SERVICE CATALOGUE

BORICA AD

Last updated on: 01 November, 2025

TABLE OF CONTENTS

1. REGULATED AND PAYMENT SERVICES 5
1.1. BISERA 5
1.2. Online card switching 6
1.3. BORICA payment system 6
1.4. Conversion and redirection of international transactions 7
1.5. SWIFT Service Bureau 7
1.6. Services in connection with The Payment Service Directive PSD2 8
1.6.1. Access to Account Gateway (XS2A Gateway) 8
1.6.2. Consent management 8
1.6.3. Developers help-desk 8
1.6.4. Publishing of additional interfaces (API) 9
1.6.5. Check in the EBA (European Banking Authority) register of providers that offer payment services or electronic money services 9
1.6.6. SmartHUB 9
1.7. MOBILE LOOKUP 10
1.8. Blink Value-Added Partnership Services (blink VAPS) 10
1.8.1. Parking in a zone 10
1.8.2. Paying a fine for improper parking 10
1.8.3. Parking payment 10
1.9. STAND-IN 11
2. CARD SERVICES 12
2.1. ATM 12
2.1.1. ATM management 12
2.1.2. ATM Settings 13
2.1.3. Provision of statistics, data and information 14
2.1.4. Additional ATM services 15
2.1.5. Transactions at ATMs with domestically issued cards 15
2.1.6. Transactions at ATMs with cards issued abroad 17
2.2. POS 17
2.2.1. POS maintenance in BORICA system 17
2.2.2. Initial POS set-up 17
2.2.3. Additional POS services 18
2.2.4. Domestic card transactions on POS 19
2.2.5. Foreign card transactions on POS 19
2.3. Card management 20
2.3.1. Authorization of card payments 20
2.3.2. Card management 21
2.3.3. Additional Card services 22
2.4. Production of cards and PIN 22
2.4.1. Data preparation 22

2.4.2. Personalization of magstripe and embossing 23
2.4.3. EMV personalization 23
2.4.4. Card enveloping delivery to end user 23
2.4.5. PIN printing and/or electronic delivery 24
2.4.6. Express Virtual Card 25
2.5. e-Commerce and mobile services 25
2.5.1. Card management in 3D Secure scheme 25
2.5.2. Digital wallet for issuers 27
2.5.3. Virtual POS servicing in 3D Secure scheme 27
2.5.4. Technical support for virtual merchants 28
2.5.5. Transactions at virtual POS terminals 29
2.5.6. Acceptance of Apple Pay and Google Pay Payments for E-commerce Merchants 30
2.5.7. Electronic notification 30
2.6. Risks management and compliance 31
2.6.1. Anti-fraud Monitoring 31
2.6.2. Contact center services 24/7 32
2.6.3. Chargeback management 32
2.6.4. Risk based authentication 33
2.6.5. ATM certification to card schemes 33
2.6.6. POS certification to card schemes 33
2.6.7. Card products certification to card schemes 34
2.7. Card back-office 34
2.7.1. Card Back Office as a Service - CMSaaS 34
2.7.2. CMS eVouchers - Electronic Voucher Management 35
2.7.3. CMS Closed Loop - Management of cards in a limited network 36
2.8. Loyalty schemes 36
3. Services for Financial Fraud Prevention and Anti-Money Laundering (Anti-Fraud and AML) by BORICA 37
3.1. Consulting Services for Financial Fraud Prevention 37
3.2. Integration and Configuration of a Financial Fraud Prevention System: 37
3.2.1. IBM Safer Payments Integration 38
3.2.2. Rule Configuration 38
3.2.3. Case Management System 38
3.3. Ensuring Protection of All Key Payment Channels 38
3.3.1. Real-time monitoring 38
3.3.2. Preventive Actions 39
3.3.3. Notification Configuration 39
3.4. List Management (Blacklists and whitelists) 39
3.5. Protection Against BIN Attacks 39
3.6. Anti-Money Laundering Prevention Service Package 40
3.6.1. Sanction List Screening 40
3.6.2. Politically Exposed Persons (PEP) Screening 40

3.6.3. Transaction Screening for High-risk Merchants 40
3.7. Trainings and Thematic Workshops 41
3.7.1. Trainings and Thematic Workshops 41
3.7.2. Specialized Sessions 41
4. SOFTWARE PRODUCTS 42
4.1. PGATE 42
4.1.1. BSTAR Client 42
4.2. DISTRAINS 43
4.3. SAFE 43
4.4. SEBRA Client 43
5. INFRASTRUCTURE SERVICES 44
6. TRUST SERVICES 45
6.1. B-Trust 45
6.1.1. Cloud-based Qualified Electronic Signature Certificates 45
6.1.2. Qualified certificates issued on hardware media 45
6.1.3. Qualified certificates for advanced electronic signature 45
6.1.4. Specialized PSD2 certificates for Payment Service Providers 46
6.1.5. (Browser Independent Signing Service) 46
6.1.6. B-Trust Signing Service 46
6.1.7. Platform for remote signing of e-documents with a Cloud-based QES 47
6.1.8. My B-trust Portal 47
6.1.9. PIC portal 48
6.1.10. B-Trust QTSS (Qualified Time Stamp Service) 48
6.1.11. B-Trust e-mail 48
6.1.12. Remote Online Identification 48
6.1.13. Qualified service for electronic identification 48
6.1.14. Remote digital video identification 49
6.1.15. Qualified service for digital registered mail 49
6.1.16. Archiving long-term preservation service (QLTPS) 49
6.1.17 Qualified validation of electronically signed documents (QSVS) 49
6.1.18 Cards and Readers 49
6.1.19 Technical assistance for the installation of B-Trust products 49
6.2 B-Token 49
7 FINTECH SERVICES 50
7.1 E-faktura 50
7.2 InfoPay 52
7.3 InfoPay Checkout 53
7.4 INFOBANK 2 54

1. REGULATED AND PAYMENT SERVICES

1.1. BISERA

BISERA is a payment system for servicing client transfers in EUR, based on the rules, practices and standards of the Single Euro Payments Area (SEPA), and providing finality of the settlement in the Trans-European Automated Real-time Gross Settlement Express Transfer TARGET.

Description

BISERA is a payment system with finality of settlement for servicing client transfer orders in EUR and a SEPA compatible clearing house, according to the classification of the European Payments Council.

BISERA processes transfer orders in EUR between participants, payment service providers (PSPs) with access to the system and payment service providers, executed internally or through interconnections with other SEPA compatible clearing houses. The limit of transfer orders processed by BISERA is in accordance with the SEPA schemes of the European Payments Council.

BISERA implements settlement procedure B (simultaneous and multilateral settlement) in TARGET for SEPA payments in euro from/to interoperable clearing houses and settlement procedure D with the use of pre-funding for the prepaid settlement model of domestic payments and payments through STEP2.

To ensure the accessibility of the participants to BISERA, BORICA AD provides a connection of BISERA with other SEPA compatible clearing houses by concluding bilateral agreements. Such agreements have been signed with the German Deutsche Bundesbank and the Dutch German clearing house equensWorldline. BISERA provides full reachability for SEPA credit transfers through access to the STEP2 system of EBA Clearing, with the direct participation of the Bulgarian National Bank. Full reachability for SEPA instant credit transfers is provided through the TIPS (TARGET Instant Payment Settlement) system.

Participants in BISERA can be: the Bulgarian National Bank; National central banks (NCBs) of the EEA; A bank licensed in Bulgaria to conduct banking services; a Bank branch from a third country with a licence, issued by the BNB under the provisions of Art. 17 of the Law on Credit Institutions; a Bank branch of a Member State, operating on the territory of the Republic of Bulgaria under the provisions of Art. 20 and 21 of the Law on Credit Institutions; Banks or branches of foreign banks established on the territory of the EEA, Payment and electronic money institutions licensed by the BNB; Other payment service providers licensed in Member States

Services

- SEPA credit transfers (SCT),
- SEPA instant credit transfers (SCT Inst),
- Generating and sending information in the form of various types of reports.

Type of agreement

A Framework Service Agreement of BORICA AD, compliant with the Rules of the BISERA payment system, which applies to all payment system participants and PSPs with the right of autonomous access. Appendices to it are: Rules of the system and Tariff.

Pricing

The services are paid on the basis of the applicable BORICA AD Tariff.

1.2. Online card switching

BORICA AD, as an operator of a payment system for payment transactions, associated with cards, provides switch of interbank payments with payment cards in the country. For this purpose, online interface connections of the type host-to-host are built and maintained with banks and payment institutions with separate authorization centers.

Switch processing includes:

- Registration and redirection of the transaction;
- Generation and sending the output data for the result of the transaction.

Host to host connections

The connection between the BORICA authorization system and other systems shall be established after negotiation of the type and parameters of the connection that will be carried out.

Type of agreement
A Standard contract for all participants in the BORICA payment system, with annexes: System Rules and Tariff.

Pricing
The services are paid on the basis of the applicable BORICA AD Tariff.

1.3. BORICA payment system

BORICA is a payment system with settlement finality, which processes payment transactions associated with cards, and makes a net settlement at a particular time in RINGS.

Description
The Rules of Operation of the system have been developed in accordance with the requirements of the Law on Payment Services and Payment Systems. The settlement agent of BORICA is the Bulgarian National Bank. Settlement of interbank payments with payment cards on the territory of the country is made through the BORICA payment system.
Services
Settlement via RINGS of interbank financial transaction – transaction processing includes:

- Processing of the received information for executed interbank transactions;
- Charging interbank fees for the executed operations;
- Recalculating on a multilateral basis the mutual obligations of bank;
- Preparation of the request for settlement based on the recalculated net positions of the participants;
- Sending the request for settlement to RINGS;
- Receiving the result from RINGS;
- Providing the result from RINGS to the banks.

Type of agreement

A Standard contract for all participants in the BORICA payment system, with annexes: System Rules and Tariff.
Pricing
The services are paid on the basis of the applicable BORICA AD Tariff.

1.4. Conversion and redirection of international transactions

The conversion and redirection of international transactions service is related to the authorization protocols conversion (ISO8583) and redirection of authorization requests or transactions to/from international card schemes – ICS (VISA, MC) from/to the relevant financial institution, acquiring or issuing payment cards.

The service is applicable to institutions with their own systems, connected to the relevant ICS via H2H interface connection with BORICA.

1.5. SWIFT Service Bureau

SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a cooperative society owned by its members that provides the financial world with a fast, safe and confidential way to conduct business operations. BORICA AD is registered under the Shared Infrastructure Program of SWIFT as a Service Bureau and is certified according to the requirements for Standard Operational Practice level. The main services it provides to its clients are indirect connection to SWIFTNet (Shared Connection) and full outsourcing of SWIFT infrastructure (Shared Infrastructure).

Description

- The Shared Connection service is designed for clients, having their own platform for processing SWIFT messages (e.g. Alliance Access/Entry). By the use of Service Bureau they can use third-party SWIFTNet services such as Information and Control Module (ICM) of TARGET2 and the EBA STEP2 Browse Service of EBA Clearing. The Service Bureau, in its capacity of an administrating institution (Shared Security Officers), could also manage the SWIFTNet PKI client security.
- By the use of the Shared Infrastructure service, clients are provided with a platform for complete processing (creation, verification, authorization, sending, receiving) of all kinds of SWIFT messages. Since for this service all software and hardware components are installed and administered by the Service Bureau, clients don't have to build, maintain and administer their own SWIFT infrastructure.
- SWIFT Service Bureau guarantees safety, reliability and quality to its clients.
- Safety is ensured by the architecture of the Service Bureau and the used technological solutions. Maximum reliability is achieved through reservation of all elements of the infrastructure. The Service Bureau services are available 24/7 and their quality is guaranteed by the Service Level Agreement (SLA), negotiated between the Service Bureau and the client.

Type of agreement

For the use of SWIFT Service Bureau agreements are concluded as follows:

- Access to SWIFT Net (Shared Connection): Agreement with annexes to it;
- Use of SWIFT Net services through Alliance Access (Shared Infrastructure) – Agreement with annexes to it;
- Agreement for the use of SWIFTNet services through the SWIFT infrastructure of the Service Bureau;
- Contracts have SLA annex – "Service Level Agreement".

Pricing

Services are paid based on the applicable BORICA AD Tariff.

1.6. Services in connection with The Payment Service Directive PSD2

1.6.1. Access to Account Gateway (XS2A Gateway)

A Service directed to banks' obligations as Account Servicing Payment Service Providers (ASPSP) in compliance with Directive (EU) 2015/2366 (PSD2).

Description

The Service is based on the National technical standard BISTRA (Bank Interfaces for Standardized Payments) and is compliant to the Law on Payment Services and Payment Systems (LPSPS) and Directive (EU) 2015/2366 (PSD2). The Service scope includes:

- Publishing of application programming interfaces (API) according to BISTRA;
- Main functionalities – "Account Information Service", "Payment Initiation Service" and "Confirmation on the Availability of Funds Service";
- PSP validation (certificate validity, PSP register);
- Administrative portal for monitoring and reports;
- Developer portal, including documentation and test environment (sandbox).

For APIs' publishing are used IBM products – IBM API Connect and IBM Data Power – leading world class provider of similar technologies.

Developer portal is branded with the logo, colors and fonts of the Bank.

1.6.2. Consent management

The Service gives the possibility for storing and managing consents of the Payment Service Users (PSU) which they provide to the Account Servicing Payment Service Provider (ASPSP) according to Directive (EU) 2015/2366 (PSD2).

Description

The Service scope includes:

- Register storing the consents;
- Interfaces (API) for managing consents (including creation, reading, updating and deleting operations);
- Portal to access and manage the consents by authorized users;
- Client portal where Payment Service Users (PSU) can revise and manage their consents. The portal may be branded with the logo, colors and fonts of the Bank.

The Service allows obtaining status and details for the consents, which gives a possibility the register to be synchronized with other registers, used by the Bank.

