established rules. The role of the payment gateway in the entire payment chain from the payer to the merchant can be described by analyzing the transaction path (Fig. 12a and Fig. 12b):

cardholder — merchant – payment gateway – acquiring processor – international payment system (for example, VISA/Mastercard) – issuer processor – card issuing bank.

In other words, a payment gateway is a software and hardware module for routing payments between a merchant and various acquirers through a single protocol for interaction of various payment terminals with a payment gateway.

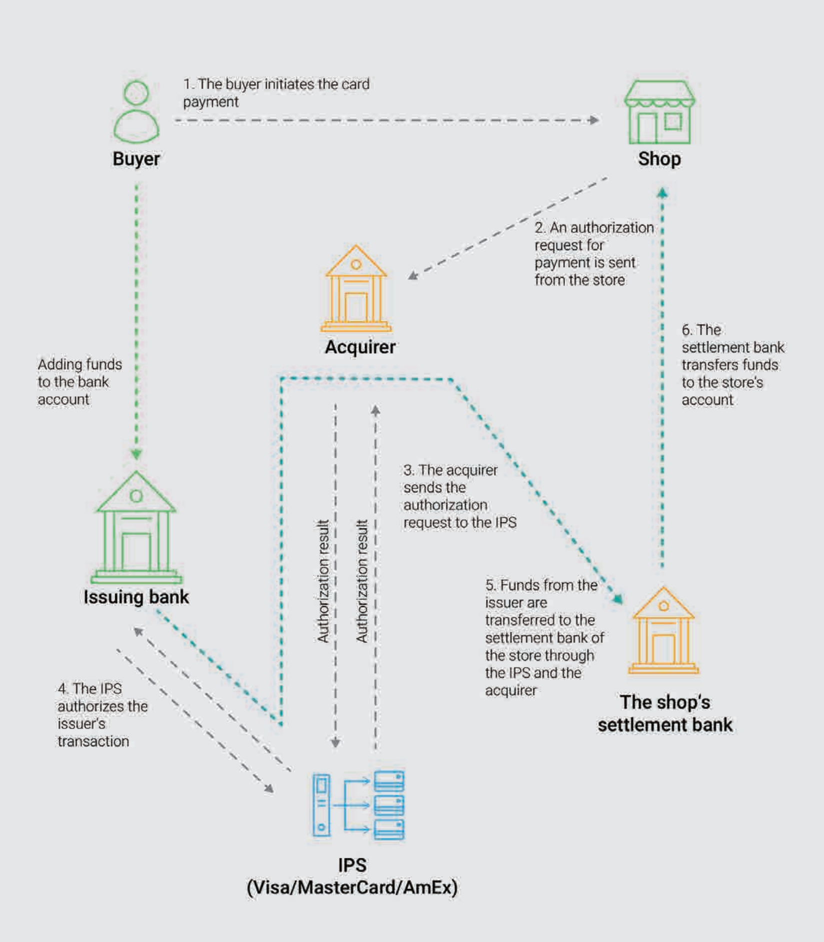

1. The buyer initiates the card payment
Buyer
Shop
2. An authorization request for payment is sent from the store
Acquirer
6. The settlement bank transfers funds to the store's account
Adding funds to the bank account
3. The acquirer sends the authorization request to the IPS
Authorization result
Authorization result
Issuing bank
5. Funds from the issuer are transferred to the settlement bank of the store through the IPS and the acquirer
4. The IPS authorizes the issuer's transaction
The shop's settlement bank
IPS (Visa/MasterCard/AmEx)

Fig. 12a. The scheme of traditional acquiring.

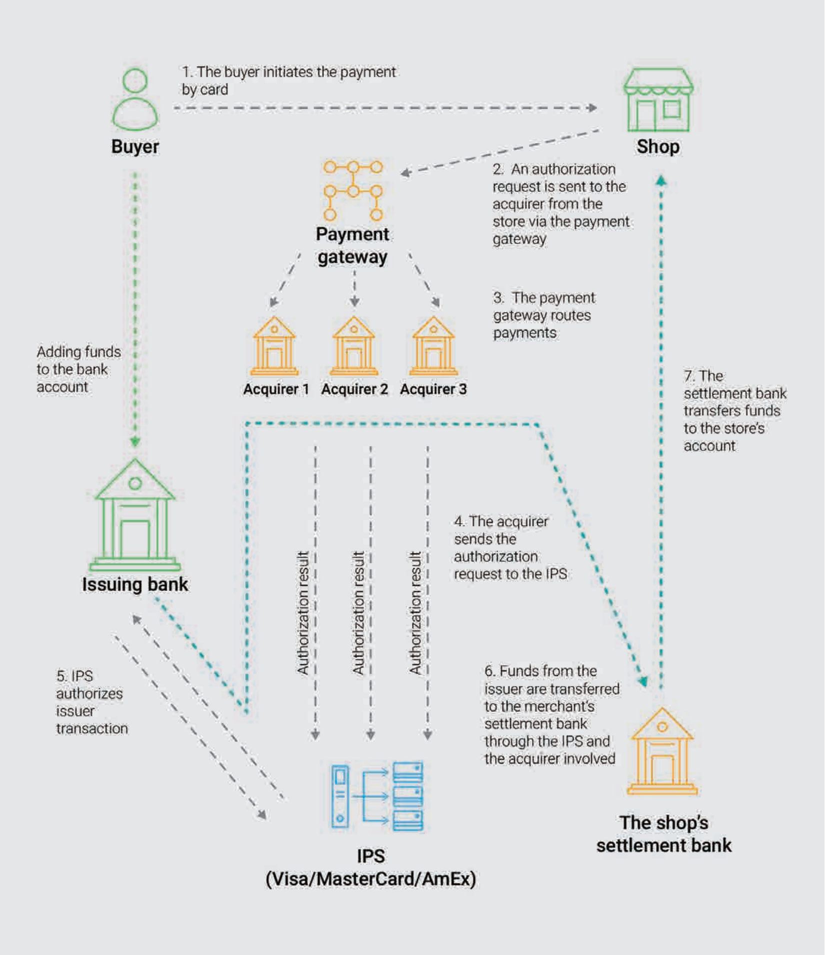

1. The buyer initiates the payment by card
Buyer
Shop
2. An authorization request is sent to the acquirer from the store via the payment gateway
Payment gateway
3. The payment gateway routes payments
Acquirer 1
Acquirer 2
Acquirer 3
Adding funds to the bank account
7. The settlement bank transfers funds to the store's account
Issuing bank
4. The acquirer sends the authorization request to the IPS
Authorization result
Authorization result
Authorization result
5. IPS authorizes issuer transaction
6. Funds from the issuer are transferred to the merchant's settlement bank through the IPS and the acquirer involved
The shop's settlement bank
IPS (Visa/MasterCard/AmEx)

Fig. 12b. The scheme of acquiring through a payment gateway.

When making payments in an e-commerce environment, the customer selects the product or service that interests him and proceeds to the payment procedure. After placing an order, the customer is redirected to a secure payment page, and the transaction data (payment card number, expiration date, CVV code) is encrypted and sent to a specific payment processor through the gateway. The payment processor contacts the issuing bank of the payment card and receives a message from it in the form of confirmation or rejection of the transaction. Next, the response is transmitted to the payment gateway, which transmits it to the seller's website – where the information is interpreted and the corresponding response is generated. If the transaction was approved, the seller fulfills the order.

The payment gateway facilitates the smooth flow of such transactions by encrypting sensitive data and transferring it between the payment portal (website or mobile device) and the bank/payment processor. Since security is a core component of all payment gateways, every transaction between a merchant and an issuing bank is encrypted to protect confidential financial information.

At the prepayment level, the payment gateway helps merchants with integration, counteracts and minimizes fraud and risks. It conducts payments and supports back-office activities.

At the post-payment level, the payment gateway provides the preparation of reports, the management of charge disputes, and the management of settlements and reconstitution (a control procedure that consists in identifying and verifying the execution of each transfer using at least three indicators defined by the payment system) [39].

Payment Service Provider (PSP) is a company (often a third-party company) selected by the merchant to process payments through various channels using various payment instruments. An example of a PSP provider is PayPal, which provides such services.

2.3. Transaction Routing in Complex Acquiring Ecosystems

Routing is the mechanism by which the rules for selecting the payment route are configured in accordance with the specified parameters. Routing payments to multiple acquirers is the automatic distribution of transactions by the payment gateway to the acquiring banks, for example, based on card numbers to match the acquiring bank and the issuing bank. Routing payments to two banks allows you to combine the issuing bank and the acquiring bank to deliver the payment to the acquiring bank that is the issuer of the corresponding card, which makes it possible to exclude several links in the chain of the transaction. Therefore, the acquiring bank can conduct an internal (On-us) operation, which significantly reduces the cost of the transaction.

Processing incoming transactions is one of the main functions of any payment system, and transaction routing in systems with online authorization is an important element of this process. At the same time, the cost of processing a payment in acquiring is largely determined by the type of payment transaction.

There are only four types of payment transactions characterized by the amount of interbank remuneration (or interchange, short for interchange fee), which is received by the issuing bank each time that the card issued by it is used as a means of payment in a transaction processed by the acquiring bank.

The size of the interchain depends mainly on the type of card (debit or credit; latter further subdivided as Classic, Gold, Platinum, etc.). In addition, there are business cards for which the interchain rate is the highest, while the debit card rate is the lowest.

Interchain is included in the commission fee to the acquiring bank; it is paid by the merchant. The size of the interchain is set by the payment system, whose members are both the issuer and the acquirer. Acquiring fees for merchants and processing companies offering payment aggregator services depend on the size of the interchange amount.

The following transaction types are listed in ascending order of the interchain rate:

1. ***On-us*** is a transaction for which the same bank is both the issuer of the payment card and the acquirer processing the payment with its participation. In this case, the interchain rate is zero.

2. ***Domestic*** is a transaction for which the issuer and the acquirer are located within the same country. Depending on the payment system, the interchain rate can range from an average of 0.2% (as in the EU) to 1% or more of the payment amount.

3. ***Intraregional*** is a transaction for which the issuer and the acquirer are located in different countries, but within the same geographical area established by the payment system. In this case, the interchain rate varies on average from 0.6% to 1% and above of the payment amount.

4. ***Interregional*** is a transaction for which the issuer and the acquirer are located in different geographical zones. The interchange rate for such transactions is the highest.

The computing center of the acquiring bank or processing center identifies the transaction, determining whether it is initiated by a client of this acquiring bank, or by a client of another bank of the payment system. If in the first case the transaction is processed on-site, then in the second case it is forwarded to some processing node of the system, where it is either processed or further routed.

The question of where the transaction is processed depends on the level of technical development of the payment system. Processing power in the initial period is usually concentrated in a single center of the system, and the processing center is also assigned part of the functions of the acquirer.

Let us note that the configurable automatic routing of the transaction to the desired acquiring bank, depending on the card's *BIN* (*BIN routing*), significantly reduces the cost of processing the transaction for all participants in the chain which allows the acquirer to offer the merchant a more favorable acquiring rate without losing margin for the cost of their services. So, the processing company can redirect payment transactions for processing to those acquiring banks for which these transactions are *Intraregional*, *Domestic* or even *On-us*.

To illustrate *BIN routing*, let's look at the operation of a specific online store in Lithuania, the main sales volume of which falls on the EU and US regions. Let's assume that this store has its own PSP, which provides it with the ability to route transactions to various acquiring banks in the EU and the USA, depending on the BIN of cards served in the payment terminal. Since when a customer enters their bank card number, the processing platform can use the card's BIN to determine the issuing bank and the country in which it is located, it will automatically redirect such a transaction to the appropriate acquirer for processing it.

Meanwhile, the PSP gets the opportunity to offer the online store to accept card payments at lower rates without reducing its own margin, and the latter, in turn, gets the opportunity to optimize and reduce its costs for accepting card payments.

2.4. Processing Center Software

Often, financial organizations face the question of how they should process card transactions: whether to use an external resource for this purpose or create a processing center of their own.

The question of whether to outsource processing services or not, whether fully or partially, has no clear answer. The choice of the optimal operating model depends on the internal potential and development strategy of the company. Regardless of the chosen model, there is a question of choosing the software for the processing center. There is currently a number of companies offering such software available on the global market.

2.4.1. The Universal BASE24-eps Solution by ACI Worldwide

ACI Worldwide (USA) supports electronic payments for more than 6,000 organizations worldwide. More than 1,000 of the world's largest financial institutions and intermediaries, as well as thousands of the world's leading merchants, rely on ACI every day to complete transactions totaling $14 trillion in payments and securities transactions. ACI provides world-class cloud payment solutions and services to more than 4,200 organizations worldwide in order to reduce their time to market and minimize technical, operational, and business risks.

In the payment processing industry, managers are increasingly faced with the challenge of improving business profitability, along with maintaining a constant flow of new transactions, channels, and technologies. The need to reduce dependence on legacy systems, reduce the cost of hardware, operating systems, and their maintenance has become paramount for financial institutions. We will look at the BASE24-eps system created by ACI Worldwide, which is able to function as the main processor for processing all types of transactions – both traditional (which organizations manage today) and transactions of the future.

BASE24-eps is an integrated, universal software solution for acquiring, authenticating, routing, switching, and authorizing financial transactions across multiple channels [41]. UP Retail Payments with UP BASE24-eps support is a corporate level payment solution that provides a complete set of features to support electronic payment transactions. This includes debit and credit transactions at ATMs and points of sale, as well as banking services at branches and via phone, mobile commerce and online banking, regardless of the payment instrument used.

BASE24-eps is an implementation of a new generation of payment platform, based on ACI years of experience in the development and support of payment software, taking into account the presence of a global customer base. BASE24-eps has multiplatform options that include Red Hat Enterprise Linux / x86. Research shows that by leveraging this environment, organizations can reduce technology operating costs by more than 50%, while maintaining the same performance, scalability, reliability, and high availability. UP BASE24-eps also runs on HP NonStop, IBM Zseries z, IBM Series p, and Oracle Sun servers. In addition, retail payments with BASE24-eps are available on-premises or in a private cloud environment. Private cloud services help to avoid unnecessary initial costs, freeing IT staff from everyday operational tasks.

Key features of the solution:

- *processing large amounts of data with high availability thanks to a scalable fault-tolerant software architecture;*
- *support for multiple platforms, including Red Hat Enterprise Linux / x86;*
- *compatible with the PA-DSS security standard;*

- *flexible switching and routing to major network cards, processors, and hosts;*
- *powerful mechanism for authorization scenarios according to individual business logic;*
- *multi-institution coverage and multicurrency;*
- *built-in EMV support, including EMV cards for multiple applications;*
- *support for non-card-related electronic payment transactions;*
- *support for traditional card delivery channels and e-commerce, including the Internet. and mobile devices;*
- *external use of core transaction processing and application security services;*
- *customizable software development tools to speed up the connection of new endpoints;*
- *built-in integration with ACI back office, risk management and monitoring applications.*

2.4.2. WAY4 Solution by OpenWay Group

WAY4 is a full-featured platform for electronic banking, payment and non-payment card processing, and omnichannel remote banking. Developed by the Belgian company *OpenWay Group*. It is used in more than 100 banks in various countries of the world (in particular, in the Russian Sberbank). The *WAY4* platform supports Internet and mobile banking, ATMs, and EFTPOS/POS terminal networks.

Let us recall that *omnichannel* is a marketing term that refers to the mutual integration of disparate communication channels into a single system in order to ensure seamless and continuous communication with the client.

The platform’s capabilities provide support for services such as e-wallets, issuing plastic cards from retailers and branded bank cards, trade acquiring, financial switching, and channel management. *WAY4* serves as the foundation for building digital banking solutions, national or local payment systems, and is used by leading banks, payment operators, and payment gateways around the world. The *WAY4* platform was used to create a single payment space that provides online routing of authorization requests and clearing of settlements between banks participating in a number of projects. *OpenWay* client banks use it to process financial transactions for all types of cards and a number of other services.

WAY4 is distinguished by high performance indicators, such as the level of security (confirmed by international certificates), the volume of processing operations per second and the speed of processing transactions.

2.4.3. Tieto Card Suite Solution by Tieto

Tieto Card Suite of the Latvian company *Tieto*, part of the Scandinavian IT holding *TietoEnator*, is designed to solve a variety of tasks related to payment cards, including issuing, acquiring, terminal management, fraud prevention, etc. In particular, the *Card Suite Acquiring Management* technology solution provides rapid response to market changes and support for full-cycle acquiring-from registration and accounting of merchant data to the formation of reports on the results of activities.

The integrated solution *Card Suite Acquiring Management System* is designed to organize acquiring activities of financial institutions: the system is focused on the entire range of tasks for organizing the acceptance of payment cards by merchants. *Card Suite Acquiring Management* contributes to the expansion of the payment service and optimization of routine business processes, depending on the requirements and activities of acquiring partners. In particular, the system takes into account multi-level merchant hierarchies, allows convenient configuration in accordance with business needs, and supports various transaction and settlement currencies.

The bank's transition to the *Card Suite Acquiring Management System* will allow developing solutions for various merchants and offering customers options for conducting settlements and forming payments, depending on their wishes. In addition, the system can be used to create directories, ensuring the integrity of the stored data and simplifying the work of registering and maintaining retail outlets. It also provides for the possibility of automating processing and determining the sequence of work performed.

2.4.4. TranzWare Family of Products by Compass Plus

The *TranzWare* family by the Russian company *Compass Plus* is an open software platform for creating payment services. *TranzWare* family products have many features, including:

- *effective settlement tool to support a payment environment of any complexity and structure;*
- *secure transaction processing, providing a high-speed, multi-scale, fault-tolerant service;*

- *preventive monitoring of fraudulent transactions and risk management;*
- *remote (including internet and mobile) banking services;*
- *multi-aspect analysis for the purpose of generating and presenting statistical data in data marts, in systems for statistical modeling of the behavior of complex objects, etc.;*
- *multi-factor authentication for the modern user, transaction and session security;*
- *stress testing of processing hosts.*

In particular, *TranzWare* has the following advantages:

- *multi-channel, with support for financial transactions via mobile phones, Internet access points, payment terminals and ATMs-all on a single platform;*
- *security, as the solutions fully comply with industry security standards, combine preventive risk management, fraud detection system, multi-factor user authentication and audit tools, as well as reliable access control systems;*
- *organization of forwarding authorization requests via communication channels to authorization centers, providing service for cards of international payment systems and other cards, by routing information on them to the appropriate processing centers;*
- *PIN block translation, PIN verification;*
- *acceptance of authorization requests addressed to issuers, granting of permits for operations or refusals (using electronic and local cards of participating banks);*
- *ability to set limits and activity limits for cards that are authorized in the processing center [42].*

PIN block is the value of the PIN code of the card, which is packed in a special way in a block of 8 bytes. No encryption is used in this process.

2.5. A Brief Overview of Software for Integrating Payments in Acquiring Systems

As the volume of transactions increases (and the number of senders and recipients of payments increases), the load on routing systems increases.

TranzAxis is an integrated open software platform for creating payment services, developed by the Russian company *Compass Plus*. By the way, the processing center of *Compass Plus* itself also operates on this platform.

The *Payment Gateway* service is based on a highly efficient fault-tolerant solution and offers switching and routing of transactions when making electronic payments. The service has an accredited connection to the VISA and MasterCard payment systems and facilitates all types of transactions for all available customer service channels, and, thanks to a flexible API, it is possible to perform any operations through a single software interface.

The *Debit card* service has the ability to integrate with any banking system; it provides the necessary set of tools for effective management of the "card portfolio" and processing of all transactions in a secure processing environment.

TranzWare Online is a solution with a set of front-office functionality, including management of various terminal devices, routing and authorization of transactions, interaction with both international and local payment systems and third-party authorization hosts. In particular, with the help of *TranzWare Online*, it is possible to route transactions, as well as configure devices. *TranzWare Online* supports all the components that make up POS processing, including support for various types of transactions, payment terminals and terminal protocols:

- *terminal network management, parametric routing, and transaction authorization;*
- *support of cards of international payment systems (VISA, MasterCard, AMEX, Diners Club, JCB) and local systems (China Union Pay, Banknet VN, etc.);*
- *comprehensive set of transactions (extended set of transactions for POS terminals and 130+ transaction types for ATMs);*
- *support of all types of payments and transfers;*
- *remote monitoring of the terminal network using FIMI;*
- *security: DES, 3DES, RSA, MAC, VISA PVV/CVV/CVV2, IBM PIN Offset;*
- *EVM compatibility;*
- *support of payment terminals from different manufacturers.*

Another example is the end-to-end payment platform *PXP Financial* provides a full range of solutions for accepting online payments on mobile devices and at points of sale. Thanks to the presence of internal global acquiring, more than 200 alternative payment methods and financial services, *PXP* can annually process transactions totaling more than 16 billion euros through its single gateway [40].

SmartVista is a banking platform developed by the Russian company *БПЦ Банковские технологии*. The *Switch* solution, which is part of the *SmartVista* platform, is intended for issuers, acquirers and processing companies [44]. The solution is functionally compatible with a wide range of industrial hardware platforms, which frees the customer from dependence on only one hardware supplier. The solution can replace the previous generation routing system or work in parallel with existing systems. All *SmartVista* modules are designed as a single complex. The *Switch* solution is based on algorithms that optimize the routing of authorization requests. The message format can be quickly changed to meet specific requirements. In addition, *Switch* provides the ability to manage networks, monitor their status, and automatically reconnect in case of problems.

2.6. Solutions for Managing the Fleet of Payment Terminals

Ingenico's new modular *Estate Manager* solution for managing its fleet of payment terminals offers a wide range of basic and advanced features, including software provision, preventive maintenance, and terminal lifecycle management. These new features facilitate proactive and proactive fleet management, reducing maintenance costs. In addition, *Estate Manager* has advanced features for users thanks to the new web interface [49].

With this management tool, the owners of payment terminals can get complete information and complete control over their property. The advantages of the *Estate Manager* solution include:

- *maximum uptime of terminals for making transactions in retail outlets;*
- *acceleration of entry into the market of payment solutions at points of sale;*
- *full terminal lifecycle monitoring tools;*
- *Total Cost of Ownership (TCO) control for optimizing business solutions*.

Among the numerous products for managing the fleet of payment terminals, we should also mention the *PAX* software package for managing the terminal network – *CyberTMS* [48]. The component part of this complex (PTMS) is a graphical application that is designed to configure and remotely load parameters and software to PAX terminals. According to the vendor, the use of PTMS offers the following advantages:

- *maintaining a database of installed terminals;*
- *full control of software versions and settings of installed terminals;*
- *remote editing of software settings from a single workplace;*

- *fast launch of the terminal when transferring to another point of sale or when you need to change the settings;*
- *simplified learning and usage through a single graphical interface;*
- *easy editing of parameters based on shared profiles-assigned to the terminal.*

Let’s list the main functions of PTMS:

- *create a database of terminals that will allow you to download the required software and settings necessary for the successful operation of the terminal application;*
- *maintaining a list (database) of terminals with the ability to prohibit (allow) downloading to certain terminals;*
- *editing terminal parameters – the list of terminal acquirers, the list of issuers, the list of accepted cards, the list of currencies served, EMV card settings, and cryptographic information sets;*
- *adjustment of the structure of the existing database (and, accordingly, files) to ensure that the functionality of the terminal application can be changed;*
- *import database structure and data from existing PTMS Light file sets;*
- *ensuring data security (using Microsoft SQL Server 2000).*

Another example: *МСТ Компани* is a Russian multi-vendor outsourcing company that provides comprehensive services for acquiring and ATM networks of banks, banking and cash register equipment, as well as other IT services. The cross-platform software *JoinPOS* for payment terminals developed by this company consists of four main parts, which together represent a flexible tool for managing the network of payment terminals, making payments, and attracting new customers and partners to the trade acquiring service [45]. *JoinPOS* is designed for processing and storing electronic images of cash receipts and customer signatures on a remote server. This is a scalable cloud-based system that allows the bank to remotely manage many of its payment terminals with the *JoinPOS* software installed.

Using *JoinPOS*, banks get the opportunity to operate a fleet of equipment of various brands in a single complex. The *JoinTMS* terminal monitoring system is designed to provide up-to-date information about managed terminals, reduce downtime, and improve the efficiency of its use.

The system displays the number of operations performed, the version of installed software and OS, the operability of terminals, as well as operational information on data exchange between terminals and the TMS server (Terminal Management Service). The system allows you to upload basic EMV commands to the payment terminal, which allows you to change the configuration of terminal equipment, without resorting to a large-scale update of the entire acquiring network. Last but not least, this circumstance has a positive effect on the availability of the service.

RetailBUD is a cloud-based dashboard for businesses that allows you to create high-quality analytics of the processes of a retail outlet where the equipment is installed. Using the service, the business owner can track and analyze transactions performed, as well as the current status of devices connected to the service. In addition to analytical tools, your merchant profile includes training materials on working with payment terminals, such as videos and articles, technical support requests, and a built-in store for accessories and consumables for payment terminals. The user can select a point of sale from the list of terminals and go to the personal page of a particular terminal, which displays complete information about both the terminal itself and all transactions made on it.

Modern solutions offer a combination of functionality for routing transactions and managing the fleet of terminal payment terminals. They can be used to manage the entire infrastructure for card transactions and physical maintenance points within a single user interface.

Nevertheless, the solutions discussed above differ markedly from each other both in the completeness of their functional tools and in their cost. While some solutions offer a full range of tools, but are not commercially available to all potential customers, others, on the contrary, are quite affordable, but they lack a number of important components. So, some of them can only be installed as software directly on the terminals, when the client may need a cloud solution. Some may not sufficiently take into account the requirements for cloud systems, or such solutions are not suitable for specific countries, etc. Therefore, as in any industry, the question is not the exclusivity of a particular idea and its implementation, but the right combination between flexibility and the ability to build almost any business model, the availability of a wide range of functions within TMS and transaction switching, and a pricing policy that allows you to meet the needs of customers in different countries of the world.

Below we will describe one of the modern solutions — *TransLink*.iQ, which has received recognition in the market due to the fact that it has just such a combination of features, i.e., it advantageously combines all the necessary functionality and an acceptable pricing policy for the solution.

ASHBURN
INTERNATIONAL

Penki
Kontinentai
GROUP

TransLink.iQ

POS terminal network management and transaction routing

www.ashburn.eu | mail@ashburn.eu

Chapter 3. TransLink.iQ Software and Hardware Complex by ASHBURN International

TransLink.iQ software and hardware complex (included in the family of software solutions *.iQ*) is developed by *ASHBURN International* to manage the network of EFTPOS/POS terminals, deliver transactions, monitor their flow, as well as supervise the technical condition of EFTPOS/POS terminals in real time.

The solution *TransLink.iQ* allows you to centrally and remotely manage the fleet of payment terminals of various models and manufacturers, as well as simultaneously configure parameters, install and update software on any number of terminals to ensure maximum availability of the service, as well as enable new functions. It supports the development of acquiring equipment functionality, as well as provides additional features to the basic set of payment terminal functions (such as dynamic currency conversion or payment by installments), which help increase customer loyalty.

TransLink.iQ solves most of the problems that companies face when managing a large network of payment terminals. So, it allows you to perform remote activation and parameterization of terminals, install and update software, as well as monitor the technical condition of devices in real time. All this makes it possible to automate and simplify the processes associated with managing the EFTPOS/POS terminal fleet as much as possible, reduce associated costs and ensure operational efficiency of the acquiring business (Fig. 13).

TransLink.iQ also provides an opportunity to link an EFTPOS/POS terminals with non-payment (non-card) hosts: before creating a payment (card) transaction, the terminal can contact the non-card host in order to get the amount and details of further payment (for housing and utilities services, customs duties, etc.) based on the payer’s number. Then the classic payment procedure is performed. This option gives *TransLink.iQ* an additional advantage over other solutions from competitors.

The flexible architecture of *TransLink.iQ* allows you to customize it according to the needs and the infrastructure of the client, so that expanding the set and adding non-classical functions will not require large resources.

The *TransLink.iQ* platform is designed to meet the requirements of *VISA International* and *MasterCard International* payment systems for servicing magnetic, chip, contactless and other types of cards, and meets the requirements of the PCI PA-DSS payment application security standard.

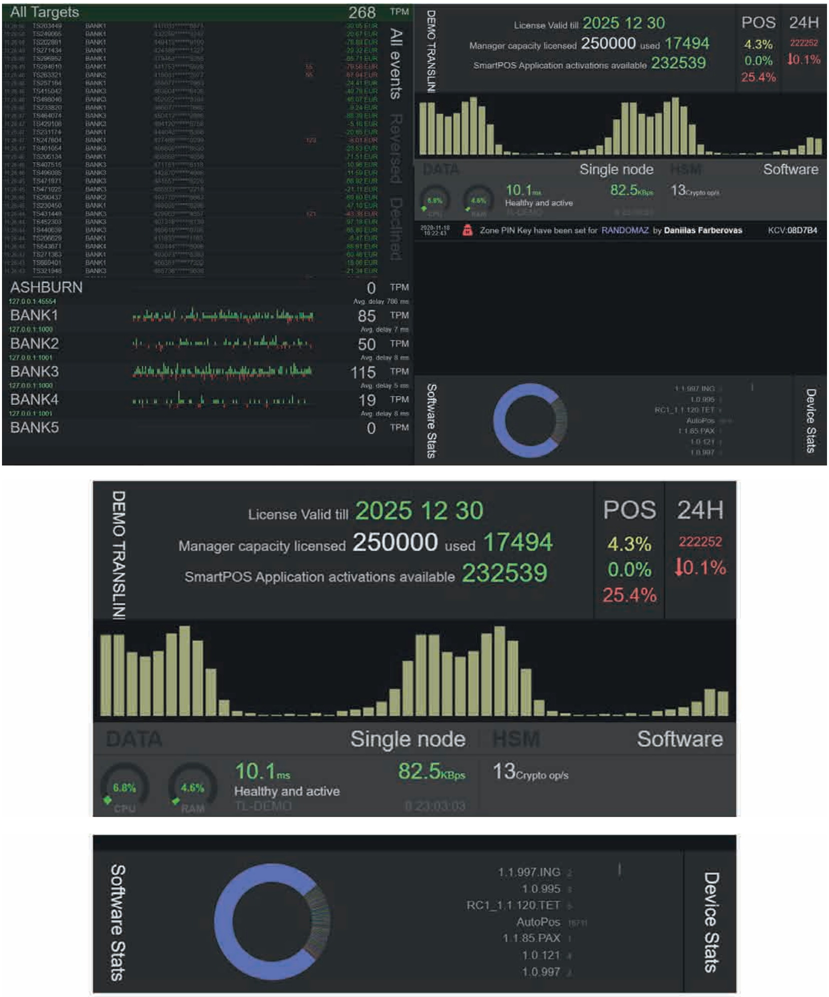


Fig. 13. TransLink.iQ operator interface.

Currently, there are over 300 thousand POS devices are managed with *TransLink.iQ*.

3.1. TransLink.iQ: a Comprehensive Solution for EFTPOS/POS Terminal Network Administration and Transaction Routing

The *TransLink.iQ* solution consists of four software modules, each of which provides its specific functionality – and is an integral part of a single ecosystem, including *TransLink.iQ Manager*, *TransLink.iQ Smart POS*, *TransLink.iQ XConnect* and *TransLink.iQ Reporting* (Fig. 14).

TransLink.iQ Manager ensures transaction routing, network management of payment terminals, comprehensive real-time monitoring of devices, remote software loading and data exchange with the acquiring system of the processing center.

TransLink.iQ SmartPOS is an application designed to support payment functions of terminals from different manufacturers.

TransLink.iQ XConnect is used for communication between the *TransLink.iQ SmartPOS* application and the cash register software using asynchronous data transfer.

TransLink.iQ Reporting is an application for working with databases, uploading data to external systems, and generating various analytical reports.

TransLink.iQ Insight is a solution for online monitoring of the technical condition and activity of the network of EFTPOS/POS terminals.

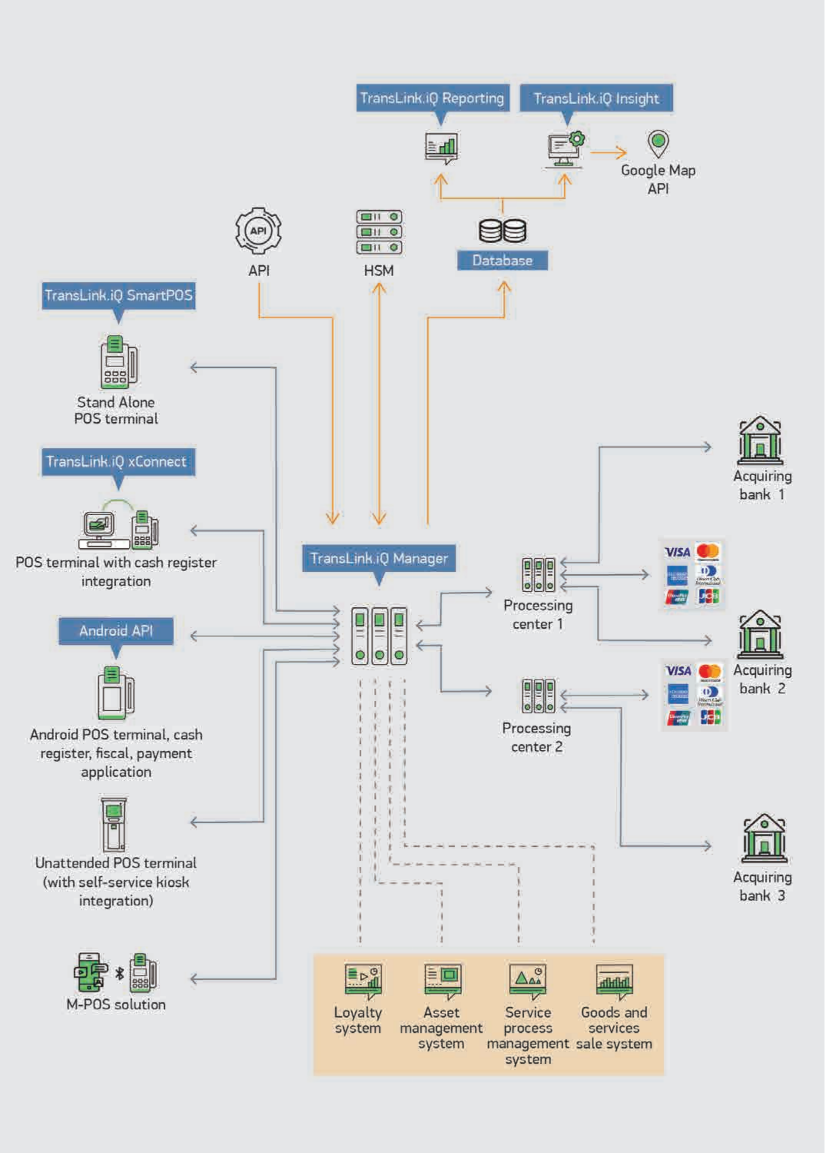


Fig. 14. Operation diagram of the TransLink.iQ software solution.

Let's list the main functionality of *TransLink.iQ* (Fig.15).

Centralized management of the EFTPOS/POS terminal fleet. Ability to remotely manage a fleet of different types of devices, configure parameters, and install software used on the EFTPOS/ POS terminal.

Decentralizing terminal distribution. You can distribute devices to regional service and distribution centers, which simplifies and speeds up the process of installing or replacing a merchant's terminal, as well as reduces logistics costs.

Automated management of encryption keys. Thanks to the use of asymmetric data encryption technology (RSA), *TransLink.iQ* allows you to automate the management of encryption keys and significantly reduce the costs associated with this process with the necessary level of security.

Comprehensive monitoring of transactions and the status of EFTPOS/POS terminals in real time. Within the framework of a single user interface, it is possible to collect and display information about the working status of each payment terminal in the network, software and device parameters, track the intensity of the transaction flow and get detailed information on each completed payment, etc.

Analytical reporting on the operation of EFTPOS/POS terminals and the passage of transactions. This functionality is used to upload a variety of data about the operation of payment terminals and the passage of transactions in the form of visual reports.

Support of the multi-banking function. It is important to emphasize the advantage of *TransLink.iQ* as a new technological opportunity to switch the EFTPOS/POS terminal service from one acquiring network to another in accordance with the requirements of each acquirer. In addition, in the payment processing process, you can work with several acquiring banks.

Support of the multi-hosting feature. TransLink.iQ allows you to deliver various types of transactions to processing centers and other systems.

Support for the multi-merchant function. You can use just one physical device to make payments to multiple sellers of goods and services – or send transactions to different accounts of the same merchant.

Transaction flow recognition. Each transaction in the shared flow can be identified by various attributes for subsequent logical separation.