1.6.3. Developers help-desk

The Service provides possibility to the developers of the Third Party Providers (TPP) to receive assistance in case of difficulties with the integration between their applications and the published by the service "Access to Account Gateway (XS2A Gateway)" interfaces (API).

Description

Developers of the Third Party Providers (TPP) may receive assistance in any moment by competent and experienced employees for:

- Questions about documentation of the published APIs;

- Problems upon searching published APIs;
- Other integration related questions.

Developers register their problem via electronic form available on the Developers' portal. Communication is in English or Bulgarian language.

1.6.4. Publishing of additional interfaces (API)

The Service provides possibility for additional interfaces publishing (API) in addition to the already published in compliance with BISTRA. These interfaces (APIs) are published on the platform on which the service "Access to Account Gateway (XS2A Gateway)" is built, using the advantages of the platform – security, reliability, efficiency and scalability.

Description

A Bank using the service "Access to Account Gateway (XS2A Gateway)" can publish additional interfaces (API) out of the scope of Directive (EU) 2015/2366 (PSD2). All additional interfaces that the Bank is willing to publish, shall be published by the Provider.

Check in the EBA Register of Payment and Electronic Money Institutions

The service allows for checking in the EBA Register of Payment and Electronic Money Institutions.

1.6.5. Check in the EBA (European Banking Authority) register of providers that offer payment services or electronic money services

The service provides the possibility to check the EBA register of providers that offer payment services or electronic money services within the European Union (EU) and the European Economic Area (EEA).

1.6.6. SmartHUB

Service aimed at banks, willing to take advantage of the business opportunities, provided by Directive (EU) 2015/2366 (PSD2). As Third Party Providers (TPP), the participants in the Hub can service clients of other Account Servicing Payment Service Providers (ASPSP).

Description

The service is based on the National technical standard BISTRA (Bank Interfaces for Standardized Payments) and is compliant to the Law on Payment Services and Payment Systems (LPSPS) and Directive (EU) 2015/2366 (PSD2).

The service scope includes:

- Account information;
- Payment initiation.

The Hub enables its customers, through a single integration, to build a connection with plenty of Account Servicing Payment Service Providers (ASPSP). The hub aims at implementing all the specifics in the interfaces of the Account Servicing Payment Service Providers (ASPSP), as well as to provide the subsequent support of its integration with them, thus facilitating its customers to a great extent.

The Hub is integrated with all Account Servicing Payment Service Providers (ASPSP) on the territory of Bulgaria that have published specialized interface to access their customers' accounts as required by the PSD2. Upon customer's request, the hub may be integrated with other banks outside the territory of Bulgaria.

The communication between the Hub and its customers can be both synchronous and asynchronous and is carried out through the already established internal network between the parties.

1.7. MOBILE LOOKUP

The Mobile Lookup service is intended for payment service providers, current and future customers of BORICA AD, and allows for the execution of instant payments in BGN using only the mobile number or another recipient's IBAN identifier.

Mobile Lookup supports a centralized database of mobile number and payment account matches and provides a service that responds to incoming lookup requests, enabling payment initiation. In addition to retrieving the necessary P2P payment data, the service will offer to end users served by PSPs the ability to check which of their existing personal phone contacts are also participating in the payment (proxy) network.

1.8. Blink Value-Added Partnership Services (blink VAPS)

Blink VAPS provides a solution designed for Payment Services Providers (PSP) - participants in the National Card and Payment Scheme (NCPS) that they can integrate with their mobile applications and through which to enable their customers to request services and pay for them with blink instant payment. Blink Value-Added Partenrship Services are mediated by NCPS and, in addition to their speed of payment (instant credit transfer under NCPS "blink" brand), bring additional value to PSPs and their end customers by creating new ordering and interaction channels. Blink VAPS are made possible by the provision of centralised services by NCPS, acting as an intermediary in ordering and payment processes, and by building centralised partnerships with established market segment-specific service providers and/or multi-vendor service aggregators.

For the purposes of blink Value-Added Partenrship Services, a blink API Gateway has been developed to enable communication between parties that do not have a direct connection to each other - such as the PSP of the customer requesting the services (the Originator) and the Provider of the respective services. Blink API Gateway is the only sufficient point to connect the Originator's PSP with the Service Provider and vice versa. The following ancillary services are also developed:

- User interface for monitoring the placed service orders and the corresponding payments.
- API for creating and managing lists of customer vehicle profiles with the respective brand and logo.

1.8.1. Parking in a zone

Paid parking of a car or other vehicle in an area controlled by a municipal entity or structure in a populated place. This centralised service provides an API with a list of zones for which NCPS or an integrated Aggregator has a distribution contract, as well as the possibility to submit a parking request, extend a stay and geolocation check whether a vehicle is within a paid parking zone.

1.8.2. Paying a fine for improper parking

The centralised service provides an API to check for fines imposed for an improper use of a "parking in a zone" service, with the subsequent possibility to make a payment to release the impounded car.

1.8.3. Parking payment

Paid parking of a car in an area subject to access control through a checkpoint. This centralised service provides an API for a list of parking lots with which NCPS or an integrated Aggregator has a distribution contract, a geolocation check in which private car park the customer is located, a check of parking obligations in a private parking lot by vehicle registration number or parking ticket number, with a subsequent option for payment.

1.9. STAND-IN

The Stand-In is a service of BORICA AD, targeting payment service providers (PSP), who are unable to meet the requirements for the processing of Instant payments in BGN at any time of the day, 365 days a year. This service ensures the continuity of the processing of instant transfers, when the main (core) bank information system of the respective participant or PSPs with rights of access to BISERA6 is not available.

The Stand-in service is integrated on the one hand with the central payment infrastructure of BISERA6, and on the other, with the core banking system. It stores information on payment accounts, their limits and balances, with provided mechanisms for synchronization with the core banking system (online and in batch mode).

2. CARD SERVICES

The card services provided by BORICA AD are divided into online and Back office services.

Online services: Acceptance; Secure payments (3D Secure) in the Acceptance section; Authorization; Secure payments (3D Secure) in the Authentication section; Anti-Fraud monitoring (EMS); Blocking cards; PIN via SMS; Loyalty programs; Authentication module Sucard ATX (SaaS).

Back office services: ATM and POS servicing; Card management; Card personalization; PIN printing; Management system for disputed transactions; Card Back-office.

Type of agreement:

For all card services "Standard agreement for acceptance for all participants in BORICA payment system" is concluded, with annexes System Rules and Tariff, unless the description of the service specifies otherwise.

Pricing

Card services are paid on the basis of the applicable BORICA AD Tariff, unless the description of the service specifies otherwise.

2.1. ATM

Description

For their customers who manage and support ATM networks, BORICA AD provides connectivity to functional and operational environments, operational and monitoring systems, as well as additional resources and equipment requisite for ATM devices to function properly. BORICA supports the two widest-spread ATM application-transaction protocols – NDC and DDC, which facilitates the registration of all ATM models available on the market into its system.

At present, BORICA operates and supports two authorization systems for ATM management – Tandem and Way4. Before the transition process to managing all ATMs in an Way4 environment is finalized, BORICA will continue to maintain its “old” authorization system, Tandem (until July 2022).

New ATM registrations into the Tandem system are allowed only by exception, and in such cases the installation preparation process for ATM terminals is carried out in specialized BORICA facilities.

2.1.1. ATM management

Services

- ATM management and support in Tandem – for ATMs registered in the Tandem system, BORICA makes available a financial application, by which interoperability with the authorization system is provided. The ATM application is developed and supported by BORICA. Operations that can be performed include financial and nonfinancial operations, payment of bills to merchants, sending and receiving of funds ordered for payment, etc. BORICA provides connectivity both to all national

issuers of electronic payment instruments, and to international card schemes (VISA, MasterCard and Amex), thus also ensuring cross-border transaction traffic.

Two types of communication connectivity of ATMs are possible:

- via the bank's VPN;
- directly via the VPN of BORICA.

- Management and support of ATMs in Way4 – BORICA provides to the devices registered in Way4 the full package of communication and functional characteristics provided by Tandem. With a view to improving the methods of ATM management and support, the financial application, used locally on the ATMs for their management in Tandem, is removed and they are managed centrally by the authorisation system. Charging of registered ATMs in Way4 is determined depending on the selected service package and the functionalities provided through ProView/VynamicView:

ProView/VynamicView main package – provides an opportunity by a web version of the system for:

- Monitoring the overall condition of the ATM, and of individual modules and components;
- OS - SW patch update;
- Detailed status of cash availability by denomination and cassette;
- Performance of remote commands to the ATMs – performance can follow a schedule preset by the users;
- Possibility for in-depth and detailed definition of different levels of access and monitoring, both by the bank's staff, and by external organisations servicing the ATM network;
- Automation of processes based on a sequence of events;
- Standard reports of the performance and cash status of the ATM network;
- Providing access rights to external ATM maintenance organisations.

ProView/VynamicView full extended package – includes everything provided in the basic package plus:

- Receiving personalised reports according to a preset schedule.
  - ATM statuses – including technical condition;
  - financial position by cassette and denomination (referring to Cash out ATMs);
  - reports of incidents that occurred on the individual ATM level;
  - performance statistics of the ATM network;
- Access to electronic transaction logbooks stored on a server at BORICA, providing detailed information of the status and stages of development of an ATM operation – information used by FIs for protection in case of disputed customer transactions. The information is stored on servers at BORICA, rather than locally on the ATMs, which allows for access for a longer period of time.
- Access to photo recordings made by ATM cameras (where such are installed and operating);
- Distribution of files to the ATM network – promotional video clips, etc.;
- Receipt by e-mail of incident notifications;
- Inventory information of the hardware components and software applications.

2.1.2. ATM Settings

In exceptional cases, where an ATM is registered for operation in the Tandem system, preparations for installation of the device are done at specialised BORICA premises, and include VPN configuration, software uploading, parameter configuration, cryptographic keys on a keyboard and HSM (Hardware

Security Module), preparation of an encryption security module, and checking the proper operation of the device with BORICA's authorisation system - Tandem.

For all ATMs managed in Way4, for optimization of time, finances and operations, BORICA has provided an ATM preparation process in specialised rooms at the servicing organisations providing ATMs to end customers.

Upon request by the servicing bank, by means of a remote uploading system BORICA provides the distribution in the ATM networks of promotional video clips and other types of messages.

Services
ATMs managed by the Tandem authorisation system:

- initial communication configuration of the VPN connection of the ATM to BORICA;
- remote uploading of a promotional video clip via the system for file distribution on ATMs.
- generation and uploading of keys for the HSM and the EPP (Encrypting Pin Pad) – encrypting keyboards for ATMs.

ATM managed by the Way4 authorisation system:

- configuration of data and parameters for ATMs in the authorisation and in the back office systems;
- registration of ATMs in the monitoring and management system (ATM Monitoring and Management ProView/VynamicView);
- configuration of user access levels and monitoring and management rights in ProView/VynamicView for the staff of the financial institution, and of external servicing organisations – upon the financial institution's request to be provided that service;
- processing and digital transfer of data for ATM installation to the service organisation responsible for the physical installation – by rights of access, specially provided to the respective organisation, to a system where incoming requests for ATM installation are registered;1
- generation by the HSM and initial uploading of cryptographic keys for EPP
  - manual uploading by BORICA information security officers
  - remote uploading via the Remote Key Loading system

2.1.3. Provision of statistics, data and information

BORICA provides various types of statistics and transaction logbooks of ATMs operating within the Tandem authorisation system. Where assistance is needed, the Company provides expert assistance for analysis of the financial status of ATMs.

Services in the Tandem authorisation system:

- provision of statistics of the condition of a terminal;
- subscription for summary monthly statistics;
- provision of an ATM logbook;
- analysis in case of lack of financial reconciliation of an ATM.

Services in the Way4 authorisation system:

For ATMs registered in the Way4 system, financial institutions can receive reference information via the ATM monitoring and management system - ProView/VynamicView. The variety of statistics and data is shown in item 2.1.1 above.

In addition to the above listed ones, the system allows for generation of individual reports, which are subject to additional definition and assessment with the customers.

2.1.4. Additional ATM services

BORICA conducts specialised training in working with ATMs for cashiers. Participants in the training can be employees of the banks, and of the companies servicing their ATMs. Training includes theoretical and practical sessions for all models supported by the Company. They cover a syllabus of subjects and questions relevant to ATMs connected to one of the two authorisation systems supported – Tandem or Way4. After the training the employees have the required knowledge and skills for the proper servicing of ATMs.

To ease the process of migration of ATMs to the Way4 authorisation system, and for better knowledge of the specifics of servicing terminals in the new authorisation environment, BORICA organises training courses for employees who have been already trained for work with ATMs. For its customers' added convenience, BORICA training lecturers can conduct courses at locations designated by the customers. The training locations should meet the relevant requirements for conducting such training. Again, to make things easier for customers and their employees facing difficulties to attend BORICA's weekday training courses, the Company organises such on Saturdays – according to a schedule agreed in advance with the customer. In addition to training courses with physical attendance, BORICA prepares and provides video instructions for work with ATMs in Way4.

BORICA provides to banks, whose ATMs are connected to Tandem, an online system (SAM) for monitoring the cash availability and technical condition of the ATMs. The system provides optionally an additional functionality for transmission of financial data to the bank and their processing by the cash management systems.

BORICA provides assistance to customers by conducting certification tests of various software applications and programmes – operational and application ATM software – for their interoperability with the authorisation systems.

Services

- Training of operators to service ATMs;
  - training of operators to service ATMs – participation in a 4-day course in groups of 6 to 12 trainees;
  - one-day training for servicing ATMs – applicable to up to 10 trainees from one financial institution;
  - one-day remote training course in Way4 for cashiers, at a location chosen by the customer - applicable to up to 10 trainees from one financial institution;
  - one-day Saturday training course in Way4 for cashiers who have attended a previous BORICA training course;
- Information of the technical condition and cash availability of ATMs;
- Assistance for certification of BNA terminals.
- BORICA is providing access to test environment and test transaction logs during ATM certification process with International Card Organizations
- BORICA is delivering certification cards and specialized certification tool for a period of 5 working days during ATM certifications process with International Card Organizations.