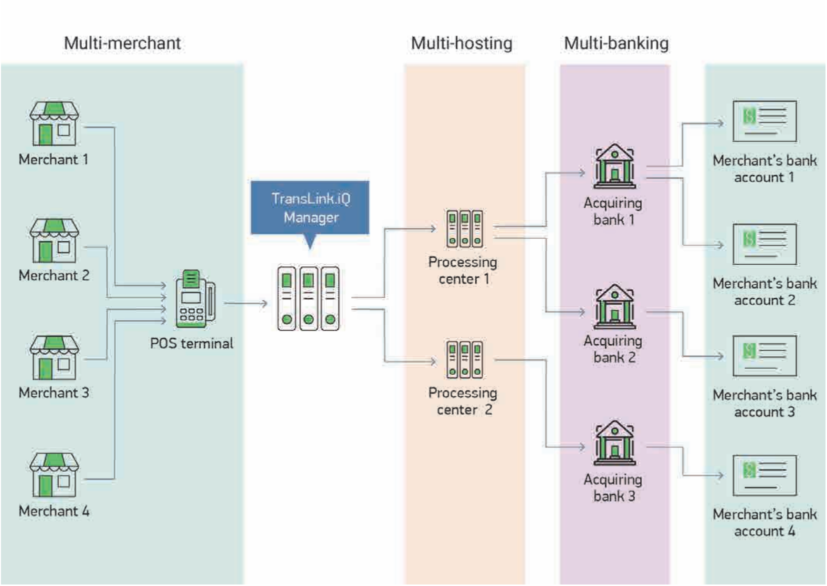


Fig. 15. Basic functionality of the TransLink.iQ system.

Working with equipment by different manufacturers. The solution can be successfully applied to a fleet of devices consisting of EFTPOS/POS terminals of various models from various manufacturers.

3.2. TransLink.iQ Manager: Basic Functionality and Transaction Routing

The TransLink.iQ Manager module has the following main functions:

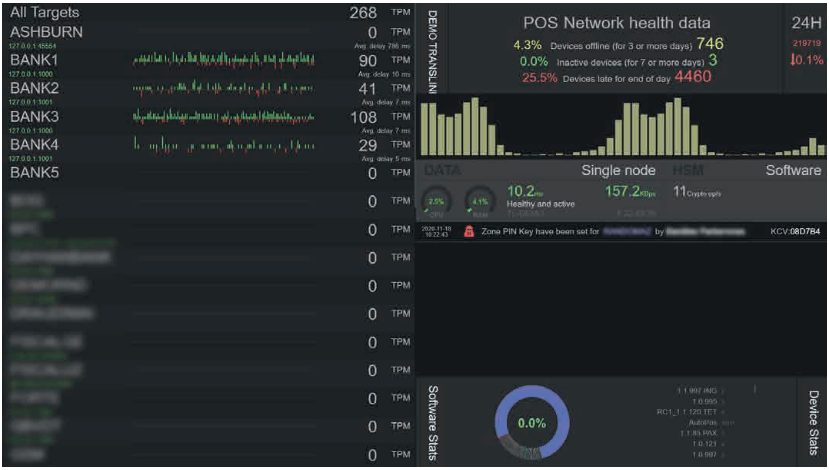
- *transaction routing;*
- *EFTPOS/POS terminal network management;*
- *comprehensive real-time monitoring of terminal devices;*
- *remote software download;*
- *data exchange with the acquiring system of the processing center;*
- *data exchange channel encryption;*
- *automated management of encryption keys;*
- *transfer of fiscal data to an external system.*

When first launched on any new machine, *TransLink.iQ* (abbreviated *TL*) will deprive the novice user of access to the user interface and provide a graphical window for creating a certificate based on the new user's data and adding it to the browser. After getting access to *TL*, you need to start installing the certificate for a new user and get a message on the screen about its successful installation.

In the new *TL Manager* window, the new user will see the full list of currently available tabs (Fig. 16). After initial software installation, the tabs are empty, which is expected, given the lack of data to collect.

Fig. 16. The new TransLink.iQ Manager will display a complete list of tabs that are currently available for the first user.

In the first tab – Dashboard (Fig. 17) – it is possible to track all relevant data of *TL Manager* and the terminal fleet in real time.



All Targets	268	TPM
ASHBURN 127.0.0.1:45554	0 Avg. delay 786 ms	TPM
BANK1 127.0.0.1:1000	90 Avg. delay 10 ms	TPM
BANK2 127.0.0.1:1001	41 Avg. delay 7 ms	TPM
BANK3 127.0.0.1:1000	108 Avg. delay 7 ms	TPM
BANK4 127.0.0.1:1001	29 Avg. delay 5 ms	TPM
BANK5	0	TPM
[redacted]	0	TPM
[redacted]	0	TPM
[redacted]	0	TPM
[redacted]	0	TPM
[redacted]	0	TPM
[redacted]	0	TPM
[redacted]	0	TPM
[redacted]	0	TPM
[redacted]	0	TPM
[redacted]	0	TPM

DEMO TRANSLINE

POS Network health data — 24H

4.3% Devices offline (for 3 or more days) 746 — 219719

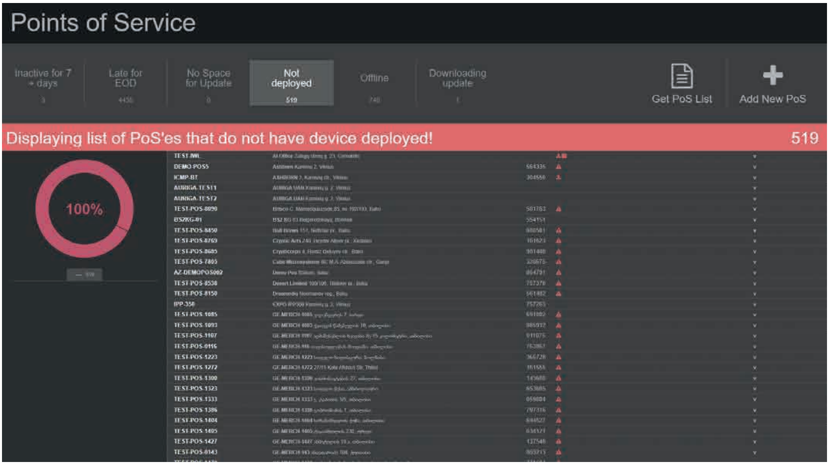
0.0% Inactive devices (for 7 or more days) 3 — ↓0.1%

25.5% Devices late for end of day 4460

2020-11-18 10:22:43 Zone PIN Key have been set for [redacted] by [redacted] KCV:08D7B4

Fig. 17. Dashboard tab.

The second tab – *Point of Service* (PoS, Fig. 18) – allows you to view, add and change data on your fleet of terminals. You can also see general information about the PoS in the list, including the merchant's alias and location, activation code (if any), and the app versions currently installed on this device.



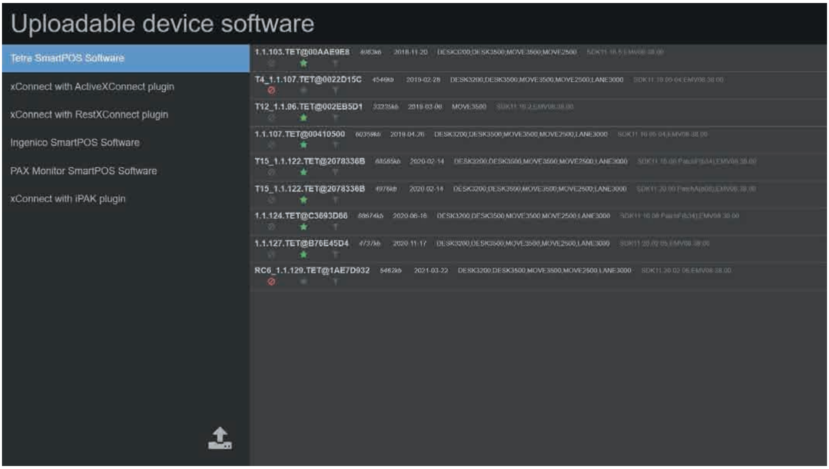
Points of Service

Displaying list of PoS'es that do not have device deployed! 519

TEST-JWL	Al Office Zalgiry [illegible] 21, [illegible]	
DEMO-POS5	[illegible] Kareivu 2, Vilnius	564336
ICMP-BT	ASHBURN 2, Kareivu str., Vilnius	304550
AURIGA-TEST1	AURIGA UAB Kareiviu g. 2, Vilnius	
AURIGA-TEST2	AURIGA UAB Kareiviu g. 2, Vilnius	
TEST-POS-8090	[illegible] 85, [illegible] 192/193, Baku	581763
BSZKG-01	BSZ BG [illegible], [illegible]	554151
TEST-POS-8450	[illegible] 151, [illegible], Baku	888581
TEST-POS-8769	Cryptic Arts 240 [illegible], [illegible]	161623
TEST-POS-8685	Cryptocorps 4, [illegible] str., Baku	901400
TEST-POS-7865	[illegible] M.A. [illegible] str., Ganja	328675
AZ-DEMOPOS002	Demo Pos Station, Baku	864791
TEST-POS-8538	Desert Limited 100/106, [illegible] st., Baku	757376
TEST-POS-8150	[illegible], Baku	561482
IPP-350	EXPO IPP350 Kareiviu g. 2, Vilnius	757265
TEST-POS-1085	GE-MERCH-1085 [illegible] 7, [illegible]	691882
TEST-POS-1093	GE-MERCH-1093 [illegible] 10, [illegible]	885912
TEST-POS-1107	GE-MERCH-1107 [illegible]	911075
TEST-POS-0116	GE-MERCH-116 [illegible]	753867
TEST-POS-1223	GE-MERCH-1223 [illegible]	366728
TEST-POS-1272	GE-MERCH-1272 27/15 Kote Afkhazi St, Tbilisi	161555
TEST-POS-1300	GE-MERCH-1300 [illegible] 27, [illegible]	145688
TEST-POS-1323	GE-MERCH-1323 [illegible]	653685
TEST-POS-1333	GE-MERCH-1333 [illegible] 3/5, [illegible]	059804
TEST-POS-1386	GE-MERCH-1338 [illegible] 1, [illegible]	797316
TEST-POS-1404	GE-MERCH-1404 [illegible]	844527
TEST-POS-1405	GE-MERCH-1405 [illegible] 230, [illegible]	636127
TEST-POS-1427	GE-MERCH-1427 [illegible] 10 a, [illegible]	137546
TEST-POS-0143	GE-MERCH-143 [illegible] 106, [illegible]	865213

Fig. 18. Point of Service tab.

The third tab is *Downloadable device software* (Fig. 19). This tab contains information about the terminal and *XConnect* software versions that will be used for remote updates.



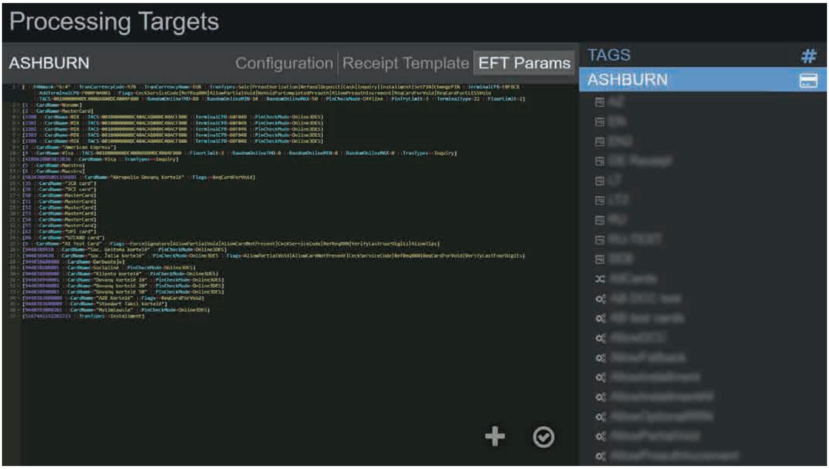
Uploadable device software

- Tetra SmartPOS Software
- xConnect with ActiveXConnect plugin
- xConnect with RestXConnect plugin
- Ingenico SmartPOS Software
- PAX Monitor SmartPOS Software
- xConnect with iPAK plugin

```
1.1.103.TET@00AAE9E8      4083kb   2018-11-20  DESK3200;DESK3500;MOVE3500;MOVE2500           SDK11.16.5;EMV08.38.00
T4_1.1.107.TET@0022D15C   4546kb   2019-02-28  DESK3200;DESK3500;MOVE3500;MOVE2500;LANE3000  SDK11.18.05.04;EMV08.38.00
T12_1.1.96.TET@002EB5D1   3323kb   2019-03-08  MOVE3500                                      SDK11.16.2;EMV08.38.00
1.1.107.TET@00410500      60359kb  2019-04-26  DESK3200;DESK3500;MOVE3500;MOVE2500;LANE3000  SDK11.16.05.04;EMV08.38.00
T15_1.1.122.TET@2078336B  68565kb  2020-02-14  DESK3200;DESK3500;MOVE3500;MOVE2500;LANE3000  SDK11.16.08.PatchF(634);EMV08.38.00
T15_1.1.122.TET@2078336B  4976kb   2020-02-14  DESK3200;DESK3500;MOVE3500;MOVE2500;LANE3000  SDK11.20.00.PatchA(600);EMV08.38.00
1.1.124.TET@C3693D66      68674kb  2020-06-16  DESK3200;DESK3500;MOVE3500;MOVE2500;LANE3000  SDK11.16.08.PatchF(634);EMV08.38.00
1.1.127.TET@B76E45D4      4737kb   2020-11-17  DESK3200;DESK3500;MOVE3500;MOVE2500;LANE3000  SDK11.20.02.05;EMV08.38.00
RC6_1.1.129.TET@1AE7D932  5462kb   2021-03-22  DESK3200;DESK3500;MOVE3500;MOVE2500;LANE3000  SDK11.20.02.06;EMV08.38.00
```

Fig. 19. Uploadable device software tab.

The fourth tab — Processing Targets (Fig. 20) – allows you to create, edit or delete (in extremely rare cases for all these options) destinations for delivery and processing of transactions, as well as routes and parameters of processed maps.



Processing Targets

```
[ ::PANmask="6:4" ::TranCurrencyCode=978 ::TranCurrencyName=EUR ::TranTypes=Sale|Preauthorization|Refund|Deposit|Cash|Inquiry|Installment|SetPIN|ChangePIN ::TerminalCPB=E0F8C8
  ::AddTerminalCPB=F000F0A001 ::Flags=CeckServiceCode|RefReqRRN|AllowPartialVoid|NoVoidForCompletedPreauth|AllowPreauthIncrement|ReqCardForVoid|ReqCardForCLESSVoid
  ::TACS=0010000000DC4000A800DC4004F800 ::RandomOnlineTHD=80 ::RandomOnlineMIN=10 ::RandomOnlineMAX=50 ::PinCheckMode=Offline ::PinTryLimit=3 ::TerminalType=22 ::FloorLimit=2]
[1 ::CardName=Noname]
[2 ::CardName=MasterCard]
[2200 ::CardName=MIR ::TACS=0010000000DC40ACA8000C40ACF800 ::TerminalCPB=60F048 ::PinCheckMode=Online3DES]
[2201 ::CardName=MIR ::TACS=0010000000DC40ACA8000C40ACF800 ::TerminalCPB=60F048 ::PinCheckMode=Online3DES]
[2202 ::CardName=MIR ::TACS=0010000000DC40ACA8000C40ACF800 ::TerminalCPB=60F048 ::PinCheckMode=Online3DES]
[2203 ::CardName=MIR ::TACS=0010000000DC40ACA8000C40ACF800 ::TerminalCPB=60F048 ::PinCheckMode=Online3DES]
[2204 ::CardName=MIR ::TACS=0010000000DC40ACA8000C40ACF800 ::TerminalCPB=60F048 ::PinCheckMode=Online3DES]
[3 ::CardName="American Express"]
[4 ::CardName=Visa ::TACS=0010000000DC4000A800DC4004F800 ::FloorLimit=2 ::RandomOnlineTHD=0 ::RandomOnlineMIN=0 ::RandomOnlineMAX=0 ::TranTypes=-Inquiry]
[4188020080813836 ::CardName=Visa ::TranTypes=+Inquiry]
[5 ::CardName=Maestro]
[6 ::CardName=Maestro]
[5824700950911334899 ::CardName="Akropolio Dovanų Kortelė" ::Flags=+ReqCardForVoid]
[35 ::CardName="JCB card"]
[36 ::CardName="DCI card"]
[50 ::CardName=MasterCard]
[51 ::CardName=MasterCard]
[52 ::CardName=MasterCard]
[53 ::CardName=MasterCard]
[54 ::CardName=MasterCard]
[55 ::CardName=MasterCard]
[62 ::CardName="UPI card"]
[86 ::CardName="UZCARD card"]
[9 ::CardName="AI Test Card" ::Flags=+ForceSignature|AllowPartialVoid|AllowCardNotPresent|CeckServiceCode|RefReqRRN|VerifyLastFourDigits|AllowTips]
[9440380410 ::CardName="Soc. Geltona kortelė" ::PinCheckMode=Online3DES]
[9440380420 ::CardName="Soc. Žalia kortelė" ::PinCheckMode=Online3DES ::Flags=AllowPartialVoid|AllowCardNotPresent|CeckServiceCode|RefReqRRN|ReqCardForVoid|VerifyLastFourDigits]
[944038600000 ::CardName=Darbuotojo]
[944038600005 ::CardName=Socialinė ::PinCheckMode=Online3DES]
[944038900000 ::CardName="Kliento kortelė" ::PinCheckMode=Online3DES]
[944038900001 ::CardName="Dovanų kortelė 10" ::PinCheckMode=Online3DES]
[944038900002 ::CardName="Dovanų kortelė 20" ::PinCheckMode=Online3DES]
[944038900003 ::CardName="Dovanų kortelė 50" ::PinCheckMode=Online3DES]
[9440383600000 ::CardName="A20 Kortelė" ::Flags=+ReqCardForVoid]
[9440383600009 ::CardName="Standart Taksi kortelė"]
[9440393000201 ::CardName="Mylimiausia" ::PinCheckMode=Online3DES]
[5167442252202723 ::TranTypes=-Installment]
```

Fig. 20. Processing Targets tab.

In the fifth tab (*TL Manager Users*, Fig. 21), you can change user data and their access rights to all other tabs and functions that they can perform with *TL Manager*.

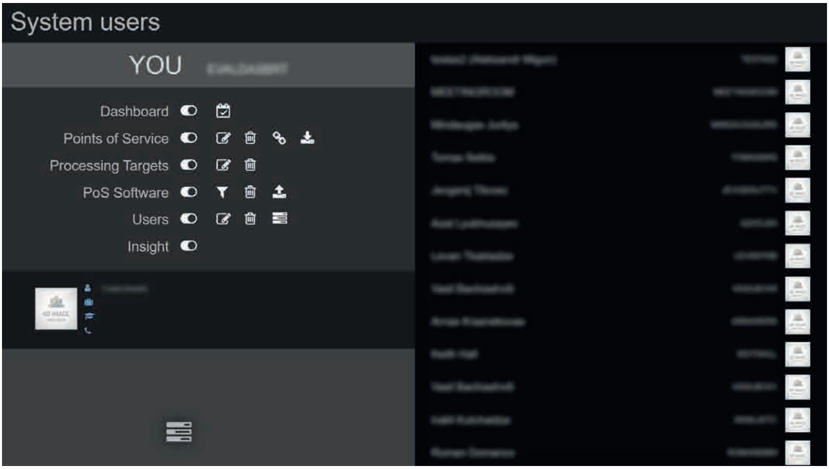


Fig. 21. TL Manager Users tab.

You can select the language of the TL Manager user interface, which allows you to display all the built-in TL Manager text in the selected language.

If you already have a user base that processes goals with parameters and software, then go to the Points of Service tab (hereinafter referred to as PoS), where each configuration will be used before creating a PoS.

TL Manager has an extended permissions manager that allows a user who has permission to edit permissions to define roles for other users (see Fig. 22).

It should be clarified that “Processing targets” are simply banks. In a technical sense, this is a configuration where the IP addresses and ports of bank servers are available. It also specifies what parameters will be used, and routes and directions for the map. First, the user will need to create the first “delivery destination” (target) using the Create target command.

Configure EFT Parameters is one of the three tabs that you can see in “Delivery Destinations”.

In EFT Parameters, you will need to add the main parameters that are used for this delivery destination. In general, EFT Parameters can store a variety of parameters: for example, panning the map (part of the digits from the map number); the more digits you add from the map number, the more accurate the parameters will be and some form of settings that will be used for this purpose for all maps, for example, currency and its code.

You can add basic elements such as the currency code of the transaction with its name, transaction types that will be available for all PoS that have these “Delivery Destinations”. Some basic flags, such as ReqCardForVoid are focused on the “Destination for delivery”. You can also add other additional routes and parameters to improve these settings.

The “Destination for Delivery” configuration (settings) is provided by the actual operating bank.

There are three additional types of parameters that you can create. Each of them can be included in POS parameters in the “Destination configuration for delivery” section.

Additional routings option, which is used to improve the routing of the target map, can be selected in the additional parameters at the bottom of the list. In other words, you can specify maps, their names, and select PoS route for the map on the PoS screen. It is used when there are PoS locations with many “Delivery Destinations” and the default parameters have one or two numeric prefixes. You can use Additional routes to create special prefixes for specific cases: some merchants may not need them, but others may find them vital. On the create routing screen, you need to set a name for a specific routing (using a name that makes it easy to understand routing features), and then you can add new prefix entries.

Note that the transaction will be routed to the delivery destination that has the longest applicable card number prefix for this Purpose.

Let’s summarize the main functionality of TL Manager:

- *manage a network of payment terminals of various types, which can be owned by different owners (banks, processing centers, service providers, large retail chains, etc.);*
- *modern and user-friendly graphical user interface;*
- *ability to transfer transaction data to acquiring banks that are served in the same or different processing centers;*
- *setting individual parameters for each bank and / or processing center;*
- *remote connection of the payment terminal to the system. The terminal is sent to the installation point with the universal software loaded and remotely configured already on the merchant’s territory within 30-40 seconds (depending on connection quality);*

- *remote installation and modification of terminal parameters (payment parameters, set of functions performed, receipt templates, etc.);*
- *remote software update (system library and application) of payment terminals in the background without interrupting customer service processes;*
- *automatic registration of the physical terminal number (Serial number) and its binding to the logical device number (Terminal ID);*
- *ability to route financial and non-financial transactions to different processing centers and other external systems. Tracking various failures in the transaction processing process;*
- *real-time monitoring of the terminal network operation, server and encryption module (HSM) load, transaction processing speed at different stages, and software update processes tracking.*

Encryption of the data exchange channel. Data from the payment terminal to the *TransLink.iQ Manager* server is transmitted according to a scheme based on the DUKPT mechanism using AES128 encryption algorithms.

In turn, data is transmitted from the *TransLink.iQ Manager* server to the acquiring system of the processing center via a dedicated communication channel and/or using the security system offered by the processing center.

3.3. TransLink.iQ SmartPOS: EFTPOS/POS Terminal Application

The TransLink.iQ SmartPOS application provides card servicing capabilities for most international payment systems. It has a multi-platform architecture and supports payment functions on the most popular line of EFTPOS/ POS terminals on the market from the largest manufacturers.

TransLink.iQ SmartPOS can be quickly adapted to the equipment from new manufacturers or line within the same ideology (without changing the management system).

Other features of TransLink.iQ SmartPOS include:

- *software adaptation for servicing local, including national, payment systems:*
- *performing various types of financial and non-financial transactions:*
- *setting the closing time of the day of payment terminals in automatic or manual mode;*
- *support for multi-merchant functionality;*
- *setting a unique template for printing the receipt (placing the acquirer's or service provider's logo and other additional information);*
- *support for the cardholder's language*.

SmartPOS software supports transactions with card data reading using a magnetic stripe reader, as well as the main contactless payment technologies, including *VISA payWave*, *MasterCard Contactless* (*PayPass*), *American Express ExpressPay*, *UnionPay International QuickPass*.

The *SmartPOS* app interface supports multiple languages. For EMV transactions, messages to the client, including a request to enter a PIN code, tips, etc., are displayed in the first corresponding supported language from the list of map languages. If the list of map languages does not include *SmartPOS*-supported languages, all messages will be displayed in English. *SmartPOS* also supports entering barcode data using a USB or COM scanner.

3.4 . TransLink.iQ XConnect Communication Module

The *TransLink.iQ XConnect* module provides communication between *TransLink.iQ Smart POS* and various operating systems of cash register equipment using the asynchronous data transfer principle.

Fig. 22. TransLink.iQ XConnect communication module.

Using this module reduces the likelihood of making mistakes during the cashier's operational activities. As a result, the total cost of the card maintenance solution is reduced. This module also helps prevent cases of double debiting (or lack of charge). The client's funds are provided by means of communication between the payment terminal and the cash register using a specialized protocol to ensure correct service.

Other advantages of the module include reducing the time required for servicing the customer and providing banking and non-banking operations via a single payment terminal.

3.5. Report Generation Module TransLink.iQ Reporting

The TransLink.iQ Reporting module is designed to work with different databases containing structured information about operations performed. The module has an intuitive web interface with a flexible access granting system and provides such functions as:

- generating reports using templates (standard or separately designed to meet the customer's needs);
- automatic distribution of reports to each user with the ability to configure their frequency;

- export data from *TransLink.iQ* to external systems for business intelligence and other purposes;
- importing data from external systems to the current database to optimize working processes on the customer's side according to the templates required by the customer.

3.6. TransLink.iQ Insight: a Solution for Online Monitoring of the Technical Condition and Activity of the Network of EFTPOS/POS Terminals

TransLink.iQ Insight is a module that is designed to process and store the status of payment terminals during regular connections with them in the *TransLink.iQ Manager* system. The main data sources for this solution are technical data about the terminal status transmitted by the *TransLink.iQ SmartPOS* application from the terminal with a set frequency (pinging). Information consists of static and dynamic data about the terminal and merchant (including transaction data) stored in the *TransLink.iQ Manager* system.

Data from the sources mentioned above is uploaded in pseudo-online mode and stored in the *TransLink.iQ* database. However, security-sensitive data is not transmitted to the module. The information stored in the database is mostly technical (raw data), while monitoring requires additional analytical data processing processes. The specified processing processes are started automatically with the specified regularity in order to avoid excessive load on the system.

ASHBURN
INTERNATIONAL

Penki Kontinentai GROUP

TransLink.iQ
Insights

Comprehensive analytics for POS terminal network management

www.ashburn.eu | mail@ashburn.eu

3.7. Round-the-Clock Call Reception Service Service Desk.iQ and Its Main Tasks

Service Desk.iQ is a software product developed by *BS/2* (*Penki Kontinentai Group*) for automating equipment maintenance processes for banks, retailers and other organizations. He is responsible for opening, distributing, executing, and closing customer requests for equipment maintenance, organizing the work of the service company's staff, and generating reports [51].

The call acceptance service based on this software is designed to respond quickly and address current business needs.

In particular, the *Service Desk.iQ* service is successfully applied in the banking sector, retail trade and the service sector, helping to ensure an optimal level of service availability for end users.

Moreover, *Service Desk.iQ* has proven its effectiveness for managing logistics and documentation, accounting for the life cycle of service objects, their components and parts.

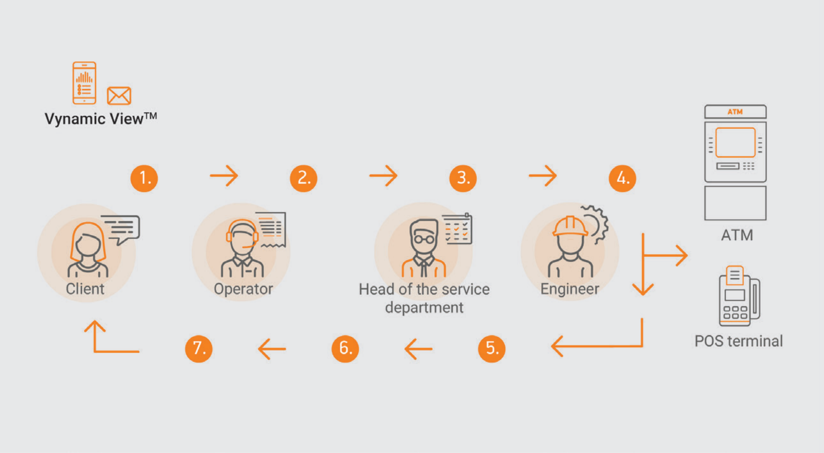


Fig. 23. Workflow in Service Desk.iQ.

In general, the *Service Desk.iQ* software platform automatically collects and aggregates data, distributes it to users with the help of an operator, and helps them process current business processes using only one tool.

Let’s list the main tasks of *Service Desk.iQ*:

- *control of contractual obligations during the execution of each request (Service Level Agreement, SLA);*
- *planning of work according to the standards and level of qualification of performers;*
- *incident and service request management;*
- *providing system users with alerts and operational information for decision-making;*
- *provision of statistical reports;*
- *accounting for labor costs, equipment and spare parts used in the execution of service requests;*
- *monitoring the movement (transportation) of spare parts;*
- *accounting of fuel and lubricants consumption during service work;*
- *track critical situations*.

The solution allows you to track the status of each request and warn in advance about possible violations of contractual obligations at various stages of implementation (in accordance with ITIL recommendations), thereby increasing the level of availability of services.

3.7.1. Workflow in Service Desk.iQ

The use of *Service Desk.iQ* is motivated by the desire to reduce the cost-of-service support and improve the quality of service.

For example, a special *SRM* module included in *Service Desk.iQ* allows you to manage all incoming requests, translating them into tasks for specific service engineers in accordance with their location, skill level, and workload.

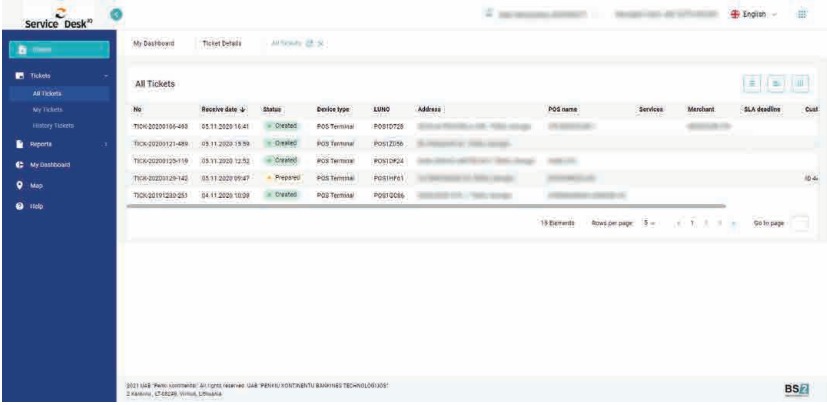
The solution allows you to keep track of the movement of components, equipment and spare parts, registering all events in the life cycle of accounting units and planning their purchase and write-off. It also takes into account the working hours of service personnel, consumables, spare parts, transportation costs and local repairs. This ensures accurate calculation of the cost of services provided by the maintenance company.

The system provides the ability to integrate with the primary systems for registering service requests, allowing you to synchronize their opening and closing. You can use it to create various analytical reports on the performance of work, as well as calculate key service performance indicators and track trends in their changes.

Service Desk.iQ allows you to get full control over the service process, starting from receiving a service request and ending with issuing an invoice for completed work.

The workflow in *Service Desk.iQ* includes:

1. *Receiving information about an incident by phone, email, or in automatic mode (integration with monitoring and notification systems).*
2. *Automatic processing of information and creation of a service request, which the operator transmits to the service department.*
3. *Distribution of work to eliminate the incident according to the work schedule and the level of qualification of engineers.*
4. *Receiving a task by a specific engineer (notification to a mobile device or computer) and completing it.*
5. *The engineer updates the task completion status in real time.*
6. *The supervisor checks the work report, accepts the completed task, or assigns additional work.*
7. *The operator checks for violations of the service level (SLA), generates a report for the customer, and closes the request.*



All Tickets

No	Receive date ↓	Status	Device type	LUNO	Address	POS name	Services	Merchant	SLA deadline	Cust
TICK-20200106-493	05.11.2020 16:41	Created	POS Terminal	POS1D728	[redacted]	[redacted]		[redacted]		
TICK-20200121-489	05.11.2020 15:59	Created	POS Terminal	POS1Z056	[redacted]					
TICK-20200125-119	05.11.2020 12:52	Created	POS Terminal	POS1DF24	[redacted]	[redacted]				
TICK-20200129-142	05.11.2020 09:47	Prepared	POS Terminal	POS1HF61	[redacted]	[redacted]				ID 4
TICK-20191230-251	04.11.2020 10:08	Created	POS Terminal	POS1GC86	[redacted]	[redacted]				

15 Elements Rows per page: 5 ‹ 1 2 3 › Go to page

2021 UAB "Penki kontinentai". All rights reserved. UAB "PENKIŲ KONTINENTŲ BANKINĖS TECHNOLOGIJOS"
Z Kalvarijų, LT-08249, Vilnius, Lithuania

Fig. 24. Monitoring requests in Service Desk.iQ.

Service Desk.iQ automates the following processes:

- *fault detection;*
- *control over the quality of work performed;*
- *data collection and storage;*
- *formation of documentation and reporting;*
- *logistics tracking;*
- *maintaining accounting records;*
- *resource volume monitoring;*
- *monitoring the operation of devices;*
- *distribution of tasks and their direct observation on the map;*
- *other business management processes*.

Self-service platforms have been created to facilitate the work of the business sector, mobility and customer convenience:

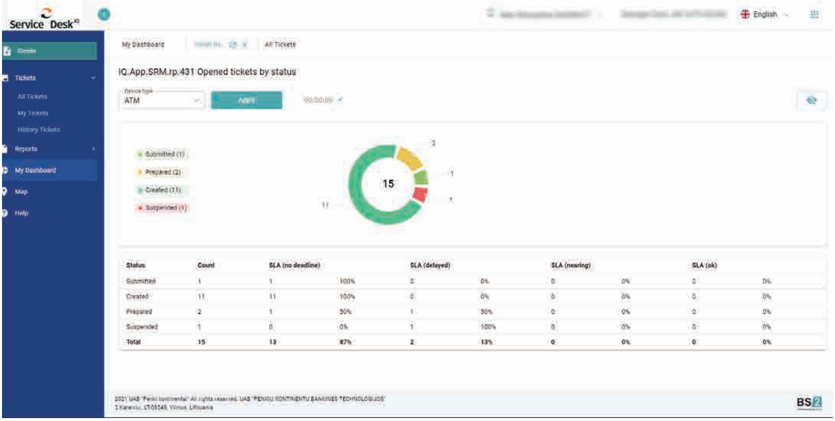
The security of data collected and stored in the *Service Desk.iQ* system is ensured by international standards: the information security management system *ISO 27001* (guarantees confidentiality, integrity and availability of data) and the IT services management system *ISO 20001* (ensures high-quality management of IT services based on good ITIL practices).

3.7.2. Service Desk.iQ System Modules

Service Desk.iQ consists of eight modules that allow you to quickly and efficiently manage tasks that require high qualifications:

SRM.iQ (*Service Request Management*).

This module automatically manages customer requests by providing SLA requirements. The module manages the entire request cycle-from receiving the request to creating and sending a completed report.



IQ.App.SRM.rp.431 Opened tickets by status

Device type: ATM

Status	Count	SLA (no deadline)		SLA (delayed)		SLA (nearing)		SLA (ok)	
Submitted	1	1	100%	0	0%	0	0%	0	0%
Created	11	11	100%	0	0%	0	0%	0	0%
Prepared	2	1	50%	1	50%	0	0%	0	0%
Suspended	1	0	0%	1	100%	0	0%	0	0%
Total	**15**	**13**	**87%**	**2**	**13%**	**0**	**0%**	**0**	**0%**

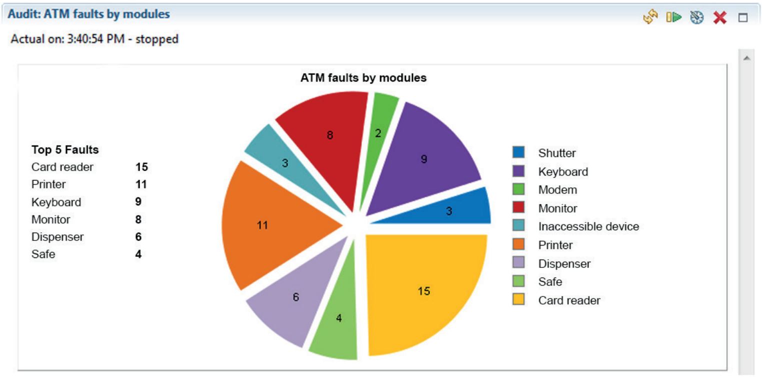
2021 UAB "Penki kontinentai" All rights reserved. UAB "PENKIŲ KONTINENTŲ BANKINĖS TECHNOLOGIJOS"
1 Kareivių, LT-08248, Vilnius, Lithuania

Fig. 25. Work orders in the Service Desk.iQ system.

SLA.iQ (*Service Level Agreement*).

The *SLA.iQ* module enters formalized data into the system. They are based on methods for calculating general management parameters, an agreement on the services provided, and additional conditions. The use of this data determines the quality of services provided to customers.

SRP.iQ (*Service Repair Parts; accounting for resources required for troubleshooting*). The *SRP.iQ* module captures information about all events related to material and technical resources used to resolve problems in the provision of services. This means that spare parts units and related processes are recorded, i.e., the system records the movement of spare parts and materials between warehouses, the service company, and financially responsible persons.