2.1.5. Transactions at ATMs with domestically issued cards

BORICA's authorisation and Switch systems guarantee acceptance of all payment cards issued in Bulgaria at all ATM terminals included in the system. Transactions can be:

- Financial:

From participants' point of view, they fall into:

'On-Us' pure – transactions executed with an electronic payment instrument at an ATM – both managed by the same financial institution

- cash withdrawal
- cash deposit – the service is presently applicable only to 'On-Us' transactions pure.

'On-Us' for BORICA – a transaction executed with an electronic payment instrument at an ATM – issued and supported by **different** financial institutions, but **both are serviced** by the BORICA systems.

- cash withdrawal

'Off-Us' financial transactions – with a payment instrument issued by an external for BORICA financial institution, at an ATM included in the BORICA system. Transactions of this type are processed and transmitted between the participants via the Transaction Switch system.

- cash withdrawal
- reversal – technical

- Nonfinancial:

These services are applicable to all participants supporting the relevant services for the payment instruments issued by them.

- statement of card balance;
- statement of the latest five transactions;
- PIN change.

- Other transactions:
  - The Interbank ATM deposit service provides to the cardholders of one Financial institution a possibility to perform deposit transaction on their card by using an ATM of another Financial institution. Prerequisite for successful service is both Financial institutions to be registered for the service in BORICA.

Service specifications:

The process for performing deposit transaction on ATM serviced by institution different than the card issuer the following:

- The cardholder chooses an ATM of Institution (X) different than the institution (Y) which issued his card and is registered in the interbank deposit scheme;
- The cardholder inserts his card in the ATM and chooses "deposit" transaction. After that the ATM send to the Host a card verification message, based on which the card and the cardholder PIN are checked;
- If the verification is successful, the ATM opens the shutter for cash deposit and the cardholder inserts the amount desired;
- After the transaction is completed the ATM prints a receipt with the amount deposited.

Benefits:

- Increased cardholder possibilities for performing deposits on their cards;
- Expansion of the deposit ATM network.

Prerequisites for using the service:

- Intend for service inclusion from the Financial institution – acquiring ATM deposits and/or issuing payment cards;
- Performing UAT with the respective institution.

2.1.6. Transactions at ATMs with cards issued abroad

For transactions with electronic payment instruments issued outside Bulgaria, the BORICA systems provide routing of authorisation enquiries from ATMs to the international card schemes MasterCard, VISA, AMEX, Diners Club, Discover.

Supported types of transactions:

Financial transactions:

- cash withdrawal at ATM terminals;
- cash withdrawal at ATMs with dynamic currency conversion (DCC)*;
- reversals of the above transactions.

Nonfinancial transactions:

- statement of the funds available at the ATM;
- change of payment card PIN

Other transactions:

- rejected (unsuccessful) authorisations at ATMs;

* Cash withdrawal at ATMs with dynamic currency conversion (DCC) – a service in which the cardholder has an option to choose if the executed transaction should be converted into the original currency of the card used. In a transaction of this type, the amount in the original currency, with which the customer's account will be debited, is seen on the ATM screen. The exchange rate of the transaction is set by the financial institution operating the ATM. Through its systems BORICA provides an opportunity to include up to 10 currency options for the service.

2.2. POS

2.2.1. POS maintenance in BORICA system

Services

- Close inactive POS;
- Change a specific parameter of POS device.

2.2.2. Initial POS set-up

BORICA AD prepares POS terminals for installation. The preparation involves uploading the necessary software and parameters in the POS terminal, its registration in the authorization system and performing operations to verify the correct operation of the terminal in BORICA system.

The service "Startup of POS with basic parameters" is provided, which includes loading application, initial parameters of the merchant, TID, keys and registration in TMS and the authorization system, on the grounds of a standard (basic) request submitted by the bank.

BORICA AD also performs initialization of POS terminals after repair or replacement of POS terminals.

Upon activation of POS, the terminal is loaded with the specific parameters of the merchant and the location, which is serviced by the POS terminal. They replace the parameters of the initial merchant in the systems.

Upon deactivation, the parameters of the POS terminal return to the basic state with formal data. The terminal keeps TID, and upon request for activation it can be installed with another merchant, without being physically returned to BORICA AD.

System for registration of requests for terminals (TermReq)

Requests for installation of ATM and POS terminals, POS startup with basic parameters, POS activation and deactivation, as well as changes to individual parameters of POS terminals are submitted by banks and payment institutions through the system TermReq, operated by BORICA AD.

Benefits
The services related to the initialization of POS terminals, as well as the possibility for startup with basic parameters, and subsequent activation and deactivation of POS, as well as change to its parameters, allow banks and payment institutions an easy and flexible management of the network of POS terminals and merchants they service, without requiring the terminals to be taken to BORICA AD for service upon any change.

2.2.3. Additional POS services

Services

- Initial POS certification;
- Testing a new version of the POS software;
- Testing a new POS model;
- Technical services at POS;
- BORICA is providing access to test environment and test transaction logs during POS certification process with International Card Organizations
- BORICA is delivering certification cards and specialized certification tool for a period of 5 working days during POS certifications process with International Card Organizations.
- Test POS device preparation – BORICA AD provides the service of test TID creation, SW loading, parameters and key settings of POS in test environment upon a client's request;
- POS outsourcing - BORICA AD provides its own fully functioning POS devices to the end-customers (merchants) on behalf of their Payment Service Provider (PSP);
- Software POS - BORICA offers its clients Software POS application, which allows acceptance of payments through NFC on Android based devices, including smartphones and tablets. The software provides the functionality of a physical POS terminal and allows contactless payments acceptance, including mobile devices which are digitizing cards, including wearables, smartphones and tablets.

The software POS solution could be implemented in several ways:

- White label – mobile application for contactless payments acceptance branded with the logo and colors of the financial institution.
- Software Development Kit (SDK), which allows integration with existing mibile app of the financial institution. The SDK provides a set of tools, libraries, documentation, code samples, processes and manuals allowing the institution to integrate the functionality for contactless payments acceptance in their own Android based mobile applications..

- bPOS - mobile application for contactless payments acceptance, cobranded with BORICA and the financial institution that provides the service.

- Payment Facilitator - the service provides to financial institutions the technical possibility for servicing payments through their physical and virtual POS terminals as an indirect member (Payment Facilitator) by using the infrastructure and the IPS registration of another (direct) member;
- Device Host to Host – Implementation and support of online connection for authorizations by the acquiring institution. The Device Host to Host (DH2H) service ensures the possibility for connecting the system of the institution which is handling POS devices as a front-end (including physical connectivity, application software, parametrization, key management , monitoring etc.) to BORICA's authorization system, which is servicing the institution's POS devices as back-end (including authorizations, transaction processing, merchant payments, commissions and fees, clearing and settlement, reporting etc.).

2.2.4. Domestic card transactions on POS

The BORICA card system provides for acquiring payment cards at POS terminals which are part of the system.

Description

BORICA card system provides acquiring of all payment cards, issued on the territory of the country, at all POS terminals, included in the system. BORICA card system provides routing of authorizations with foreign cards to international card schemes MasterCard, VISA, AMEX, Diners Club, Discover.

Services

The service "Interbank financial transactions and On-US transactions at POS with cards outside the BORICA system" includes the following transaction types:

- Transactions performed at POS, serviced by one PSP* by cards, issued by another PSP;
- Transactions performed at POS of one PSP, connected to the BORICA system by cards, issued by the same PSP that are not registered in the BORICA system;

The service "On-Us transactions Acquiring at POS (card and terminal of the same bank in the BORICA system)" includes only the transactions, where at a POS of the same PSP, connected to the BORICA system, is accepted a card issued by a the same PSP and registered in the BORICA system.

Financial transactions at POS include:

- Payment of goods and services and cash withdrawal via POS terminals;
- Reversals of the above-mentioned transactions.

Non-financial transactions at POS include:

- Check available balance at POS;
- Check last 5 transactions at POS;
- Other transactions include:
- Rejected (unsuccessful) authorizations at POS;
- Re-authorizations.

2.2.5. Foreign card transactions on POS

Financial transactions at POS include:

- Payment of goods and services and cash withdrawal via POS terminals;
- Offline transactions;
- Reversals of the above-mentioned transactions.

Other transactions include:

- Rejected (unsuccessful) authorizations at POS;
- Re-authorizations.

2.3. Card management

2.3.1. Authorization of card payments

BORICA AD provides banks and payment institutions, issuing cards through the BORICA system, with authorization of requests for transactions, made with their cards on physical and virtual ATMs and POS in the country and abroad.

Description

The authorization of each transaction request, made with a payment card on physical and virtual terminals in the country and abroad, is performed by verification of a number of parameters:

- Validity of the card (card number, expiration date);
- Account balance or card credit limit;
- Card limits (daily, weekly, etc.);
- Security codes CVC/CVV, EMV parameters;
- PIN (if required);
- Card status (active, blocked);
- Other parameters (permitted operations, cryptograms, etc.).

Services

The service "Interbank financial transactions and On-US transactions from terminals outside the BORICA system" includes the following transaction types:

- Transactions executed with cards, issued by one Payment Service Provider (PSP), to terminal devices of another PSPs;
- Transactions executed with cards issued by one PSP and registered in the BORICA system at terminal devices of the same PSP that are not connected to the BORICA system;The service "On-Us transactions Issuing (card and terminal of the same bank in the BORICA system)" includes only card transactions, issued by a single PSP and registered in the BORICA system on a terminal device of the same PSP connected to the BORICA system.

Financial transactions include:

- Cash withdrawal and/or cash deposit via ATM terminal;
- Payment of goods and services and cash withdrawal via POS terminals;
- Transfer between payment accounts via ATM terminals;
- Payment of services via ATM terminals;
- Reversals of the above-mentioned transactions.

Non-financial transactions include:

- Check available balance;
- Check last 5 transactions;

- Change payment card PIN code with or without card activation.

Other transactions include:

- Rejected (unsuccessful) authorizations;
- Re-authorizations.

The service “Card activation after PIN change” – provides additional level of security for cardholders, enabling them to activate a new or reissued card by themselves by changing PIN code at an ATM.

BORICA AD provides the possibility for the so-called authorization at the issuer, where the check of the account balance is carried out at the bank through an established online connection. Thus, the cardholder may use the entire balance on their card account at any time.

Another possibility for maintenance of a current card account balance is by establishing an online connection, whereby the bank promptly updates any change in the account balance in the BORICA system, and can make checks for completed transactions, in order to maintain up-to-date balance in its own system, as well.

Benefits

The authorization of each payment ensures a high level of security of the transaction, which protects the cardholder from fraud. Using the interface for authorization by the issuer, the cardholder can, at any time, use the entire balance on their card account.

2.3.2. Card management

BORICA AD enables banks and payment institutions, issuing cards through the BORICA system, to manage the status, account balance, limits, Internet transactions and other parameters of the cards serviced by them.

Description

Support of management (change) of the following parameters of the payment cards, registered in BORICA system, which are used in the payment authorization process:

- Card status (active, blocked, deactivated);
- Account balance or card credit limit;
- Card limits (daily, weekly, etc.);
- Transactions management on the Internet;
- Other parameters (permitted operations, etc.);
- Push notifications provide the ability to send a notification to the issuer via an electronic channel for various types of card events, and Pull notifications allow the issuer to retrieve card information via an electronic channel.

Services

The service "card management in the BORICA system, providing opportunity for transactions management on the Internet" is related to raising a special flag for cards in the STEPS system, which prohibits Internet transactions or taking down, allowing cards for the same transactions. The flag can be managed either manually by the bank employees operating with the system, or automatically by submitting a file to BORICA for a large number of cards. Banks submit to BORICA a written request for the BIN numbers to be registered for the service, where the registration and the pricing shall be made for all active cards in the requested BINs.

The standard way to change the card parameters, which BORICA AD provides for banks and payment institutions, is through a file transfer along specified interfaces. For this purpose, a system for file sharing is maintained, including the option for automatic transfer. Client applications are provided, which allow secure transfer of files.

Besides file transfer, BORICA AD provides online tools for a change to the card status (blocking and unblocking) and change to the balance through remote access to the authorization system and online interface.

BORICA AD provides an electronic channel that the issuer may use to retrieve various card information that is agreed in advance with the issuer (pull notification). Objects of the service are all payment cards that are supported in the BORICA Tandem authorization system.

The main data the issuer receives may be:

- pending successful and all failed authorizations with the card for a certain period;
- card status;
- current card balance/fund availability;
- card limits.

BORICA AD provides the possibility to send a notification to the issuer via an electronic channel (push notification) upon the occurrence of various card events that are agreed in advance with the issuer. Objects of the service are all payment cards that are supported in the BORICA Tandem authorization system.

The main events of which the publisher is notified may be:

- upon successful and unsuccessful authorization with a card that is approved by the BORICA Tandem system;
- in case of a card status change.

Benefits

The management of the cards registered in BORICA system allows you to change the status and to set parameters (limits, availability, etc.) at card level, which will subsequently be used for authorization of executed payments. Obtaining card information via an electronic channel (push and pull notifications) is a prerequisite for improving the process of servicing cardholders.

2.3.3. Additional Card services

Services

- Establishing a connection for on-line authorization with the card issuer;
- Automatic file transfer for back office;
- Generation and loading a key in HSM;
- Keys export for Visa and MasterCard;
- DIGIPASS GO1 device;
- Training for operation with systems servicing card services;
- Developing software for card services.