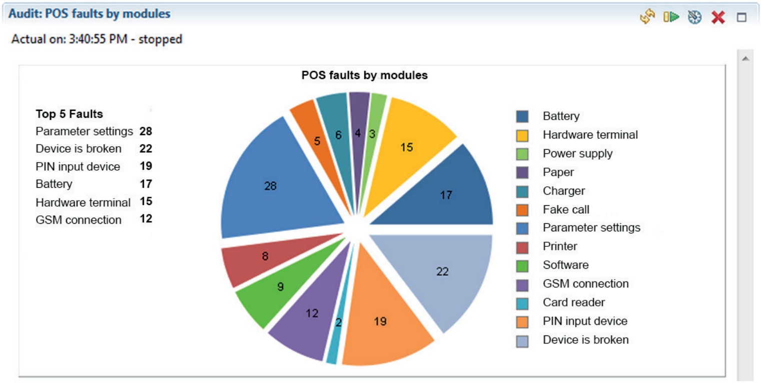


Audit: ATM faults by modules

Actual on: 3:40:54 PM - stopped

ATM faults by modules

Top 5 Faults	
Card reader	15
Printer	11
Keyboard	9
Monitor	8
Dispenser	6
Safe	4



Audit: POS faults by modules

Actual on: 3:40:55 PM - stopped

POS faults by modules

Top 5 Faults	
Parameter settings	28
Device is broken	22
PIN input device	19
Battery	17
Hardware terminal	15
GSM connection	12

Fig. 26. Accounting for local repairs in the Service Desk.iQ system.

LRM.iQ (Local Repair Management; accounting for local repairs).

The *LRM.iQ* module registers the work of the local repair department, revealing the list of spare parts for the repair of the taken controlled objects. This module (similar to the *SRP.iQ* module) records the workflow cycle of the local repair department and generates local repair orders.

FCM.iQ (*Fuel Consumption Management*).

The *FCM.iQ* module allows you to enter data automatically or manually to track the remaining fuel and fuel resources. In this way, fuel consumed by vehicles owned by the company is recorded, as well as distances and fuel payments.

GCM.iQ (*Geographical Control and Monitoring; monitoring devices in real time*). You can use this module to track devices, tasks, and their status on the map in real time.

KPI.iQ (*Key Performance Indicators; evaluation of performance indicators*).

The *KPI.iQ* module measures and evaluates the performance and efficiency of processes and tracks their trends. It provides an accurate assessment of progress in achieving a specific goal. At the same time, various expert reports are provided for analysts who evaluate the effectiveness of these processes. The selected reports are generated.

BBM.iQ (*Basic Billing Management; basic settlement management*).

The *BBM.iQ* module periodically calculates accounts payable and receivables for services rendered. This record is kept for contracts signed by the company with customers and subcontractors.

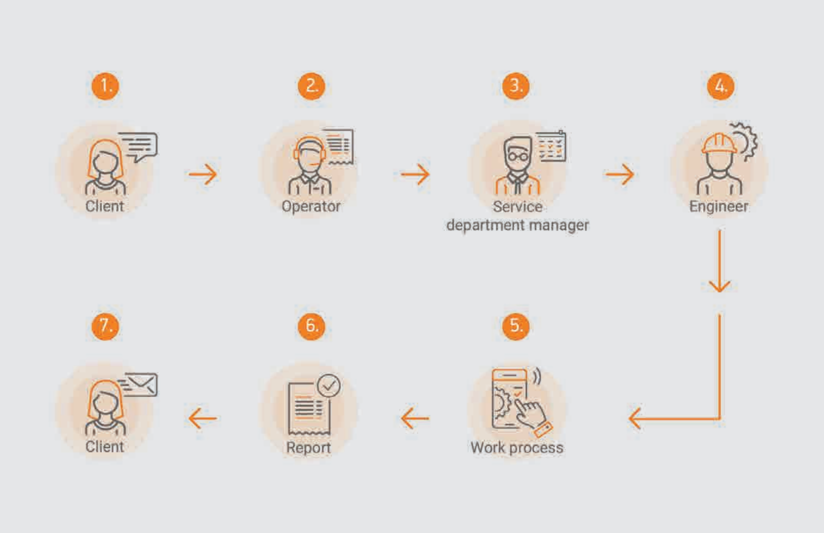


Fig. 27. Service request lifecycle diagram in the Service Desk.iQ system

As you can see in Figure 27, information about the problem is provided by phone, email, or other monitoring systems in automatic mode (*Vynamic View*, etc.). The *Service Desk.iQ* system automatically processes this information and creates a request that the operator assigns to a specific service department. The manager of the service department plans works to fix the problem in accordance with the work schedule and the qualification of the engineer. An engineer receives a job request on-site or via a mobile device and completes the task. The engineer marks real-time control points for work completion and sends a report to the system. The service department manager examines the received work report and confirms its completion, if no additional work is required. The operator checks that the service contract has not been violated and sends a report to the client.

BS2
Penki kontinentai group

Penki
Kontinentai
GROUP

Service Desk.iQ

Automation of service maintenance processes

www.bs2.lt | connect@bs2.lt

3.7.3. The Mobile Service Desk.iQ App

Mobile Service Desk.iQ is a mobile application for the service system designed to support remote engineers and technical service employees who receive requests and need to quickly solve problems that arise.

The mobile app provides remote access to the *Service Desk.iQ* system, regardless of the user's location. It provides communication between operators, service center managers, and engineers, allowing you to effectively set tasks in accordance with the qualifications and location of personnel.

The solution allows you to keep track of employees ' working hours and monitor the status of tasks in real time. Operational control of all processes contributes to the fast and high-quality execution of work, as well as reduces the total cost of service.

Mobile Service Desk.iQ allows you to increase the efficiency of interaction between traveling staff and the quality control department, which contributes to the automation of business processes of service maintenance.

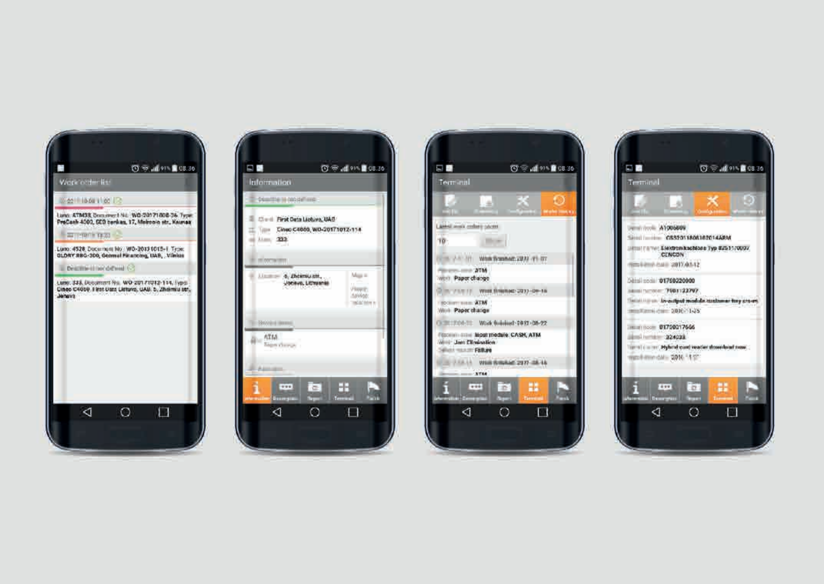


Fig. 28. Examples of the user interface for Mobile Service Desk.iQ

Among the advantages of the mobile app, it is worth noting:

- *prompt performance of service work;*
- *ability to monitor all business processes in real time;*
- *increase the efficiency of staff work by monitoring the work performed;*
- *lower service support costs.*

A new version of the mobile app *Mobile Service Desk.iQ version 2.3.13 iQ* for Android devices with a new interface and features is already available on Google Play.

3.7.4. Web Service Desk.iQ Browser Solution

Web Service Desk.iQ is a tool that provides customers with the ability to record incoming requests, track their status and provide prompt solutions to problems via a web browser. For example, a system user authorized through a web browser can create service requests, group them by various parameters, and view them in a user-friendly interface, monitoring their progress and monitoring the level of service provided.

SLA.iQ provides complete information about current and past service requests, including the total number and frequency of incidents depending on the device type, region, quality of service (SLA), and other parameters. This data is combined into reports that can be automatically sent to analysts and managers at various levels in order to optimize the company's work processes.

The *Service Desk.iQ* solution can be configured according to the requirements of a particular client. At the same time, the design of user interfaces can be changed according to the corporate style.

3.8. TSP-Services of ASHBURN International

For more than 15 years, *ASHBURN International* has been engaged in TSP-activities, providing acquiring organizations with a full range of outsourcing services for acquiring networks, and conducting technical and business consultations for payment service providers. At the same time, the company provides outsourcing services for the existing acquiring infrastructure, which can be managed by any software used by the bank for these purposes. In this case, monitoring the operation of terminal networks and monitoring the delivery of transactions are carried out within the capabilities of this software [55]. In addition, one of the company's activities is the supply of POS terminal equipment and its service support.

The company not only implements its own *TransLink.iQ* software solution, but also applies it in its work. Our own experience of using the platform allows *ASHBURN International* to set tasks for its development: to develop and add new functions for terminals, based on the needs of customers and their existing infrastructure.

To expand the functionality of acquiring equipment, *ASHBURN International* has its own highly qualified IT team – thanks to whom all work on the development of additional functionality and the introduction of new services for customers is carried out quickly and efficiently.

As part of its TSP-activities, the developer company *ASHBURN International* annually passes an audit for compliance with the requirements of the international PCI DSS Level 1 standard and PCI PIN certification.

ASHBURN International takes care of all the preparation, installation and maintenance of EFTPOS/POS terminals, routing and delivery of transactions. Using the *TransLink iQ* solution. provides a comprehensive service for acquiring networks, and the acquiring bank and, accordingly, the merchant receives a kind of uninterrupted payment terminal. The described activities of the company itself are expanding to cover new regions with the participation of subsidiaries of the *Penki Kontinentai Group* and independent partners. Similar structures are created based on the accumulated knowledge about the company's product.

Chapter 4. Outsourcing of Acquiring Networks – a Trend in Modern Banking

Outsourcing (*outer-source-using*) is the transfer by an organization, on the basis of a contract, of certain non-core or highly specialized types/functions of its activities to another company specializing in the relevant field.

The full range of acquiring network outsourcing services includes:

- *comprehensive maintenance of acquiring equipment: from commissioning to training of technical personnel;*
- *a support line (call center), where specialists can solve current technical issues and give necessary advice;*
- *round-the-clock call reception service (service desk) with user profiles;*
- *departure of a specialist to the place of equipment installation to restore the operability of equipment and software;*
- *create and upload software configurations;*
- *installation and connection of equipment;*
- *organization of a replacement fund of equipment;*
- *software updates;*
- *prevention of equipment according to the regulations;*
- *delivery of consumables;*
- *remote diagnostics and monitoring of equipment;*
- *delivery and routing of transactions*.

Speaking about outsourcing of acquiring services, it is necessary to clearly distinguish from this list those services that will be provided by the company that performs the corresponding outsourcing.

In recent years, financial institutions have shown an increasing interest in outsourcing business activities, including in order to reduce costs and increase their flexibility and efficiency.

In the context of digitalization and the growing importance of new financial technology providers (fintech), financial institutions are adapting their business models to use such technologies. Some have stepped up the use of fintech solutions and launched projects to improve their cost-effectiveness in response to the decline in intermediary margins in the traditional banking business model, which is under pressure from a low-interest-rate environment.

These organizations realized that outsourcing is a way to get relatively easy access to new technologies and achieve economies of scale.

As a rule, professional support functions for the smooth operation of individual systems and infrastructure are outsourced on the basis of a long-term contract (at least one year). Outsourcing allows not only to increase the efficiency of the enterprise as a whole, but also to focus the released organizational, financial and human resources on solving the main strategic and production tasks.

According to the *Outsourcing Institute* (USA), outsourcing is a growing type of optimization of enterprises activities, with the greatest growth observed in the field of finance and accounting.

The most common forms of outsourcing. Currently, there are many types of *business process outsourcing* in the world, as well as several typical examples that can be implemented for most enterprises, regardless of their size. For example,

- *outsourcing in the field of infocommunication system maintenance of the enterprise;*
- *financial outsourcing;*
- *outsourcing of IT systems placement (Software as a Service model; SaaS).It is a type of information process outsourcing.*

Unlike conventional hosting, a SaaS outsourcer not only provides the client with physical equipment for hosting information systems, but also provides their installation, support, and updates. In the SaaS model, the customer pays not for owning the software itself, but for renting it (for example, for using it via the web interface). Thus, unlike the classical software licensing scheme, the customer incurs relatively small recurring costs, and he does not need to invest significant funds in the purchase of the system.

The SaaS schema clearly demonstrates the relationship between different types of business process outsourcing. For example, a company that develops SaaS systems for managing acquiring networks may also be a service provider in this area.

From an economic point of view, outsourcing allows the company to significantly reduce costs, since at the same time it will be able to get rid of the additional structure and staff. Transaction costs may also decrease. Some fixed costs can be transformed into variables depending on the needs of the company in a particular period of time.

From the point of view of implementing strategic tasks, outsourcing makes it possible to concentrate resources on the main production, as well as improve operational control. In addition, it facilitates the process of introducing new technological or managerial operations.

On the technological side, outsourcing provides access to cutting-edge technologies. If the staff does not have the necessary specialists, they can be attracted through an outsourcing program. The quality of service in the case of outsourcing significantly increases, because a third-party company undertakes to control the quality of work provided under the contract. For example, due to the specifics of their business, online stores often use the services of outsourcing companies when organizing their business processes.

In general, outsourcing seems to be a good deal for many companies that do not have sufficient resources for total control of all stages and processes of production. This conclusion is confirmed by world statistics. A survey conducted by the *American Management Association* among 600 firms found that 20% of them have already outsourced some financial operations, and 80% - administrative functions. This gives us the right to assume that an increasing number of companies in the world will look at the possibility of using outsourcing [52].

4.1. Why Do Banks Outsource Non-Banking Activities?

Banking outsourcing is the process of full or partial transfer of individual functions or business processes by a bank to a third-party organization that acts as a service provider and manages the process of implementing this service or business process within its own activities [53].

Service delivery requires highly qualified engineers, a large network of branches and a warehouse of original spare parts. In addition, the response time, in accordance with the provisions of the *Service Level Agreement* (*SLA*), is always strictly limited. Proper procurement planning and inventory control of component parts is an important component of an effective warehouse management program, which is associated with the risk of increasing the cost of parts due to changes in foreign exchange rates.

In order to increase the availability of self-service devices, first of all, IT solutions for integrated monitoring of ATM networks are needed. Thus, timely detection and rapid troubleshooting of any problems, including communication problems and unexpected breakdowns, significantly reduces the cost of owning a fleet of self-service devices. In turn, the speed of troubleshooting depends on the quality of work of the bank’s service department or outsourcing company.

For example, the company's well established process chain – from accepting applications to delivering spare parts from its own warehouse and troubleshooting – significantly speeds up maintenance processes. Another important aspect of providing services is interaction with the equipment manufacturer, its support in technical and software issues. The company's engineers are trained in factories and are certified by manufacturers.

It is extremely important for owners of self-service devices to minimize the number of rejected transactions and downtime of ATMs. Regardless of whether a financial institution owns 1000 or 10 devices, you must ensure that they work smoothly. According to statistics, in 6 cases out of 10, the inability to perform operations on terminals is due to their technical condition. Every minute when the device is idle entails not only customer dissatisfaction, but also financial losses.

When outsourcing, the bank receives a comprehensive solution for the installation, monitoring and guaranteed recovery of payment terminals by competent specialists. The main advantage of outsourcing services is the full cycle of service delivery. The Bank is exclusively engaged in the banking business, selling acquiring services to customers. Everything else is handled by an outsourcing company that provides outsourcing services to the bank.

Let's list the advantages for a bank when outsourcing an acquiring network:

- *reduced network maintenance costs;*
- *improving the quality of service for the end customer;*
- *increased transparency and control of network maintenance;*
- *reducing the risks of late maintenance of the terminal;*
- *quick installation of terminals in new businesses;*
- *guaranteed recovery of working capacity in the shortest possible time.*

Among the main reasons for using outsourcing in the banking sector, we can also highlight the possibility of using advanced technologies and experience of other companies, reducing and sharing risks associated with the implementation of business processes, freeing up resources for other projects, and reducing the time required to access new market segments.

Penki Kontinentai Group of companies, including *BS/2* and *ASHBURN International*, successfully demonstrate all these advantages of outsourcing in their operations, using well-established technological chains to improve the quality of service and speed up maintenance processes.

4.2. Recommendations of the European Banking Authority and the Basel Committee on Financial Supervision on Outsourcing

Over the past decade, technological developments have not only affected customer expectations for banking services, but also changed the way banks provide these services and how they operate. These developments continue to impact the banking sector around the world.

They are, however, treated differently in different legal frameworks, even in eurozone countries. In particular, the advent of cloud computing has had a significant impact on how banks structure their businesses, and what they think should be done in-house and what should be outsourced to third-party service providers.

These developments provide banks with still undisclosed business opportunities and convenient access to services and expertise outside of traditional banking practices. However, simultaneously with these opportunities, the problem of managing the corresponding risks arises. These risks are the focus of European banking authorities ‘ attention.

The *European Banking Authority* (*EBA*) is an independent EU body established to ensure effective and prudential regulation and supervision of the European banking sector. The main objectives of the *EBA* are to maintain the EU's financial stability and ensure the integrity, efficiency and orderly functioning of the banking sector. In addition, the Office plays an important role in promoting convergence of supervisory practices and is empowered to assess risks and vulnerabilities in the EU banking sector.

The *European Central Bank* (*ECB*) has also instructed the *EBA* to develop regulatory technical standards for financial companies, such as credit institutions and investment firms, in the EU's internal market. These rules should support the integrity of the financial sector, ensure market transparency, stabilize the financial system, regulate supervision of financial institutions, and so on.

Outsourcing services can make banks vulnerable to new sources of risk and new threats – some of which may include loss of control over the business itself and the information needed to manage the bank, dependence on the supplier, or loss of know-how. The lack of transparency in the procurement of outsourced services can also lead to a number of other problems that can expose banks to the risk of corruption and fraud.

In order to counteract possible risks in outsourcing activities, in February 2019, *EBA* prepared a final report with recommendations (guidelines) for risk management [57]. Although these guidelines were developed for the banking sector in the European Union, they provide useful guidelines for risk assessment and mitigation that are applicable to any company working with third-party service providers.

In terms of governance structures, these recommendations identify strong governance mechanisms and third-party risks. So, within the framework of the general internal control system, payment institutions should have a complete risk management system on their own scale, covering all areas of activity and all internal divisions. In accordance with this framework, payment institutions must identify and manage all their risks, including those caused by agreements with third parties.