2.4. Production of cards and PIN

2.4.1. Data preparation

The “Data preparation” service covers the data processing on previously set parameters, required for the creation (production) of the card, via the following technologies:

- „Card personalization via indenting/ emobossing“
- „Card personalization via flat printing“
- „Card personalization via laser engraving“

2.4.2. Personalization of magstripe and embossing

BORICA AD offers a full set of services for personalization of payment cards, including the preparation of data for personalization of magnetic stripe and chip, computing of classified data and physical personalization of payment cards.

Description

BORICA AD is a processor certified by VISA and MasterCard for personalization of all their card products. We provide personalization of both magnetic and chip cards, compliant with EMV standard. The chip cards may have two interfaces (contact and contactless), providing contactless payments in accordance with the PayPass specifications of MasterCard and PayWave of VISA.

Profiling and card personalization via Entrust Datacard “Durable Graphics ®” technology and laser engraving technology:

- Profile preparation and setting for card personalization via the technologies "Durable Graphics ®" and laser engraving, according to the Issuer’s requirements and the requirements of the card schemes - one-time setting of a profile indicating the physical positions of the card requisites (name, account number, good thru date, vector logo, etc.).
- One-sided or two-sided personalization of cards, using Entrust Datacard “Durable Graphics ®” technology or laser engraving technology

Both technologies allow usage of one personalization profile for multiple Issuer’s products, unless they do not require re-positioning of the card requisites.

Benefits

- Increased efficiency and long-lasting personalization
- UV-curable technology
- Choice of 4 colors – white, black, metallic gold and metallic silver (one per side)
- Visa Quick Read Printing
- Flat surface keeps the card thickness and prevents from antenna damages

2.4.3. EMV personalization

BORICA AD provides EMV cards personalization under several technologies: PRISMA, IDEMIA, Austria card, Thales (Gemalto), Plastic Card, EASTCOMPEACE.

2.4.4. Card enveloping delivery to end user

In order to address and send individual letters and personalized cards by post to each recipient in an easy, fast and secure way, BORICA AD provides automated envelop handling of personalized cards. The personalized card is attached to a letter submitted by the issuer, followed by monitoring of compliance with the individual client data printed in the letter. The letter is folded and put automatically in an envelope with a window for the address and other visible individual data; additional materials can also be put in the envelope, in compliance with certain conditions. The prepared envelope is sealed and ready to be sent to the address specified by the issuing bank.

Under the “Sorting and packing cards as per points of delivery” service the cards and PIN codes shall be sorted and packed with a delivery protocol in compliance with the point of delivery nomenclature.

BORICA AD offers print design on each individual card – it could be created by the cardholders themselves, or selected from a pre-designed gallery of images.

The service "Generation and printing of additional attributes on a cover letter" allows adding a barcode or QR code, which optimizes the subsequent process of cards' sorting and distribution to the cardholders. The additional attributes are printed at the address field of the cards' cover letters and their size should be in accordance with the size of the envelope's window.

Description:
The service allows issuers to request personalization and PIN printing of a card with an electronic PIN code, which can be delivered to the cardholder's address by courier.

- For this purpose, the Issuer's card management system submits to BORICA requests for card personalization and generation of PIN codes (ePin), containing an indicator for delivery to the cardholder's address. BORICA generates a bill of lading in the courier's system, and its tracking number is returned to the Issuer in the file with a response to the processing, in order to track the shipment.
- Based on the requests, submitted by the Issuer, BORICA performs card personalization, PIN generation and PIN printing of the card by printing the bill of lading number as a barcode on the letter, accompanying the card, visible through the transparent part of the envelope.
- BORICA submits the shipments to a courier, who notifies the recipient (cardholder) of an expected shipment via an electronic message to a mobile number, specified by the Issuer.
- Undelivered or refused shipment to a cardholder's address is automatically forwarded to a servicing branch of the Bank, specified in the initial request, and for this purpose a new bill of lading is generated by the courier company.

2.4.5. PIN printing and/or electronic delivery

BORICA AD provides a system for electronic delivery of PIN.

Description
The system for electronic delivery of PIN provides an alternative way for delivery of a newly manufactured bank card's PIN to a cardholder. The PIN shall be sent after the cardholder provides the unique identifier and authentication code that have been sent together with the card.

The PIN can be delivered through two channels:

- SMS message to an indicated mobile number;
- Another electronic channel - for example by visualizing in the electronic banking of the issuing bank.

Upon SMS delivery, the PIN can be sent to the cardholder either directly or by using a matrix and shifts in it. The client sends the unique identifier and the authentication code to a short SMS number and receives SMS message, containing the PIN or the shifts in the PIN table, making up the PIN.

When a matrix is used, the provided information shall be divided into two parts and shall be sent in the accompanying letter to the card and in the SMS.The accompanying letter contains a table with two rows – the first row indicates the digit shifts forming a user PIN, and the second row contains digits in the range 0-9. The SMS message contains the shifts in the PIN table, making up the PIN.

The system keeps all the sensitive cardholder data in an encrypted form and does not store card numbers.

Benefits:

- Saves costs for printing and delivery of PIN envelopes;
- Faster delivery of PIN codes;
- Enhances the security by providing a second delivery channel, independent of a courier service;
- The delivery is made directly to the cardholder, thus eliminating the risk of abuse;
- Guaranteed support of the cardholders in case of problems, through the Contact Center of BORICA AD.

2.4.6. Express Virtual Card

Description

The service is aimed at providing issuers with a functionality to issue Express Virtual Cards. Unlike centrally issued cards, which are processed in session mode, Express Virtual Card requests are processed at the time of receipt of the request in BORICA, and as a result of the processing, the issuer receives data for a finished virtual card.

The request for issuance of an Express Virtual Card, as well as its subsequent management, is carried out via web services, and the functionality of the service is fully compliant with the security standards imposed by international card schemes through PCI Card Production. In this way, virtual cards can be used in a matter of minutes after being requested by the cardholder.

2.5 e-Commerce and mobile services

2.5.1. Card management in 3D Secure scheme

BORICA AD enables the card issuers to provide their cardholders with secure Internet payments through the 3D Secure scheme. The following protocols are supported within 3D Secure:

- 3D Secure v.1;
- 3D Secure v.2.x, developed by EMVCo and supported by the card scheme programs: B-Secured for cards Bcard, Visa Secure and Mastercard Identity Check.

Description

The service provided by BORICA AD enables issuers to manage card registration in the Access Control Server (ACS) and to authenticate their cardholders when shopping from Internet merchants.

Issuers can execute card management in ACS by:

- Sending a file – TI and MI;
- Web service;
- ATM, migrated to BNG/WAY4;
- Administrative web interface provided by BORICA.

Issuers can use one or more of these card management methods.

BORICA AD offers different methods of authentication to card issuers for their cardholders, namely:
A) One-time password;
B) Static and one-time password;
C) Mobile authentication (authentication by biometric features).

Method A) meets the requirements of 3D Secure v.1, Methods B) and C) meet the requirements of 3D Secure v.2.x., including Strong Customer Authentication (SCA).

According to methods A) and B), the one-time password generated by BORICA may be provided:

- Directly to the cardholder as SMS message;
- Via a web service to the card issuer, who shall provide it to the cardholder.

In case the issuer chooses to use method B), a static password must be generated. The static password can be:

- Initial/temporary - subject to mandatory change by the cardholder prior to the first authentication, respectively an online transaction. The change shall be performed at a specially created for the purpose ACS internet page.
- Permanent – can be used directly by the cardholder for authentication.

The options for generation and provision of static passwords are as follows:

- The issuer can create a static password, provide it to the cardholder and send information about its value to ACS;
- BORICA can generate a static password (initial or permanent) and provide it together with the PIN code in a PIN envelope or by using Electronic Delivery of PIN as SMS or via a web service;
- BORICA can generate an initial static password and sent it to the cardholder via SMS.

BORICA AD offers mobile authentication (authentication by biometric features), with the following options:

- B-Token through B-Trust Mobile;
- OpenWay mobile application, as stand-alone mobile application and SDK options;
- Integration with external solutions.

The initial password for registration of the OpenWay mobile application can be provided as follows:

- Directly to the cardholder as SMS message;
- Via a web service to the card issuer, who shall provide it to the cardholder.

An issuer can register the same card for a static and one-time password authentication method and for their chosen mobile authentication method. In these cases, the cardholder selects the authentication method within the transaction itself. The leading method, which is loaded by default, is mobile authentication, and the cardholder may manually choose to switch to a "static and one-time password" method.

BORICA AD provides cardholders with access to ACS page (Customer Portal) where they can perform operations such as:

- Change static password (initial or permanent)
- Change mobile phone number. The issuer may subscribe to a notification service, providing information about changes made by its cardholders;
- Change the Personal Assurance Message;
- Change the language.

BORICA AD provides access for the cardholder’s employees to an administrative web interface (Way4Web Workbench), through which can be executed operations such as:

- Management of cardholder’s registration for 3D Secure;
- Management of card registration for 3D Secure.
- Benefits
- The cardholder authentication process provides more data for better security and minimizes the losses of the issuer from fraudulent and disputed online transactions;
- The issuer has a wide range of methods for authenticating its cardholders;
- The use of biometric features contributes to a high level of security and improved customer experience;
- The service ensures compliance with the regulatory requirements.

2.5.2. Digital wallet for issuers

The service allows card tokenization in mobile telephone application in order to perform contactless transactions at POS and ATM, or internet payments.

Description

The service provides interfaces for card tokenization when it is registered in virtual wallet, and detokenization during the transaction. By that means, the merchant/acquiring institution uses the token to perform the transaction and the issuer receives the PAN, which is necessary to authorize the operation.

Services

- During the tokenization – web service for card status check (service „Cards management“, described in p. 2.3.2);
- During the detokenization – interfaces to IPS to receive PAN for each transaction, and to provide information for transaction's result;
- Insertion of additional fields in transaction files submitted by BORICA in order to differentiate token transactions and provide information to the issuer about the digital wallet used.

Benefits

- Follows the newest market trends;
- Security – each card is tokenized individually for each device, thus in case one device is compromised card data are not at risk;
- Convenience for the cardholder – payment at POS and cash withdrawal at ATM are performed with the mobile device and it is not necessary the cardholder to carry the plastic card.

2.5.3. Virtual POS servicing in 3D Secure scheme

BORICA AD enables the acquirers to provide their merchants with secure Internet payments through virtual POS terminals in Way4 and the 3D Secure scheme. The following protocols are supported within 3D Secure:

- 3D Secure v.1 protocol;
- 3D Secure v.2.x protocol, developed by EMVCo and supported by the card scheme programs: B-Secured for cards Bcard Visa Secure, Mastercard Identity Check and Discover ProtectBuy.

Description

BORICA provides a payment portal and 3DS Server / MPI (Merchant Plug-In) by which is carried out the communication with the central servers of the card organizations, as well as with the card issuer. The design of the payment portal is adaptive and can be customized for a specific merchant. The service provides Internet merchants with a flexible interface and enables them to accept payments after cardholder authentication through 3DS Server / MPI within the 3D Secure technology.

BORICA AD provides merchants with access to the Merchant Portal which allows the following features and functionalities:

- Information portal for monitoring of terminals and transactions;
- Searching transactions by specific terminal/period.

BORICA AD provides access for the acquiring institution's employees to an administrative web interface (Way4Web Workbench), through which can be executed operations such as:

- Easy and convenient registration of merchants and terminals
- Verification and editing static merchant data
- Verification of transactions and searching (by terminal / merchant / period)

- Access management to Merchant Portal for merchants

Benefits

- By 3D Secure v.2.x protocol the service provides cardholder authentication for purchases in both browser and mobile applications, which facilitates payments with a mobile phone;
- The cardholder authentication process provides more data for better security and minimizes the losses of the acquiring institution and its merchants from fraudulent and disputed online transactions;
- Cardholder authentication through 3D Secure v.2.x improves customer experience and accordingly increases merchant revenue;
- The service ensures compliance with the regulatory requirements.

BORICA offers functionality for card registration at a merchant, participating in the 3D Secure scheme in Way4 MPI / 3DS Server.

Description

The Service "Card token at a merchant in the 3D Secure scheme" provides the acquiring banks with the possibility to offer to the cardholder the service of registering cards on a merchant's Internet site or mobile application for the purpose of performing subsequent payments.

The card registration at a 3D Secure merchant is done through a successful card transaction on a virtual 3D Secure terminal of the merchant.

The card is registered at the merchant and the merchant receives the card token only after successful 3D Secure authentication and approved by the issuer transaction.

Benefits

- The merchant does not need to store sensitive data, nor to be certified under PCI DSS.
- The service meets the cardholders' needs for a quick and secure method of performing payments to known merchants;
- An option is provided for generation of subsequent Merchant Initiated Transactions.

2.5.4. Technical support for virtual merchants

BORICA AD offers to acquiring institutions using its MPI/3DS Server to outsource the technical support of their virtual merchants.

Description:

The service includes:

- Upon request received from the Acquirer - merchant/terminals registration in Way4 and identifiers creation;
- Creation of access to Merchant Portal.

BORICA carries out the correspondence with the merchants and fully supports them during the test period, answers merchants' technical inquiries related to vPOS behaviour in test or production environment, assists when merchants need to make some amendments or upgrades to their system, resets the password for Merchant Portal etc.

The above allows the acquiring institution to fully focus on its core business. Of course, merchant's assessment and their compliance with regulatory requirements and internal rules, specific commercial or financial issues remain as acquirer's prerogatives.

Advantages:

By outsourcing technical support of virtual merchants to BORICA, it frees the Acquirer's employees from complex technical tasks and the role of intermediary between clients and BORICA and allows them to devote more time to commercial activities.

BORICA's team has in-depth knowledge and significant experience in serving e-merchants. Taking over the end-to-end technical process by BORICA will make the process easier and simpler for clients and will significantly reduce the time to market for their vPOS.

2.5.5. Transactions at virtual POS terminals

Transactions at virtual POS terminals registered in the BORICA system

Description

The BORICA system provides acquiring of all payment cards issued in the territory of the country at all virtual POS terminals included in the Way4 system. BORICA enables authorizations with Bulgarian and foreign cards by sending requests to the card schemes Bcard, Mastercard, VISA, Diners Club, Discover.

Services

The service "Interbank transaction at a virtual POS registered in the BORICA system" includes the following types of transactions:

- transactions executed at a virtual POS operated by one PSP with cards issued by other PSPs;
- transactions executed at a virtual POS of a PSP connected to the BORICA system with cards issued by the same PSP, which are not registered in the BORICA system.

The service "On-Us transaction at a virtual POS registered in the BORICA system" includes only transactions where a card issued by a PSP and registered in the BORICA system is acquired at a virtual POS of the same PSP connected to the BORICA system.

The service "International transaction at a virtual POS registered in the BORICA system" includes transactions at a virtual POS of a PSP connected to the BORICA system with cards issued abroad.

Financial transactions at a Virtual POS include:

- payment for goods and services via virtual POS terminals, including with card retention at a merchant for future payments (tokenization);
- reversals (cancellations) of the above transactions.

Transactions at virtual POS terminals with cards registered in BORICA

BORICA AD provides to banks and payment institutions, which issue cards through the BORICA system, authorization of requests for transactions made with their cards at virtual POS terminals in the country and abroad.

Description

Authorization of each request for a transaction executed with a payment card on virtual terminal devices in the country and abroad is carried out by checking multiple parameters:

- card validity (card number, expiry date);
- card account balance or credit limit;
- card limits (daily, weekly, etc.);
- CVC/CVV security codes;
- card status (active, blocked);
- other parameters (allowed transactions, etc.).

Services

The service "Interbank transaction at a virtual POS with a card registered in the BORICA system" includes the following types of transactions:

- transactions executed with cards issued by one Payment Service Provider (PSP) at virtual terminal devices of other PSPs;
- transactions, executed with cards issued by one PSP and registered in the BORICA system, at virtual terminal devices of the same PSP, which are not connected to the BORICA system;

The service "On-Us transaction at a virtual POS with a card registered in the BORICA system" includes only transactions executed with a card issued by a PSP and registered in the BORICA system at a virtual terminal device of the same PSP connected to the BORICA system.

The service "International transaction at a virtual POS with a card registered in the BORICA system" includes transactions at a virtual POS of a PSP abroad with cards registered in the BORICA system.

Financial transactions include:

- payment of goods and services via virtual POS terminals
- reversals (cancellations) of the above transactions.

2.5.6. Acceptance of Apple Pay and Google Pay Payments for E-commerce Merchants

BORICA AD provides acquiring institutions using its MPI/3DS Server solution the ability to enable their e-commerce merchants to accept payments via Apple Pay and Google Pay.

Description:

The Apple Pay and Google Pay functionality is seamlessly integrated into BORICA's Payment Page by adding a "Pay with Apple Pay/Google Pay" button. By selecting this option, cardholders can complete payments without manually entering their card details. This service requires no additional development effort from the merchant or acquiring institution. BORICA handles all necessary connectivity with Apple Pay and Google Pay platforms to facilitate secure and efficient payment processing. As a PCI DSS-certified entity, BORICA complies with the stringent security standards set by Apple and Google for payment processors.

Advantages:

- **Simplified Payment Process** - digital wallet payments offer cardholders a faster, easier, and more secure way to complete online transaction;
- **Enhanced Customer Experience** - providing modern payment options improves customer satisfaction and loyalty;
- **Increased Transactions** - the convenience of Apple Pay and Google Pay can lead to higher transaction volumes for merchants.

2.5.7. Electronic notification

The service offers a fast and flexible way of sending individualized or group messages via SMS and email. Possible applications include message of transaction at ATM/POS terminal, bank account movement, upon received order, sent goods, expiring subscription, etc.

Description
Fixed price for all Bulgarian mobile operators; easy and quick sending of a desired number of SMS messages (up to 160 symbols in Latin) or e-mail to one or a group of recipients; setting a schedule for automatic sending of messages; real time monitoring of the status of the messages and statistics;

keeping a detailed log of sent messages; automatic delivery to mobile subscribers, transferred numbers to another operator – transparency for the sender.

2.6. Risks management and compliance

2.6.1. Anti-fraud Monitoring

In response to the growing globally digital fraud, BORICA AD has modernized its payments' monitoring and fraud prevention system, based on a solution provided by world leader in anti-fraud solutions – IBM Safer Payments platform. The updated solution aims to take a central place and role in the market in the fight against the fraud and provide Financial Institutions with ability to carry out monitoring and fraud prevention not only in cards' transactions, but also in the field of instant payments, as well as in any other type of payments, initiated through digital channels. Safer Payments makes the process of tracking, detecting and preventing fraud in electronic payments extremely efficient.

In order to upgrade the payment operations' monitoring and fraud-prevention system, BORICA AD is in process of expanding the functionalities provided by the cloud-based solution with services in the field of transfers, initiated both in bank offices and via digital channels integrated to the platform, such as internet, mobile banking, etc. Utilizing the functionalities of the Safer Payments platform, BORICA AD will assist Financial Institutions in applying the regulatory requirements for checking individuals, groups and organizations for their presence in various sanction lists. Thus, the solution offered by BORICA will provide additional protection for customers and their payments, while at the same time it will build behavioral models and profiling of each user, regardless of the channel through which the respective operation was initiated.

The system is offered to the Financial Institutions as a service (SaaS), which makes it extremely convenient and adaptive to clients' requirements, thus not requiring additional investments in hardware, software and support. The solution is based on rules and classes that serve to identify operations meeting specific, predefined criteria. The main advantages of the platform are related to the ability to perform behavioral analysis, profiling, risk assessment, including through AI (Artificial Intelligence) and machine learning.

Features of Safer Payments platform and benefits for Financial Institutions and system users:

- Analysis and prevention – the platform provide an opportunity to detect and prevent fraud by analyzing transaction flows and identifying high-risk ones. Monitoring, as well as the ability to perform detailed analysis, allow the creation of various precise combinations of predefined criteria/rules for subsequent prevention, aimed at reducing not only losses from fraudulent transactions, but also the so-called false positive rate levels.
- Users Profiling – the activity of each user in the system (cardholder, payer or payee) enables tracking and behavior pattern creation that allows recurring fraud patterns to be identified easily.
- Cases Generation – the system offers clients an option for automatic generation of cases, based on rules fired by transactions.
- Bank Call Center – as part of the monitoring and prevention service, BORICA supports Bank Call Center who performs 24/7 transactions' monitoring in order to prevent BIN attacks.
- User access – the platform provides an opportunity for employees of Financial Institutions to have different roles and levels of access, depending on the specific needs.
- Security and compliance – being part of BORICA's infrastructure, the system meets all requirements and standards for security and compliance applicable to the activity, including PCI DSS.

2.6.2. Contact center services 24/7

The services of BORICA's Bank Call Center include:

- Identification of bank cardholders by telephone;
- Card activation;
- Blocking cards in case of theft, loss, damage for security reasons;
- Unblocking cards;
- Unblocking cards when entering 3 wrong PINs;
- Provision of information for card balance;
- Provision of information for last 5 transactions;
- Provision of information for rejected transactions;
- Issues related to Internet payments;
- Services - blocking/unblocking 3D password for secure payments – a telephone number change, providing of a new temporary password for registration;
- POS – questions, answers, errors/by list;
- InfoPay – questions, answers, errors;
- B-Trust
    - Remote identification
    - Issuance of a certificate
    - Browsers setup
- E-Factura – questions, answers, errors.

2.6.3. Chargeback management

BORICA AD provides access to the Dispute Resolution System, which enables exchange of information between the users, in connection with fraud and incidents.

The system keeps records of received information (incidents, fraudulent transactions, disputed transactions, etc.) for a period of 10 years.

The scope of the system includes:

- Chargeback by Issuer;
- Goodwill procedure by Issuer;
- Settlement of file for disputed transactions;
- Reporting fraudulent transactions;
- Arbitration Committee.

Benefits

- Management system of cases related to chargebacks and refund of disputed amounts;
- Automating the process of document exchange and switch to an entirely electronic documents exchange;
- Ensuring traceability and a long-term archive of each chargeback history;
- Possibility to initiate a refund by the BNB Gross Settlement System RINGS after the end of the dispute;
- Possibility to report fraudulent transactions and keep the information for the purpose of settling disputes and statistics;
- Register keeping;
- Electronic Bulletin.

2.6.4. Risk based authentication

BORICA AD enables the usage of risk based authentication (RBA) with the following results:

- Allow – direct approval (frictionless process);
- Challenge – detailed identification of the client's identity is required;
- Decline – rejected transaction.

Applying the RBA and risk rules enables you to take advantage of the advanced and improved capabilities of our new 3D Secure solutions, providing you with the following benefits of e-commerce transactions:

- Meeting the requirements of the international card organizations and implementing the options provided for in Articles 10 to 20 of Regulation (EU) 2018/389
- Increasing customer satisfaction by applying the so called frictionless process for low risk transactions that does not require cardholder authentication
- Increasing the security level by introducing appropriate restrictions on Issuing and Acquiring e-commerce transactions

2.6.5. ATM certification to card schemes

In order to improve the implementation or certification process with international card schemes (ICS) and to optimize the interaction between BORICA and the banks in these projects, BORICA has established a procedure for coordination of the projects between the parties.

Description

Upon initiation of a project by the Bank to the International Card Schemes (ICS), BORICA AD offers overall coordination of the project from its start up to its successful completion. For this purpose, BORICA AD appoints a project coordinator, who assists the Bank in completing all the necessary forms and documents, manages and allocates project activities, conducts expert consultations, plans and monitors the tests execution, informs and coordinates with the relevant departments in BORICA AD the necessary settings and parameterizations of the systems in relation to the service.

Benefits

- A single point of contact through the whole project
- Expert assistance during implementation
- Better planning of deadlines for execution, respectively reducing the Bank's expenses to the ICS

2.6.6. POS certification to card schemes

In order to improve the implementation or certification process with international card schemes (ICS) and to optimize the interaction between BORICA and the banks in these projects, BORICA has established a procedure for coordination of the projects between the parties.

Description

Upon initiation of a project by the Bank to the International Card Schemes (ICS), BORICA AD offers overall coordination of the project from its start up to its successful completion. For this purpose, BORICA AD appoints a project coordinator, who assists the Bank in completing all the necessary forms and documents, manages and allocates project activities, conducts expert consultations, plans and monitors the tests execution, informs and coordinates with the relevant departments in BORICA AD the necessary settings and parameterizations of the systems in relation to the service.

Benefits

- A single point of contact through the whole project
- Expert assistance during implementation

- Better planning of deadlines for execution, respectively reducing the Bank's expenses to the ICS

2.6.7. Card products certification to card schemes

In order to improve the implementation or certification process with international card schemes (ICS) and to optimize the interaction between BORICA and the banks in these projects, BORICA has established a procedure for coordination of the projects between the parties.

Description

Upon initiation of a project by the Bank to the International Card Schemes (ICS), BORICA AD offers overall coordination of the project from its start up to its successful completion. For this purpose, BORICA AD appoints a project coordinator, who assists the Bank in completing all the necessary forms and documents, manages and allocates project activities, conducts expert consultations, plans and monitors the tests execution, informs and coordinates with the relevant departments in BORICA AD the necessary settings and parameterizations of the systems in relation to the service.

Benefits

- A single point of contact through the whole project
- Expert assistance during implementation
- Better planning of deadlines for execution, respectively reducing the Bank's expenses to the ICS

2.7. Card back-office

2.7.1. Card Back Office as a Service - CMSaaS

Purpose:

CMSaaS is designed for banks and non-bank financial institutions (FIs) to manage their local and international debit and credit card businesses, as well as the operations of ATMs, merchants, and both physical and virtual POS devices.

Description:

The system provides comprehensive automation and management of business processes, including card issuance and management, credit card servicing, accounting, and financial analysis. It supports various hierarchical levels for managing merchants and their associated POS terminals. The system is compliant with the requirements and standards of local and international card schemes (bcard, AMEX, Mastercard, Visa, China Union Pay, Diners/Discover, and others). It offers a set of standardized online and offline interfaces for integration with the FI's core information system, ensuring full data redundancy and business continuity.

Key Features:

Card Issuance:

- Issue and manage various types of cards (debit, credit, prepaid, etc.)
- Issue virtual cards with e-PIN
- Support for various card technologies, including magnetic stripe, chip, and contactless cards (NFC)

Card Acquiring:

- Merchant management
- Management of POS terminals (physical/software and virtual)
- ATM management

Transaction Management:

- Processing of various card transactions, including cash withdrawals, deposits, bill payments, payments at merchants, online payments, and account transfers
- Implementation of 3D Secure for more secure online transactions
- Fees and commissions management
- Support for different fees and commissions structures across products
- Automatic calculation and application of due fees and commissions

Authorization and Clearing:

- Real-time transaction authorization
- Processing of clearing files and management of interbank settlements

Integration with External Systems:

- Connectivity with various payment schemes (Visa, Mastercard, Diners/Discover, etc.)
- Integration with core banking systems and other payment infrastructures

Reporting and Analytics:

- Generation of various reports on transactions, cards, and other data
- Capabilities for business analysis and monitoring of card operations

The system fully complies with the requirements of local and international card schemes and PCI DSS standards.

The CMSaaS model eliminates the need for FIs to purchase hardware/software, resulting in lower costs for maintaining technical centers, servers, and databases.

2.7.2. CMS eVouchers - Electronic Voucher Management

Overview:

CMS eVouchers is a powerful solution for efficiently managing meal electronic vouchers, built on a SaaS model. The system features an intuitive interface and robust functionalities, allowing e-voucher operators to seamlessly manage their entire business. The product is fully compliant with regulatory standards and meets all operational requirements.