Before entering into any outsourcing agreement, payment institutions should identify and evaluate: whether such an outsourcing agreement relates to their critical or other important function; whether the conditions for outsourcing supervision are met; and all relevant risks of the outsourcing agreement. This includes conducting a proper legal review of the potential service provider, as well as the potential conflict of interest that such outsourcing may cause.

In addition, payment institutions should assess the potential impact of outsourcing agreements on their operational risk. They should consider the results of the evaluation when deciding whether they should outsource this function to the service provider, and whether they should take appropriate steps to avoid unnecessary additional operational risks before outsourcing.

However, the assessment should include, as appropriate, scenarios of possible risk events, including high-severity operational risk events. As part of the analysis, payment institutions should assess the potential impact of failures or inadequate services, including risks caused by processes, systems, people, or external factors.

As for data and system security, payment institutions must ensure that service providers comply with the relevant IT security standards. In some cases (for example, in the context of cloud or other infocommunications outsourcing), payment institutions must define data and system security requirements within the framework of an outsourcing agreement and constantly monitor compliance with these requirements.

The Basel Committee on Banking Supervision is an organization attached to the Bank for International Settlements that develops common standards and methods for regulating banking activities in various countries. It was founded in Basel, Switzerland, in 1974 by the heads of the central banks of the Group of Ten (G10) countries. Currently, the Committee includes representatives of the central banks of major countries.

The guidelines for the implementation of banking outsourcing are set out in the provisions of the document *Outsourcing in Financial Services* of The *Basel Committee on Banking Supervision* [60]. It also sets out the recommended list of works and services outsourced by credit institutions. These include: transport and repair services; real estate management; marketing; processes associated with the use of information technology; activities of call centers; logistics; cleaning, security and auditing activities; activities to attract customers and processing applications (for example, these activities in mortgage lending can be sent to the companies in the face of real estate agents and mortgage brokers); activities related to work on the problem of debt (transferred to the outsourcing of debt collection agencies); Bank card processing.

Along with looking at outsourcing trends (and recognizing the significant benefits it can provide) for the financial sector, the paper highlights the potential risks that outsourcing activities can pose to firms.

To help firms (and regulators) review their outsourcing activities, the document sets out a set of nine principles. They outline the issues that should be addressed in the outsourcing process. At the same time, it is indicated that the top management of the company continues to be responsible for the activities outsourced.

The first seven principles cover the responsibilities and responsibilities of supervised entities (regulated entities, including credite institutions) when they outsource some of their activities (functions), and the last two define the role and responsibilities of regulators. In particular, it is recommended that before outsourcing certain activities, the supervised financial institution should formulate certain policies and criteria for making outsourcing decisions. They should include an assessment of what activities, and to what extent, are suitable for outsourcing. The risk of concentration, acceptable limits of the overall level of outsourcing activities, and risks arising from outsourcing many activities to the same service provider should be taken into account. At the same time, the regulated entity (financial institution) must take measures to ensure that the service provider ensures that confidential information (both the financial institution itself and its customers) is protected from deliberate or careless disclosure to unauthorized persons.

Principle 8 states that regulators should consider outsourcing activities as an integral part of their ongoing assessment of the entity they regulate. Regulators should provide themselves with appropriate means to ensure that any outsourcing arrangements do not interfere with the regulated entity’s ability to meet its regulatory requirements.

According to principle 9, regulators should be aware of the potential risks assumed when outsourcing activities of many controlled entities are concentrated among a limited number of service providers. In cases where a limited number of outsourcing service providers (sometimes just one) provide these services to many supervised financial institutions, operational risks are correspondingly concentrated – and can pose a systemic threat. As long as concentration risks are present, there are also deterrent tools available.

The document also discusses issues to consider when drafting contracts and contingency planning.

According to the recommendations in this document, banks are required to maintain a register of contracts concluded with outsourcing organizations and follow the following principles when working with them:

- *confidentiality of information;*
- *security of information transmission;*
- *protection of personal data and information constituting a bank secret;*
- *it is not allowed to outsource banking operations, except in cases when the bank performs outsourcing when disclosing certain information with the client’s consent.*

In their turn, the client must:

- *give the bank consent to transfer your personal information, and*
- *agree on the list of persons to whom such information will be provided.*
- *In addition, the client should be aware of:*
- *the purpose of using such information, and*
- *the period during which such information may be shared with third parties.*

The client also has the right to refuse such consent and revoke the previously provided consent (in whole or in part).

Although the recommendations of the *Basel Committee* are not binding, they are nevertheless reflected in the legislation of the participating countries.

4.3. Outsourcing of Acquiring Networks: Risks or New Opportunities?

Discussions about whether a bank can outsource critical functions for its work have been going on for a long time. Currently, an increasing number of banks around the world outsource the maintenance of their acquiring networks. Partial or complete delegation of operational processes that support the operation of the payment terminal fleet helps financial organizations to focus directly on banking activities, as well as significantly reduce the cost of maintaining devices and increase the availability of payment acceptance services.

However, outsourcing services to banks can make them vulnerable to new sources of risk and new threats. Experts' opinions differ on the outsourcing of acquiring and processing functions by financial organizations: while some believe that for most financial organizations, acquiring and processing functions are inseparable from purely banking functions, others, on the contrary, believe that these functions do not relate to the main banking activity. Therefore, all business models now co-exist on the market. At the same time, the position of banks in this issue is largely influenced by the factor of trust (or distrust) of potential outsourcers.

Speaking about outsourcing risks, it should be borne in mind that consumer banking has a long history of serious financial and reputational crises resulting from mistakes made by third parties. There are frequent reports that hundreds of thousands, and sometimes millions, of customers of the world's largest retail banks were unable to withdraw funds or view their account balances due to computer failures. Another undesirable situation is related to the theft and illegal sale of personal data of customers.

At the same time, it is possible to distinguish both the advantages of outsourcing implementation in banks and its disadvantages. The advantages of using such a mechanism are:

- *quality of services provided and ensuring their long-term sustainability while maintaining approximately the same level of costs;*
- *cost savings;*
- *increase the profitability of the financial institution and its other financial indicators by reducing maintenance costs;*

- *save your work space;*
- *ability to optimize tax payments;*
- *access to experts in a specific area where you don't have employees: outsourcing usually also means being able to access people with the knowledge, professional training, and experience of working with the right products;*
- *mitigate potential risks and distribute some responsibility among outsourcing partners; if a partner is involved for a specialized event, this company, which is an expert in a particular field, applies its experience and knowledge to plan and develop a strategy for a specific task, which reduces the potential danger.*

The disadvantages of outsourcing, on the contrary, are:

- *risk of loss of confidential data and loss of confidentiality when transferring activities or processes to third parties;*
- *loss of management control and inability to control operations related to outsourced activities or processes;*
- *the imperfection of the legal framework in the field of outsourcing, the lack of guarantees for maintaining the confidentiality of customer information, the inability to control the quality of operation of individual devices, and insufficient security prevent the widespread use of such a mechanism in the banking business;*
- *hidden costs or their growth – possible if the company outsources too many processes; in addition, the implementation of an outsourcing system requires careful calculation of costs and comparing them with the expected economic impact;*
- *the danger of concentrating technological processes in one place, which may deprive the company of flexibility in certain business processes.*

4.4. International Experience in Outsourcing Payment Infrastructures

An analysis of the global practice of outsourcing payment infrastructure in various countries (both within and outside the euro ee area) shows that there are significant differences in the conditions of regulatory oversight. When compared with the activities of supervisors outside the euro area, it seems that there is only one common and mandatory element in their approach to outsourcing: in all the countries where the assessment was conducted (including the UK, USA, Australia, Canada, Malaysia and Switzerland), banks are presented with the expected conditions for the outsourcer's activities; however, in none of these countries (with the exception of the UK), banks themselves are not required to provide supervisors with preliminary information about their planned outsourcing of their functions. Instead, various tools are used, including regular supervisory assessments of overall risk management, including outsourcing risk, or subsequent on-site inspections of certain external services [59]. In the Baltic states, which are also members of the euro area, central banks have sufficient supervisory powers to control such services.

Thanks to outsourcing in the banking sector, which goes beyond non-core check processing and IT services and performs high-tech functions, banks around the world respond to the competitive environment by providing services for money management, research, analytics and other processes that were previously considered basic. The results of a study conducted by *Accenture* among 30 retail and commercial banks in the U.S. with assets of more than $3 billion, showed that half of these banks have outsourced not only such functions as processing credit cards, personnel management and it, but also Finance and accounting, including tax accounting, fixed assets, accounts payable and accounts receivable, account management, capital management.

Many banks face a lack of knowledge and experience – and decide to outsource part of their business [61]. For example, retail *Metro Bank PLC* (the 1st new bank in the last 100 years in the UK) completely outsourced its entire IT infrastructure even before its official opening in the summer of 2010. The Dutch banking and financial services corporation *ING* outsourced all its international settlement and accounting operations in London, New York, Hong Kong and Singapore to *Bank of New York* in 2002. This decision was the result of *ING's* strategy to provide high-quality clearing and settlement services with variable costs – and the result of fraud at *ING Securities* in the amount of 500 million yen in Tokyo. When *HSBC* decided to outsource some of its cash management and accounts payable functions at the end of 2004, this decision was motivated by the *Basel II* recommendations and the opportunities provided by India (the main center of outsourcing services).

The world's largest outsourcer is the American corporation *Electronic Data Systems* (*EDS*). In 1998, it had 9,000 customers, served by 100,000 employees in 44 countries. In the framework of the agreement on the provision of services in the field of outsourcing of banking technologies between *EDS* and the Italian *Banca di Roma* in 1998, a period of more than 10 years and a volume of $1.5 trillion, all the data centers, networks, and other resources of the IT consortium

Bank Group (that includes *Banca di Roma*, *Banca Nazionale della Agricoltura* and *Banca Mediterranea*) were transferred to *EDS*, who have extensive experience with financial institutions. In the US, *EDS* works with *Citibank* and manages all its technical services; in Australia, it works with the *Commonwealth Bank of Australia*; in the UK and Switzerland, it works with *Credit Suisse Group*; and in the UK, *EDS* processes cheques with the *Royal Bank of Scotland*. *EDS* is the largest non-bank owner of ATM networks.

The leaders in the business process outsourcing market are also known as the B*ig Five* of companies: *Pricewaterhouse Coopers*, *Deloitte Touche Tohmatsu*, *KPMG*, *Andersen* and *Cap Gemini Ernst & Young*. In recent years, the *Big Five* companies have been operating in both the banking and non-banking sectors of the economy.

4.5. Payment Innovations: What's Next?

More and more countries are now opting to upgrade their payment ecosystem to faster payments: more than 50 countries around the world have either already implemented or are planning to implement instant payment solutions, many of which are funded by regulators. At the same time, due to the growing competition and the desire for large-scale changes, the entire payment industry is becoming more consolidated: companies specializing in payments are conducting mergers and acquisitions in order to gain additional opportunities and enter new markets. 2019 was marked by several notable such deals, including the merger of *Fiserv-First Data* and *FIS-Worldpay*, responsible for processing payments worth $1.6 trillion per year. The question arises – what will payments look like in the next decade? They are expected to be invisible, transparent and real-time; they are likely to mean more than just transactions. At the same time, a whole range of new value – added services should become the norm, such as personal data protection, real-time cash management, as well as a new understanding of purchases that both customers and merchants will appreciate. Differentiation and pricing will increasingly depend on "payments +" services. Digital currencies, most likely supported by regulators, will also become the norm. New platforms will require new digital payment mechanisms [56].

To illustrate, let's take a closer look at *Ingenico Group's* forecasts of innovations that can radically change the field of payments in the near future [4].

Social commerce and voice commerce. By 2030, such concepts as *social commerce* and *voice commerce* can become an integral part of the payment industry. This will allow you to make payments using chatbots on any site or social network, as well as make instant payments using the user's voice.

Payments using a refrigerator. The payment sector is becoming one of the most automated based on the *Internet of Things* (*IoT*) technology. It is likely that we will soon be able to use such everyday things as a mirror, refrigerator, or car to conduct payment transactions.

Impact of new payment methods on data security. Since data security remains a priority, especially when it comes to advanced payment technologies, users themselves will have to set the appropriate rules. It is likely that new technological developments will focus on the use of biometric authentication, integration of mobile wallets, adaptation to cryptocurrencies, and the use of artificial intelligence and machine learning to ensure permanent payment protection.

Payment as a key factor in customer service. Since consumers prefer the convenience and speed of the payment process, as well as the transfer of control over its execution into their hands, the leaders will be those payment service providers who will be able to combine physical and online purchasing systems, creating a multi-channel customer service system.

Open innovations that work for the payment solutions of the future. In order for payment providers to deliver the best possible solutions, the payment industry must be supported by corporate and institutional organizations, fintech companies, and venture capital investors. In addition, payment providers need to gain consumer confidence, which is so necessary for mass adoption of their solutions.

Cashless retail stores without the cashier (for example, *Amazon Go*) come to the forefront of the high-level POS technology. They use mobile applications, RFID, artificial intelligence (AI), cameras and weight sensors shelves – enabling customers to take a desired product from the shelf and then just walk out with their purchases, since a credit card (via mobile app) was scanned at the entrance to the store the funds for the purchase was automatically charged. While this technology remains futuristic in many ways, it can provide a clear picture of the future of retail POS systems.

The Amazon Go concept store. In order to use *Amazon Go* services, you need to have a modern smartphone (iPhone or Android OS), and create an account in the free *Amazon Go* app. Then, by scanning the QRcode from the app at the store entrance, you can start making purchases. After that, you simply leave with your purchases, bypassing the checkout. You will receive a receipt for all purchases made, and your bank card, which is also linked to your *Amazon* account, will be charged for these purchases.

Paying for purchases is not the only operation that can be automated. It is expected that a new generation of supermarkets with a high degree of use of digital technologies can reduce the number of man-hours by almost 40%. All this is achieved through the use of Just Walk Out technology, which is able to automatically detect when goods are delivered or returned to shelves, and track them in a virtual “buyer’s basket”.

Scan-and-go mobile solutions. These solutions are one of the main trends for most American food retailers in the near future. The future of seamless checkout is likely similar to *Amazon Go;* it will rely heavily on computer vision to identify the customer and what they are picking up from the shelves. [21]

Shoppers increasingly expect seamless shopping experiences that allow them to shop how, when, and where they want. Therefore, merchants will look for POS systems that will help them create a unified environment for their customers. They will also look for POS technologies to apply to offer their customers the convenience of automatically ordering in goods and services.

BS2
Penki kontinentai group

Penki
Kontinentai
GROUP

Development of the banking self-service channel

www.bs2.lt | connect@bs2.lt

Annex. Key International Security Standards for Card Operations and POS Systems

In the current increasingly complex regulatory environment, improving the security of payment systems and cardholder data has become a major challenge in the industry. This is especially true for any merchant, financial institution, or other entity that specializes in storing, processing, or transmitting bank cardholder data.

Back in 2004, a uniform set of security requirements for such data was developed — *Payment Card Industry Data Security Standard 1.0* (*PCI DSS 1.0*), which combined the requirements of a number of payment system security programs – *VISA*, *MasterCard*, *American Express*, *Discover Card* and *JCB*. Subsequently, in 2006, *PCI DSS* established a specialized *Payment Card Industry Security Standards Council* (*PCI SSC*) to develop and promote the *PCI DSS* standard. It included *American Express*, *Discover Financial Services*, *JCB*, *MasterCard Worldwide*, and *VISA International*.

The main functions of the *Standards Council* are the development and publication of *PCI* standards and related documentation, defining requirements for companies planning to obtain certification for conducting *PCI DSS* audits (*Qualified Security Assessor*; *QSA*) and scans (*Approved Scanning Vendor*; *ASV*). In addition, these materials describe the stages of conducting both certification itself and training sessions for future *QSA* auditors, and performing quality control of the audit.

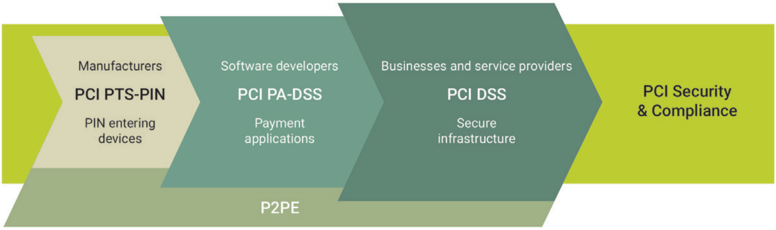


Fig. 29. Ecosystem of payment devices, applications, infrastructure, and users [62].

In turn, international payment systems accept reports based on the results of audits and evaluate the performance of QSA.

PCI DSS Standard

(*Payment Card Industry Data Security Standard; developed by the Payment Card Industry Security Standards Council PCI SSC*) defines security requirements for protecting information that relates to a payment card and should be used when the card number is stored, processed, or transmitted [66].

Starting from 2019, all confirmations of compliance with PCI DSS requirements must comply with at least PCI DSS v3.2.1. The requirements specified in the PCI DSS Standard are designed to ensure the security of payment card data by improving the security of automated systems in which this data is processed. In general, compliance with the PCI DSS Standard should mean that the system is secure and that data cannot be compromised in it.

In particular, the PCI DSS data security standard sets operational and technical requirements for those organizations that accept and process payment transactions, as well as software developers and manufacturers of applications and devices used in these transactions.

Figure 29 shows the hierarchical structure of links between *payment card industry security standards*.

The PCI DSS standard is a set of only 12 detailed requirements for ensuring the security of payment cardholder data that is transmitted, stored and processed in organizations' information infrastructures. Taking appropriate measures to ensure compliance with the requirements of the standard implies a comprehensive approach to ensuring the information security of payment card data. The PCI DSS standard applies to all merchants and service providers working with international payment systems, i.e., all those who transfer, process and store cardholder data.

Cardholder data includes the card number (PAN), the cardholder's name, the card expiration date, and the service code.

The requirements of the PCI DSS standard apply to organizations that process information about payment card holders. If an organization stores, processes, or transmits information about at least one card transaction or payment cardholder during a year, it must comply with the requirements of the PCI DSS standard. Examples of such organizations are goods and service providers (retail stores and e-commerce services), as well as service providers related to the processing, storage, and transmission of card information (processing centers, payment gateways, call centers, storage of backup data carriers, organizations involved in card personalization, and so on).