CMS eVouchers provides extensive reporting and analytics capabilities, catering to both regulatory compliance and a variety of business insights. The system includes a range of standardized online and offline interfaces for the integration and management of eVoucher products, along with a user-friendly graphical interface (GUI).

Key Features:

- Employers Registry
- Office Network Registry for Employers
- Merchants Registry
- Employee Cards Registry
- Card Management and Fund Loading
- Reporting and Monitoring

Core Operational and Regulatory Reports:

- Consolidated Transaction Report
- Consolidated Report on Vouchers Redeemed by Employers
- Consolidated Data on Vouchers Redeemed by Merchants
- Cardholder Transaction Statement
- Report on Funds Loaded onto Electronic Vouchers

- Report on Vouchers Issued to Employers
- Report on Payments to Suppliers
- Report on Vouchers Expiring by Employer

2.7.3. CMS Closed Loop - Management of cards in a limited network

Overview:

CMS Cards is a cutting-edge system designed for managing cards within closed loop networks of merchants and services. Built on a SaaS (Software as a Service) model, this system offers an intuitive, user-friendly interface that enables issuers to fully manage their operations within a defined network. The product is fully compliant with regulatory standards and meets the operational needs of various organizations that use cards for restricted access or specialized purposes.

CMS Closed Loop provides robust reporting and analytics tools that empower effective management and monitoring of card activities. The system supports a comprehensive set of standardized online and offline interfaces, making it easy to integrate with external systems and additional platforms. All of this is supported by an intuitive graphical user interface (GUI), which simplifies the work for issuers and reduces training time.

Key Features:

- Register of Card Issuers
- Register of Merchants in a Closed loop Network
- Register of Cards and Employees
- Card Management and Fund Loading
- Reporting and Monitoring
- Ability to manage employee access, including access to multifunctional devices (MFDs)
- Integration with other systems

Core Operational and Regulatory Reports:

- Consolidated Transaction Report
- Consolidated Report on Cards Used by Merchants
- Data on Card Loadings and Transactions
- Card Balance Reports
- Report on Payments Merchants
- Report on Expiring Card Balances

2.8. Loyalty schemes

The loyalty scheme is a scheme, enabling the bank cardholders to accumulate bonus points for POS transactions executed by them, and other banking products used by them, and to spend the accumulated points at specified POS terminals and on other banking products.

The system operating the loyalty scheme is supported and operated by BORICA AD and is offered as a service to banks. The management of the program settings, including and excluding merchants from the program, defining campaigns and monitoring the Scheme are carried out by the users of the bank through the website of the system.

3. Services for Financial Fraud Prevention and Anti-Money Laundering (Anti-Fraud and AML) by BORICA

BORICA AD is a reliable and strategic partner for financial institutions in Bulgaria in the context of increasing digital fraud and regulatory requirements. Through its "Financial Fraud Prevention Services" Directorate, the company offers expert solutions including consulting, implementation and configuration of risk management systems, real-time monitoring, behavioral analysis, customer profiling, regulatory compliance, and training. At the core of these services is the leading IBM Safer Payments platform, which ensures fraud prevention and detection in card, banking, instant, and digital payments. With its experience and technologies, BORICA supports clients in building sustainable security strategies and a trusted digital financial environment.

3.1. Consulting Services for Financial Fraud Prevention

BORICA provides in-depth consulting services for assessing and optimizing the framework for financial fraud prevention and anti-money laundering measures in financial institutions:

- Analysis of current fraud protection – review of policies, processes, and technologies to identify strengths and risk areas.
- Evaluation of product features – identification of potential vulnerabilities and increased risks in financial product functionalities.
- Customer behavior analysis – development of behavioral profiles used to detect anomalies.
- Identification of Key Risk Indicators (KRI) – highlighting events and parameters that signal potential fraudulent activity.
- Risk model development – personalized modeling based on real transaction and incident data.
- Prevention strategy – creation of a balanced fraud prevention strategy that considers customer experience.
- Support and development – periodic review of rules and flexible consulting for new needs.
- Upon receiving a request for consulting services, BORICA analyzes the business requirements and scope of the requested consultation and defines a consulting project with an implementation plan.

3.2. Integration and Configuration of a Financial Fraud Prevention System:

Description:

Based on the IBM Safer Payments platform, BORICA offers full integration and adaptation of a risk management system, providing a reliable and effective tool for monitoring and preventing financial fraud. The platform ensures 99.5% availability and uninterrupted 24/7 operation, thereby guaranteeing stability and continuity of processes critical to the operations of financial institutions.

IBM Safer Payments offers a wide range of functionalities that can be customized to the specific needs of the client—both operationally and technologically. The system allows for the creation of individual control rules, automated transaction tracking, and effective response to suspicious activities. This ensures a higher level of protection and significantly reduces the risk of fraud, while also supporting optimal organization of workflows related to monitoring, analysis, and prevention of financial events.

The scope of prevention and monitoring services includes both card channel transactions (card payments) and digital channels such as SEPA, SWIFT, BLINK, and SEBRA, providing comprehensive protection of payment flows critical to financial institutions.

Services:

3.2.1. IBM Safer Payments Integration – The integration service involves detailed technical execution carried out jointly with the financial institution and/or its banking software providers, in full compliance with the client's existing systems and infrastructure. This process ensures the provision and proper structuring of the necessary data to feed the IBM Safer Payments platform. Based on this data, the system monitors transaction flows, analyzes behavior, and prevents potential fraudulent activities. The integration is tailored to the individual requirements and processes of the financial institution, ensuring seamless compatibility with its internal environment and maximum efficiency of the implemented risk management system.

3.2.2. Rule Configuration - Rule configuration in the Safer Payments system is a key element of the implementation and effective use of the fraud monitoring and prevention platform. After successful integration with the payment service provider's systems, BORICA's "Financial Fraud Prevention" team configures and inputs specific rules that enable automated monitoring and control of transaction flows. Rules can be predefined and submitted by the client according to their own risk profile and customer base specifics. In this case, BORICA specialists handle their implementation and optimization in the system. If the client does not have predefined rules, they can use a starter rule package provided by BORICA, covering a wide range of common fraud scenarios. This package is further developed and adapted through joint work between both parties to best meet the bank's needs and requirements. The process is dynamic and includes regular review and updates of the implemented rules to maintain high system efficiency and ensure timely detection of emerging fraud schemes.

3.2.3. Case Management System – As part of the IBM Safer Payments platform functionalities, the client gains access to a Case Management system that enables comprehensive structuring and optimization of the monitoring and prevention process. Through successful integration and configuration of predefined monitoring rules, the system automatically generates cases when events matching the set criteria occur. This provides the bank with a tool for effective handling of incidents related to transactional activity and potential fraudulent behavior.

Case Management allows for the creation of various queues, which can be individually adapted to the financial institution's workflow. Each automatically generated case contains detailed information about transactional behavior, historical data, and the specific rule that triggered its creation. This ensures quick orientation and facilitates timely decision-making by staff involved in fraud prevention.

Additionally, the system guarantees full traceability of actions taken, enabling effective reporting and providing the necessary transparency for internal or external audits. Thus, the Case Management module significantly supports both daily operations and long-term risk management within the financial institution.

3.3. Ensuring Protection of All Key Payment Channels – Card Payments and Bank Transfers.

3.3.1. Real-time monitoring – This service provides real-time evaluation of transactions based on predefined risk rules. The scope includes the entire transaction flow, and when certain criteria are met, the system automatically generates an alert and creates a case for further processing. This enables the client's team to promptly identify potential fraudulent activities and take the necessary actions to prevent them.

3.3.2. Preventive Actions – The service offers the ability to automatically block suspicious transactions, place transactions on hold, and generate alerts for further review. Preventive actions are based on pre-configured rules that deny or restrict transactions when risk indicators are present.

The system allows:

- Automatic blocking of transactions when specific criteria are met;
- Creation of a case for each event requiring further analysis;
- The ability for a specialist to review and give final approval or rejection before the transaction is completed.
- This ensures timely response to suspicious operations and provides effective control over all key stages of the fraud prevention process.

3.3.3. Notification Configuration – Upon client request and in accordance with the organization's workflow, a service is offered for configuring automatic notifications. When an event is generated in the system, an email and SMS are automatically sent to predefined recipients, ensuring immediate alerting and minimizing response time. This functionality supports effective management of monitoring and prevention processes by enabling quick review of emerging cases and timely decision-making. In this way, delays in transaction processing are avoided, and a higher level of control over fraud prevention is ensured.

3.4. List Management (Blacklists and whitelists)

The flexibility of the IBM Safer Payments system allows for the creation and maintenance of blacklists and whitelists, which contribute to the completeness of the monitoring process and optimal prevention. Upon client request and specification of conditions, initial lists are created, which can then be managed by the client or modified (additions and removals) via a request to BORICA.

- Blacklists provide blocking or restriction of transactions related to risky entities, thereby minimizing opportunities for fraud.
- Whitelists allow certain entities (e.g., card number, IBAN, or merchant ID in acquiring) to be excluded from checks when it has been established that they do not pose a risk.
- Option for self-management by the client.

This functionality ensures a balance between effective protection of financial flows and maintaining a seamless customer experience, while also providing a high level of flexibility in configuring prevention rules.

3.5. Protection Against BIN Attacks

This service is provided by BORICA's Banking Call Center for continuous monitoring and merchant blocking in response to identified cases of potential BIN attacks, based on predefined rules in the Safer Payments system.

A BIN attack is an attempt to guess the correct combination of a payment card number, confirmation code for card-not-present transactions (CVV2/CVC2), and expiration date, using a method of testing generated card numbers. Once valid transactional data is identified, fraudsters attempt to "drain" funds from the cards. Due to the nature of how payment data is obtained, BIN attacks are typically characterized by a large number of failed operations, most often rejected by issuers with the reason "non-existent card."

The service is available 24/7 and ensures protection for card issuers.

BORICA can provide standard rules for detecting BIN attacks, which the client can review and approve. Alternatively, the client may submit their own rules for configuration in Safer Payments. The service is activated once the client confirms that the rules meet their business requirements.

3.6. Anti-Money Laundering Prevention Service Package

Description:

Financial institutions explicitly listed in Article 4 of the Measures Against Money Laundering Act (MAMLA) are required to monitor and assess the risk of payment operations to identify suspicious activities. When identifying risks, obligated entities must be able to detect risk factors such as connections to sectors associated with higher corruption risk; sectors linked to increased risk of money laundering and terrorist financing; and others exhaustively listed in Article 17, paragraph 2 of the MAMLA Implementing Rules. Another key risk factor is the sender/recipient country and whether it falls under the scope of Regulation (EU) 2016/1675, which lists high-risk third countries.

BORICA AD, through its "Financial Fraud Prevention" Directorate, offers a package of services to support compliance with regulatory requirements, including PSD2/SCA and Regulation (EU) 2015/847. These services are delivered via the Safer Payments system.

Services:

3.6.1. Sanction List Screening - Upon provision of the necessary data by the financial institution, the system enables automated checks against public sanctions lists in accordance with Bulgarian and European legislation. This includes:

- OFAC (Office of Foreign Assets Control)
- United Nations (UN) Sanctions Lists
- European Union (EU) Sanctions Lists
- Checks can be configured based on the client's needs and operational setup, with options for:
- Real-time screening– performed during each transaction or specific events.
- Post – event screening– conducted periodically for existing data or transactions

This service ensures regulatory compliance and minimizes the risk of processing transactions involving sanctioned individuals or organizations.

3.6.2. Politically Exposed Persons (PEP) Screening

The Safer Payments system offers functionality for screening politically exposed persons (PEPs). This feature can be activated if the financial institution has a contract and access to data provided by an external provider.

Once this data is integrated into the system, checks can be performed:

- Real time screening– performed during each transaction or specific events.
- Ex post– through periodic scanning of databases or historical transactions

3.6.3. Transaction Screening for High-risk Merchants – Financial institutions are required to implement enhanced measures for screening transactions involving high-risk merchants and businesses, including:

- Cryptocurrency exchange platforms

- Businesses operating in high-risk countries
- Organizations or individuals with suspicious source of funds

The Safer Payments system has capabilities for:

- Configuring specific rules to identify such transactions
- Creating blacklists and whitelists
- Generating reports and summaries of transfers to high-risk entities

After consultation with experts from BORICA's "Financial Fraud Prevention Services" Directorate, individual criteria can be defined to improve the accuracy and effectiveness of the checks. The more detailed the data provided by the financial institution, the more precise and comprehensive the profiling and monitoring of transactions will be.

3.7. Trainings and Thematic Workshops

Description:

Дирекция „Услуги за превенция на финансови измами" предоставя на финансовите институции постоянна подкрепа за надграждане на процесите по мониторинг и превенция на финансови измами.

Услуги:

3.7.1. Trainings and Thematic Workshops – „Financial Fraud Prevention Services" Department offers training and workshop sessions fully tailored to the need of the financial institution Trainings can be general – focused on new practices in financial fraud and effective detection methods – or based on specific cases and scenarios provided by the institution Both initial and follow-up trainings are available, aimed at expanding knowledge and skills. Additionally, workshop sessions can be organized upon request, during which the functionality of the Safer Payments system is demonstrated and explained. These sessions are suitable for onboarding new users as well as for additional training when there are uncertainties or a need for deeper understanding of the system.

3.7.2. Specialized Sessions – Upon request from the financial institution, experts from BORICA's "Financial fraud prevention services" department can organize specialized and narrowly focused sessions. These are aimed at recognizing and identifying fraudulent behaviors and provide specific guidance for optimizing internal processes within the financial institution. The goal of these sessions is to support effective risk management and strengthen organizational mechanisms for financial fraud prevention.