Depending on the number of transactions processed, each payment system assigns a certain level to the company with a corresponding set of requirements that must be met without fail. These can be:

1. *annual audit performance,*
2. *quarterly network scans, or*
3. *annual completion of the Self-Assessment Questionnaire, a special questionnaire developed PCI by PCI SSC.*

All the requirements of the standard are divided into 12 sections, grouped into 6 groups:

Building and maintaining a secure network:

1. *Installing and administering firewall configurations to protect cardholder data.*
2. *Prohibiting the use of system passwords and other security settings set by the manufacturer by default.*

Cardholder data protection:

3. *Cardholder data must be protected during storage.*
4. *Cardholder data transmission over public networks must be encrypted.*

Implementing a vulnerability management program:

5. *Regularly updated antivirus software must be used.*
6. *Security must be maintained when developing and maintaining systems and applications.*

Implementation of strict access control measures:

7. *Access to cardholder data should be restricted for business reasons.*
8. *Each person who has access to computing resources must be assigned a unique identifier.*
9. *Physical access to cardholder data must be restricted.*

Regular network monitoring and testing:

10. *All access to network resources and cardholder data must be monitored and monitored.*
11. *Regular testing of security systems and processes should be performed.*

Maintaining the information security policy:

12. *A policy that regulates the activities of all employees should be maintained.*

Let’s take a closer look at the requirements of VISA and MasterCard payment systems for verifying compliance with the PCI DSS requirements in the CEMEA region, which they bring to the attention of QSA auditors:

VISA:

The scope of verification during the annual audit should include at least all systems that support payment authorization, clearing, and settlement processes, as well as fraud monitoring, dispute resolution, and customer support (call centers).

MasterCard:

The scope of review during the annual audit should include at least all systems that support payment authorization, clearing, and settlement processes.

Payment card industry organizations are developing a common standard that regulates, among other things, the security aspects of PIN entry devices (*PIN entry devices*; *PEDs*). The requirements for such devices regulate the methodology for testing devices and the approval process for certified devices, and include requirements for PIN code protection.

The task of PCI PED is to make sure that the device that accepts the PIN code protects sensitive information – such as resident keys, cardholder PIN, etc.

The purpose of the requirements is to provide a uniform, consistent and accurate standard for all PIN input devices worldwide.

Different international payment systems have different requirements for the PCI DSS certification process. There are different levels of certification for retailers and service providers.

These are the following methods for verifying compliance with the PCI DSS standard:

- *external QSA audit performed by the PCI QSA company at the facility of the organization being audited;*
- *completing a self-assessment sheet;*

- *automated ASV scanning of network perimeter vulnerabilities*.

The method of checking compliance, or a combination of methods, is selected в depending on the level of certification of the retailer or the service provider.

The requirements of the standard apply to all companies working with *VISA* and *MasterCard* international payment systems. Depending on the number of transactions processed, each company is assigned a certain level with a corresponding set of requirements that they must meet. The requirements of the standard include annual audits of companies, as well as quarterly network scans.

Since September 2006, the standard has been introduced by the *VISA* payment system in the CEMEA region CEMEA (Central Europe / Middle East / Africa) as mandatory; respectively, including Russia. Therefore, service providers (processing centers, payment gateways, Internet service providers) that work directly with *VisaNet* must pass the audit procedure for compliance with the requirements of the standard.

Payment Application Security Standard PA-DSS

Following the launch of the PCI DSS certification program for organizations that process cardholder data PCI DSS, the activities of the PCI SSC Council to ensure the security of the payment industry were developed in the form of the launch of a program to improve the security of payment applications. For this purpose, the Council established the PA-DSS standard, which is, on the one hand, a development of the *VISA PABP* regulation (*Payment Application Best Practices*), and on the other hand, an adaptation of the requirements of the PCI DSS standard to applications.

The standard for payment terminals *PA-DSS* (*Payment Application Data Security Standard*) has become one of the most relevant requirements. This standard was developed by *VISA*, *MasterCard*, and other payment systems to describe the security requirements of software that processes payment transactions using bank payment cards. The requirements of the PA-DSS Standard are derived from the requirements of the PCI-DSS Standard and PCI DSS (*PCI DSS Security Audit Procedures*). These documents provide a detailed description of the data security requirements that retailers and service providers must meet to comply with the PCI DSS standard (and, consequently, which payment system application must be used to ensure compliance with this standard). The requirements of the PA-DSS standard also apply to applications that process cardholder data at the stage of transaction authorization. The only exceptions are self-developed applications or those custom-designed for a single user (which are not subject to PA-DSS requirements).

PA-DSS certificate ensures that the cardholder's important data is protected from illegal use or theft. All payment applications released to the market must be certified according to the PA-DSS standard, which can only be performed by those companies that have the PA-QSA status. International payment systems require retailers and service providers to use only PA-DSS certified applications, the list of which is published and regularly updated by the PCI SSC Council [65].

A list of software that has successfully passed PCI PA-DSS certification is available on the PCI Security Council website: https://pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html

Point-to-Point Encryption (P2PE)

The PCI SSC Security Standards Development Council has published recommendations for using point-to-point encryption (P2PE) [66].

The document entitled Payment Card Industry (PCI) Point-to-Point Encryption Solution Requirements: Encryption, Decryption, and Key Management within Secure Cryptographic Devices contains items that describe:

- *roles and responsibilities of parties in the process of authentication, implementation, and evaluation of P2PE hardware solutions;*
- *providing security for hardware solutions at six levels (encryption device, encryption environment, application security, data transmission, data decryption, and key management);*
- *steps required to create and validate P2PE solutions;*
- *example of a standard P2PE implementation;*
- *the relationship between P2PE authentication requirements and other PCI standards, such as PIN Transaction Security (PTS) Point-of-Interaction (POI) Security Requirements, PIN Transaction Security Requirements (PCI PIN), PA-DSS standards, and PCI DSS [65].*

Thus, the P2PE standard defines the requirements that a particular solution must meet in order to be accepted as a PCI-validated P2PE solution. A solution is a complete set of hardware and software, gateway, decryption, device handling, and so on. However, only solutions as a whole can be checked;

individual pieces of equipment (such as card readers) cannot be checked. Often, solutions approved by P2PE are mistakenly referred to as "certified" (there is no such certification).

These requirements focus on ensuring the security of systems and devices, implementing monitoring and feedback processes, developing and maintaining secure applications, protecting confidential data, and methods for securely managing cryptographic keys.

Payment solutions that offer similar encryption but do not comply with the P2PE standard are called end-to- end encryption solutions (E2EE). End-to-end encryption is a method of data transmission in which only users participating in communication have access to messages, i.e., the use of end-to-end encryption does not allow third parties to access cryptographic keys.

The goal of P2PE and E2EE is to provide a payment security solution that instantly converts sensitive payment (credit and debit) information to an unencrypted code while reading the card data to prevent hacking and fraud. It is designed to provide maximum security for payment card transactions in an increasingly complex regulatory environment.

When a payment card passes through a reader (point of interaction device; POI) at the point of sale, the information contained on the card is immediately encrypted (a device that is part of the P2PE solution, certified by PCI, uses an algorithmic calculation method for this). Then the encrypted (and non-encrypted) codes are sent from the POI to the payment gateway or processor for decryption. Since the keys for encryption and decryption are never available to the merchant, this makes the card data completely invisible to the merchant. When encrypted codes are located in the secure data zone of the payment processor, they are decrypted to the original card numbers and then transmitted to the issuing bank for authorization. The bank approves or rejects the transaction, depending on the state of the cardholder's payment account, and notifies the merchant of payment acceptance or rejection to complete the process, along with a token that the merchant can save. The specified token is a unique reference number to the original transaction, which the merchant can use in case they need to conduct research or refund money to the client, even without knowing the client's card information (tokenization).

The responsibility for determining the compliance of a solution with the P2PE standard is borne by qualified P2PE Security Evaluators (P2PE-QSA) - these are independent third-party companies that hire evaluators who have met the requirements of the PCI SSC Council for Education and Experience, and have passed the necessary exam. At the same time, the PCI SSC Board does not check their decisions.

There are also qualified Integrator and Reseller companies (QIR) that are authorized to implement, configure, and / or maintain PA-DSS verified payment applications and perform their qualified installation.

PA P2PE solution provider is a third-party organization (for example, a processor, acquirer, or payment gateway) that has overall responsibility for developing and implementing a specific P2PE solution and manages P2PE solutions for its trading clients [43, 66].

Note that the hardware solution for P2PE provides for the use of cryptographic devices for data encryption and decryption.

Requirements for a P2PE solution vary depending on the deployment environment and technologies used for a particular implementation. The above document provides requirements covering each domain for environments that use Secure Cryptographic Devices (SCDs) to encrypt, decrypt, and manage cryptographic keys. This scenario is intended for merchants who do not store or decrypt encrypted data in their P2PE environment - and use proven solutions consisting of hardware encryption and third-party hardware decryption.

In June 2015, the PCI SSC Council published an important update to one of the eight security standards related to the use of payment cards. According to PCI SSC, the update will simplify the development and use of point-to-point (P2PE) data encryption solutions. In this case, encryption is performed by a crack-resistant module directly at the reading point, which makes data from the card inaccessible to conventional reading methods and reduces the value of stolen data for an attacker.

The PCI Point-to-Point Encryption Solution Requirements and Testing Procedures Version 2.0 specification is intended for vendors of P2PE components and services that perform P2PE requests and can be embedded in P2PE solutions. Along with certified P2PE solutions and applications, the PCI Council will maintain a list of certified P2PE components, making it easier for integrators to select them. In addition, the new version of the standard gives merchants the opportunity to implement their own P2PE solutions and manage them independently in retail outlets. Requirements include:

- *secure encryption of payment card data at the point of interaction (POI);*
- *P2PE-approved application(s) at the point of interaction;*

- *secure management of encryption and decryption devices;*
- *management of the decryption environment and all decrypted account data;*
- *use secure encryption methodologies and operations with cryptographic keys, including key generation, distribution, uploading / embedding, key administration, and key usage.*

PCI DSS Service Provider Certification Levels

Service providers are organizations that provide various services (mainly in the field of IT) merchants, acquiring banks, issuers, and directly international payment systems. At the same time, the service provider organization gets access to data about cardholders. Table 1 describes the levels of PCI DSS certification of service providers according to the *VISA* and *MasterCard* payment system classifications:

	VISA classification	**MasterCard classification**
Level 1:	• *All processing centers connected to VisaNet;* • *Service providers that process, store or transmit data on more than 300,000 transactions per year.* ***Certification requirements:*** • *annual audit performed by a QSA auditor at the organization's facility;* • *quarterly ASV scan.*	• *All processing centers.* • *Service providers that process, store or transmit data on more than 300,000 transactions per year.* • *All processing centers and service providers through whose systems cardholder data was compromised.* ***Certification requirements:*** • *annual audit performed by a QSA auditor at the organization's facility;* • *Quarterly ASV scanning.*
Level 2:	• *Service providers that process, store or transmit data on less than 300,000 transactions per year.* ***Certification requirements:*** • *annual self-assessment of compliance with the completion of the questionnaire (SAQ);* • *quarterly ASV scan.*	• *Service providers that process, store or transmit data on less than 300,000 transactions per year.* ***Certification requirements:*** • *annual self-assessment of compliance with the completion of the questionnaire (SAQ);* • *quarterly ASV scan.*

Table 1. Levels of PCI DSS certification of service providers.

Examples of service providers are: processing centers, payment gateways, data centers, point-to-point tokenization and encryption (P2PE) service providers.

Glossary

3-D Secure is a VISA technology that allows you to additionally authorize the user using the issuing bank’s funds. *The 3-D Secure Security Requirements* program defines the physical and logical security requirements for the Enrollment Servers (ES) and/or Access Control Servers (ACS) infrastructure that support the Verified by VISA service. These requirements are additional to the PCI DSS requirements that must also apply to ES/ACS infrastructures to ensure the confidentiality, integrity, and availability of the service provider’s infrastructure.

Access Control Server (ACS) is an element of the *3-D Secure* infrastructure that provides validation of the payer on the issuing bank’s side.

Acquiring bank — a credit institution with which the merchant’s current account is opened and which provides equipment for acquiring. Implements and operates a payment gateway.

Acquiring bank’s payment gateway is an automatic system that allows the merchant to accept and send payments to the client via the Internet using bank cards.

Acquiring network — a network of terminals usually of a bank (processing center) in stores or retail outlets, where payment is possible using payment cards.

Acquiring — the ability to receive payments for goods and services by bank cards.

Approved Scanning Vendor (ASV) is a scanning service provider that has an official status from the PCI SSC Council.

Bank card payment system – a payment system that combines ATMs of various banks.

Bank Identification Number (BIN) — a six-digit number assigned by the international payment system, used to identify issuers during authorization, processing and clearing, by which you can get complete information about the issuing bank.

BASE24-eps is an integrated universal software solution for acquiring, authenticating, routing, switching, and authorizing financial transactions across multiple channels.

Basel Committee on Banking Supervision (BCBS) is an organization operating under the Bank for International Settlements that develops common standards and methods for regulating banking activities adopted in various countries around the world.

Basel II is a document of the *Basel Committee on Banking Supervision* adopted in 2004: new approaches", which contains methodological recommendations in the field of banking regulation.

BBM.iQ (Basic Billing Management) is a module that periodically calculates accounts payable and receivables for services rendered.

Biometric payment terminal — a payment terminal that uses biometric technologies to provide users with maximum security – such as fingerprint recognition.

Card Verification Value / Cardholder Verification Code (CVV/CVC) — a three-digit code, most often located on the back or side of a payment card, which is used during authorization when making purchases on the Internet. It is intended to verify the authenticity of the payment card.

CEMEA (Central Europe / Middle East / Africa) is a region that includes the countries of Central Europe, the Middle East, and Africa.

Clearing center — an organization that deals with clearing, i.e., non-cash payments. The subject of transactions can be either goods supplied to each other, according to the agreement, or any securities and other services that use mutual offsetting, taking into account the total balance of bank payments.

Clearing is a non-cash settlement procedure in which a clearing entity acts as an intermediary, taking on the role of buyer and seller in a given transaction in order to secure orders between two parties.

CTLS — (1) a convenient remote keyboard for Verifone stationary terminals, designed for the client to enter a PIN code. It has a built-in contactless reader, which allows you to expand the capabilities of the POS terminal.

CTLS — (2) short for ConTactLeSs (i.e., contactless). Accepted as a name for a technology that allows payments to be made without physical contact between the bank card and the payment device. Most often, the prefix CTLS can be seen in the name of a bank payment terminal or any other device that supports contactless payment technology.

EFTPOS (electronic funds transfer at point of sale) — (1) an electronic payment terminal that provides electronic money transfers based on the use of payment cards, such as debit or credit cards, at points of sale; (2) an electronic payment system that includes electronic money transfers based on the use of payment cards in payment terminals at points of sale.

EFTPOS/POS terminal — an electronic hardware and software device for accepting payment cards for payment; it is capable of accepting cards with a chip, magnetic stripe and contactless cards, as well as other devices that have contactless pairing.

Electronic funds transfer (EFT) is an electronic transfer of money from one bank account to another, either within the same financial institution or in several institutions, through computer systems without direct intervention of banking personnel.

Electronic payment system is a subspecies of a payment system that provides electronic payment transactions through networks (for example, the Internet) or payment chips. Electronic (digital) cash (English e-cash; electronic cash; digital cash) is a term used in payment systems for the ability to make electronic payments, similar to paying in regular cash, without the mandatory intermediary of a third party.

EMV (Europay + MasterCard + VISA) is an international standard for transactions on bank cards with a chip. It was developed jointly by *Europay*, *MasterCard* and *VISA* to improve the security of financial transactions.

European Central Bank (ECB) – the central bank of the countries that make up the Eurozone.

FCM.iQ (Fuel Consumption Management) — a module that allows you to automatically or manually enter data to track the remaining fuel resources.

GCM.iQ (Geographical Control and Monitoring). You can use this module to track devices, tasks, and their status on the map in real time.

Hardware security modules (HSM) are *Thales* payment security modules that guarantee the security and reliability of data in any environment, while maintaining the efficiency of the business.

Integrated terminal / PIN pad — a payment terminal that works only in conjunction with the cash register software.

International Monetary Fund (IMF) is a specialized agency (monetary fund) of the United Nations. IMF 189 member countries are represented in the IMF. The IMF provides short- and medium-term loans in case of a state's balance of payments deficit.

International payment system — a payment system in which a payment organization (both resident and non-resident) operates on the territory of two or more countries, ensuring the transfer of funds within this payment system, including from one country to another. Examples of such payment systems are *VISA*, *MasterCard* and *Мир*.

Issuing bank — a credit institution that issues bank cards, payments from which are accepted by terminals.

ITIL (IT Infrastructure Library). Currently, this is a separate methodology that is widely used in the world. As the library of IT infrastructure has evolved, the focus has shifted over time to service management and the lifecycle approach. Since 2013, ITIL has been owned by *AXELOS Ltd.* — a joint venture between *Capita Plc* and the UK Cabinet Office.

KPI (Key Performance Indicator) is a tool that helps to analyze the effectiveness of a particular activity, as well as the level of achievement of goals.

KPI.iQ (Key Performance Indicator) is a module that measures and evaluates the productivity and efficiency of processes, as well as tracks their trends. Provides an accurate assessment of progress in achieving a specific goal.

LRM.iQ (Local Repair Management) is a module that registers the work of the local repair department, revealing the list of spare parts for the repair of the taken controlled objects.

Merchant — a trade and service enterprise that sells goods or provides services.

Mobile Service Desk.iQ is a mobile application for the service system designed to support engineers and technical service employees who receive requests and need to quickly solve problems that have arisen.

MPI (Merchant Plugin Interface) is a *3-D Secure* and *SecureCode* technology component that can be placed on the payment system side or on the store side.

Multi-banking — the ability to work with multiple acquiring banks while processing payments.

Multi-hosting — the ability to deliver various types of transactions to different processing centers and other systems.

Multi-merchant — the ability to use only one physical device to make payments to several sellers of goods and services or send transactions to different accounts of the same merchant.

Offline payment terminal is a separate device that is not connected to the cash register software. It includes a reader for magnetic, chip, and contactless cards, a digital PIN keyboard, and a receipt printer.

Offline transaction — a transaction that is performed with a certain time delay.

Omnichannelling is a term that refers to the mutual integration of disparate communication channels into a single system, in order to ensure seamless and continuous communication with the client.

Online acquiring — accepting payment for payment cards and electronic money via the Internet using a specially designed web interface designed for payments in online stores and payment for services.

Online cash register with acquiring is an integral part of the cash register equipment, which is a two-in-one device: an EFTPOS/POS terminal and an online cash register.

Online sales register is a device designed to automate cash transactions and financial accounting.

Online transaction is a type of transaction that is characterized by the instantaneous execution of the operation (crediting funds, debiting them, or transferring them).

Outsourcer — a specialized organization of class B2B, an outsourcing service provider.

Outsourcing (outer-source-using) is the transfer by an organization, on the basis of a contract, of certain non-core types / functions of its activities to another company specializing in the relevant field.