4. SOFTWARE PRODUCTS

Clients are provided with the software products against a one-time fee, with the right to use them for an unlimited term. The client receives software product support against payment of periodic maintenance fee. New versions of the product, made due to changes in software platforms, regulations, or legislation, are provided free of charge to clients paying a fee for software product maintenance. Extension of the functionality requested by the client is provided under the maintenance agreement and may result in a new one-time fee for the right to use the new software, and an increase of the periodic fee.

The service is available during working hours.

Type of agreement

The standard contracts are "Development and Grant Agreement" and "Maintenance and Support Agreement".

Pricing

The provision of software products (tariff codes SW.xx.xx.xxx) is subject of negotiation with the client regarding the type of product, functionalities and specific requirements.

4.1. PGATE

PGATE is a centralized unified platform for automation of the business processes for management of all types of payments in BGN and foreign currency, initiated from and to a bank.

Scope

- PGate includes automation of the entire spectrum of processes for processing of all incoming and outgoing cash flows from:
- Client and bank to bank transfers in BGN with settlement in RINGS – transfers executed via RINGS, BISERA, BORICA, etc.
- Domestic and cross-border transfers in EUR from and to EEA banks executed via TARGET2.
- Domestic and cross-border SEPA transfers: SEPA direct debit (SDD) and SEPA credit transfer (SCT).
- Correspondent interbank SWIFT foreign exchange payments.

Benefits

Automates business processes for preventive controls and liquidity management. Generates and updates the current balance of the bank settlement account. Provides centralized management and complete automation of the bidirectional exchange processes for transportation, control, registration, transfer of information, journaling and monitoring of processes. It provides plenty of statistical information for managers and dealers for financial and comparative analyses. Ensures continuous and secure exchange of the required protection against loss, duplication or change without the sender's knowledge.

4.1.1. BSTAR Client

Software for integration with the automated environment for automated asynchronous data exchange BSTAR of BORICA AD. BSTAR Client is used for automation of operations related to information exchange with the Company’s systems.

Benefits

Automates daily operational activities at the bank. Allows tracking the transfer of information from the bank to BORICA systems, and ensures delivery of the sent information.

4.2. DISTRAINS

"Distraint" is software application integrated with the core banking system for centralized registering, processing and storing distraint messages, generating responses to the Enforcement Bodies (EB), imposing blockings and lifting imposed distraints.

Description

The system automates the bank activities regarding the execution of distraint messages in their capacity of liable third party. It effectively services processes such as checking whether a debtor in a lawsuit is a client of the bank, obtaining information about accounts and used bank products, blocking and unblocking amounts, etc.

"Distraint" allows the creation and maintenance of the following main registers: Register of EB contains information about Private enforcement agents, National Revenue Agency, National Social Security Institute, Public Internal Financial Control, State Receivables Collection Agency, Customs authorities, other local and government bodies. The register of distraint notifications stores information of received distraint notifications, such as: distraint for collateral, distraint for execution; disposition; lifting of distraints.

"Distraint" visualizes information from the main system of the client's accounts and bank safes, as well as blockings imposed on them. The system stores in an archive scanned documents, in electronic format, of distraint orders and responses to distraint notices for the entire legally regulated period.

Benefits

- Centralizes activities related to receiving and processing of distraint orders in the bank.
- Optimizes the time the bank needs to impose/lift the distraints, as well as their execution.
- Reduces the cost of servicing the growing flow of distraint orders.
- Creates centralized registers and maintains an electronic archive of documents related to the correspondence between the enforcement body and the bank.

4.3. SAFE

Safe is a safe deposit box management system for automating the business processes related to rental of safe deposit boxes and safes. It is applicable to a single safety vault, as well as to a large branch network. With the option of a single pricing and business policy or supporting various individual preferences for branch network.

Centrally maintained information registers for safety vaults, safes, contracts and clients.

Possibility for integration with the core information systems for automated maintenance of a uniform client register, payment of services from an account, accounting of operations.

Interface for data exchange with the Register of Bank Accounts and Safe Deposit Boxes at the BNB under Ordinance No.12.

4.4. SEBRA Client

Designed to service payments of budget entities, included in the Single Account System. SEBRA Client was developed according to the BNB and MoF Guidelines for servicing accounts of budget entities and budget payments, and is independent of the accounting system of the servicing bank.

5. INFRASTRUCTURE SERVICES

The service is provided to clients willing to put their hardware equipment at BORICA's server premises or to use the hardware and system software of the company as a service for their own purposes.

Description

Infrastructure and services provided in a computer center such as equipment colocation, infrastructure as a service, private cloud. These services are also available with reservation from the two computer centers of BORICA - main and back up.

Benefits

- Ensuring business continuity, respectively IT services and the necessary infrastructure and communications, aiming to reduce the risk of discontinuity as a result of natural disasters and events of catastrophic nature;
- Outsourcing of distinct parts of IT infrastructure and services that require high capital and operating expenses, qualified personnel and the need for dynamic change of the technologies;
- Achieving better flexibility, efficiency and speed of deployment and change of the IT infrastructure depending on the needs of business;
- Meeting regulatory or business requirements with regard to the level of execution and operation of computer centers for which there is no competence and/or require unreasonably high investment and time;
- Equipment protection and 24x7 security, monitoring, “remote hands” service, etc.

6. TRUST SERVICES

Pricing

The Trust services are paid based on the applicable Tariff of BORICA AD for B-Trust, published on the website of the services at https://www.b-trust.bg.

6.1. B-Trust

B-Trust is the trademark of BORICA AD in its role as an accredited trust service provider. The Company's trust services are fully compliant with Regulation (EU) No 910/2014, which confers it a qualified status.

6.1.1. Cloud-based Qualified Electronic Signature Certificates

- **Cloud-based Qualified Electronic Signature** – acts as a substitute of a handwritten signature used for signing documents. The cloud-based qualified electronic signature is used from a mobile application having access to Internet, by means of the B-Trust Mobile application and the portal My B-Trust for signing via a personal computer. Its issuance is free of charge for the user, only usages are paid.
- **One-off Cloud-based Qualified Electronic Signature** – the certificate is issued for signing a particular electronic document. It may not be used after completion of the activity for which it was issued, even though its validity has not yet expired. After the end of its validity term, the certificate automatically becomes null and void.

6.1.2. Qualified certificates issued on hardware media

- **Qualified certificate for personal qualified electronic signature** – designed for natural persons. Its validity may be one or three years. The service includes electronic signature issuance, electronic signature renewal, electronic signature reissuance; electronic signature suspension; electronic signature resumption; electronic signature termination.
- **Qualified certificate for professional qualified electronic signature** – designed for legal entities: companies and freelancers. Its validity may be one or three years. The service includes electronic signature issuance, electronic signature renewal, electronic signature reissuance; electronic signature suspension; electronic signature resumption; electronic signature termination.
- **Qualified certificate for qualified electronic seal** – issued only to legal entities and used to authenticate the source and integrity of the data or electronic statements and the Creator's connection with their public key. In addition to certifying the authenticity of a document issued by a legal entity, electronic seals can be used to certify the authenticity of the digital assets of a legal entity, such as a software code or servers.

6.1.3. Qualified certificates for advanced electronic signature

- **Qualified certificates for personal advanced electronic signature** – issued to natural persons and certifies the electronic identity of the Signatory. The certificate for advanced electronic signature is used in sending protected and encrypted electronic messages and in protected and in encrypted communications, access to information and online transactions requiring a significant level of security.
- **Qualified certificates for professional advanced electronic signature** – issued to legal entities and certifies the electronic identity of the Signatory. The certificate for advanced electronic signature is used in sending protected and in encrypted electronic messages and in protected and encrypted communications, access to information and online transactions requiring a significant level of security.
- **Qualified certificates for advanced electronic seal** – used by legal entities in creating an advanced electronic seal by the Creator, as specified in the certificate, to electronic documents and in

electronic transactions, requiring a significant level of information security. The certificate is used only to authenticate the source and integrity of the sealed electronic documents/statements (by an electronic' office/organization).

- **Website (organization) authentication certificates** – issued to a User – legal entity and certify the User's electronic identity and accreditation with high level of security for the browser customers that the website they are accessing is owned by the organization identified in the certificate.
- **Website (domain) authentication certificates** – issued to a legal entity or a natural person and certify the electronic identity of the domain owner hosting a website with high level of security for the browser customer. The website (domain) authentication certificate is used to identify the domain owner and the accreditation of the person with sufficient level of security for the browser customers that the website they are accessing is owned by the organization identified in the certificate.
- **Application-oriented certificate** – a specialized type of signature for access to a server, protected electronic mailbox or virtual private network, encryption and decryption of data, and for specific applications tailored to the customer's specific needs and requirements.

6.1.4. Specialized PSD2 certificates for Payment Service Providers

PSD2 certificates for Payment Service Providers (PSPs) are issued in accordance with ETSI TS 119 495 V1.1.2 and with DELEGATED REGULATION (EU) 2018/389, based on Regulatory Technical Standards (RTS), namely:

- **Qualified certificate for qualified electronic seal** - issued to a Payment Service Provider (PSP) according to PSD2 and used to prove the integrity and origin of the data
- **Qualified certificate for website domain validation** - issued for website authentication, related to a Payment Service Provider (PSP) according to PSD2.

Certificates are issued depending on the role of the Payment Service Provider:

- Account Information Service Provider
- Payment Instruments Issuer Service Provider
- Account Servicing Payment Service Provider.

6.1.5. (Browser Independent Signing Service)

BISS (Browser Independent Signing Service) is an application software providing for operation with qualified electronic signature certificates for all popular browsers under MS Windows, Linux and MacOS operating systems. It applies a technology allowing for signing with an electronic signature locally without using an active component in a web browser. A great advantage of using BISS is the independence from the browser used, and from its limitations or inability to support Java applets or ActiveX controls.

6.1.6. B-Trust Signing Service

- **BSecure DSSLite** – the service provides a possibility for extending an already created digital signature (PKCS1) to the unified European formats for signing with an electronic signature consistent with Regulation (EU) 910/2014.
- **BSecure DSS** – the product is used for signing electronically files with random extensions and validation of electronically signed files, by using Advanced Certificates stored as a PFX file or Qualified Certificates for Qualified Electronic Signature (QES) stored on a smart card. The service is suitable for automation of processes involving the need of signing electronically a large number of electronic documents.
- **B-Trust Desktop Signer** – a desktop user application for signing electronic documents/files with a Qualified Certificate for Qualified Electronic Signature, pursuant to the Law on Electronic

Document and Electronic Trust Services. The product allows for manual or automated signing of one or more electronic documents/files. There is an option for adding a Time Stamp to the electronic signature, as well as for encryption/decryption of files in various formats.

6.1.7. Platform for remote signing of e-documents with a Cloud-based QES

The Cloud QES Platform is integrated into the B-Trust infrastructure for qualified trust services of BORICA AD as a qualified trust service provider (QTSP) and provides centralized storage and management of private keys to Signatories and remote QES generation in an environment with a high level of security and strict administration and operational procedures with physical and logical protection. The service signs electronic documents (files) of random format. Pursuant to COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 and depending on the format of the signed document (random, xml, pdf), the service supports the following signing formats: CAdES, XAdES и PAdES.

The Platform for remote signing of e-documents with a Cloud-based QES is compliant with Regulation (EU) 910/2014 (eIDAS).

- **User authentication** – the service allows for establishing users' identity by means of a cloud-based QES. A pre-arranged identifier is used for the purpose (the user should be registered with this identifier in the service) and an authentication request generated at the entry into the system. The customer receives on the mobile application B-Trust Mobile a notification of received entry request. Based on the entry request signed by the user, the service sends back via the programme interface data from the Qualified Electronic Signature on the submitted request (Signatory's identifier and names in Roman letters).
- **Signing of electronic documents** – through the user interface of an application system the Signatory selects one or more electronic documents for signing by a cloud-based QES. Irrespective of the operation mode (hash or a whole document), for signing a single document or more electronic documents the application system supplies the documents prepared for signature with instructions regarding the format, level and type of the electronic signature to the Cloud QES Platform. The Signatory receives on the mobile application B-Trust Mobile a notification of received request and confirms signing, accordingly.
- **Signing of electronic documents by an one-off/limited signature** – a service for issuance through the user interface of the application system of an one-off electronic signature to a Signatory, issued for a particular purpose and with a limited validity for signing of a particular electronic document. Issuance of an electronic signature requires the Signatory's identification immediately before issuing of the certificate. Irrespective of the operation mode (hash or a whole document), for signing a single document or more electronic documents, the application system supplies the document(s) prepared for signature with cloud-based QES and instructions regarding the format, level and type of the electronic signature to the Cloud QES Platform.
- **Automated (batch) signing of electronic documents** – the service provides a mechanism for automated signing of documents with no need for the Signatory to confirm them by a PIN code. The Signatory's one-off prior consent is required, signed electronically by entering the PIN code of the certificate via the mobile application B-Trust Mobile. Based on the request of consent signed by the certificate owner, the sent documents proceed to an automated signing process with no need of any consent by the customer for each and every one of them via the mobile application.

6.1.8. My B-trust Portal

- **Portal for individuals** - My B-Trust is a web-based solution for signing documents, which is used by individuals, using Cloud Qualified Electronic Signature. To access the portal, all users need B-Trust Mobile application, active profile and a valid certificate for Cloud QES or QES on a smart card. The

portal allows sending and signing single or multiple documents to one or more users. The portal allows tracking the status of sent and received documents.

- **Portal for legal entities** - My B-Trust for business is a web-based solution that allows requesting identification, signing and automated distribution of electronic documents in a company or outside it as per its relationships with its counterparties, without requiring complex integrations with different systems. My B-Trust for business allows the creation of business accounts and the delegation of management to users in companies. The process of signing document/s is carried out by using the mobile application for Cloud Qualified Electronic Signature B-Trust Mobile or QES on a smart card. The portal supports simultaneous signing of single or multiple documents with multiple signatories, ensuring efficient and secure processes.

6.1.9. PIC portal

Specialized web portal intended for Pension Insurance Companies. The portal provides an opportunity for electronic signing of documents with One-Time Cloud QES for participation or transfer to a pension fund by an insured person. The specialized web portal offers an intuitive user interface, accessible from standard workstations and mobile devices with smart functions

6.1.10. B-Trust QTSS (Qualified Time Stamp Service)

B-Trust QTSS (Qualified Time Stamp Service) is a service for generation of secure QETSs, keeping records of issued and delivered QETSs, verification and validation of QETSs. B-Trust issues a TST (Time Stamp Token) – a QETS electronically signed by B-Trust QTSA for the existence of digital content of an electronic document prior to a particular time indicated in the certificate and for the unchangeability of the content after this time. The Qualified Electronic Time Stamp provides calibrated official time that certifies in a secure and traceable manner the existence of digital data, including the content of an electronic document prior a specified time.

6.1.11. B-Trust e-mail

B-Trust e-mail – provides an address and an electronic mailbox in the “b-trust.org" domain for the purposes of servicing the use of electronic signatures. B-trust mailbox supports POP3, SMTP, IMAP with a certain volume and duration. The service is requested only upon purchasing a QES and has a separate price.

6.1.12. Remote Online Identification

The service provides a possibility for a third party to identify a customer remotely by obtaining identification data about them. Identification is made by a browser on a stationary or mobile device with no need to install any additional applications.

6.1.13. Qualified service for electronic identification

The service provides a possibility for a third party to identify a customer remotely by obtaining identification data about them. As a result of the service, an electronic identity certificate is issued, which contains a unique national identifier and other personal data of the person. Based on the certificate, an unequivocal distinction can be made of one person from another in a virtual environment. The service is compliant with Regulation (EU) 910/2014.

6.1.14. Remote digital video identification

During the automatic remote identification process, the photo of the person, who is present in the identity document is matched to the image, captured by the camera of the mobile device (Selfie). In case of a certain percentage of discrepancy between the Selfie and the photo from the ID document, the client may be provided with the opportunity to initiate a video conference call with an operator. The conversation is

carried out through a web platform, within the framework of the remote identification process initiated by the client. During this interactive session, direct communication is carried out with the client, who shall answer certain questions and perform certain actions. The video identification process is executed by specially trained qualified employees of BORICA.

6.1.15. Qualified service for digital registered mail

Qualified digital registered mail allows for the secure transfer of user content between sender and recipient, ensuring high level of security regarding the identification of the sender and recipient. The service provides legal proof of the delivery and receipt of the transferred data, including its integrity and delivery time. The qualified digital registered mail is the digital equivalent of the traditional registered mail with proof of receipt and has the same legal force.

6.1.16. Archiving long-term preservation service (QLTPS)

The Qualified Long-Term Preservation Service (QLTPS) is designed for storing documents with an electronic signature/seal. The service constitutes a long-term preservation repository of electronically signed/sealed data and documents, preserving evidence of authenticity and integrity. All files received into the service are stored for a ten-year period. Only electronic documents containing at least one eIDAS compliant electronic signature or seal are subject to archiving.

6.1.17. Qualified validation of electronically signed documents (QSVS)

The QSVS service (Qualified Validation of Qualified Electronic Signatures/Seals) provides a possibility for a third party to get a report on the process of signature/seal validation in an automated and reliable manner. The report is signed by a qualified electronic seal of the Provider. The service guarantees that the signatures and seals are generated and verified in accordance with the European legislation (EIDAS) and the standards (ETSI) related to it.

6.1.18. Cards and Readers

The Law on electronic Documents and Electronic Trust Services (LEDETS) requires qualified electronic signatures to be stored on a device with high level of security. Such a device is the smart card, on which the electronic signature certificate is stored, along with the public and private key. Access to the information stored on the card is gained by a secret PIN code. More than one electronic signature can be saved on one smart card. There are two types of smart cards and card readers - SIM format and standard format. In SIM format the card and the reader are located in a single device, while in the standard format the two devices are separate. The price is for a card and a reader separately or as a set.

6.1.19. Technical assistance for the installation of B-Trust products

This is a highly qualified service for service level 2 requests related to arising problems, need for consulting and training of customers using B-Trust products and services. The service includes servicing of B-Trust customers by phone and on-site; testing smart cards and card readers for operation with electronic signature; testing services and products for operation with electronic signature

6.2. B-Token

The solution is a software token that is part of the established mobile application B-Trust Mobile, using biometrics or a code as a standardized means of strict e-authentication and a nonqualified electronic signature. Its implementation allows institutions to perform strong consumer authentication (SCA) in accordance with PSD2 and RTS.

Description:

The scheme of issuance and support of SCA tokens for strict authentication and dynamic connection (transaction signing) is based on an application PKI-hierarchy, divided into autonomous security domains of the institutions participating in the scheme. By means of B-Token every participating institution issues to and support SCA tokens of its customers or users effecting remote payment transactions and/or access to payment accounts in its security domain. A different B-token is issued and supported for every participating institution.

B-Token uses an established secure mobile application B-Trust Mobile for performing 2-factor authentication. The application combines a B-Token for all participating institutions with possible existing cloud-based QES (Qualified Electronic Signature) certificates in the mobile application. The mobile application has the required security level for remote signing by QES.

In addition to meeting the institutions' needs in the context of PSD2, B-Token can be used as a means of signing documents /files or authentication (Login) for an application, where this need not be done applying a highest security means, namely a Qualified Electronic Signature. Documents signed by B-Token have the force of being signed with a nonqualified electronic signature.

Benefits:

The software tokens issued standardize the SCA procedure, while the institutions participating in the scheme preserve the autonomy of their security domains. On the other hand, the B-Trust Mobile application is a combination of different means of authentication and means of electronic signature, hence end customers can use a unified and known interface working in different environments

7. FINTECH SERVICES

7.1. E-faktura

Electronic invoicing is an automated process of issuing, sending, receiving and processing invoices electronically. Electronic invoicing is part of business processes, called "order - collection", from the supplier's perspective, and "purchase - payment " from the buyer's perspective. The electronic invoices are delivered in a XML-structured format. Documents accompanying the invoices, e.g. delivery notes,

notifications, advertisements, certificates, insurances, detailed print-outs, etc. can be attached to the electronic invoices. These documents can be in any format.

E-faktura service includes**:**

- **Sending and receiving e-invoices** – The issuer has previously compiled electronic invoices through their system or by means of converting tools. The invoices are signed with a Qualified Electronic Signature, then loaded into efaktura.bg. The system notifies the recipient that there is an invoice/s sent to them. The recipient accesses the system and after acknowledging the receipt of the invoices, may examine them, print or store them locally. The system provides an opportunity for online disputes between the recipient and the supplier, if necessary. The dispute may continue until a decision is reached. Upon receipt, many suppliers can transfer invoices to the recipient, who receives them through the system.
- **EDI** – provides the option for sending electronic invoices in EDI format (electronic exchange of structured business documents) via AS2 VAN.

Additional services

- **Issuer integration in the system –** Developing a visualization of electronic invoices. Help for the provider or their developer to prepare XML standard of the system. Tool adapting (efTool) for converting data from the ERP system of the provider in XML, signing with QES and uploading into e-Faktura.
- **Payment of invoices through internet banking –** service providing invoice payment through a bank's Internet banking. Payment orders are filled automatically with the data of the issuer of the invoice, the amount and the grounds for payment, indicated by the issuer of the invoice. Payment of invoices can be done only through banks, which have connectivity.
- **Payment of invoices with a card via VPOS and 3D secure** – Payment of invoices by the Buyer with payment card via merchant's VPOS (issuer of the invoice)**.**
- **Acceptance of contents** – ensures acceptance of the contents of invoices by recipients in efaktura.bg. After the invoices are signed with a Qualified Electronic Signature (QES) by the recipients, it is deemed that they have accepted the contents of the invoice**.**
- **Electronic archive –** storage of electronic invoices in the efaktura.bg system.
- **Information about unpaid invoices** – Loading information by the issuer about unpaid invoices, and informing the recipient of invoices that shall be paid.

<u>Benefits</u>

Saves time and money when sending electronic invoices and documents; stable form of the electronic document; reduction of errors; fast process for disputing invoices; electronic payments; improvement of the connections between providers and clients; electronic archive.

Type of agreement

- Standard agreement for issuer and recipient of electronic invoices – the use of the service E-faktura is provided under a standard agreement for issuers and recipients of electronic invoices.
- Standard agreement for recipient of electronic invoices - the use of the service E-faktura is regulated by the general terms and conditions, published on the company's website, which are accepted by an electronic statement – for the recipients of electronic invoices/they do not sign an agreement with the company/.

- Standard agreement for issuer of electronic invoices with additional option for using EDI format – the use of the service is provided under a standard agreement for issuers of electronic invoices using EDI format.
- PrePay E-faktura – prepaid packages – they can be used only by clients who have Qualified Electronic Signature B-Trust. Each package is with validity term for the number of invoices specified in it. PrePay does not require signing an agreement. One-time payment upon the request of the respective package of invoices.

Pricing

The services are paid on the basis of the applicable BORICA AD Tariff for E-faktura (tariff codes EF.xx.xx.xxx), published at: http://www.efaktura.bg/.

7.2. InfoPay

InfoPay is an open banking platform providing informational service to legal entities, based on the PSD2 Directive of the EU and the Bulgarian Law on Payment Services and Payment Systems. The service provides automated access to business customers with bank accounts in several banks.

Via a special web platform consumers get quick and easy remote access to their financial profile. Customers registered in the platform can obtain consolidated information about their bank accounts and bank transactions in multiple banks at each moment through one single point. Besides owners, managers, and accountants in corporate and small and medium- size business companies, the service is suitable for accounting firms maintaining many customers accounts in different banks. At present BORICA AD has been integrated with 13 banks and the list continues to expand.

To use the service, it is necessary that:

- Customer accounts be accessible online;
- The customer register Consent for access to their accounts by the InfoPay platform. Consent for access to accounts is approved through the customer's online banking profile in the respective bank.

The platform provides:

Consolidated information for payment accounts such as:

- balances
- movements
- transaction details
- reports

Role-based access and individual rights

- The platform allows providing different controlled accesses to accounts for company employees according to their direct obligations.

Easy to use interface

- Intuitive navigation guides users conveniently and easily in the menus and they get the information they want in seconds.

Benefits:

- Optimized financial management

Using a single platform allows for easy and convenient tracking of company finances. Consumers receive information about all their accounts registered in several banks, instead of receiving such information from every single bank

- Reduced time for preparing of report
- More efficient working processes
- Reducing the routine activities in the everyday work of the employees, thus providing them with more opportunities to focus on more significant tasks.
- 24/7 funds control
  With the InfoPay platform, consumers can always obtain prompt information about balances and movements for all their registered accounts at any time, from any point
- Role-based access and individual rights
  The platform allows providing different controlled accesses to accounts for company employees according to their direct obligations.

Type of agreement

Registration on the platform InfoPay can be made in two ways:

- Online at www.infopay.bg, using Qualified Electronic Signature or Cloud Electronic Signature, issued by BORICA AD or through remote video identification provided by BORICA AD.
- At a BORICA Branch by the legal representative of the legal entity which is a customer of InfoPay.

If the registration is performed by a legal representative of the company, it can be made eighter at a BORICA Branch or online at www.infopay.bg
If the registration is performed by an authorized representatives or the company is representing by two representatives, the registration can be made only at a BORICA Branch.

7.3. InfoPay Checkout

InfoPay Checkout is a service aimed at merchants who want to provide an alternative payment method to their customers besides card payment. The service provides merchants and their customers with an additional option for online payments via bank transfer, directly in their online stores or platforms.

Service Features and Characteristics:

The process of payment initiation is according to Directive (EU) 2015/2366 (PSD2).

- The Service is an API through which a payment can be initiated from an online store or merchant site.
- Provides information about the status of the payment;
- Initiated payments received on merchant/supplier accounts can be tracked through the interfaces of the Payment Service Provider (PSP) or through InfoPay - a web application or API for ERP integration;

InfoPay Checkout relies on increased security in the entire payment process.

Advantages:

- Easy process to make payment by bank transfer for the customer.
- Errors in preparing payment orders to the merchant are reduced.
- Optimizing the process of reconciliation.
- Merchant receives his money within 10 seconds.

- Lower costs than card schemes
- Automated entry of account movements through ERP integration.

To use the service, you need:

To register as a customer of the InfoPay platform and set up the data for your online store or platform via the InfoPay Checkout menu.

7.4. INFOBANK 2

Web-based system, offering in one place up-to-date information on the status of the received and ordered payments on the clients' accounts in all banks.

Description

The main goal of the product is to gather information and at the same time provide it in the most convenient way, suitable for various analyses. Infobank has a well-developed system for reports, sorting information, printing and exporting in various formats. Infobank may be used through a web-interface for online monitoring or work in integration with ERP/accounting software. For this purpose, the information is provided through SOAProtocol and downloaded automatically to the client's system.

- Infobank with Web access – the service includes uploading in the system, by the servicing banks, of statements with movements in bank accounts of clients requesting the service; the clients of the service receive consolidated information of their excerpts from all banks; the access to the system is by QES, username and password.
- Infobank integrated with Information System – the service includes: receiving information about the movements in the accounts via SOAP web service; providing information on statements which are "final". A final statement is a statement of an account for a date, for which a statement is entered for the following working data.
- Benefits
- Suitable for companies with a large number of bank accounts and/or a wide network of branches and offices throughout the country.
- Consolidates or combines information from the client's various accounts and banks;
- Possibility for the development of a data file, search, reports and export in various formats;
- Possibility for filtering of the information in the statements;
- Possibility for integration with accounting and ERP systems.

Pricing

Services are paid on the basis of the applicable BORICA AD Tariff for Infobank (tariff codes IB.xx.xx.xxx), published at: https://www.borica.bg.