PA-DSS (Payment Application Data Security Standard) is a set of security standards created by the *PCI SSC* to guide payment application vendors in developing secure payment applications.

PAN (Primary Account Number) — each bank card has its own number, which can be printed or embossed (squeezed out). In the English-language documentation, it is called PAN and is represented on the bank card by the number on its front side.

Payment gateway — a service that authorizes and processes debit/credit card payments for online merchants and traditional retail and offline merchants.

Payment Service Provider (PSP) is a company that provides online services for merchants and banks to make electronic payments in various ways, including smart cards, bank payments, and other banking operations.

Payment system — a set of rules, procedures and technical infrastructure that ensure the transfer of value from one economic entity to another.

PCI DSS (Payment Card Industry Data Security Standard) is a standard developed by the *PCI SSC* that defines security requirements for protecting information related to a payment card.

PCI PIN Security is a standard designed to protect PIN codes when performing transactions at ATMs and payment terminals of the merchant. Implementation of its requirements ensures the protection of PIN codes from the moment they are entered on the ATM keyboard or payment terminal, to processing in the acquirer's and issuer's payment systems.

PCI SSC (Payment Card Industry Security Standards Council) is an organization that develops and publishes PCI standards and all related documentation, as well as defines requirements for companies planning to obtain certification for conducting *PCI DSS* audits. It includes *American Express*, *Discover Financial Services*, *JCB*, *MasterCard Worldwide*, and *VISA International*.

PIN pad is a device designed for making secure transactions.

Point of sale (seller, merchant) — an organization that sells goods or services, initiates the activation of acquiring; pays a commission for using acquiring.

Point-to-Point Encryption (P2PE) – a document containing recommendations for using point-to-point encryption of the *PCI SSC*; contains requirements for all organizations engaged in trading that intend to use point-to-point encryption that supports the *PCI DSS* data security standard.

POS system — a hardware complex for automating the work of cashiers based on fiscal registrars.

Processing center — a legal entity or its structural division that provides information and technological interaction between settlement participants.

Processing is the processing of information that is used in making payment transactions.

Prudential regulation is a type of banking regulation designed to ensure the stability and reliability of banks, as well as protect the interests of their depositors.

QR code (Quick Response Code) — a type of matrix or two-dimensional barcodes-a machine-readable optical label containing information about the object to which it is linked; originally developed for the automotive industry in Japan. The term itself is a registered trademark of the Japanese company Denso.

QSA (Qualified Security Assessor) is an independent security company that is certified by the *PCI SSC* to confirm compliance of an organization with *PCI DSS* standards. During audits, *QSA* auditors collect evidence of compliance with the requirements of the standard and retain it for three years.

Refund — a partial or full reimbursement of funds to the buyer's card in case of refusal to receive the goods (services) or their return.

Reversal — lifting the lock on funds on the buyer's card. This feature is available for a limited time, and the exact terms of this feature must be specified in the bank.

Routing — a mechanism used to configure the rules for choosing a payment route in accordance with the specified parameters. Routing payments to multiple banks means that transactions are automatically redistributed by the payment gateway to the corresponding payment card issuing banks.

RSA (short for Rivest, Shamir, and Adleman) is a public-key cryptographic algorithm based on the computational complexity of factoring large integers. It is used in a variety of cryptographic applications.

SaaS (Software as a Service) is a form of cloud computing, a service model in which subscribers are provided with ready-made application software that is fully serviced by the provider. In this model, the vendor manages the application independently, providing customers with access to functions from client devices, usually via a mobile app or web browser.

SecureCode is a *MasterCard* payment system technology that allows you to additionally authorize the user using the issuing bank's funds. Technologically equivalent to *3-D Secure*.

SEPA (Single Euro Payments Area) — a single area in which the differences between domestic and international payments in euros are completely eliminated. The first SEPA-related changes came into effect on January 28, 2008.

Service Desk.iQ is a software product of *BS/2* (*Penki Kontinentai Group*); a solution for automating equipment maintenance processes for banks and retail enterprises, responsible for opening, distributing, executing and closing customer requests, organizing the work of the service company's staff and generating reports.

SET (Secure Electronic Transaction) is a standardized protocol for conducting bank card transactions over insecure networks, including the Internet.

SLA (Service Level Agreement) is a term of the ITIL methodology that denotes a formal contract between the customer (in the ITIL recommendations, the customer and the consumer are different concepts) This document contains a description of this service, the rights and obligations of the parties and, most importantly, the agreed level of quality of the provision of this service.

SLA.iQ is a module for entering formalized data into the system. It is based on methods for calculating general management parameters, an agreement on services provided, and additional conditions.

SRM.iQ (Service Request Management) is a module that automatically manages customer requests by providing SLA requirements.

SRP.iQ (Service Repair Parts) is a module that records information and all events related to resources used to troubleshoot service provision. This means recording spare parts units and related processes.

SWIFT (Society for Worldwide Interbank Financial Telecommunications) is a system that provides an international system for transmitting financial data. Allows financial institutions around the world to send and receive information about financial transactions in a secure, standardized and reliable form.

Switching — depending on the context, it is most often considered synonymous with routing, i.e., managing the distribution of transactions in different directions.

Tieto Card Suite is a software product of *Tieto* designed to solve various tasks related to payment cards, including issuing, acquiring, managing terminals, fraud prevention, etc.

Transaction (from Lat. transactio - agreement, contract) — in the general sense, a transaction involving the exchange of data with subsequent adjustments to the system. In banking practice, this term is often used to refer to the movement of funds during the purchase and sale process.

TransLink.iQ Manager is a module that provides transaction routing, network management of payment terminals, comprehensive real-time monitoring of devices, remote software loading and data exchange with the acquiring system of the processing center.

TransLink.iQ Reporting is an application for working with databases, uploading data to external systems, and generating various analytical reports.

TransLink.iQ SmartPOS is an application designed to support payment functions of terminals from different manufacturers.

TransLink.iQ XConnect is a module for communication between the *TransLink.iQ SmartPOS* application and cash register software using asynchronous data transfer.

TransLink.iQ — software and hardware package by *ASHBURN International* (*Penki Kontinentai Group*) for managing the network of payment terminals and transaction delivery, as well as for monitoring the transaction flow and technical condition of POS terminals in real time.

TranzAxis is an integrated open software platform for creating payment services developed by the Russian company *Compass Plus*.

TranzWare is an open software platform for creating payment services for the Russian company *Compass Plus*.

Virtual payment terminal — a web interface that replaces a physical payment terminal based on the customer - operator - virtual payment terminal service scheme.

Vulnerability scanner — a software / hardware tool for performing diagnostics and monitoring of network computers, which allows you to scan networks, computers and applications for possible security problems, evaluate and eliminate vulnerabilities for the presence of “holes” that can be exploited by intruders.

WAY4 is a processing platform developed by the Belgian company *OpenWay Group*, which is used by more than 100 banks in various countries of the world.

Web Service Desk.iQ is a tool developed by *BS/2* (*Penki Kontinentai Group*), which allows customers to record incoming requests via a web browser, track their status, and provide prompt solutions to problems.

References

1. Annual Reports 2018 / HPS Worldwide. *https://www.hps-worldwide.com/sites/default/files/investor/Annual%20Report%202018.pdf*

2. Žoržas Šarafanovičius. How to become a Payments Service Provider. ASHBURN International, DIEBOLD NIXDORF PARTNER SUMMIT EUROPE 2018 | BUDAPEST, HUNGARY | JUNE 6.

3. Shaun Packiarajah, Mobile Ecommerce, Mobile Wallets, and Payment Safety Digital Payments Report 2019, p. 36; *https://www.statista.com/study/41122/ fintech-report-digital-payments*

4. ТОП-5 трендов, которые изменят платежную индустрию — прогноз Ingenico. *https://psm7.com/review/top-5-trendov-kotorye-izmenyat-platezhnuyu-industriyu-prognoz-ingenico.html*

5. Ashburn International exec cites importance of 'terminal as a service'. *https://www.atmmarketplace.com/articles/ashburn-international-cites-importance-of-terminal-as-a-service/?utm_source=AMC&utm_medium=email&utm_ campaign=EMNA&utm_content=2020-02-25*

6. Запущен универсальный сервис мгновенных платежей "QR-online". *http://uzdaily.uz/ru/post/49837*

7. Процессинговый центр. *http://dengi.polnaya.info/platezhnye_sistemy/processingovyy_centr/*.

8. Mexico's new QR-based payments system — will it succeed? *https://www.atmmarketplace.com/blogs/mexicos-new-qr-based-payments-system-will-it-succeed/?utm_source=AMC&utm_medium=email&utm_campaign=EMNA&utm_content=2019-10-15*

9. *A*SHBURN INTERNATIONAL makes TOP 10 payment service providers in Europe. *http://www.ashburn.eu/index.php?id=1908*

10. SERVICE DESK.IQ – maintenance service management and optimization. *https://www.bs2.lt/ru/programmnoe-obespechenie/ semeystvo-produktov-iq/service-deskiq/*

11. Mobile POS Payments. *https://www.statista.com/outlook/331/100/mobile-pos-payments/worldwide*

12. Chaum, David (1983). "Blind signatures for untraceable payments" (PDF). Advances in Cryptology Proceedings. 82 (3): 199–203.

13. POS terminals by Ingenico. *http://ingenico.ru/product_list.html*

14. Countertops, PIN pads, Multilane. *https://www.Verifone.com/en/us/countertops-pin-pads-multilane*

15. Unattended Retail Is the Future and We're Helping You Get in the Game *https://www.globalpaymentsinc.com/en-us/blog/2019/03/06/unattended-retail-future*

16. Lori Fairbanks. The Best POS Systems of 2020. *https://www.business.com/categories/best-pos-systems/*

17. payShield HSM family of Payment HSMs. *https://www.thalesesecurity. com/products/payment-hsms*

18. Кредитка под угрозой: охотники за POS-терминалами. *https://www.kaspersky.ru/blog/ohotniki-za-terminalami/2849/*

19. Biometric Payment Solutions. *https://www.biometricupdate.com/service -directory/pos-authentication*

20. EFTPOS – advantages, disadvantages and why you need one. *https://www.tyro.com/blog/eftpos-advantages-disadvantages-and-why-you-need-one/Advantages of EFTPOS*

21. Rimma Kats. Is Scan-and-Go the Future of Retail? Feb 11, 2019. *https://www.emarketer.com/content/is-scan-and-go-the-future-of-retail*

22. *https://cdn.ingenico.com/binaries/content/assets/corporate-en/press-releases/2014/11/20141104-telium-tetra-en.pdf*

23. Biometric facial verification to replace passwords and ID documents for online services in Singapore. *https://www.biometricupdate.com/202003/biometric-facial-verification-to-replace-passwords-and-id-documents-for-online-services-in-singapore*

24. POS-трансформация: интеллектуальные терминалы и сервисы Verifone. *https://www.plusworld.ru/Verifone/*

25. *https://uploads.strikinglycdn.com/files/a087216d-609a-4381-94de-4e13831bd17f/PAX%20Classic%20Terminals%20Booklet.pdf*

26. Our Smart Devices in the News. *https://www.pax.us/products/*

27. Recent Cyber Intrusion Events Directed Toward Retail Firms. *https://krebsonsecurity.com/wp-content/uploads/2014/01/FBI-CYD-PIN-140117-001.pdf*

28. Кибергруппа FIN6 атакует PoS-терминалы в Европе и США. *https://www.securitylab.ru/news/495470.php*

29. POS Attacks Possible as Different Types of Malware Infect 4,000 ElasticSearch Servers. *https://securityintelligence.com/news/pos-attacks-possible-as-different-types-of-malware-infect-4000-elasticsearch-servers/*

30. Charles Henderson. When Souvenirs Cost More Than Pocket Change: Mobile Point-of-Sale Hazards. *https://securityintelligence.com/when-souvenirs-cost-more-than-pocket-change-mobile-point-of-sale-hazards/*

31. Kromtech Discovers Massive Elasticsearch Infected Malware Botnet. *https://kromtech.com/blog/security-center/kromtech-discovers-massive-elasticsearch-infected-malware-botnet*

32. Биометрия и будущее платежных операций. *https://www.plusworld.ru /daily/tehnologii/biometriya-i-budushhee-platezhnyh-operatsij/?utm_source=sendpulse&utm_medium=email&utm_campaign=zhurnal-plas-2020*

33. Китай ввел стандарты для систем распознавания лиц. *http://www.tadviser.ru/index.php/Статья:Системы_распознавания_лиц_(Facial_recognition)#.2A_.D0.9A.D0.B8.D1.82.D0.B0.D0.B9_.D0.B2.D0.B2.D1.91.D0.BB_.D1.81.D1.82.D0.B0.D0.BD.D0.B4.D0.B0.D1.80.D1.82.D1.8B_.D0.B4.D0.BB.D1.8F_.D1.81.D0.B8.D1.81.D1.82.D0.B5.D0.BC_.D1.80.D0.B0.D1.81.D0.BF.D0.BE.D0.B7.D0.BD.D0.B0.D0.B2.D0.B0.D0.BD.D0.B8.D1.8F_.D0.BB.D0.B8.D1.86*

34. Goodbye, passwords. Hello, biometrics. *https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-biometrics-payments-study.pdf*

35. Biometric point-of-sale payments growth led by India, China. *https://www.biometricupdate.com/201912/biometric-point-of-sale-payments-growth-led-by-india-china*

36. Lane/3000 Designed for fast payment at lane. *https://cdn.ingenico.com/binaries/content/assets/corporate-en/library/datasheets/ing_fiche_lane3000---jan20.pdf*

37. Приложение 3. Коды ответа - расшифровка actionCode *https://pay.alfabank.ru/ecommerce/instructions/merchantManual/pages/ index/appendix_actioncode.html*

38. TransLink.iQ Manager. Technical User Manual. V3.1.5

39. Роль платежного сервиса в онлайн-транзакциях. *https://habr.com/ru/company/fondy/blog/322738/*

40. Retail. *https://cdn2.hubspot.net/hubfs/5565783/content/WJ4287_PXP_Financial_Retail_download_June_2019_vs2.pdf*

41. UP BASE24-eps. *https://www.aciworldwide.com/-/media/files/collateral/data-sheets/aci-base24eps-fl-us.pdf*

42. Обзор информационных систем по работе с банковскими электронными картами. *http://www.guidebanking.ru/gbanks-464-1.html*

43. Point to Point Encryption. *https://en.wikipedia.org/wiki/Point_to_Point_Encryption*

44. Решение SmartVista Switch. *https://cdn2.hubspot.net/hubfs/6845371/resources/brochures_RU/BPC-SmartVista-Switch-Brochure_RU.pdf*

45. Кроссплатформенное ПО для POS-терминалов JoinPOS. *https://mst-company.ru/uslugi/platjozhnye-resheniya/universalnoe-po-dlya-pos-terminalov*

46. Новый ландшафт защиты данных 2019 Доклад Thales об угрозах данным. *https://dnadis.ru/wp-content/uploads/2019/07/Otchet2019-1-1.pdf*

47. Программный комплекс для управления сетью терминалов – CyberTMS. *http://www.posterminal.biz/PTMS.html*

48. Fleet management. *https://www.ingenico.com/pos-solutions#fleet-management-solutions*

49. Evaldas Gučius TransLink.iQ Manager Technical User Manual V3.1.5. 2021-04-14, ASHBURN International

50. Nikolaj Jevplov.TransLink.iQ SmartPOS Manual V1.0.1 2018-10-01

51. Service Desk.iQ – управление и оптимизация сервисного обслуживания. *https://www.bs2.lt/ru/programmnoe-obespechenie/ semeystvo-produktov-iq/service-deskiq/*

52. Что такое аутсорсинг. *http://predp.com/fin/terms/chto-takoe-autsorsing.html*

53. Банковский аутсорсинг. *https://www.banki.ru/wikibank/bankovskiy_autsorsing/*

54. Аутсорсинг эквайринговых сетей. *https://www.ashburn.eu/ru/autsorsing-ekvajringovyh-setej/*

55. Критически важные функции в банке могут быть на аутсорсинге при одном условии! *https://infobank.by/infolineview/kriticheski-vazhnye-funkcii-v-banke-mogut-bytj-na-autsorsinge-pri-odnom-uslovii/*

56. 2020 banking and capital markets outlook. *https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-outlooks/banking-industry-outlook.html#payments-remaining-relevant-as-f*

57. Final Report on EBA Guidelines on outsourcing arrangements. *https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf*

58. Outsourcing opportunities and challenges. *https://www.bankingsupervision.europa.eu/press/publications/newsletter/2018/html/ssm.nl180214_3.en.html*

59. Аутсорсинг в банках фактически запрещен, но как-то работает. Разбираемся, как? *https://infobank.by/infolineview/autsorsing-v-bankax-fakticheski-zapreshhen-no-kak-to-rabotaet-razbiraemsya-kak/*

60. Outsourcing in Financial Services. *https://www.fsb.org/2005/02/cos_050215/*

61. Outsourcing in the Banking Sector: Problems and Prospects. *https://www.theglobaltreasurer.com/2007/08/28/outsourcing-in-the-banking-sector-problems-and-prospects/*

62. MAINTAINING PAYMENT SECURITY. *https://www.pcisecuritystandards.org/ pci_security/maintaining_payment_security*

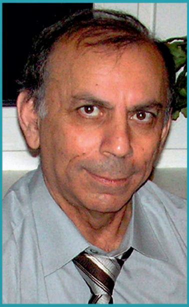
63. Хакеры заинтересовались POS-терминалами. *http://www.pcidss.ru/articles/249.html*

64. VALIDATED PAYMENT APPLICATIONS. *https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications?agr*

65. Стандарт безопасности данных индустрии платежных карт (PCI DSS). *https://ru.pcisecuritystandards.org/_onelink_/pcisecurity/en2ru/minisite/en/docs/PCI_DSS_v3_05Nov13_Final_RU-RU.pdf*

66. Payment Card Industry (PCI) Point-to-Point Encryption. *https://www. pcisecuritystandards.org/documents/nb59Y8Qqv/P2PE_Hardware_Solution_%20Requirements_Initial_Release.pdf*

Takhmasib Dadashev



Currently an Associate Professor of the Moscow Institute of Physics and Technology (Russia). Holds a degree of Candidate of physical and mathematical sciences.

Is the author of over 40 research articles and 10 books on innovative technologies, facial recognition, and programming. Among those – “Java in action. Microsoft Visual J++”, “Horizons of new-century television”, “Modern Video Security Platforms in the Banking Industry”, “Cash Management: History and Horizons”.

In 2005-2007 was invited as the scientific expert to the “Branch Optimizer” project carried out by BS/2 in collaboration with Wincor Nixdorf (Germany). Also took part in several BS/2 projects including “ASOMIS” (Cash Logistics).

9 786099 500768

ISBN 978-609-95007-6-8

2021